Future Smart Connected Communities to Fight COVID-19 Outbreak

Deepti Gupta∗, Smriti Bhatt †, Maanak Gupta ‡, and Ali Saman Tosun §

1Department of Computer Science, University of Texas at San Antonio, San Antonio, Texas 78249, USA
2Department of Computing and Cyber Security, Texas A & M University-San Antonio, San Antonio, Texas 78224, USA
3Department of Computer Science, Tennessee Technological University, Cookeville, Tennessee 38505, USA

Abstract

Internet of Things (IoT) has grown rapidly in the last decade and continue to develop in terms of dimension and complexity offering wide range of devices to support diverse set of applications. With ubiquitous Internet, connected sensors and actuators, networking and communication technology, and artificial intelligence (AI), smart cyber-physical systems (CPS) provide services rendering assistance 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 current technological deployments to curtail this disease. IoT and smart connected technologies together with data-driven applications can play a crucial role not only in prevention, continuous monitoring, and mitigation of the disease, but also enable prompt enforcement of guidelines, rules and government orders to contain such future outbreaks. In this paper, we envision an IoT-enabled ecosystem for intelligent monitoring, proactive prevention and control, and mitigation of COVID-19. We propose different architectures, applications and technology systems for various smart infrastructures including E-health, smart home, smart supply chain management, smart locality, and smart city, to develop future connected communities to manage and mitigate similar outbreaks. Furthermore, we present research challenges together with future directions to enable and develop these smart communities and infrastructures to fight and prepare against such outbreaks.

Keywords: COVID-19; Internet of Things; Cloud Computing; Edge Computing; Artificial Intelligence (AI); Machine Learning; Smart Communities; Multi-layered Architecture; Security; Privacy; Coronavirus.

∗deepti.mrt@gmail.com
†sbhatt@tamusa.edu
‡mgupta@tntech.edu
§ali.tosun@utsa.edu
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 World Health Organization (WHO[1]), COVID-19 has already affected 215 countries and territories around the world and continue to spread rapidly across other regions. The highly contagious coronavirus outbreak was declared a “pandemic” on March 11, 2020. WHO[2] reports that the number of positive cases has dramatically surged, with nearly 3 Millions reported cases and 272,000 fatalities as of April 30, 2020. The fatalities are assuredly the most tragic cost of this disease. In order to control the spread the pandemic, lockdowns, quarantines and stay home orders have been issued by several nations across the globe, which have 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 rate[3] spiked to 14.7% – its highest level since the Great Depression, in addition to fear of stronger second wave of the disease looming during winter.

Currently, with no cure or vaccine for this disease, the first line of defense to fight against this pandemic is 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 personal protective measure (PPE), 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 huge 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 technologies including cloud computing and artificial intelligence (AI) and data-driven applications can play an important role.

There are several existing examples of use of technology to control the spread of COVID-19 and manage the large gatherings of already infected patients and possibly infected cases. The U.S. CDC has introduced a self-checker[5] application enabled with cloud platform, which helps a patient to make decision to find appropriate healthcare service through questionnaires. However, most people do not have any symptoms who are also known as the silent spreaders/asymptomatic carriers. Therefore, conducting

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
large scale testing for everyone should be mandatory to slow the spread. South Korea tested 395,194 people from January 3, 2020 to March 30, 2020 and identified 9,661 positive cases. Taiwan leveraged database from national health insurance and integrated it with its immigration and customs database to begin the creation of big data for analytics, and generated real-time alerts during a clinical visit based on travel history and clinical symptoms to aid case identification. Similarly, Chinese government installed CCTV cameras at home or apartment door of those under a quarantine period to monitor the patient activity. 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 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 behaviors. 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.

In the United States, 13% positive cases belong to New York which has become the battlefront. 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 the models have predicted that the number of cases and fatalities will increase as the country moves towards reopening businesses and cities. These evidences 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 enforcing proper sanitizing, social distancing, mass quarantine for mild-symptoms people, and testing at large scale for early detection. According to Harvard Global Health Institute, 31 states in 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 example, New York, the state with the largest number of cases, would need to increase testing by more than 10,000 per day. Due to lack of enough testing kits, an antibody test online is offered for those people who recently got sick and think that they might have

---

6https://www.weforum.org/agenda/2020/03/south-korea-covid-19-containment-testing/
7https://jamanetwork.com/journals/jama/article-abstract/2762689
8https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html
9https://pdi.voxel51.com/
10https://www1.nyc.gov/site/doh/covid/covid-19-data.page
11https://www.nytimes.com/2020/05/04/us/coronavirus-live-updates.html
12https://globalepidemics.org/2020/04/27/states-that-fall-short-on-testing/
COVID-19.

Over the last few years, there has been a huge surge in the number of IoT devices and different types of smart sensors have been introduced. With new technological advancements, this trend is expected to continue and grow in the future. IoT market\(^\text{[13]}\) is currently valued at $267 billion per year and is expected to reach $520 billion by 2021. Another recent article\(^\text{[14]}\) predicted more than 100 billion devices will be Internet-connected by 2025. In today’s connected world, not having network capability in a device limits the market potential for that device. As a result, there are large number and various types of network connected IoT devices providing convenience and ease of life to humans. 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, however, 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, preventing, and mitigating diseases like COVID-19.

IoT includes large number of novel consumer devices including HDMI sticks, IP cameras, smart-watches, 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 user and their requirements. IoT technology including smart sensors, actuators, and devices and data driven applications can enable smart connected com-

\(^\text{[13]}\)https://www.forbes.com/sites/louiscolumbus/2018/08/16/iot-market-predicted-to-double-by-2021-reaching-520b/#8267491f948

\(^\text{[14]}\)https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf
munities to strengthen the health and economical postures of the nations to fight against the current COVID-19 situation and other future pandemics efficiently.

In this paper, our main goal is to present a holistic vision of IoT-enabled smart communities utilizing various IoT devices, applications, and relevant technologies (e.g., AI, Machine Learning (ML), etc.). Here, we propose a vision of smart connected ecosystem, as shown in Figure 1, with real-world scenarios in various applications domains with a focus on detecting, preventing and mitigating COVID-19 outbreak.

The major contributions of this paper are outlined below.

- We outline some of COVID-19 symptoms, preventive measures, mitigation strategies, and current problems, challenges and present an overview of adaptable multi-layered IoT architecture and depict interactions between layers focusing on smart communities for COVID-19 requirements.

- We design a smart connected ecosystem by developing multiple conceptual IoT application frameworks including E-Health, Smart Home, Smart Supply Chain Management, Smart Locality, and Smart City. We introduce use-cases and applications scenarios for early COVID-19 detection, prevention, and mitigation.

- We identify and highlight challenges to implement this smart ecosystem including security and privacy, performance efficiency, interoperability and IoT federation, implementation challenges, policy and guidelines, machine learning and big data analytic. Finally, we discuss the interdisciplinary research directions to enable and empower future smart connected communities.

The remainder of this paper is organized as follows. Section 2 discusses the essential characteristics to diagnose, prevent and mitigate COVID-19 disease. Section 3 presents the multi-layered architecture for IoT, whereas Section 4 discusses smart connected ecosystem scenarios in various IoT application domains. Section 5 highlights open research challenges and future directions. Finally, Section 6 draws conclusion to this research paper.

2 Essential Characteristics to diagnose, prevent and mitigate COVID-19

Coronavirus is transmitted mainly by the infected person’s saliva and nasal drips which spread during coughing and sneezing and infects 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 the 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 added six new possible symptoms including chills, muscle pain, headache, sore throat and new loss of taste or smell. New York City 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 affects 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 and other resources explained early signs and symptoms, some preventive measures, and mitigation strategies.

On March 19, 2020, the WHO released the first edition of interim guidance on infection prevention

| Early Signs and Symptoms | Mitigation Strategies | Problems and Challenges |
|--------------------------|-----------------------|-------------------------|
| Common symptoms include fever, dry cough and myalgia or fatigue. | 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. | 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. | Manufacturers use of all cleaning and disinfection products, follow the workplace protocols, 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, CDC says a sudden confusion or an inability to wake up and be alert may be a serious sign. | 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. | 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. |
| Pneumonia, kidney failure and dyspnea more frequent in most severe cases. | Follow travel restrictions (domestic flights only for essential services, No sail order) | Reopening the country phases in highly contagious environment without data analytic, unified decision-making frameworks and some policies that span the country. |
| Normal or low white blood cell count or reduced lymphocyte in early onset. | Update periodically to follow WHO, and country guidelines. | No strict and defined guidelines from agencies due to ever changing dynamics of the virus. |

Table 1: COVID-19 Symptoms Prevention Mitigation and Challenges. (Items within the same row are unrelated)

---

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
and control (IPC) strategies for identifying the coronavirus infection. On March 28, 2020, the U.S. Food and Drug Administration (FDA\textsuperscript{24}) 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\textsuperscript{25} warned against 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 \textsuperscript{1} provides a comprehensive overview of the symptoms, preventive measures, mitigation strategies and some challenges fighting COVID-19 disease.

One of the easiest preventive measure 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 outdoor locations, and to 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 human body. Respiratory hygiene is another protective measure. There is a need to avoid cough or sneeze into the hands, and to cover mouth and nose with a tissue or bent elbow during cough or sneeze 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 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 the 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 mechanisms can be scaled up or down depending on the evolving local situation. At individual level, if a person is infected with coronavirus, then he/she should self-isolate and follow the guidelines of quarantine provided by hospital. The hospitals must support healthcare workforce, increase testing and intensive care capacity, and availability of personal protective equipment. City governments can appoint task

\textsuperscript{24}https://www.fda.gov/media/136537/download
\textsuperscript{25}https://www.fda.gov/drugs/drug-safety-and-availability/fda-cautions-against-use-hydroxychloroquine-or-chloroquine-COVID-19-outside-hospital-setting-or
force, 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 and spread awareness and up-to-date information across communities through appropriate technology. Consequently, it is essential to address the challenges with significant research and implementation of strategies as shown in the Table.

3 Multi-Layered 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 hospitals, grocery retail stores, transportation, and city etc. as shown in Figure 2. Our proposed architecture extends and adapts existing IoT and CPS architectures [1-6], and focuses on the need of 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 pandemics. 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, road side infrastructures, vehicles, etc. These physical objects are spread across and implemented in smart communities like 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 [7] 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) [8], 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. Cloud layer provides various services like remote storage, computation, big data analysis, and data-driven AI applications etc. for huge amount of information generated by billions of IoT devices connected to the cloud. We defined 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 run 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. 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 the Section 4 and different use case scenarios can be mapped and implemented using relevant technologies associated with each layer of the architecture.

4 Smart Connected Ecosystem Scenarios

In this section, we discuss various IoT use case scenarios to monitor, diagnose, detect, and mitigate COVID-19 infection. With many unanswered questions in this COVID-19 pandemic, one of the critical aspects is continuous monitoring is to track pre and post-infection characteristics of COVID-19 and its affect on human population. Thus, we propose various case studies deploying novel smart devices and data driven applications 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.
4.1 E-Health

It is expected that the global Internet of Medical Things (IoMT) market will grow to a 136.8 billions in year 2022. As of 2020, there are 3.7 million medical devices in use that are connected and monitor body parameters of the users to inform data-driven applications in making real-time healthcare decisions. Improving the efficiency and quality of healthcare services in hospitals have been an important and critical challenge during the COVID-19 pandemic time.

In E-health use cases, we will discuss three important scenarios which can help reduce the risk and spread of coronavirus infection. E-health set up comprises of a smart hospital, a remote patient monitoring, and a smart testing booth as shown in Figure 3. These use-cases involve connected smart sensors, connected devices, robots, patients, hospital practitioners, workers etc. together with IoT applications, edge devices and cloud services to offer data-driven services. Other scenarios including smart pharmacy, smart ambulance and smart parking in hospital’s parking area, are also briefly discussed. Such scenarios can be extended with the current proposed architectures described in Section 3.

4.1.1 Smart Hospital

Various components of smart hospital concept has been studied in the literature. However, it is still a challenge to track COVID-19 patient’s record and keep track of essential resources in hospital during

https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/#57b39d4f4a3c
such pandemic crisis. The hospitals are overflowing with patients, and running out of hospital beds, PPE and other essential resources needed for treatment and prevention. To overcome these problems, we propose a smart hospital use case here, while extending the existing infrastructure to enable coordinated actions for coronavirus patients. Within a smart hospital, RFID sensors can be used to track inventory items like masks, face shields, gauzes, disposable patient examination papers, boxes of gloves, and plastic bottles and vials. These RFID tags also could be an ideal way to keep track of large equipment as well, such as smart beds, ventilators within a smart hospital. Towel, sheets, and blankets must be washed and disinfected regularly, and such items also can be tracked through RFID laundry tags. In Wuhan, Wuchang field hospital provided wearable smart bracelets and rings embedded with multiple sensors to each patient in the hospital, where these IoT devices are synced with the cloud AI platform so that patient’s vital signs, body temperature, heart rate and blood oxygen levels, can be monitored regularly by hospital practitioners. In addition, all hospital workers and staff members also wear these smart bracelets and rings to notice any early symptoms of coronavirus infection.

IoT devices generate tremendous amount of data and this data can be collected using edge servers deployed in the hospital facilities. These data sets can be used for training with Federated Deep Learning [14] technique to enhance the intelligence of data-assisted applications which can be used to predict coronavirus infections for hospital practitioners, staff members and also provide insights on coronavirus characteristics and infection trends for the future. Hospital practitioners can check the patient’s data through remote applications which will also help in reducing the number of visits to the patient’s room to measure her/his vital parameters. In this way, hospital practitioners can not only collect more data in less time with minimal in-person contact but can also reduce the risk for cross-infection from the patients. This technique can significantly help reduce the workload and increase the efficiency of hospital practitioners. Moreover, smart hospitals can utilize smart beds, which sense the presence of a COVID-19 patient and automatically adjust the bed to a good angle if the patient is short of breathe to provide proper support without the need for a nurse to intervene. A Singapore based medical device company invented a smart ventilator, which allows inpatient monitoring process through remote access via an online portal. These ventilators measure the amount of oxygen automatically, or monitor the rate of delivery to the patient, as high pressure to force in more oxygen can damages the lungs of the patient also. These smart ventilators can communicate through patient’s smart bracelets with embedded sensors and can respond according to patient’s body parameters.

Besides, there are other IoT devices, such as disinfected robots which can autonomously disinfect a patient room regularly and after the patient is discharged, or a specific hospital area post contamination.

[27]https://www.cnbc.com/2020/03/18/how-china-is-using-robots-and-teledmedicine-to-combat-the-coronavirus.html
[28]https://www.biospectrumasia.com/opinion/27/15822/worlds-first-iot-enabled-tele-ventilator-to-regulate-COVID-19-patient-management.html
as needed. A study discussed how UV Disinfection (UVD) robots are used to disinfect patient rooms and operating theaters in hospitals and trials are underway in Florida. Autonomous robots can also help in healthcare systems as virtual clinic, smart guard and food service. Similarly, smart cameras for continuous monitoring (patients, inventory, hospital resources, peak hours, etc.), and smart alarm and notification systems can be installed at various points in the hospital, for example, when a new patient arrives in hospital as new case or transfer from another hospital or areas. In addition, the patients should be able to remotely request assistance from hospital room/bed when they feel uncomfortable or need assistance. As such having these IoT sensors and devices connected through edge computing and Cloud platforms enabling an intelligent connected medical facility communication network of things as part of smart hospital are essential in such pandemic situations.

4.1.2 Remote Patient Monitoring

Some COVID-19 patients have high-risk enough to warrant quarantine but not serious enough to warrant smart hospital care. The U.S. Centers for Disease Control and Prevention (CDC) warned that mild-symptom patients who are tested positive from COVID-19 should follow self-quarantine protocol. Hospital practitioners can monitor and track such patients remotely. All the vital data for the patient including body temperature, BP level, pulse rate, coughing frequency, ECG, etc. can be collected using wearable IoT sensors and the data collected is stored securely in a central cloud. Patient, family members and hospital practitioners can monitor and track the data and analyze through IoT applications in their smart phones but should be granted different levels of access control due to security and privacy concerns.

In addition, machine learning (ML) and deep learning approaches can be applied to this data to detect current and predicted critical conditions of a patient, and inform the hospital emergency staff members or autonomous smart ambulance regarding whether to bring the patient to the hospital. Patient can also receive in-build corrective recommendations regarding medicines and extra precautions at home. Family members can use IoT applications to monitor and communicate with the patient.

Apart from the common wearable sensors, other smart devices including inhalers, insulin pen (only for diabetes patient), infrared body temperature, or connected indigestible sensors can be used in a E-Health scenario. The frequency of smart inhaler use by a patient can be monitored remotely through the cloud. If frequency exceeds a threshold, alert can be send to hospital practitioners. Similarly, family members of the patient can also be monitored by hospital practitioners to detect early symptoms of COVID-19. Local public health administration staff can only view the location of patient to monitor and enforce social distancing during self-quarantine. If patient violates the protocol of self-quarantine,
smart applications can send alerts to local public health administration and hospital staff. Furthermore, if the person goes out during his quarantine time and breaks any guidelines, the wearable device can initiate a notifications that sound repeatedly and loudly to inform the others in the vicinity. Local workers can access the records of patient’s history of movements to help them quickly identify the cross-infected areas and possibly infected coronavirus patients in a swift and timely manner.

4.1.3 Smart Testing Booth

Boston hospital\(^\text{30}\) developed an innovative coronavirus testing booth to keep healthcare workers safe while swabbing possibly infected patients and conserve PPEs. A smart testing booth can involve 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 based smart cameras. Single person at a time can enter one side of the glass-walled testing booth and identified through RFID tag based wearable device or face recognition camera. In-built sensors in the booth can record person’s body temperature and oxygen level and store the data on cloud storage. An individual can receive the result of COVID-19 test through a phone application and also set an alert on his 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 on-board assistants to help patients and find optimal paths, using ML services to the Hospital, in case of emergency. Smart parking at hospital can tremendously reduce the parking search and wait time for the patients. IoT sensors and data can provide a smart parking management system. This system can identify COVID-19 patients and can assign special spots to park their car. Another application scenario is in pharmacies, where a pharmacist would receive a notification if a patient is in the car. The pharmacist communicates with patient through an application and provides prescribed medicine to them. Before attending the other person, the pharmacist must take some time to sanitize the smart pickup box. 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 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 these challenges in detail in Section 5.

4.2 Smart Home

Various aspects of smart home for health have been investigated in the literature\(^\text{15-29}\). It is nearly impossible to keep everything in the real-world virus-free. However, individuals must exercise due pre-
caution to keep our homes clean and disinfected. The first step to reduce number of COVID-19 cases around us is by sanitizing our homes. Currently, smart light and temperature control with their compatible sensors have become ubiquitous in smart home environments enabled by Wireless Sensor Networks (WSN) [30]. According to global tech market advisory firm [31], voice control device based orders and shipments will grow globally by close to 30\% over 2019. Using voice control allow people to avoid commonly touched surfaces around the home including smartphones, TV remotes, light switches, thermostats, door handles, and others. In this subsection, we elaborate three different scenarios within the context of smart home which can offer a more connected ecosystem to mitigate contagious disease spread, as shown in Figure 4.

### 4.2.1 Patient Home Isolation

In situations where a family member has been diagnosed with COVID-19, it is expected the individual is quarantined to prevent the spread to other members. In such a scenario, it is expected that the patient should easily be monitored by hospital practitioners, family members and local state authorities with different level of authorization requirements. Family members of a patient can track patient’s body parameters through smart sensors, communicate with the patient through voice control assistant or monitor the coughing frequency using a cough detection application [32]. Patient and family members

[31]https://www.techrepublic.com/article/COVID-19-pandemic-impact pushing-smart-home-voice-control-devices-to-predicted-30-growth/

[32]https://neurosciencenews.com/ai-cough-coronavirus-16145/
can control the environment (e.g., room temperature, lighting, humidity level for ease in breathing) in isolation and quarantine zone based on patients conditions, and at the same time members can also send reminders for medicines intake to the patient. For a home isolation situation, all family members are required to follow the guidance for implementing home care of the patient. In addition, these guidelines are updated frequently and people can receive alert through voice assistants when new guidelines are available.

4.2.2 Smart Sanitize

The novel coronavirus has people boarded up inside their homes due to lockdowns and stay home orders. However, people can still go outside for essential services. It is critical to take precautions during outside time and must be aware of possibly infected items and exposure to the virus that they may accidentally bring home. It is paramount to keep our smart homes disinfected and sanitized using different IoT assisted technologies, sensors and devices. Some of the devices useful in home during this situation include smart disinfect robots, smart UV-floor mats, UV-clean phone sanitize devices, smart UV light boxes, voice-control smart dustbins, voice-control hand sanitize pumps, voice control door knobs and cabinet handles, smart cameras, smart door-bells, etc. These devices constantly gather and share data with IoT applications and services and communicate with the users and other devices.

Individuals can use smart UV-floor mat at the main door of their house. This smart UV-floor mat will kill the viruses which may come on the floor through the shoes. Smart door bell can identify the face of a visitor using facial recognition. Voice control lock can also recognize the voice and identify the face through smart camera, and unlock the door for home owner and other residents. UV-clean phone sanitize box can be used to disinfect the phones and smart UV light box can be used for other stuff like car keys and wallets. In our daily life, we touch doorknobs, sinks, cabinet handles, refrigerator doors, remote controls, and etc. In smart homes, people can use voice control devices including hand sanitize pumps, smart water tabs and avoid touching. Smart vehicles can be sanitized through vent steam sanitizing. In homes, each pet can wear sensor to track the location of pet in case the pet visit outside accidentally. In rural areas, these devices in a home can communicate through smart hubs that enable local connectivity and communication.

In addition, during the pandemic, schools, universities, and other academic institutions are closed indefinitely. These learning institutions should evolve novel approaches to use IoT devices to assist student learning at home. In such scenarios, it is important to envision how smart devices can create a classroom like environment at home for daily learning and understanding teaching methodologies. Video conferencing together with IoT can offer innovative classroom teaching experience to students without compromising the outcomes of the course during the coronavirus pandemic.
4.3 Smart Supply Chain Management

During the pandemic, there is a requirement to improvise supply chain management to adapt automatic business processes and also improve the inventory with delivery of essential items. In this subsection, we will discuss two scenarios: smart inventory, and smart retail stores, which illustrate how IoT devices and technologies can enable efficient supply-chain and help in slowing the COVID-19 spread using various prevention and detection mechanisms. The complete scenario of smart supply chain management is shown in Figure 5.

4.3.1 Smart Inventory

Various aspects of smart inventory systems have been investigated in the literature [31–37]. Most of them involve IoT devices where staff use handheld readers to scan the bar code of goods, and then write the storage information to the RFID tags to complete the inventory.

Smart inventory systems show how IoT technology can be leveraged globally to plan and respond under the current pandemic situation. 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 to the workers using IoT technologies. Within the inventories, drones can be used to track all the employees to check their temperature using thermal sensors, and also measure their social distancing practices. Inventory manager can also provide smart wearable devices connected to the centralized cloud.

Figure 5: Smart and Connected Supply Chain Management Scenario.
to each employee to monitor and track them. If an employee or his/her family member is infected with coronavirus, inventory manager can get notification through data-driven IoT applications. In addition, disinfectant spray can be attached to the shelves and can start to spray when associated sensor senses the sound of sneezing.

California had the earliest stay-at-home order issued on March 1.[33] In California, there has been an early rise in truck activity since the week of March 1. Autonomous delivery robots can also help in smart inventory and help to reduce cross infection. However, truck activity in California has fallen 8.3% from early February. IoT sensors like thermal sensors, GPS, motion sensors can be attached with delivery trucks to maintain the temperature for perishable items and to track the location. This data can be stored on inventory cloud, and can help predict demand and supply for next month.

An IoT-based drone that monitors inventory in real time and sends alerts in case there are no available units left. Smart inventory will use RFID tags, RFID sensors, and RFID antenna to track the items, where RFID tags are attached with all items in inventory. Currently, people are facing the issue of shortages of PPE to disinfecting items. Supply chain managers implement the new ways of managing the supply chain, including using Internet of Things (IoT) data, analytic and machine learning (ML). These tools will become the foundation on which supply chain managers gain insight into their markets and erratic supply and demand trends. The RFID antenna scans the number of units on the sales floor and alerts a store manager in case it’s low. IoT allows store managers to automate product orders, is capable of notifying when a certain product needs to be re-ordered, gathers data regarding the popularity of a certain item, and prevents employee theft. The retail industry is seeing a rapid transformation, with The IoT solutions taking the center stage in the sector.

4.3.2 Smart Grocery Store

Smart grocery store have been widely investigated in the literature [35, 38–42]. IoT along with AI and ML technologies can help slow the spread of infection by enforcing prevention and detection mechanisms through connected sensor devices in a smart grocery store. Due to the stay home order, people are panicking and stocking up grocery items. They need to stand in queues for hours outside the store to buy groceries. By employing IoT sensors around the store and wearable IoT devices, a store manager can get a better understanding to slow the spread in the store. Chinese tech firm Kuang-Chi Technologies[34] has developed a smart helmet that is used to identify and target those people who are at high-risk for virus transmission in the retail store. The customer will wear a RFID tag based smart bracelet at the store. At the entrance each customer’s smart bracelet will be scanned by a scanner, which will show

[33]https://talkbusiness.net/2020/04/groups-share-data-quantifying-COVID-19-impacts-on-trucking-industry/
[34]https://www.yicaiglobal.com/news/chinese-tech-firm-debuts-five-meter-fever-finding-smart-helmet
his/her body parameters. If the records shows any symptoms of COVID-19, an alert can be sent to the store manager and individual can be restricted to enter in the store. Similarly, there can be thermal camera35 and microphone sensors installed at the store which can detect the people who are coughing in store during shopping and take pictures. These areas will be disinfected and identified individuals may be reported for testing based on their other symptoms and will be categorized as risky customers. This information can be maintained in store for short-period of time to assist in identifying these individuals during their future visits to the store.

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 get items from the smart shelves, which will allow to pick some limited number of items as per family size, and then put items in the smart cart. Smart shelves will have three common elements - an RFID tag, an RFID reader, and an antenna. Data collected by smart shelves during the day will be analyzed and shopper buying trends, patterns, shopper traffic, etc. will be shared with a store manager to provide customer-related insights to efficiently manage the store inventory and restocking goods.

Most retail stores now allow only ten people at 30 minutes shopping interval slot to avoid large gatherings inside the store. Social distancing can be measured and enforced by autonomous retail worker (robot) together with smart cameras, and smart microphone sensors and speakers to alert the customers, using AI technologies. If two customers come in same aisle and violate the physical distancing norm, an autonomous retail worker will go there to warn them or a loudspeaker attached with smart camera will announce to keep maintain social distancing. Autonomous retail worker can roam around the store and can take note of misplaced items, or products running out of stock (smart shelves also keep track of items and can send alert for restocking as needed). AT&T36 with Xenex and Brain Corporation has already launched IoT robots to help grocery stores in keeping them clean, killing germs and maintaining well stocked shelves more efficiently. The UVD Robot also uses ultraviolet light to zap infection viruses and sanitize surfaces.

In smart pickup, sensors and other AI based techniques are used to determine whether order is ready to pickup and a person is here to pickup his order. For instance, a parking space or driveway at the store might allow COVID-19 patient or elderly people firstly to avoid waiting time. Smart pickup can automatically allow most vulnerable and infected people first and enforce these rules to inform the vehicles. A restaurant takeout service can follow the same protocol for smart pickup. Intelligent Transportation System (ITS)43 can support to deliver resources to essential services and delivery

35https://spectrum.ieee.org/news-from-around-ieee/the-institute/ieee-member-news/thermal-cameras-are-being-outfitted-to-detect-fever-and-conduct-contact-tracing-for-covid19
36https://www.fiercewireless.com/iot/at-t-4g-lte-connects-iot-robots-to-kill-germs-keep-shelves-stocked
robot can enhance contact-less delivery, which reduce the spread of the virus. Gupta et al. [44] have also elaborated how ITS and smart city infrastructures can be used to enable and enforce social distancing community measures in COVID-19 outbreak.

4.4 Smart Locality

Smart localities have been widely investigated in the literature [45–51]. Such localities are a collection 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 assist in adapting/changing these systems. Here, we discuss two scenarios, which can help humans avoid coronavirus infections and adapt to the ‘new normal’ in COVID-19 situation living in the smart locality. These two scenarios including other relevant scenarios are shown in Figure 6.

4.4.1 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 the locality common areas. In a smart locality, motion sensors and cameras will sense and count the number of people and send the data to the locality cloud-1 as shown in Figure 6.

Cloud Smart Analytics[37] service can analyze the locality data and send notification to people regarding

---

[37]https://cloud.google.com/solutions/smart-analytics/
number of positives cases and categorize risk zones with different colors (e.g., red - high risk, yellow - medium risk, and green - low risk) in smart neighborhood. When a person will go for a walk in a smart neighborhood, he/she will receive an alert if any infected person/pet are around and also alert them to avoid high risk (red) zones in smart neighborhood. There will be disinfected sprinkler installed that can spray on the possibly infected areas, such as pedestrian path, common areas, etc. when sensor will sense the presence of infected person in the area through notifications from the locality cloud-1.

4.4.2 Smart Child Care and Nursing Home

The U.S. CDC\(^{38}\) have issued the guidelines in order to safely open child care in the locality. Smart child care can utilize monitoring and tracking sensors, devices for children and can provide access to their parents. The sensors can be attached to kid’s clothes to measure their sleep patterns, breathing patterns, body temperature, and body position and can store the data on edge devices of smart child care. AI assisted camera can be installed in child care room to measure social distancing among children and teachers. However, it is a challenging undertaking to maintain physical distancing in child care. In such 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. In a smart child care, it should be mandatory to wear mask and gloves for all teachers and staff as well as for kids throughout the day. They can receive a notification to change their mask and gloves through IoT application using mask sensor and glove sensor, when their masks and gloves are infected from virus and germs or after certain time period. The smart child care director and administrators can monitor body temperature, frequency of coughing, oxygen level of teachers, staff members, and kids through the application and get insights from ML techniques.

Coronavirus-linked fatalities at nursing homes and other long-term care facilities in the U.S. have surpassed 10,000 in New York, according to news report\(^{39}\). Japan’s artificial intelligence expertise\(^{40}\) is transforming the elder care industry, with niche robotic caregiving accomplishing more than just taking pressure off the critical shortage of caregivers. In a smart nursing home, if a person gets infected with the disease, then he/she should be treated in a quarantined area, such as isolated room. IoT devices and sensors can be utilized to help in disinfecting common areas, other people and staff members, as we have discussed in previous scenarios. Figure 6 shows that the body parameters of the elderly people can be taken through attached body bracelet and sent to edge devices and gateways. IoT devices and applications connected through locality cloud-2 can share information of COVID-19 patients to smart hospitals. The nursing home staff can monitor the patient’s body parameters regularly, and will also

\(^{38}\)https://www.cdc.gov/coronavirus/2019-ncov/community/schools-childcare/guidance-for-childcare.html

\(^{39}\)https://nypost.com/2020/04/23/coronavirus-deaths-at-us-nursing-homes-reach-over-10000/

\(^{40}\)https://thediplomat.com/2018/06/japans-robot-revolution-in-senior-care/
track other elderly people in the smart nursing home.

In a smart gym, multiple sensors, devices, autonomous devices can be connected through gateway, and gym manager/coach can access the information of each member at different access levels and can communicates to other locality through locality cloud-3. A gym member will receive a notification regarding to come to the gym, it must required to maintain the 25% occupancy at the gym and time interval to sanitize all gym equipment and surface. To enable multi-cloud secure data and information sharing and communications between locality clouds, there is need to be decentralized trust framework in place using advanced technologies like blockchain and trusted distributed computing.

4.5 Smart City

Smart and connected city infrastructures have been investigated in the literature. Daegu has setup a novel system using 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 developed a way of tracking of pedestrian, 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. Voxel51 is tracking the impact of the coronavirus global pandemic on social behavior, using a metric we developed called the Voxel51 Physical Distancing Index (PDI). Using the cutting-edge computer vision models and live video streams from some of the most visited streets in the world, the PDI captures the average amount of human activity and social distancing behaviors in major cities over time. Smart city 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. Millions of sensors and data sharing through the cloud-IoT architectures can be utilized to enforce and enable social distancing measures around the smart city. Here, we discuss two scenarios in the smart city as shown in Figure 7.

4.5.1 Smart Tracking

Countries have used cell phone data to track citizens’ movements during the pandemic. In addition, road side units, smart traffic lights and other city deployed connected drones, law enforcement etc. 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 infrastructure that is optimized for performance while reducing coronavirus outbreaks and saving lives of the citizens. The whole idea of a futuristic city when it comes

---

41https://www.smartcitiesworld.net/news/news/south-korea-to-step-up-online-coronavirus-tracking-5109
42https://COVID.view.urbanobservatory.ac.uk/#intro
43https://pdi.voxel51.com/
44https://www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3
to deployment of architecture having smart infrastructure which follows the protocols defined by federal and state agencies. In Spain, Nice city\footnote{https://www.businessinsider.com/coronavirus-drones-france-COVID-19-epidemic-pandemic-outbreak-virus-containment-2020-3} have been using drone by police to enforce the lockdown and drone 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\footnote{https://thehill.com/changing-america/resilience/smart-cities/492532-savannah-ga-to-enforce-social-distancing-with-drones} announced plans to use drones to enforce social distancing among residents. In smart city, drones can be used to measure six feet distance using AI technologies, and will warn people if the rules are violated. Drones can identify and report those people who do not follow the protocols, such as not wearing a mask. Thermal sensors can also be attached to the drone to check the body temperature of people.

As shown in the Figure\footnote{22} COVID-19 test result of a patient can be stored on city cloud-1 and shared with local healthcare staff, police and other smart devices including drones, traffic lights and road side sensors based on a need basis. This will enable patients to be easily identified using face recognition while they are in visiting different locations in a city. QR code can also help the citizens to visit city by showing the geographic data on hot spots and risk zones where people are more likely to get infection.
4.5.2 Smart Testing Vehicle

Smart and connected vehicles have been extensively investigated in the literature [64–71]. 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 and rural areas. The smart testing vehicle can include infrared body temperature, oxygen level sensors, smart test kit, camera, microphone, and local edge services. It can help reduce exposure of old-age people with preexisting conditions. In these vehicles, a person can enter from one side of the glass-walled area in the car. In-built sensors can record person’s body temperature and oxygen level and can store on City cloud-3. 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 are largely applicable and can help in testing people, as well as inform and make people aware of the COVID-19 pandemic, symptoms and preventive measures.

To flatten the curve of confirmed cases, smart city can provide mass quarantine for coronavirus patients, who have mild symptoms but with higher risk of cross-infection to others. A smart hall or large stadium or facilities can be setup for quarantine with installed sensors, smart devices, robots, and connected to city cloud-2 (as shown in Figure 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 reducing the human contact and cutting down the number of COVID-19 cases. Smart city will also provide immunity-based RFID tags to those people, who recover from the disease and 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.

5 Open Challenges and Future Directions

The development of the proposed smart connected ecosystem requires to address several challenges and needs inter-disciplinary research from an integrated perspective involving different domains and stakeholders. In this section, we will discuss these challenges in detail with examples from each of the proposed scenarios, as illustrated in Figure 8.
5.1 Security and Privacy

One of the major challenges in the deployment of the smart infrastructure is the security and privacy concerns pertaining to IoT and CPS users, smart devices, data, and applications in different application domains like healthcare, smart home, supply chain management, transportation, and smart city. In 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 is transmitted and stored 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 user and ensure privacy, differential privacy [72], and data masking techniques [73], such as pseudonymize [74] and anonymize [75], 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 and in motion. Several IoT access control models have been developed in the literature [76], with cloud-assisted IoT access control models for AWS [77], Google [24], and Azure [78]. Traditional access control models are not adequate in addressing dynamic and evolving access control requirements in IoT. Attribute-based access control (ABAC) [79,80], offers a flexible and dynamic access control model, which fits more into distributed IoT environments, such as smart home [81], connected vehicles [71,82], and wearable IoT devices [6,83].

In addition to access control, communications in terms of data flow between various components in cloud-enabled IoT platform need to be secured from unauthorized data access and modifications. Thus, attribute-based communication control (ABCC) [84] has been introduced. 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 [85] 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 recent surge in contact tracing applications, user data privacy concerns are surfacing and
Figure 8: Open Challenges and Future Directions in Smart Communities Deployment

will continue to arise in the future. Recent article\textsuperscript{47} 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 \textsuperscript{86} using which adversaries compromise user data and privacy. In order to protect the data sets, differential privacy \textsuperscript{72} can be applied to add noise. Cloud based medical data storage and the upfront challenges have been extensively addressed in the literature \textsuperscript{87,88}. Study \textsuperscript{89} 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.

In future research, there are requirements to conduct interviews of practitioners to understand the security and privacy concerns while developing the smart hospital, and need to apply similar approach involving community residents, infrastructure manufacturers and stakeholders to develop other components of the smart connected ecosystem. Privacy preserving deep learning approaches such as collaborative deep learning or federated deep learning also need to be explored to train and deploy local models at the edge devices.

5.2 Performance Efficiency

Within a connected ecosystem, users are constantly interacting with numerous smart devices and applications. One of main challenges in such an environment with billions of smart devices is performance

\textsuperscript{47}https://spectrum.ieee.org/telecom/security/tracking-covid19-with-the-iot-may-put-your-privacy-at-risk
efficiency and quality of service (QoS). High latency, response time, packet loss, and low bandwidth are various parameters in a network that affect the usability and feasibility of IoT systems. These devices generate large volumes of data which results in surge in data traffic that causes network congestion and latency.

Due to high latency, it is not recommend to perform any computation on centralized cloud for critical healthcare services in an emergency situation. End-users and front line responders prefer computation on edge devices and cloudlets to lower the wait and offer real time analytics. Research and advancements in distributed edge computing technologies, and 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 as IoT devices become more widely used and consume bandwidth. 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 remote patient monitoring, real-time vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication.

5.3 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 from, however, these devices use different communication protocols and are connected to vendor specific clouds. 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. In IoT, such developments are still lacking.

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 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 [90] suggested that IoT cloud provider allowed all devices belonging to the same private/public owner to participate in the federation process. However, currently many devices do not support other manufacturer’s application platforms. For instance, in a smart home, all sensors and
devices are connected through home assistant, and AI assisted application sends notification to 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.

5.4 Policy and Guidelines

IoT is an emerging technology that is being adopted by several nations across the world. Countries have different guidelines and policies for IoT, privacy of users and their personal data which are still evolving. Australian Privacy Principles (APP) 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 and policy initiative in this direction. The U.S. government has committed approximately $160 million 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 privacy of user and address another issues including accuracy, property and accessibility, together with infrastructure design to facilitate swift implementation of guidelines and public orders in COVID-19 like 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 and non-governmental organizations and industry partners as cloud providers, IoT manufacturers, would be beneficial.

5.5 Implementation Challenges

Enabling a smart community requires thousands of low-power and low cost embedded devices together with large scale data analytics and applications. There are several implementation challenges involved in developing such large scale smart infrastructure. Fault tolerance and resilience are the challenges for reliable delivery of sensor data from smart devices to distributed cloud service.

Various failures can occur including face recognition, community infrastructure management, and

48http://smarctcities.gov.in/content/innerpage/guidelines.php
49https://www.transportation.gov/smarcity
50https://www.govtech.com/opinion/If-Only-One-US-City-Wins-the-Smart-City-Race-the-Whole-Nation-Loses.html
emergency response in smart infrastructure. GEOgraphically Correlated Resilient Overlay Networks (GeoCRON) \cite{95} is developed to capture the localized nature of community IoT deployments in the context of small failures. Research in \cite{96} proposed a new fault-tolerant routing technique for hierarchical sensor networks. 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 \cite{97}, however in the scenario of COVID-19 pandemic, expected benefits (saving lives, economic growth) should outweigh the operational and deployment costs.

Another challenge, for instance, various IoT devices communicate to each other or server to build a prediction model. If the local model is not able to predict accurately due to data duplication or other reasons, there will be no point to build such a model. This study \cite{98} proposed a game theoretical analysis to allocate more storage capacity in a cost-effective manner, which achieves to maximize the benefits. For the 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, deep and machine learning, predictive analysis, security and privacy, and others need to be merged and collaborative research approach is necessary in implementing, deploying, and managing a smart connected ecosystem.

5.6 ML and Big Data Analytic

IoT generate tremendous amount of data collected by physical devices, and this raw data is converted into valuable knowledge using AI and machine learning technologies. The "6V" (Value, Velocity, Volume, Variety, Variability, and Veracity) Big Data challenges for IoT applications are discussed in \cite{99,100}. The volume of data from IoT devices overwhelms storage capacities. There is not only storage issue, but the data needs to be organized properly so that it can be retrieved and processed in a timely manner. Data duplication is a data storage 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 from a user which can create an issue of data duplication.

Machine Learning (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 based on early symptoms learns with the collaboration with 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 are more than smart child care. To overcome this problem, both models can learn at their edge networks using collaborative deep learning \[101\]. Research on these open challenges will help early development and deployment of future smart communities.

6 Conclusion

In this paper, we propose future smart connected community scenarios, which are blueprints to develop smart and intelligent infrastructures against COVID-19 and stop similar pandemic situations in the future. The autonomous operation with low human intervention in smart communities enable safe environment and enforce preventive measures for controlling the spread of infection in communities. Data-driven and AI assisted applications facilitate increased testing, monitoring and tracking of COVID-19 patients, and help to enforce social distance measure, predict possible infections based on symptoms and human activities, optimize the delivery of essential services and resources in a swift and efficient manner. The paper discussed different use case scenarios to reflect smart applications and ecosystem. The plethora of IoT devices enable huge data collection in different sectors including healthcare, home, supply chain management, transportation, environment, and city, which raises user concerns. In addition, the implementation of proposed smart connected scenarios face other challenges including legislation and policy, deployment cost, interoperability etc. which have also been discussed in the paper. We believe that our vision of smart communities will ignite interdisciplinary research and development of connected ecosystem to prepare our world for future such outbreaks.

References

[1] Vladimir Stantchev, Ahmed Barnawi, Sarfaraz Ghulam, Johannes Schubert, and Gerrit Tamm. Smart items, fog and cloud computing as enablers of servitization in healthcare. Sensors & Transducers, 185(2):121, 2015.

[2] Yang Li, Li Guo, and Yike Guo. Enabling health monitoring as a service in the cloud. In 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, pages 127–136. IEEE, 2014.

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

[4] Maanak Gupta, Mahmoud Abdelsalam, Sajad Khorsandroo, and Sudip Mittal. Security and Privacy in Smart Farming: Challenges and Opportunities. IEEE Access, 8:34564–34584, 2020.

[5] M Shamim Hossain and Ghulam Muhammad. Cloud-assisted industrial internet of things (IIoT)–enabled framework for health monitoring. Computer Networks, 101:192–202, 2016.
[6] Smriti Bhatt, Farhan Patwa, and Ravi Sandhu. An access control framework for cloud-enabled wearable internet of things. In *2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC)*, pages 328–338. IEEE, 2017.

[7] Mahadev Satyanarayanan, Paramvir Bahl, Ramón Caceres, and Nigel Davies. The case for vm-based cloudlets in mobile computing. *IEEE pervasive Computing*, 8(4):14–23, 2009.

[8] Michele Nitti, Virginia Pilloni, Giuseppe Colistra, and Luigi Atzori. The virtual object as a major element of the internet of things: a survey. *IEEE Communications Surveys & Tutorials*, 18(2):1228–1240, 2015.

[9] Luca Catarinucci, Danilo De Donno, Luca Mainetti, Luca Palano, Luigi Patrono, Maria Laura Stefanizzi, and Luciano Tarricone. An IoT-aware architecture for smart healthcare systems. *IEEE Internet of Things Journal*, 2(6):515–526, 2015.

[10] Sungmee Park and S. Jayaraman. Enhancing the quality of life through wearable technology. *IEEE Engineering in Medicine and Biology Magazine*, 22(3):41–48, 2003.

[11] L. Catarinucci, D. de Donno, L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi, and L. Tarricone. An IoT-Aware Architecture for Smart Healthcare Systems. *IEEE Internet of Things Journal*, 2015.

[12] N. Noury, A. Fleury, P. Rumeau, A. K. Bourke, G. O. Laighin, V. Rialle, and J. E. Lundy. Fall detection - principles and methods. In *2007 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 1663–1666, 2007.

[13] Fabrice Aixsa, P. M. Schmitt, C. Gehin, G. Delhomme, E. McAdams, and A. Dittmar. Flexible technologies and smart clothing for citizen medicine, home healthcare, and disease prevention. *IEEE Transactions on Information Technology in Biomedicine*, 9(3):325–336, 2005.

[14] Reza Shokri and Vitaly Shmatikov. Privacy-Preserving Deep Learning. In *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*, pages 1310–1321, 2015.

[15] D. J. Freitas, T. B. Marcondes, L. H. V. Nakamura, and R. I. Meneguette. A health smart home system to report incidents for disabled people. In *2015 International Conference on Distributed Computing in Sensor Systems*, pages 210–211, 2015.

[16] T. Hadidi and N. Noury. Correlation between real and simulated data of the activity of the elderly person living independently in a health smart home. In *IEEE International Conference on e-Health Networking, Applications and Services*, pages 64–69, 2011.

[17] A. Hamill and M. Benabdellah. Study and implementation of a network point health smart home electrocardiographic. In *International Conference on Advances in Biomedical Engineering*, pages 109–112, 2013.

[18] T. Hadidi and N. Noury. Model and Simulator of the activity of the elderly person in a Health Smart Home. In *IEEE International Conference on e-Health Networking, Applications and Services*, 2010.

[19] X. H. B. Le, M. Di Mascolo, A. Gouin, and N. Noury. Health smart home - towards an assistant tool for automatic assessment of the dependence of elders. In *2007 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 3806–3809, 2007.

[20] G. Sprint, D. Cook, R. Fritz, and M. Schmitter-Edgecombe. Detecting Health and Behavior Change by Analyzing Smart Home Sensor Data. In *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 1–3, 2016.

[21] M. S. Hossain. Patient status monitoring for smart home healthcare. In *2016 IEEE International Conference on Multimedia Expo Workshops (ICMEW)*, pages 1–6, 2016.
[22] P. N. Dawadi, D. J. Cook, and M. Schmitter-Edgecombe. Automated Cognitive Health Assessment From Smart Home-Based Behavior Data. *IEEE Journal of Biomedical and Health Informatics*, 2016.

[23] Olumide Kayode, Deepti Gupta, and Ali Saman Tosun. Towards a Distributed Estimator in Smart Home Environment. *IEEE 6th World Forum on Internet of Things (WF-IoT)*, 2020.

[24] Deepti Gupta, Smriti Bhatt, Maanak Gupta, Olumide Kayode, and Ali Saman Tosun. Access control model for google cloud iot. In 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), pages 198–208. IEEE, 2020.

[25] Ali Tekeoglu and Ali Şaman Tosun. A Closer Look into Privacy and Security of Chromecast Multimedia Cloud Communications. In *Multimedia Cloud Communication Workshop, Held in conjunction with INFOCOM 2015*, Hong Kong, China, April 2015.

[26] Ali Tekeoglu and Ali Şaman Tosun. Investigating Security and Privacy of a Cloud-based Wireless IP Camera: NetCam. In *Workshop on Privacy, Security and Trust in Mobile and Wireless Systems (MobiPST 2015), Held in conjunction with ICCCN 2015*, Las Vegas, USA, August 2015.

[27] A. Tekeoglu and A. S. Tosun. A Testbed for Privacy and Security of IoT Devices. In *IEEE International Workshop on Data Science for Internet of Things, MASS 2016*, pages 1–6, Oct 2016.

[28] Ali Tekeoglu and Ali Şaman Tosun. An Experimental Framework for Investigating Security and Privacy of IoT Devices. In *International Conference on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments (ISDDC 2017)*, Vancouver, CA, October 2017.

[29] O. Kayode and A. S. Tosun. Analysis of IoT Traffic using HTTP Proxy. In *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pages 1–7, May 2019.

[30] Paolo Bellavista, Giuseppe Cardone, Antonio Corradi, and Luca Foschini. Convergence of MANET and WSN in IoT urban scenarios. *IEEE Sensors Journal*, 13(10):3558–3567, 2013.

[31] Yong Liang, Jianhong Xiao, Yubo Wang, Zhenjiang Pang, Yan Li, Xueming Jin, and Geng Liu. A method to make accurate inventory of smart meters in multi-tags group-reading environment. In *2016 IEEE International Conference on RFID Technology and Applications (RFID-Ta)*, pages 123–128, 2016.

[32] J. Lin, M. Zheng, J. Chen, K. He, and E. Pan. Smart Spare Part Inventory Management System with Sensor Data Updating. In *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, pages 597–602, 2019.

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

[34] W. Raad, M. Bueno-Delgado, M. Deriche, and W. Suliman. An IoT Based Inventory System for High Value Laboratory Equipment. In *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, pages 314–319, 2019.

[35] R. Li, T. Song, N. Capurso, J. Yu, J. Couture, and X. Cheng. IoT Applications on Secure Smart Shopping System. *IEEE Internet of Things Journal*, 4(6):1945–1954, 2017.

[36] A. Oplas, M. H. Rabago, C. L. Tormes, C. L. S. Romana, and R. Laviste. Aeon: A Smart Medicine Delivery and Inventory System for Cebu City Government’s Long Life Medical Assistance Program. In *2018 IEEE 10th International


Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM), pages 1–6, 2018.

[37] Wen Ding. Study of smart warehouse management system based on the IoT. In Intelligence computation and evolutionary computation, pages 203–207. Springer, 2013.

[38] Muhammad Asad Khan, Muhammad Hayyan Bin Shahid, Hassan Mansoor, Uzair Shaﬁque, Muhammad Burhan Khan, et al. IoT based grocery management system: Smart refrigerator and smart cabinet. In 2019 International Conference on Systems of Collaboration Big Data, Internet of Things & Security (SysCoBlIoTS), pages 1–5. IEEE, 2019.

[39] S. V. Hove, A. All, and L. D. Marez. Short on Time? Context-Aware Shopping Lists to the Rescue: an Experimental Evaluation of a Smart Shopping Cart. In 2019 Eleventh International Conference on Quality of Multimedia Experience (QoMEX), pages 1–6, 2019.

[40] S. Mekruksavanich. The Smart Shopping Basket Based on IoT Applications. In 2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS), pages 714–717, 2019.

[41] Omar Raad, Majd Makdessi, Yazan Mohamad, and Issam Damaj. Sysmart indoor services: A system of smart and connected supermarkets. In 2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), pages 1–6. IEEE, 2018.

[42] G. Roussos. Enabling RFID in retail. Computer, 39(3):25–30, 2006.

[43] Maanak Gupta, James Benson, Farhan Patwa, and Ravi Sandhu. Secure V2V and V2I Communication in Intelligent Transportation using Cloudlets. arXiv preprint arXiv:2001.04041, 2020.

[44] Maanak 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.

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

[46] Y. Sun, H. Song, A. J. Jara, and R. Bie. Internet of Things and Big Data Analytics for Smart and Connected Communities. IEEE Access, 4:766–773, 2016.

[47] N. Ianuale, D. Schiavon, and E. Capobianco. Smart Cities, Big Data, and Communities: Reasoning From the Viewpoint of Attractors. IEEE Access, 4:41–47, 2016.

[48] P. A. Catherwood, D. Steele, M. Little, S. Mccomb, and J. Mclaughlin. A Community-Based IoT Personalized Wireless Healthcare Solution Trial. IEEE Journal of Translational Engineering in Health and Medicine, 6:1–13, 2018.

[49] Y. Lee, W. Hsiao, C. Huang, and S. T. Chou. An integrated cloud-based smart home management system with community hierarchy. IEEE Transactions on Consumer Electronics, 62(1):1–9, 2016.

[50] K. Axel and I. S. Khayal. Modeling ‘Thriving Communities’ using a Systems Architecture to Improve Smart Cities Technology Approaches. In IEEE International Smart Cities Conference (ISC2), pages 1–2, 2018.

[51] H. Yan and 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.

[52] Olga B Mora, Rogelio Rivera, Victor M Larios, J Raúl Beltrán-Ramírez, Rocio Maciel, and Alberto Ochoa. A use case in cybersecurity based in blockchain to deal with the security and privacy of citizens and smart cities cyberinfrastructures. In 2018 IEEE International Smart Cities Conference (ISC2), pages 1–4. IEEE, 2018.
[53] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. Internet of Things for Smart Cities. *IEEE Internet of Things Journal*, 2014.

[54] H. Chourabi, T. Nam, S. Walker, J. R. Gil-Garcia, S. Mellouli, K. Nahon, T. A. Pardo, and H. J. Scholl. Understanding Smart Cities: An Integrative Framework. In *2012 45th Hawaii International Conference on System Sciences*, pages 2289–2297, 2012.

[55] J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami. An Information Framework for Creating a Smart City Through Internet of Things. *IEEE Internet of Things Journal*, 1(2):112–121, 2014.

[56] C. Harrison, B. Eckman, R. Hamilton, P. Hartswick, J. Kalagnanam, J. Paraszczak, and P. Williams. Foundations for Smarter Cities. *IBM Journal of Research and Development*, 54(4):1–16, 2010.

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

[58] A. Solanas, C. Patsakis, M. Conti, I. S. Viachos, V. Ramos, et al. Smart health: A context-aware health paradigm within smart cities. *IEEE Communications Magazine*, 52(8):74–81, 2014.

[59] M. Naphade, G. Banavar, et al. Smarter Cities and Their Innovation Challenges. *Computer*, 44(6):32–39, 2011.

[60] S. P. Mohanty, U. Choppali, and E. Kougioumas. Everything you wanted to know about smart cities: The Internet of things is the backbone. *IEEE Consumer Electronics Magazine*, 5(3):60–70, 2016.

[61] H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri, and A. Tuncer. UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges. *IEEE Communications Magazine*, 55(3):22–28, 2017.

[62] X. Zheng, L. Tian, G. Luo, and Z. Cai. A Collaborative Mechanism for Private Data Publication in Smart Cities. *IEEE Internet of Things Journal*, pages 1–1, 2020.

[63] A. Meslin, N. Rodriguez, and M. Endler. Scalable Mobile Sensing for Smart Cities: The MUSANet Experience. *IEEE Internet of Things Journal*, pages 1–1, 2020.

[64] James Llinas and David L Hall. An introduction to multi-sensor data fusion. In *Proceedings of IEEE International Symposium on Circuits and Systems*, volume 6, pages 537–540, 1998.

[65] P. Varaiya. Smart cars on smart roads: problems of control. *IEEE Transactions on Automatic Control*, 38(2):195–207, 1993.

[66] J. P. Hubaux, S. Capkun, and Jun Luo. The security and privacy of smart vehicles. *IEEE Security Privacy*, 2(3):49–55, 2004.

[67] D. M. Gavrila and V. Philomin. Real-time object detection for "smart" vehicles. In *Proceedings of the Seventh IEEE International Conference on Computer Vision*, volume 1, pages 87–93 vol.1, 1999.

[68] P. Falcone, F. Borrelli, J. Asgari, H. E. Tseng, and D. Hrovat. Predictive Active Steering Control for Autonomous Vehicle Systems. *IEEE Transactions on Control Systems Technology*, 15(3):566–580, 2007.

[69] J. Funke, M. Brown, S. M. Erlien, and J. C. Gerdes. Collision Avoidance and Stabilization for Autonomous Vehicles in Emergency Scenarios. *IEEE Transactions on Control Systems Technology*, 2017.

[70] M. Kuderer, S. Gulati, and W. Burgard. Learning driving styles for autonomous vehicles from demonstration. In *IEEE International Conference on Robotics and Automation (ICRA)*, pages 2641–2646, 2015.

[71] Maanak Gupta, James Benson, Farhan Patwa, and Ravi 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*, pages 61–72, 2019.
[72] Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy. Foundations and Trends® in Theoretical Computer Science, 9(3–4):211–407, 2014.

[73] Emmanouil Vasilomanolakis, Jörg Daubert, Manisha Luthra, Vangelis Gazis, Alex Wiesmaier, and Panayotis Kikiras. On the security and privacy of Internet of Things architectures and systems. In 2015 International Workshop on Secure Internet of Things (SIoT), pages 49–57. IEEE, 2015.

[74] Alfred Kobsa and Jörg Schreck. Privacy through pseudonymity in user-adaptive systems. ACM Transactions on Internet Technology (TOIT), 3(2):149–183, 2003.

[75] Traian Marius Truta and Bindu Vinay. Privacy protection: p-sensitive k-anonymity property. In 22nd International Conference on Data Engineering Workshops (ICDEW’06), pages 94–94. IEEE, 2006.

[76] Aafaf Ouaddah, Hajar Mousannif, Anas Abou Elkalam, and Abdellah Ait Ouahman. Access control in the Internet of Things: Big challenges and new opportunities. Computer Networks, 112:237–262, 2017.

[77] Smriti Bhatt, Farhan Patwa, and Ravi Sandhu. Access control model for aws internet of things. In International Conference on Network and System Security, pages 721–736. Springer, 2017.

[78] Abhijeet Thakare, Euijong Lee, Ajay Kumar, Valmik B Nikam, and Young-Gab Kim. PARBAC: Priority-Attribute-Based RBAC Model for Azure IoT Cloud. IEEE Internet of Things Journal, 7(4):2890–2900, 2020.

[79] Xin Jin, Ram Krishnan, and Ravi Sandhu. A unified attribute-based access control model covering DAC, MAC and RBAC. In IFIP Annual Conference on Data and Applications Security and Privacy, pages 41–55. Springer, 2012.

[80] Smriti Bhatt, A Tawalbeh Lo’ai, Pankaj Chhetri, and Paras Bhatt. Authorizations in cloud-based Internet of Things: current trends and use cases. In 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), pages 241–246. IEEE, 2019.

[81] Maanak Gupta and Ravi Sandhu. Authorization framework for secure cloud assisted connected cars and vehicular internet of things. In Proceedings of the 23rd ACM on Symposium on Access Control Models and Technologies, pages 193–204, 2018.

[82] Paras Bhatt, Smriti Bhatt, and Myung 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, pages 223–225, 2020.

[83] Smriti Bhatt and Ravi 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, pages 203–212, 2020.

[84] Bo Tang, Hongjuan Kang, Jingwen Fan, Qi Li, and Ravi 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, pages 83–92, 2019.

[85] Samuel G Finlayson, John D Bowers, Joichi Ito, Jonathan L Zittrain, Andrew L Beam, and Isaac S Kohane. Adversarial attacks on medical machine learning. Science, 363(6433):1287–1289, 2019.

[86] Ahmad Fadzil M Hani, Irving Vitra Paputungan, Mohd Fadzil Hassan, Vijanth S Asirvadam, and Megat Daharus. Development of private cloud storage for medical image research data. In IEEE International Conference on Computer and Information Sciences, pages 1–6, 2014.
[88] G Nalinipriya and R Aswin Kumar. Extensive medical data storage with prominent symmetric algorithms on cloud-a protected framework. In *INTERNATIONAL CONFERENCE ON SMART STRUCTURES AND SYSTEMS(ICSSS’13)*, pages 171–177. IEEE, 2013.

[89] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SYMPOS) 2017*, pages 65–80, 2017.

[90] Ivan Ferris, Leonardo Militano, Michele Nitti, Luigi Atzori, and Antonio Iera. MIFaaS: A mobile-IoT-federation-as-a-service model for dynamic cooperation of IoT cloud providers. *Future Generation Computer Systems*, 70:126–137, 2017.

[91] Rolf H Weber. Internet of Things-New security and privacy challenges. *Computer law & security review*, 26(1):23–30, 2010.

[92] Akemi Takeoka Chatfield and Christopher G Reddick. A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in US federal government. *Government Information Quarterly*, 36(2):346–357, 2019.

[93] Leonie Tanczer, Irina Brass, Miles Elsdon, Madeline Carr, and Jason J Blackstock. The United Kingdom’s Emerging Internet of Things (IoT) Policy Landscape. *Tanezer, LM, Brass, I., Elsdon, M., Carr, M., & Blackstock, J.(2019).* *Rewired: Cybersecurity Governance*, pages 37–56, 2019.

[94] Xavier Caron et al. The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. *Computer Law & Security Review*, 32(1):4–15, 2016.

[95] Kyle E Benson, Qing Han, Kyungbaek Kim, Phu Nguyen, and Nalini Venkatasubramanian. Resilient overlays for IoT-based community infrastructure communications. In *IEEE International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2016.

[96] Thaha Muhammed, Rashid Mehmood, and Aiiad Albeshri. Enabling reliable and resilient IoT based smart city applications. In *International Conference on Smart Cities, Infrastructure, Technologies and Applications*, pages 169–184. Springer, 2017.

[97] M Jeroen Van Der Donckt, Danny Weyns, M Usman Ifthikhar, and Ritesh Kumar Singh. Cost-Benefit Analysis at Runtime for Self-adaptive Systems Applied to an Internet of Things Application. In *ENASE*, pages 478–490, 2018.

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

[99] Laith Farhan and Rupak Kharel. Internet of things: Vision, future directions and opportunities. In *Modern Sensing Technologies*, pages 331–347. Springer, 2019.

[100] Mehdi Mohammadi, Ala Al-Fuqaha, Sameh Sorour, and Mohsen Guizani. Deep learning for IoT big data and streaming analytics: A survey. *IEEE Communications Surveys & Tutorials*, 2018.

[101] Deepti Gupta, Olumide Kayode, Smriti Bhatt, Maanak Gupta, and Ali Siaman Tosun. Learner’s Dilemma: IoT Devices Training Strategies in Collaborative Deep Learning. *IEEE 6th World Forum on Internet of Things (WF-IoT)*, 2020.