future internet

Review

IoT Technologies during and Beyond COVID-19: A Comprehensive Review

Mohamed Yousif, Chaminda Hewage * and Liqaa Nawaf

Cardiff School of Technologies, Llandaff Campus, Cardiff Metropolitan University, Western Avenue, Cardiff CF5 2YB, UK; M.Yousif2@outlook.cardiffmet.ac.uk (M.Y.); lllNawaf@cardiffmet.ac.uk (L.N.)
* Correspondence: chewage@cardiffmet.ac.uk

Abstract: The COVID-19 pandemic provided a much-needed sanity check for IoT-inspired frameworks and solutions. IoT solutions such as remote health monitoring and contact tracing provided support for authorities to successfully manage the spread of the coronavirus. This article provides the first comprehensive review of key IoT solutions that have had an impact on COVID-19 in healthcare, contact tracing, and transportation during the pandemic. Each sector is investigated in depth; and potential applications, social and economic impact, and barriers for mass adaptation are discussed in detail. Furthermore, it elaborates on the challenges and opportunities for IoT framework solutions in the immediate post-COVID-19 era. To this end, privacy and security concerns of IoT applications are analyzed in depth and emerging standards and code of practices for mass adaptation are also discussed. The main contribution of this review paper is the in-depth analysis and categorization of sector-wise IoT technologies, which have the potential to be prominent applications in the new normal. IoT applications in each selected sector are rated for their potential economic and social impact, timeline for mass adaptation, and Technology Readiness Level (TRL). In addition, this article outlines potential research directions for next-generation IoT applications that would facilitate improved performance with preserved privacy and security, as well as wider adaptation by the population at large.

Keywords: Internet of Things; COVID-19; pandemic; IoT solutions; IoT privacy and security challenges; IoT applications

check for updates

Citation: Yousif, M.; Hewage, C.; Nawaf, L. IoT Technologies during and Beyond COVID-19: A Comprehensive Review. *Future Internet* **2021**, *13*, 105. https://doi.org/10.3390/fi13050105

Academic Editors: Dino Giuli and Eirini Eleni Tsiropoulou

Received: 16 March 2021
Accepted: 19 April 2021
Published: 23 April 2021

1. Introduction

The Internet of Things (IoT) is a collection of interconnected devices, humans, objects, and services that share data to accomplish a common objective in different areas and applications, as defined by [1]. IoT is used in many different domains, such as healthcare, agriculture, transportation, distribution, and energy production. Rapid development was made in the IoT industry due to both Wireless Sensor Network (WSN) that enables the communication between devices and Radio Frequency Identification (RFID), which allows the labelling of devices [1].

IoT currently plays an important role in many fields. Healthcare is one of the prominent sectors benefitted by the advancement of IoT [2]. In the health sector, IoT has drastically changed the lives of both the young and elderly, as it can constantly track their health [3]. These devices are of greater use with reduced cost and faster disease diagnosis. The role of the IoT landscape has been significantly changed due to the COVID-19 pandemic [4]. Some use is directly related to mitigating the spread of the virus (e.g., contact tracing, temperature screening, etc.) whereas others seek to facilitate the new normal created by the pandemic (e.g., working from home, homeschooling, home fitness, etc.) [5–7].

The coronavirus disease (COVID) is a contagious disease caused by Severe Acute Respiratory Syndrome Coronavirus 2 (SARS-CoV-2), which can be spread through nose discharge and saliva droplets from the sneezes or coughs of infected people. COVID-19 symptoms involve shortness or difficulty in breathing, fever, cough, vomiting, fatigue, and loss of taste or smell. Transmission risk is highest when the distance between the carrier and the subject is less than 2 m. Hence, limiting human-to-human interaction is the current appropriate solution [8].

It is important to be able to detect early cases, trace, and isolate infected people during pandemics. A system is needed to keep businesses running and customers and employees healthy. IoT technologies with RFID, Near Field Communication (NFC), Wi-Fi, Bluetooth Low Energy (BLE), and GPS help provide better solutions for the aforementioned cases. These technologies are now infused with small, wearable, and portable devices. Energy consumption, computational time, cost, data rate, practicality, and coverage may differ from one device to another, depending on the material and technology used. Other than patient needs, IoT helps in resolving machinery issues faster for healthcare workers, managing pharmacy inventory controls, and keeping track of tagged equipment, such as nebulizers and oxygen tanks [9].

Our paper focuses on the role of IoT during COVID-19, IoT-based solutions for COVID-19 in different industries, challenges, and threat mitigation practices for IoT. The main research question that this paper trying to address is: "What is the use and impact of IoT basic technologies during COVID-19 and beyond?".

In order to answer the above research question, a comprehensive review was conducted by the authors. Consequently, it was found that IoT provided solutions for many applications and systems in different industries (healthcare, transportation, entertainment, retail, education, and communication) during the COVID-19 pandemic and there is more potential in the post-COVID-19 era. Solutions vary from wearable devices and temperature screening to contact tracing solutions.

This article is organized as follows: Section 2 discusses the related work and reviews. Section 3 presents the paper methodology and research objectives. The role of IoT during COVID-19; the IoT inspired frameworks for tackling COVID-19, and future pandemics in different sections are discussed in Section 4. Section 5 presents the role of IoT and expectation in the post-COVID-19 era. Section 6 displays IoT privacy, polices, and security challenges. Section 7 presents IoT threat mitigations and emerging Code of Practice. Section 8 present the implications and future directions. Finally, Section 9 concludes the paper.

2. Related Work

The COVID-19 pandemic has given rise to various predictions on the future. It is envisaged that IoT will play a significant role in the new normal. This article presents, analyses, and discusses IoT-inspired solutions during the pandemic in different sectors, challenges, and opportunities beyond the pandemic.

The large number of interconnected devices used by the IoT that can track and alert different types of illness help in creating a smart network for health management systems. Patient information is captured without the need for human interaction, which could be beneficial in decision-making methods [2].

There are many wearable lightweight IoT devices [10] that could be used to limit contagious viruses such as COVID-19 and improve healthcare offerings. Some symptoms can be effortlessly monitored with the use of IoT devices. If symptoms of the virus are detected, the device can notify both the user and the closest health department. IoT can also work as a mapping network that shows places with dense population or places that have an increased number of cases and a higher risk of infection. This can improve the intervention of health department performance to detect and save individuals in critical situations (e.g., the patient is unable to contact the health department at the right time due to symptoms) and share data with different departments to come up with a faster cure and to keep civilians safe. With the use of technologies such as 4/5 G and the cloud, it is much easier to monitor patients from a great distance, especially individuals who find it difficult to reach or access healthcare facilities.

Another benefit of IoT devices in the healthcare sector is the reduction in human error, which is more frequent than machine or AI errors. IoT can provide more accurate diagnosis and patient reporting, taking into consideration that human mistakes will likely recur.

IoT technology plays a significant role in detecting the virus by using fever screening to recognize some of the virus' symptoms, limiting spread by enforcing social distancing; and managing remote health monitoring, pollution and air quality control, occupancy control, and smart parking. The use of fever screening requires no contact between people and allows multi-targets detection. Sensors and cameras provide colour temperature scales and images. Pre-screening of employees, disaster evacuees, or patients is the first line of defense against the virus [5]. This does not guarantee virus detection but can be used to determine if the subject may have symptoms of the virus, and further inspections are made for final determination. Fever screening can be used in airports, schools, warehouses, and other crowded areas. Figure 1 illustrates the temperature screening output of a solution available in the market.

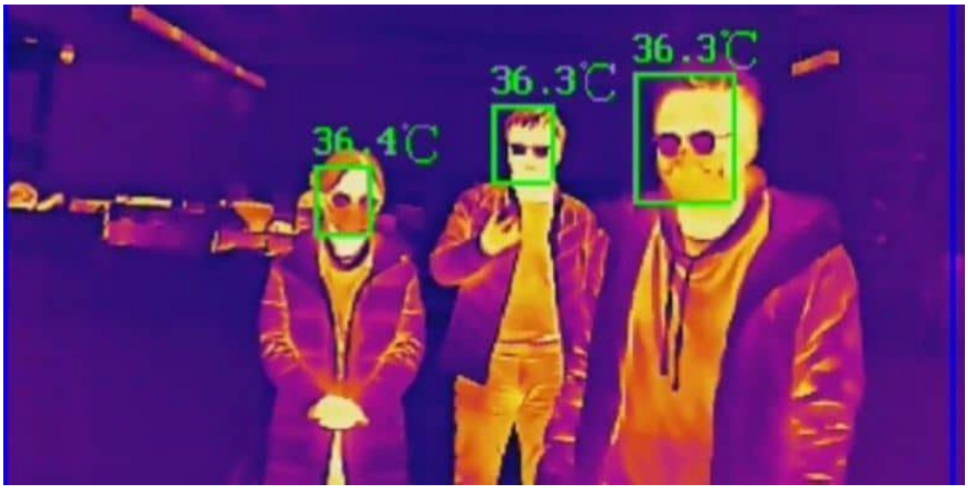

Figure 1. Temperature Screening [11].

2.1. Is the State-of-the-Art IoT Enough to Tackle COVID-19 Related Challenges?

IoT can tackle most COVID-19 challenges. It can support control of the pandemic by using it as an alerting mechanism, a warning mechanism, or a penalty mechanism, or a combination. The mechanisms can be categorized into three levels, alerting being the first level and penalty as the third level. At the alerting level, IoT can alarm the users if, for example, an area has a dense population, cases are in a specific area, and if there is going to be a lockdown. The warning and penalty levels work together. A warning could be issued, for example, for people who arrive from another city to not leave home for 14 days, and a penalty can be applied if the warnings are ignored. These mechanisms can limit the spread of the virus and control the pandemic. However, with the increased intervention, more personal data and permissions (or consent) are required from the user, which affects user privacy and security. There is a conflict between data access to provide better services and protecting user privacy. The amount of data collected from IoT devices puts individuals at risk as they become more easily identifiable with the use of profiling, tracing, and unauthorized processing, which can violate data protection laws such as General Data Protection Regulation (GDPR), due to the requirement of explicit consent from users. However, legitimate interests can play a bigger role in controlling a global pandemic such as COVID-19. Security and privacy issues associated with Coronavirus diagnosis and prognosis are discussed by the author of [12].

During the pandemic, IoT-inspired technologies provide greater use with a reduced cost and faster disease diagnosis. For instance, the ADAMM Asthma monitor that detects asthma attack [13] and the Smart Continuous Glucose Monitoring (CGM) [14] are of great examples of the use of IoT in the health sector. In these critical times, IoT can be of great help to the elderly as they are more vulnerable to the virus than the other age groups. They are also more prevalent due to the increase in life expectancy. IoT wearable devices that can perform biometric reading and activity tracking, such as the Apple smart health watch [15] and the Omron blood pressure monitor [16], can help in constantly monitoring their health remotely. Grandcare is also a useful system that allows elderly people to communicate with their loved ones and would be ideal for home monitoring [17].

A study conducted by [18] proposed eight machine learning algorithms to early identify suspected COVID cases. Five of these algorithms present more than 90% accuracy in identifying potential cases. The framework also analyses the treatment response and real-time monitoring of the patient to understand the nature of the virus. This high accuracy can help in detecting many early cases and to rush with appropriate treatment. With innovation technologies, IoT is capable of creating high-quality outcomes and customized attention and benefits to the patient by reducing the associated losses [3].

2.2. Related Reviews

A number of reviews can be found in the literature that address different aspects of IoT. Some of them are the latest reviews on COVID-19 related IoT applications and their performance and impact. The review conducted by [19] provides a survey for emerging healthcare applications in various use case scenarios. It also focuses on key application-specific viewpoints of communication technologies, highlighting the consideration of long-range and short-range communications. A review by [20] discusses the Quality of Experience (QoE) in IoT. The review presents factors impacting QoE of IoT systems, practical QoE models without human interference, and the effect of security on the QoE of automatic IoT systems. The review presented in [21] identifies different security challenges and solutions. Hence, the challenges mainly fall under privacy, secure routing, and forwarding for IoT. Rahmani and Mirmahaleh [22] highlight different strategies to face COVID-19 and their negative and positive impacts on people and then classify and analyze the treatments and prevention methods. A review of IoT application in agro-industrial fields is presented in [23]. This review presents solutions for environmental problems but declares that "future solutions will need to fully embrace Cloud services and new ways of connectivity in order to get the benefits of a truly connected and smart IoT ecosystem". The review presented in our article focuses on IoT-based technologies and applications during COVID-19 in key sectors. The sectors are selected based on the research conducted by the authors and previously published research in the literature.

3. Methodology

In order to answer the usage and impact of IoT Technologies during and beyond COVID-19 (i.e., the research question mentioned in Section 1), the below research objectives are drafted:

(a) Identification of key IoT Technologies, which had an impact on managing the COVID-19 pandemic via a comprehensive literature review
(b) Review of social-economic impact, maturity of the technology, and timeline for wider deployment
(c) Analysis and discussion of policy, privacy, and security challenges, and finally identification and analysis of best practice and code of practices for IoT technologies

In order to achieve the above research objectives, the following research methodology is followed in this study. The review was carried out using publicly available, secondary data sources, which discuss different aspects of IoT technologies in diverse sectors. The main data sources used in this review are SCOPUS library, Web of Science citation database, ACM library, IEEE Xplorer, Google Scholar, etc. A number of keyword searches were used to find relevant studies and reviews necessary to answer the research questions of our study. The main keywords combinations included "COVID-19", Coronavirus, IoT, IoE, IIoT, IoMT, and other relevant key words. An exclusion criterion was not used.

As for the review protocol, key IoT areas for the review was selected based on the number of search results that appeared for all keyword combinations. In addition to the above keyword search by the authors, recommendations by previously published research, tutorials, surveys, and reviews were used to select the sectors to focus on this review. The details of each IoT application was analyzed, categorized, and summarized. The analyzed IoT applications were categorized based on the sector and the industry. Then a deep dive into individual IoT technology under each sector was performed. Each key application was also ranked based on the potential economic and social impact it would make. These decisions were made based on the insights from the data collected about each application. In addition, the timeline for wider adaption of the each IoT technology is predicted based on the collected data about the application area. Finally, Technology Readiness Level of each IoT application is depicted based on the current maturity level. In order to determine the TRL levels, the European Union's scale of TRLs with nine categories were used [24].

The privacy and security concerns as well as best code of practices for IoT were also derived from the data collected from the relevant literature. A deep analysis is performed to identify the key challenges and opportunities for each application area under respective sector.

4. A Framework of Solutions to Tackle COVID-19 and Emerging Pandemics in the Future Using IoT

The implemented health regulations (local and national-wide lockdowns) that ensured the safety of the people had a significant impact on many different industries. This review sought to understand the usage and impact of IoT-based technologies on COVID-19. The selected applications and industry sectors are not an exhaustive list. It is chosen based on the initial research conducted by the authors and based on the recommendations by previous empirical studies. The required data for the review was collected using the methodology described in Section 3. A multitude of applications and industry sectors which used IoT-based technologies during COVID-19 were identified from the initial research. Table 1 illustrates the top search results that appeared for different keyword combinations. Based on the number of search appearances and recommendations made by previous empirical studies [25–28], the following industry sectors and applications are chosen for in-depth analysis in the study.

Table 1. Number of search results.

Database	SCOPUS Library (Journals)	ACM Library	IEEE Xplore	Google Scholar
Keywords				
IoT or Internet of Things and COVID and Health	561	75	68	11,800
IoT or Internet of Things and COVID and Transport	203	39	6	5460
IoT or Internet of Things and COVID and Education	386	62	19	9110
IoT or Internet of Things and COVID and Communication	852	87	70	12,900
IoT or Internet of Things and COVID and Retail	21	9	5	3050
IoT or Internet of Things and COVID and Entertainment	24	7	4	1870
IoT or Internet of Things and COVID and Contact tracing	206	77	13	1860

- Healthcare
- Transportation
- Education and communication
- Retail, entertainment

Furthermore, some sectors were combined to effectively evaluate the usage and impact of the chosen applications. While industry sectors such as healthcare are mentioned in almost all previous studies in the literature, some of the sectors discussed in this article are not widely researched. In addition to the selected sectors, IoT has been used in several other industries, such as agriculture and hospitality [29–31]. However, a wider usage has not been observed for those sectors, in comparison to the selected applications for this study.

Figure 2 illustrates the chosen key sectors affected by COVID-19 and growth areas identified based on the review conducted. In this figure, key application areas within each domain are also highlighted.

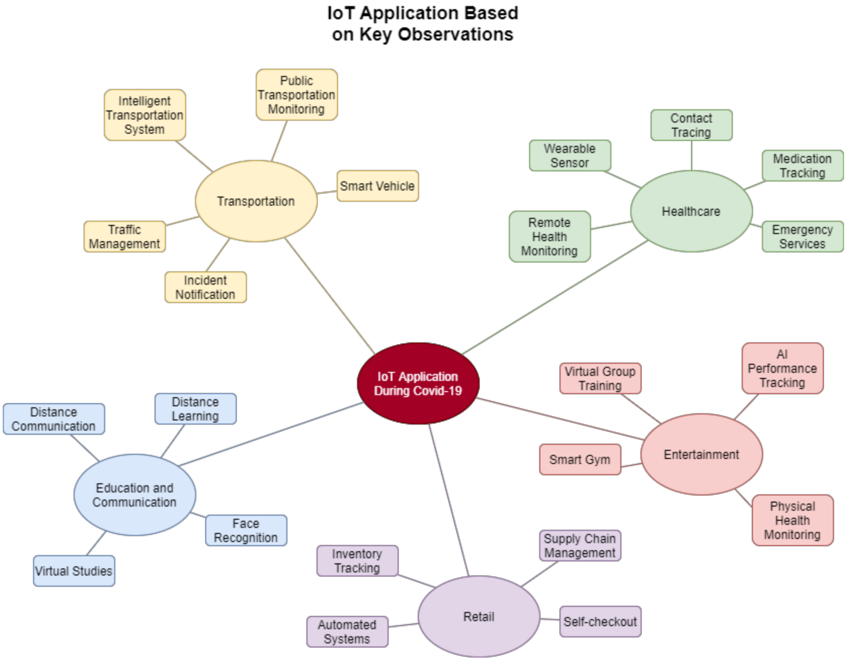

Figure 2. IoT applications based on key observations.

Figure 3 below illustrates a selected IoT applications and usage of IoT in different sectors. The following sub-sections discuss IoT solutions and frameworks that help different industry sectors to minimize the impact created by the COVID-19 pandemic.

4.1. IoT in the healthcare sector

Healthcare is one of the key sectors that benefited from IoT-inspired solutions during the COVID-19 pandemic. These solutions range from wearable solutions to support for emergency services such as paramedics. Even though some of the IoT solutions are not mature enough to deploy on a wider scale, they provided promising usage during the pandemic. This validation will help these applications to mature in the future and be deployed in a wider context with confidence.

COVID-19 is caused by the SARS-CoV-2 virus, which affects the respiratory system. Research in [32] proposes a wearable strain sensor that measures the volume and respiration rate of the user's respiratory system. These sensors can track and monitor patients' breathing conditions through the Internet of Medical Things (IoMT) and continuously update the involved doctors of the patient's respiratory condition. This is also time saving, as it is easier for the concerned doctors to make appropriate recommendations remotely. The author of [33] proposes a wearable IoT-based system to detect stress levels. This is an appropriate solution for people who are suffering from stress, anxiety, and isolation due to the pandemic.

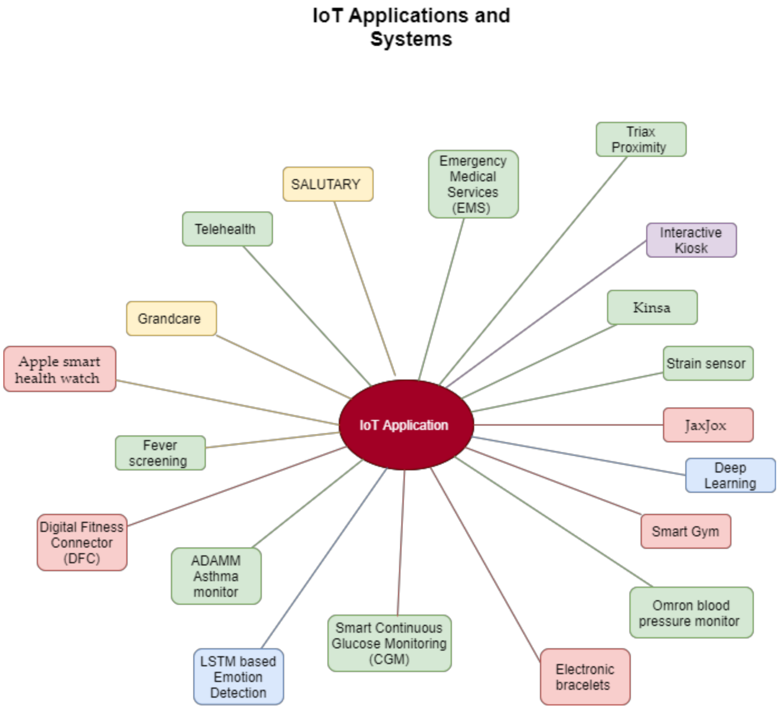

Figure 3. IoT Applications and Systems.

During the COVID-19 pandemic, the use of contact tracing has proved to be an appropriate solution to protect personal data, while keeping people safe. There are wearable light IoT devices such as Triax Proximity Trace that use contact tracing to address social distancing as it alarms users when they are too close to each other [6]. Enterprise departments can distribute wearable devices that ensure safety regulations without the need for mobile phones or downloads. Tags are sent through Bluetooth technology without the need to track a user's location. In addition, anonymized keys that change every 15 min are used for further privacy protection. The Province of Alberta has introduced contact tracing application for COVID-19. The application confirms positive cases and notifies Canadians who have been near those who have received a positive result [34].

Stanford Children's Health Hospital was able to jump from meeting 20 patients daily to more than 600 patients through a two-way, live telehealth interaction, or "virtual visit" [35]. Electronic communications—audio and video—are used to allow interaction between the patients and their consultant or healthcare provider without having to meet in person, which is a viable alternative rather than a mass gathering in the hospital with a chance of virus infection.

Another great solution for home-based health monitoring is the smart thermometer, Kinsa. The device can map fever and illness to help users to react faster with the current situation. It also keeps logs of a family's health and their health history, tracks medications and set reminders, and offers friendly features for kids' ease of use. The device connects to the Kinsa App using Bluetooth and extra information can later be sent to the concerned party [36].

During the pandemic, medical staff associated with ambulance services deal with more pressured and tense situations. Ambulance IoT aided equipment provides solutions that are time-efficient, where experts can advise the staff of necessary actions to deal with patients in critical situations [25]. IoT-based Emergency Medical Services (EMS) are great systems to save lives in critical situations. The author of [37] proposes a system that provides real-time information regarding the number of available beds, blood levels of all types, blood type availability, and doctors' availability. Real-time data can be obtained from the ambulance during major accidents and with multiple casualties.

Table 2 summarizes the key IoT applications in this domain, anticipated economic and social impact, predicted timeline for wider adaptation, and Technology Readiness Levels (TRLs) of the application for wider deployment.

Table 2. Key observations of IoT in the healthcare sector.

	IoT Application	**Societal and Economic Impact (Low, Medium, High)**	**Timeline for Wide Usage (Immediate, Post-COVID-19, Future)**	**Technology Readiness Levels (TRLs) of the Application for Wider Deployment**
1	Remote Health Monitoring [5,13,14,16]	High	Immediate	TRL9
2	Wearable Sensor [5,32,33,38–41]	High	Immediate	TRL9
3	Contact Tracing [6,34]	High	Immediate	TRL9
4	Medication Tracking [9,36]	High	Post-COVID-19	TRL8
5	Emergency Services [25,37]	High	Immediate	TRL5

Figure 4 visualizes Healthcare IoT technology in three dimensions (Societal and Economic Impact, Timeline for Wide Usage, and Technology Readiness Levels (TRLs) of the Application for wider deployment), as summarized in Table 1. This provides enhanced visualization of the technology impact, timeline, and TRL.

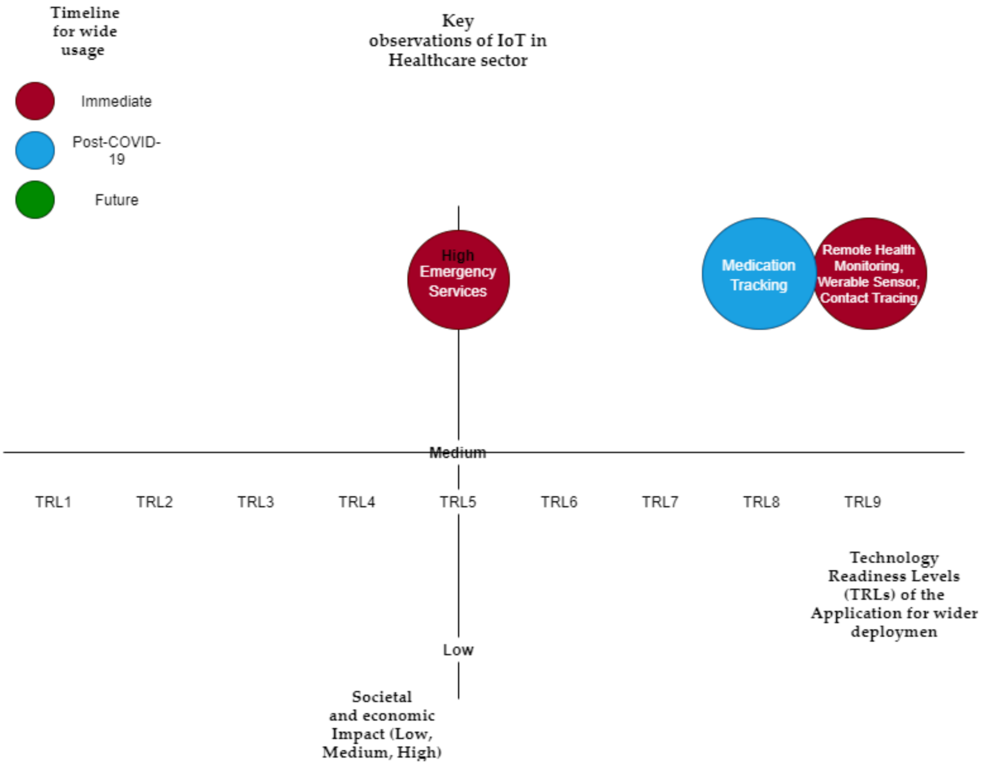

Figure 4. Key observations of IoT in the healthcare sector.

4.2. IoT in the Transportation Sector

COVID-19 has had a huge impact on the transportation industry. With the adoption of COVID prevention methods, a reduced demand for transport has been noticed [42], which has also affected other areas, such as agricultural supply chains [43]. IoT applications such as the toll and reservation ticketing system, navigation tracking and GIS mapping, control and guidance systems, supply chain management solution systems, and smart vehicle applications can tackle some problems during the pandemic to limit crowded areas and help the process of importing and exporting goods. IoT-based Intelligent transportation systems can provide automation in roadways, railways, marine, and airways [44], which help in limiting human-to-human interaction to reduce the infection risk, while enabling continuation of the workflow.

SALUTARY is a safe and reliable public transportation system that aims to make use of Information and Communication Technologies (ICT) to deal with congested situations in public transportation (bus stops, subway stations, trams, busses, trains, and railway) [45]. The system performs real-time monitoring of the number of users to predict congestion, inform the users, and adapt system operations, such as modifying routes and timetables. Adding the system to the Intelligent Transportation System (ITS) can allow innovative crowd detection and offer services such as online ticketing, reservation, and vehicle access control to limit the congestion.

Sutar proposed an IoT, GPS, and Android-based solution that addresses the issues with traffic management for public transport systems and the increased number of vehicles on the streets [46]. Al-Dweik also proposed an IoT multifunctional real-time roadside unit for intelligent transportation systems that reduce vehicle congestion and mange metering routes [47].

A framework developed by [48] uses real-time datastream and user incident reports to provide incident notification and route recommendation for users who travel mainly by bus.

Vaccine distribution became a key point with the introduction of several reliable vaccines globally. The distribution of vaccines is a critical task due to the temperatures they have to maintain for their effectiveness; for example, Pfizer is required to maintain −700 °C. Many countries have deployed IoT to monitor this cold chain of vaccine deployment. A case reported from Germany had to discard a huge quantity of vaccines since they observed that one supply could not maintain the required temperature throughout the delivery [49]. On the other hand, it was reported that hackers are trying to attack this cold chain of vaccine supply. Therefore, these IoT-based monitoring platforms should be protected from unauthorized access.

These intelligent transport solutions could provide much needed services while adhering to healthcare guidelines.

Table 3 summarizes the key IoT applications in this domain, anticipated economic and social impact, predicted timeline for wider adaptation, and TRLs of the application for wider deployment (also visualized in Figure 5).

Table 3. Key observations of IoT in the transportation sector.

	IoT Application	**Societal and Economic Impact (Low, Medium, High)**	**Timeline for Wide Usage (Immediate, Post-COVID-19, Future)**	**Technology Readiness Levels (TRLs) of the Application for Wider Deployment**
1	Public Transportation Monitoring [45]	High	Immediate	TRL9
2	Intelligent Transportation System [44,47]	Medium	Immediate	TRL3
3	Smart Vehicle [46]	Medium	Future	TRL7
4	Traffic Management [45–47]	High	Immediate	TRL9
5	Incident Notification [48]	Medium	Immediate	TRL7

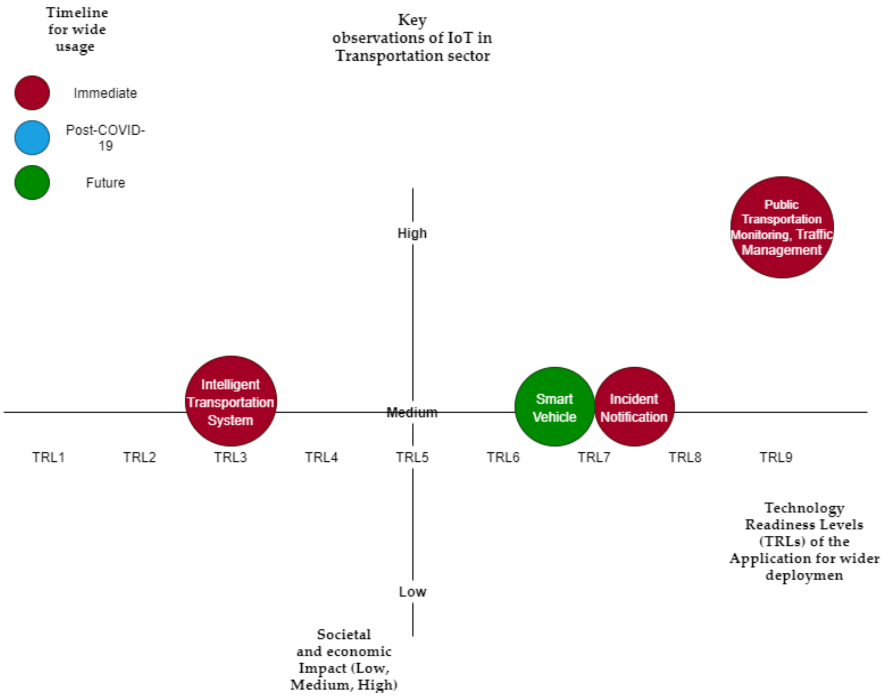

Figure 5. Key observations of IoT in the transportation sector.

4.3. IoT in the Education and Communications Sector

The pandemic has forced a change in the education system by limiting face-to-face teaching and on-campus learning [50]. Distance learners and students who study at home will be able to continue their education through IoT and advanced technologies. Studies show that some virtual studies can prepare students for laboratory exercises and essential non-cognitive skills [51].

Ilieva proposed an IoT framework to facilitate adaption of the studying process to the current situation [52]. This framework administers both teaching and examination processes via IoT. The components used are web camera for attendance, behavioural indicators, and emotional state and GPS tracker to capture movement and monitor location; a wearable device that examines brain signals, heart rate, and blood pressure; sensors that examine the collected data and detect abnormalities and notifies the lecturer; and different algorithms such as face recognition, deep learning, and classification algorithms used for monitoring and management. In addition, eye trackers, EEGs, and web cameras are used in examination for student inspection and to detect cheating. The above study shows the real use of IoT to support distance learners.

An integrated IoT framework proposed by Awais focuses on human emotion analysis [53]. The analysis of physiological signals is done through Long Short-Term Memory (LSTM) based emotion recognition to identify different emotions. This framework enables communication and recognition of human emotions in real time of above 95%, which can support student engagement, healthcare infrastructure, and educational institutions in approaching an effective distance learning paradigm while minimising COVID-19 pandemic threats.

Google and Apple recently added a COVID-19 exposure notification system for Android and Apple phones [54]. The system notifies the user when they come into contact with someone who has been reported of having COVID-19. The system also provides instructions of what to do if you have been in contact with someone with COVID-19. The system ensures the user's privacy by not sharing location and by generating random IDs to prevent tracking. The only information shared is the day of contact, the duration of the contact, and the distance between the users.

Table 4 summarizes the key IoT applications in this domain, anticipated economic and social impact, predicted timeline for wider adaptation, and TRLs of the application for wider deployment (also visualized in Figure 6).

Table 4. Key observations of IoT in the Education and Communications sector.

	IoT Application	Societal and Economic Impact (Low, Medium, High)	Timeline for Wide Usage (Immediate, Post-COVID-19, Future)	Technology Readiness Levels (TRLs) of the Application for Wider Deployment
1	Distance Learning [51,52]	Medium	Immediate	TRL6
2	Distance Communication [51,52]	High	Immediate	TRL9
3	Virtual Studies [51]	Low	Future	TRL5
4	Face Recognition [52,53]	Medium	Post-COVID-19	TRL9

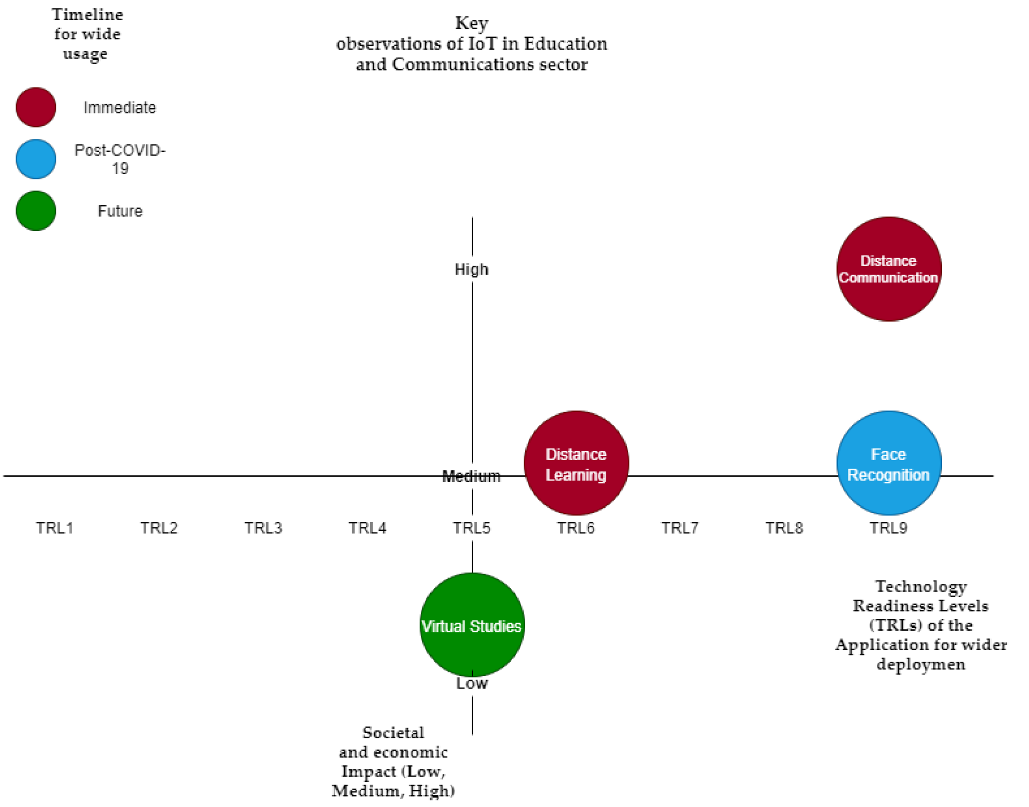

Figure 6. Key-observations in the Education and Communication sector.

4.4. IoT in the Retail Sector

There are different IoT systems that can help with the COVID-19 situation, such as industrial internet of things (IIoT). IoT retail self-checkout and warehouses both reduce human-to-human interactions and eliminate crowded and jammed areas, making it less likely for people to spread or be infected with the virus. With the use of an IoT retail self-checkout, problems such as long queues, billing, and human error can be solved [55] without human intervention. IoT can also be used to enhance supply chain management with delivery, storage, and inventory. An example of this would be the IoT automated systems used in Amazon warehouses, as they provide seamless workflow, real-time tracking, and reduced overall handling costs [56].

Connected products and devices help optimize complex supply chain operations. Inventory tracking can be improved using RFID technology. Smart tags enable real-time product adjustments and pricing [57]. This can limit the number of in-store workers and can enable home workers to easily adjust and monitor the workflow without the need to be physically present, in line with health guidelines. IoT can enhance supply chain performance in quality, cost, flexibility, and delivery with the use of information-sharing, intelligence, data auto capture, and visibility, which improve businesses' environmental, social, and financial sustainability [58].

A proposed IoT-based Standard Operating Procedure (SOP) compliance system by Bashir that checks the number of people who enter an area and monitors their body temperature, ensures physical distance, and notifies managers and the concerned authorities of any violation [59]. This system does not register personal information and does not provide contact tracing information, thus ensuring people's privacy.

Table 5 summarizes the key IoT applications in this domain, anticipated economic and social impact, predicted timeline for wider adaptation, and TRLs of the application for wider deployment (also visualized in Figure 7).

Table 5. Key observations of IoT in the retail sector.

	IoT Application	Societal and Economic Impact (Low, Medium, High)	Timeline for Wide Usage (Immediate, Post-COVID-19, Future)	Technology Readiness Levels (TRLs) of the Application for Wider Deployment
1	Supply Chain Management [56–58]	High	Immediate	TRL9
2	Inventory Tracking [56,57]	High	Post-COVID-19	TRL9
3	Automated Systems [56]	High	Post-COVID-19	TRL7
4	Self-checkout [55]	Low	Immediate	TRL8

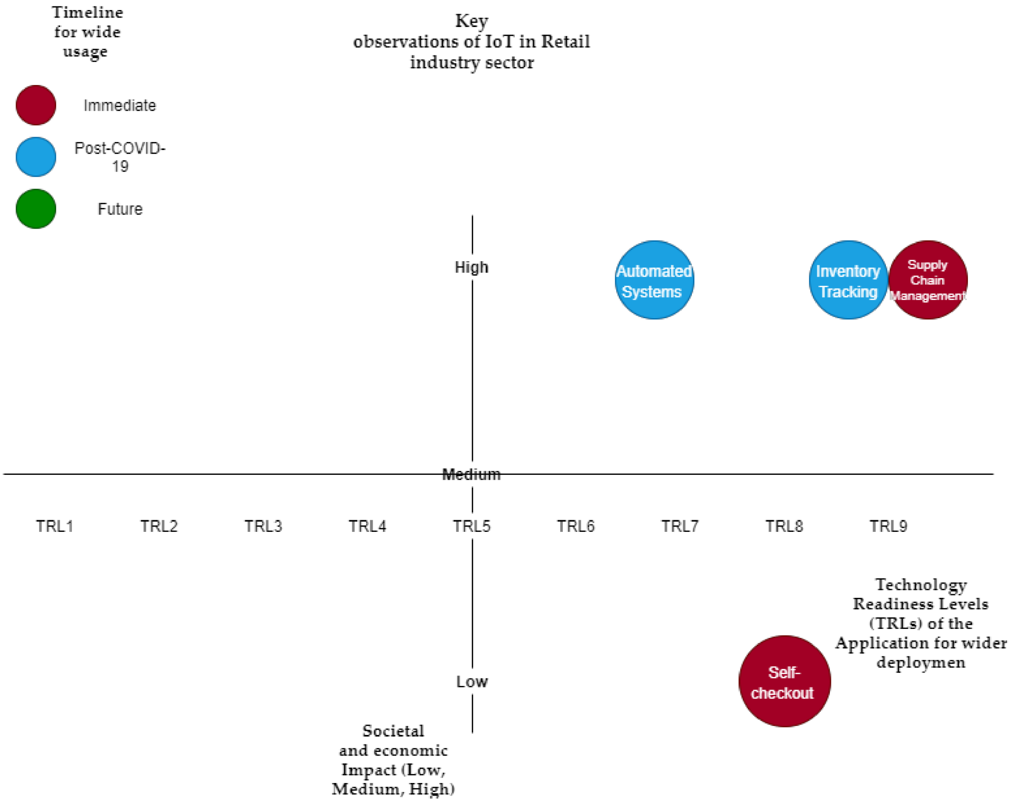

Figure 7. Key observations of IoT in the retail sector.

4.5. IoT in the Entertainment Sector

The entertainment industry has been greatly affected by the pandemic. Different activities such as going to the gym, sport fields, clubs, theatres, concerts, and travel are restricted due to the lockdown. The IoT technology can help ease these limitations by providing solutions such as smart gyms and wearable devices. IoT is used in many ways to monitor the physical environment and to collect mobility socio-economic data that save resources and time [60].

JaxJox recently announced an interactive fitness studio, which acts as a smart home gym for users. The system provides different performance data and fitness classes with AI performance tracking and personalized coaching experience. Friends and members can also work out together using the virtual group training function, providing a better experience for group workouts [7]. A framework by Jain provides efficient resource utilization in the gym and provides innovative services to the users [61]. This works as a great solution for users who are not capable of using a public gym anytime soon.

Gupta and Jilla proposed the Digital Fitness Connector (DFC), which is compatible with over 80 ANT health and fitness sensors. The sensors are able to track speed, heart rate, power, cadence, pace, and distance, which is also connected to smartphones [38]. This helps the users to monitor their physical activity in real-time and store their data.

This technology can go along with pandemic or governmental regulations as it helps reduce face-to-face interactions, imposes limits on gathering with other people, and mitigate the risk of exposure to coronavirus at any healthcare premises. These lightweight devices can also help in reinforcing and implementing these regulations. There are a few countries—Jordan, Bahrain, and Bulgaria—that use electronic bracelets as a monitoring and control mechanism to ensure that the public are in line with coronavirus quarantine measures and to ensure that the rules are respected by those who are self-isolating [39–41].

A research presented by [62] provides an indoor, cost-effective IoT monitoring system for COVID-19. The system uses Rasberyy Pi, temperature sensors, camera, and Arduino for mask detection, contactless temperature sensing, and to check the social distance between the individuals. Even though the system performance is limited to the kind of hardware used, it provides a decent result. This shows the capability of IoT with the associated technology in smaller spaces.

Table 6 summarizes the key IoT applications in this domain, anticipated economic and social impact, predicted timeline for wider adaptation, and TRLs of the application for wider deployment (also visualized in Figure 8).

Table 6. Key observations of IoT in the entertainment sector.

	IoT Application	Societal and Economic Impact (Low, Medium, High)	Timeline for Wide Usage (Immediate, Post-COVID-19, Future)	Technology Readiness Levels (TRLs) of the Application for Wider Deployment
1	Virtual Group Training [7]	Low	Future	TRL5
2	Smart Gym [7,61]	Low	Future	TRL4
3	Physical Health Monitoring [7,38,60,61]	High	Immediate	TRL9
4	AI Performance Tracking [7]	Low	Future	TRL5

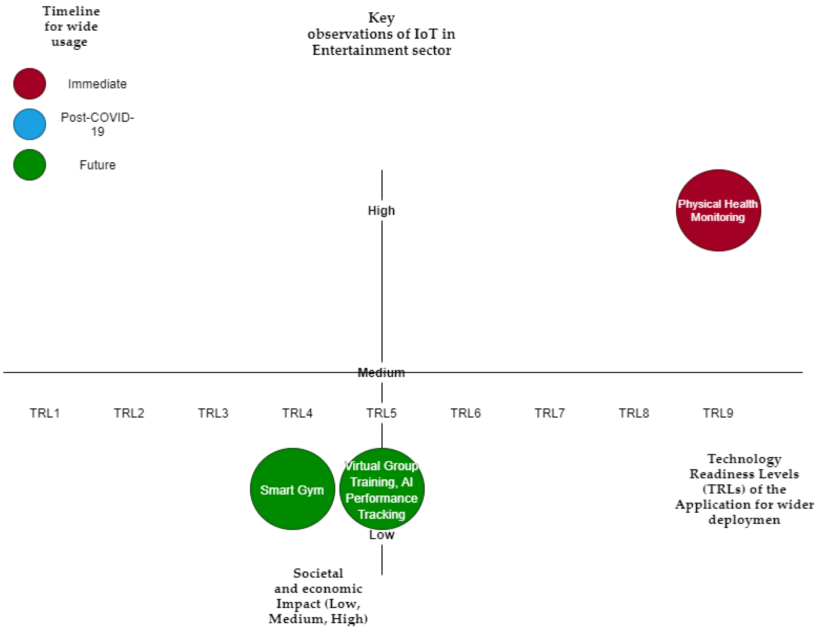

Figure 8. Key observations of IoT in the entertainment sector.

5. The Role of IoT in the Post-COVID-19 Era

The need to use IoT in these critical times will open the eyes of innovators, researchers, and developers to IoT technology, which can result in remarkable growth in the post-COVID era. IoT was known mainly for a much wider scale concept, such as smart cities, smart cars, etc. This article highlighted how different industries, which were never envisaged pre-COVID-19, would benefit from IoT beyond COVID-19. The use of IoT has its advantages and disadvantages. However, with noticeable growth in IoT research, development, and application in 2020, significant improvement may be seen soon. Some of the IoT use cases will be solely inspired due to the requirement to manage and adapt to the COVID-19 pandemic, such as contact tracing and homeschooling.

IoT has rapidly become one of the most familiar expressions across business and technology, as 20 billion devices and internet connected things were expected in 2020 [63] and the technology global market is expected to grow to around 1.6 trillion dollars in market revenue [64]. Integration of IoT with different technologies such as cloud computing and embedding actuators and smart sensors facilitate interactions with smart things, allowing ease of access in different locations, enhancing data exchange efficiency, and improving storage and computing power [65].

IoT Market and Growth

It has been predicted by HTF Market Intelligence and important players such as Intel, Cisco, and IBM that IoT will have a remarkable growth in the coming years [66,67]. Remote devices and sensors are going to become more ubiquitous and by 2030 the world may have more than 100 trillion sensors. It is estimated to see a Compound Annual Growth Rate (CAGR) of 35% during the period 2019-2022 and the market is expected to reach more than 1000 billion USD. Worldwide, China, Europe, and North America are dominant in the IoT area and it is estimated to have 26%, 24%, and 23%, respectively, of the total IoT market value in 2030 [68]. There are more than 30 billion connected devices, and it is estimated to reach 75 billion IoT connected devices by 2025 [69].

There is an increase in the direction of IoT due to COVID-19 and the current pandemic, which may affect the predicted estimates of IoT growth. The impact of changes brought on in 2020 is driving organizations to increasingly use IoT technologies for operational resiliency [70]. In the near future, we think we will see more of IoT and its capability as it plays a crucial factor during this pandemic. With growing technologies such as 5G that can increase the capabilities of IoT even more with faster networks and data gathering, managing, and analysis, consumers' demand for the technology can increase.

6. Challenges for IoT

A survey conducted on various cyber-attacks and their classification [71] shows that there is a dearth of knowledge and information regarding cyber security. This made many organizations and individuals vulnerable to these attacks due to new unethical development and practices by individuals who are abusing others using technology in the fields of cyberspace and networking. Researchers suggest that a comprehensive understanding of cyber-attacks is needed for both individuals and organizations.

A study done by [72] suggests that a more comprehensive understanding of the threats and attacks of IoT infrastructure is necessary and that cyber defenses need to be taken seriously as it is blending with our societies and personal lives. Hoque mentions that it is essential that we have a wide understanding of current systems and tools accessible in the public domain to defend and prevent networks from attacks [73]. The same paper also provides a structured survey of the current systems and tools that can be of support.

The author in [1] shows issues with the three layers that IoT operate in: application layer, network layer, and perception layer. Security was divided into two sections, general security and security issues related to each layer. The heterogeneous nature of IoT devices, energy consumption, scalability, and distributed nature poses many general security challenges, such as:

- Connecting different devices with different capabilities, vendors, complexity, versions, and functions.
- The IoT environment is always changing.
- Policies and standards e.g., (Service Level Agreement) to ensure transmission, management, and protection of data.
- Confidentiality, Integrity, and Availability (CIA).

More attacks and threats that can be generated from each layer result in more challenges, such as strength of the wireless signal, interception of the IoT sensor node, and authentication mechanisms.

The existence of cyberspace brings with it different cybercrimes. It is defined as the nonphysical space generated by networks and computers, where people interact in different techniques [74]. The interdependent network infrastructure consists of telecommunication networks, embedded processors and controllers, the Internet, and computer systems [75]. Cyberspace is described as a domain characterized by the use of electromagnetic spectrum and electronics to exchange, store, and modify data with associated physical infrastructure and networked systems [76]. Cybercrime in IoE or IoT networks will appear sooner than later.

6.1. Privacy, Polices, and Security Challenges

With the increased use of IoT in the pandemic and anticipated growth post-COVID-19, privacy and security concerns need to be addressed in depth. Without assured security and privacy, the mass adaption of IoT solutions will be limited. Developers need to follow secure and privacy design principles to produce secure applications or frameworks. In addition, due care should be provided to protect personal data collected through IoT solutions. If there is a data breach, data controllers must pay fines under GDPR (4% of Annual Turnover or 20 million, whichever is the highest) or other emerging data protection laws across the globe.

A study by [10] discusses the privacy and security effects of IoT features and the threats they are exposed to. Due to the growth rate in IoT applications, there is an increased risk of cyber-attacks, privacy, and security threats. Any security threat to important IoT technologies, such as Implantable Medical Device (IMD) or smart cars, can endanger lives or cause substantial economic losses. The study states that "IoT device vendors typically do not update and patch their devices unless the user initiates firmware updates" and "most of the enterprises and users lack awareness of privacy and security", suggesting that IoT devices are not up-to-date with security issues and may have many faults.

The automation domain in IoT faces critical threats and challenges. The authors of [77] see that IoT is a concept to extend internet technologies to WSN, rather than a technology itself. The IoT system architecture and interworking is determined by scalability, security, simplicity, real time performance, and interoperability between devices. Threats are divided among the associated layers (Application layer, Data processing layer, Networking layer, Sensors and Actuators layer). Threats to the sensors and actuators layer can be tampering, which is a physical modification on the communication link or the device itself. The sensor can also be a threat to the network, as they can be a source for DDoS (Distributed Denial of Service) attacks. In automation IoT, any effect on the network can be harmful, as real-time information is required. This article defines many attacks such as DoS and Man-in-the-middle attacks, such as eavesdropping, replay attacks, and routing attacks. Many of these attacks can be mitigated easily in other technologies but due to the limit of storage and computing power of lightweight devices, it is hard to implement firewalls and defense mechanisms. There is a need for lightweight, processing-friendly and cheap solutions. For the data processing layer, attacks such as back-door, social engineering, and password guessing could be threatening.

To mitigate the risks of spreading and worsening of the pandemic, scanning methods are being used to diagnose the presence of the virus, whilst some countries are developing contact tracing apps. Google and Apple apps provide a decentralized software architecture, and save a log of the user contacts within the app, but are not uploaded to a central server [78].

The response of the government and the tech industry to the COVID-19 outbreak has already raised concerns about the implication of using contact tracing apps on privacy during and after the COVID-19 pandemic. The impact of contact tracing apps cannot be studied in isolation, and the focus should also be on the impact of facial recognition cameras, wearable bands, and police surveillance drones. For instance, the Chinese authorities have been using street cameras with facial recognition system to apprehend, shame, and fine citizens venturing outside without face masks and have even used similar tools to identify and quarantine individuals who appeared to have been carrying the virus.

South Korea has also employed a broad surveillance mechanism, and according to a report, the Seoul government has heavily relied on information collected from CCTV footage, bank card records, and mobile phone data to deal with the outbreak. The reports also claim that the UK has used drones to track people who were ignoring COVID-19 social distancing rules. These IoT in-spired mechanisms are infringing on public privacy in one way or another. Even though the technology has the capacity to contribute to tackle the pandemic effectively, it comes at the expense of privacy rights. The biggest problem we face is visualizing the degree of surveillance and what surprises it will bring. Given a choice between privacy and health, people are likely to choose health, but it is desirable that they should choose both [12].

IoT is growing rapidly and with the implementation of both IPv6 and 5G (and now 6G), it will continue to produce possibilities and solutions to the world where it is most needed. However, there are still vulnerabilities and privacy issues when it comes to IoT, such as the lack of continuous vendor firmware and patch update due to the heterogeneous of IoT devices. Mobile IoT devices such as wearable and smart cars tend to hop from one network to another, putting it at high risk from any kind of network attacks. On the other hand, IoT devices could already be infected, spreading malware.

There is a conflict between data access to provide better services and protecting user privacy. The amount of data collected from IoT devices puts individuals at risk as they become more easily identifiable with the use of profiling, tracing, and unauthorized processing, which can violate data protection laws, such as GDPR, due to the requirement of explicit consent from users. There is an obviously visible conflict between the data minimization principle of GDPR and the practices of IoT. Under the IoT concept, organizations believe in collecting as much data to gain insights and keep them in store for long times. In theory, more data will provide greater knowledge and greater benefit to the organizations and society in general. Therefore, enforcing data minimizations will limit the success of some IoT applications. Furthermore, personal identity could be protected using mechanisms such as pseudonymization, whilst on the contrary, one can argue that removing identifiers to achieve pseudonymization could potentially undermine the quality of the results derived, as the data would be purposefully altered [12].

The gathering of mass amounts of information using IoT can be justified only if the benefits overweigh other concerns; for example, privacy and security of personal data. In such an environment, safeguarding personal identities has become a significant challenge [79] against an ever-increasing threat. It is an unpleasant fact that we all are under surveillance, whether in our homes or outside, and equally whether we use our own transport or public transport systems. There is more to be done in this aspect of IoT—addressing privacy and security concerns. Some of the best guidelines that can help this cause are discussed in the sub-sections below.

6.2. Research on Mitigation of IoT Privacy and Security Threats

The authors in [80,81] focused on developing a security architecture for the challenges and security issues that IoT technology faces. The generic layering system is as follows: the perception layer, which includes RFID and different sensors to identify objects; the network layer (Internet and mobile network) that is responsible for transmitting the data; the middle-ware layer that processes, stores, and links different information; and finally the application layer, where practical applications exist. Each layer contains different challenges, such as unauthorized access to tags and tag cloning in perception layer, DOS and sybil attack in the network layer, and sniffing and malicious code injection in the application layer. To face these challenges, hash and encryption mechanism was suggested in the perception layer, IDS in the network layer, and firewalls in the application and middle-ware layer. The security goals were confidentiality: to ensure that sensor nodes data is not revealed, integrity: to ensure data is not altered by any means, and availability: to ensure data is always available.

A study conducted by [82] provides a block chain approach where it can be more secure and add more privacy gains. This approach also affects the processing time, traffic, and energy consumption, but all that is bearable, compared to the privacy advantages it brings. The process works by having a local block chain that keeps track of communication and data between devices. Each device asks for certain data to offer services. Additional delays are not significant and do not impact the availability of the smart home device. Using this method prevents DDoS attacks by checking all outgoing traffics and making sure the data is authorized by the device. It also prevents linked attacks by using a unique key for each communication between the devices.

Another study [83] tried to overcome the challenge, where, when thousands of IoT devices are connected, a current model of server-client is used, which has some issues and limitations, and proposed a blockchain IoT system. Ethereum differentiates from a server-client model by being a distributed computing platform and data transactions are stored via consensus algorithm that attackers cannot figure or tamper with easily. This method prevents DoS and DDoS network attacks. One of its weakness is that Ethereum will not fit time-sensitive applications, as it needs time for transactions to happen. The second issue is storage that lightweight IoT devices will need, as it may require large storage.

The author in [84] suggests more research on implementing techniques and algorithms to improve the efficiency of IoT security, especially the security of ender-users, and focuses more on metaheuristic algorithms that can achieve excellent solutions. The use of Non-Dominated Sorting Genetic Algorithm (NSGA-II) offers effective solutions to solve the problem of optimizing Wireless Mesh Network (WMN) infrastructure placement [85]. For a highly effective way of finding a set of effective solutions, metaheuristic algorithms may be considered for solving IoT security issues.

A hybrid encryption algorithm was proposed by [86] for data confidentiality, integrity, and non-repudiation in IoT technology. IoT is a new network that seeks to achieve intelligent processing, reliable transmission, and perception of information by using RFID and wireless sensor connections. There are many security concerns related to wireless communication, network transmission, RFID, information processing, and privacy. The proposed algorithm uses a public key cryptography as it has less memory demand and high encryption speed. The method starts by generating a public key using symmetric encryption; the message is then encrypted by an asymmetric algorithm. The receptor that owns a private key decodes the message by private key and asymmetric algorithm. The algorithm combines both Advanced Encryption Standard (AES) and NTRU algorithms. AES is used to create the key and NTRU asymmetric encryption is used to increase the security.

7. Emerging Code of Practices for IoT

There are some codes of practices for IoT that provides guidelines and steps for both the manufacturer and the consumers to improve and protect security and privacy. These guidelines mitigate security threats such as DDoS. The author of [87] provides the following standard and recommended practices that assist in achieving compliance with the General Data Protection Regulation (GDPR) to different IoT applications, such as wearable health trackers, smart homes, home automation, smart cameras, and alarm systems.

- No default passwords
- Vulnerability disclosure policy implementation
- Continuous and periodic updates, secure storage for sensitive and personal data
- Make it easy for consumers to delete personal data
- Software integrity

The U.S. Department of Homeland Security has also created a strategic principle for securing IoT, as there are many different engaged parties to this security shortfall, such as manufacturers, suppliers, deployers, and network operators, which makes it unclear as to who is responsible for security decisions [88]. The principles to address IoT security challenges are incorporating security in the design phase, advancing security updates and vulnerability management, building on proven security practices, prioritizing security measures according to potential impact, promoting transparency across IoT, and connecting carefully and deliberately. These suggested practices will help to account for security for IoT developers, service providers, IoT manufacturers, and industrial and business level consumers.

In addition, the security of IoT devices will help to improve the quality of commercial services and control the connection with wireless infrastructure. This process offers a significant amount of automation and security control.

ISO (International Organization for Standardization), with the IEC (International Electrotechnical Commission), published the ISO/IEC TR 30164 IoT standard that describes the concepts and technologies of edge computing for IoT, the ISO/IEC 21823-2 IoT standard that specifies an interoperability framework for IoT systems, and the ISO/IEC TR 30166, which is an IoT standard for Industrial IoT (IIoT). These best practices proposed by international organizations immensely help to securely operate the IoT end-to-end chain. Furthermore, it can be observed that specific industries are also producing their own standards to provide better safety and cyber security for their systems. For example, the recent TISAX: Trusted Information Security Assessment eXchange standard provides required cyber security best practice guidelines (securing the supply chain) for the automotive industry (ENX Association, 2021) [89]. This is particularly important for automotive IoT systems since compromised cyber security system could have an adverse impact on its safety. It is crucial for driverless cars to operate within safety guidelines while talking to nearby cars (e.g., vehicle-to-vehicle communication) and responding to sensor readings in real time.

Adhering to best practice guidelines also helps organizations to demonstrate compliance to regulations and laws (e.g., ISO27001 standard facilitates GDPR compliance). For instance, EU Network & Information Systems Regulations (NIS Regulations) provides legal measures to boost the overall level of security (both cyber and physical resilience) of network and information systems that are critical for the provision of digital services (online marketplaces, online search engines, cloud computing services) and essential services (transport, energy, water, health, and digital infrastructure services). This was introduced as critical enablers of our societies and economies are increasingly underpinned by the internet and private networks and information systems. Hence, it is important to ensure a high common level of network and information security (NIS). According to this directive transport, energy, water, health, and digital infrastructure services are categorized as essential services due to their importance to citizens. In order to make sure that these services offer assured safety, operators need to integrate good cyber security practices with current health and safety of their product or service offerings.

The IET and NCSC recently published a code of practice for engineering practitioners on how these distinguished functional units within an organization can work towards lowering the risks created by lack of cyber security and safety measures (IET and NCSC: Code of Practice: Cyber security and safety, 2020) [90]. Another code of practice by IET guides cyber security practice in building industry in (IET: Code of Practice for Cyber Security in the Built Environment, 2014). The National Infrastructure Protection Plan 2013: Partnering for Critical Infra-structure Security and Resilience (Homeland Security: NIPP, 2013) in the US highlights how government and private sector organizations should work together to manage risks and achieve security and resilience outcomes for critical infrastructure. Under this initiative, the 2015 Sector-Specific plans have established goals and priorities for the sector that address their current risk environment, such as the nexus between cyber and physical security. Currently this covers 16 critical infrastructure sectors, including energy, water and wastewater, nuclear reactors, dams sector, etc. (Homeland Security: 2015 Sector-Specific Plans, 2015). Similar code of practices or best practice guidelines are in need to elaborate how organizations can jointly minimize cyber security and safety risks of modern engineering systems [91].

8. Implications and Future Directions

In this review, the authors found ample evidence to support the key role played by IoT-based applications and technologies during COVID-19. It was also discovered that several applications are ready for mass deployment and make a huge impact in the society, while some technologies require further R&D and validation before being deployed. However, the authors believe that there should be more research and development towards addressing privacy and security concerns, as reviewed in this article. This will be a key factor that decides mass adaptation of future IoT technologies. Researchers should focus more on how to ensure that the user is knowledgeable enough to deal with the technology without any risks because there is a dearth of knowledge and information regarding cyber security, as stated by [71]. Furthermore, a more comprehensive understanding of IoT threats is needed [72], as there is less research on efficient ways to deliver critical and important information to the users. An example of this is the Code of Practice for consumer IoT security [87]. These codes of practice are available to the public, but it is less likely for users to search for such practices themselves. At present, a significant research and development effort is focused within the healthcare sector. IoT has the capability to make a major difference in many sectors, as reviewed in the article. However, this necessitates more research to transfer this technology into other sectors, such as tourism, food and catering, mining, construction, and public services.

Researchers can use the systematic review presented in this article to understand IoT-based application usage during COVID-19 and beyond. Furthermore, it provides sufficient information related to different IoT technologies in diverse sectors. Readers can use this review to further explore the societal and economic impact, time for market, and technology readiness. In addition, this article elaborates on key challenges and opportunities around privacy and security aspects, which could be addressed in future research and development.

Finally, this article provides ample information to readers about the importance of code of practices in this domain and emerging best practices for IoT in general.

9. Conclusions

COVID-19 enabled emerging IoT applications to be tested in different application domains, as discussed in this review paper. Some of the IoT solutions provided much-needed support to manage the COVID-19 pandemic (e.g., contact tracing), whereas some IoT-based technologies are deployed as pilots and experiments. It is apparent that some of these technologies are not mature enough to be deployed on a mass scale. Furthermore, some specific application scenarios for IoT were identified during the pandemic (for instance, Triax Proximity, Kinsa, SALUTARY, and IoT-based Standard Operating Procedure).

Although IoT-based technology has the potential to change the way we live post-COVID-19, it requires further research and validation before mass adaptation and deployment of the technology, as discussed in the paper. This review summarized the key application domains for IoT, their anticipated socio-economic impact, the timeline for deployment, and TRL. Furthermore, this review elaborated on the challenges for application domains with special focus on privacy and security implications. In addition, this study discussed standards and emerging code of practices for IoT-based applications.

IoT has provided improved healthcare services and empowered improved clinical decisions during the pandemic. Similar to the healthcare domain, IoT presents a massive opportunity to change our lives for the better, with the potential to make an impact right across the society, especially during the new normal created by the COVID-19.

Author Contributions: Conceptualization, M.Y., C.H. and L.N.; methodology, C.H.; validation, C.H.; formal analysis, M.Y. and C.H.; investigation, M.Y.; resources, C.H.; data curation, M.Y., C.H. and L.N.; writing—original draft preparation M.Y.; writing—review and editing, M.Y., C.H. and L.N.; visualization, M.Y.; supervision, C.H. and L.N.; project administration, C.H. and L.N.; funding acquisition, C.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research has not received any external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of things (IoT) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions*; ICITST: London, UK, 2015.
2. Singh, R.P.; Javaid, M.; Haleem, A.; Suman, R. Internet of things (IoT) applications to fight against COVID-19 pandemic. *Diabetes Metab. Syndr. Clin. Res. Rev.* **2020**, *14*, 521–524. [CrossRef] [PubMed]
3. Javaid, M.; Khan, I.H. Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. *J. Oral Biol. Craniofacial Res.* **2021**, *11*, 209–214. [CrossRef] [PubMed]
4. Bocetta, S. Hands-Free Everything? The Coronavirus Impact on IoT. Available online: https://www.globalsign.com/en/blog/hands-free-everything-coronavirus-impact-iot (accessed on 23 March 2021).
5. Western Shelter. COVID-19 Screening, Monitoring, and Isolation Part 1—Western Shelter. Available online: https://westernshelter.com/blog/2020/8/3/covid-19-screening-monitoring-and-isolation (accessed on 26 February 2021).
6. Triax Technologies, Proximity Trace Triax Technologies. Available online: https://www.triaxtec.com/resource/fact-sheet/proximity-trace/ (accessed on 26 February 2021).
7. Koetsier, J. This Smart Home Gym Is the Future of Fitness. Available online: https://www.forbes.com/sites/johnkoetsier/2020/10/13/this-smart-home-gym-is-the-future-of-fitness/?sh=68691ae414bd (accessed on 26 February 2021).
8. World Health Organization. Coronavirus. Available online: https://www.who.int/health-topics/coronavirus#tab=tab_1 (accessed on 26 February 2021).

9. Frontiers. The Use of IoT Technologies to Identify and Control the COVID-19 Pandemic in Urban Areas | Frontiers Research Topic. Available online: https://www.frontiersin.org/research-topics/14707/the-use-of-iot-technologies-to-identify-and-control-the-covid-19-pandemic-in-urban-areas#overview (accessed on 26 February 2021).
10. Zhou, W.; Jia, Y.; Peng, A.; Zhang, Y.; Liu, P. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet Things J.* **2019**, *6*, 1606–1616. [CrossRef]
11. 5 Benefits of Temperature Screening Technology for your Business | IPM Group. Available online: https://ipmgroupuk.com/5-benefits-of-temperature-screening-technology/ (accessed on 22 April 2021).
12. Bentotahewa, V.; Hewage, C.; Williams, J. Security and privacy issues associated with Coronavirus diagnosis and prognosis. In Proceedings of the EAI Conference: AISCOVID19, Viana do Castelo, Portugal, 2–4 December 2020.
13. Personal Use: Meet ADAMM—Health Care Originals. Available online: http://www.healthcareoriginals.com/personal (accessed on 2 March 2021).
14. Gia, T.N. IoT-Based Continuous Glucose Monitoring System: A Feasibility Study. *Procedia Comput. Sci.* **2017**, *109*, 327–334. [CrossRef]
15. Watch—Why Apple Watch—Apple (UK). Available online: https://www.apple.com/uk/watch/why-apple-watch/ (accessed on 2 March 2021).
16. Expanding IoT through Image Sensing Technologies. 2016. Available online: http://www.healthcare.omron.co.jp/english/news/2016/0418.html (accessed on 2 March 2021).
17. Home Monitoring System for Elderly—Computers for Seniors. Available online: https://www.grandcare.com/ (accessed on 2 March 2021).
18. Otoom, M.; Otoum, N.; Alzubaidi, M.A.; Etoom, Y.; Banihani, R. An IoT-Based Framework for Early Identification and Monitoring of COVID-19 Cases. *Biomed. Signal Process. Control* **2020**, *62*, 102149. [CrossRef]
19. Alam, M.M.; Malik, H.; Khan, M.I.; Pardy, T.; Kuusik, A.; Le Moullec, Y. *A Survey on the Roles of Communication Technologies in IoT-Based Personalized Healthcare Applications*; IEEE Access: New York, NY, USA, 2018; Volume 6.
20. Fizza, K.; Banerjee, A.; Mitra, K.; Prakash, P.; Rajiv, J.; Pankesh, R. QoE in IoT: A vision, survey and future directions. *Discov. Internet Things* **2021**, *1*, 4. [CrossRef]
21. Hameed, S.; Khan, F.I.; Hameed, B. Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review. *J. Comput. Networks Commun.* **2019**, *2019*, 1–14. [CrossRef]
22. Rahmani, A.M.; Mirmahaleh, S.Y.H. Coronavirus disease (COVID-19) prevention and treatment methods and effective parameters: A systematic literature review. *Sustain. Cities Soc.* **2021**, *64*, 102568. [CrossRef]
23. Talavera, J.M.; Tobón, L.E.; Gómez, J.A.; Culman, M.A.; Aranda, J.M.; Parra, D.T.; Quiroz, L.A.; Hoyos, A.; Garreta, L.E. Review of IoT applications in agro-industrial and environmental fields. *Comput. Electron. Agric.* **2017**, *142*, 283–297. [CrossRef]
24. Technology Readiness Level | NASA. Available online: https://www.nasa.gov/directorates/heo/scan/engineering/technology/txt_accordion1.html (accessed on 31 March 2021).
25. Kamal, M.; Aljohani, A.; Alanazi, E. IOT Meets COVID-19: Status, Challenges, and Opportunities. *arXiv* **2020**, arXiv:2007.12268.
26. Chamola, V.; Hassija, V.; Gupta, V.; Guizani, M. A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact. *IEEE Access* **2020**, *8*, 90225–90265. [CrossRef]
27. Ndiaye, M.; Oyewobi, S.S.; Abu-Mahfouz, A.M.; Hancke, G.P.; Kurien, A.M.; Djouani, K. IoT in the Wake of COVID-19: A Survey on Contributions, Challenges and Evolution. *IEEE Access* **2020**, *8*, 186821–186839. [CrossRef]
28. Kumar, K.; Kumar, N.; Shah, R. Role of IoT to avoid spreading of COVID-19. *Int. J. Intell. Networks* **2020**, *1*, 32–35. [CrossRef]
29. Dutta, P.K.; Mitra, S. Application of Agricultural Drones and IoT to Understand Food Supply Chain During Post COVID-19. In *Agricultural Informatics*; Wiley: Hoboken, NJ, USA, 2021; pp. 67–87.
30. Agriculture IoT Market Worth $32.75 Billion by 2027- Market Size, Share, Forecasts, & Trends Analysis Report with COVID-19 Impact by Meticulous Research®. Available online: https://www.globenewswire.com/news-release/2021/03/22/2196690/0/en/Agriculture-IoT-Market-Worth-32-75-Billion-by-2027-Market-Size-Share-Forecasts-Trends-Analysis-Report-with-COVID-19-Impact-by-Meticulous-Research.html (accessed on 15 April 2021).
31. Suleman, H. How to Use the IoT to Keep Your Restaurant Clean and Safe | FoodSafetyTech. Available online: https://foodsafetytech.com/column/how-to-use-the-iot-to-keep-your-restaurant-clean-and-safe/ (accessed on 15 April 2021).
32. Singh, S.; Hamidon, N.; Zuber, M.; Kamarul, A. Wireless Sensing Technology with IoMT approach for Continuous Monitoring of Breathing Rate and Volume during COVID-19. *Front. Sustain. Cities* **2021**, *3*, 6.
33. Uday, S.; Jyotsna, C.; Amudha, J. Detection of Stress using Wearable Sensors in IoT Platform. In Proceedings of the International Conference on Inventive Communication and Computational Technologies, ICICCT 2018, Coimbatore, India, 20–21 April 2018.
34. ABTraceTogether | Alberta.ca. Available online: https://www.alberta.ca/ab-trace-together.aspx (accessed on 3 March 2021).
35. Stanford Children's Health. About Telehealth Services (Virtual Visits)—Stanford Children's Health. Available online: https://www.stanfordchildrens.org/en/telehealth/about-virtual-visits (accessed on 26 February 2021).
36. Kinsa Health. Kinsa Smart Thermometers | Kinsa Inc. Available online: https://www.kinsahealth.co/products/ (accessed on 26 February 2021).

37. Isabella, M.A.; Seetha Lekshmi, K.; Thamizhvaani, E.P.; Vishali, S. IOT Based Emergency Medical Services. *Int. J. Eng. Tech.* **2018**, *4*, 1–4.
38. Gupta, N.; Jilla, S. Digital Fitness Connector: Smart Wearable System. In Proceedings of the 1st International Conference on Informatics and Computational Intelligence, ICI 2011, Bandung, Indonesia, 12–14 December 2011.
39. McArthur, R. Bahrain Launches Electronic Bracelets to Keep Track of Active COVID-19 Cases | MobiHealthNews. Available online: https://www.mobihealthnews.com/news/emea/bahrain-launches-electronic-bracelets-keep-track-active-covid-19-cases (accessed on 26 February 2021).
40. Saiidi, U. Hong Kong Uses Electronic Wristbands to Enforce Coronavirus Quarantine. Available online: https://www.cnbc.com/2020/03/18/hong-kong-uses-electronic-wristbands-to-enforce-coronavirus-quarantine.html (accessed on 26 February 2021).
41. BBC News. Coronavirus: People-Tracking Wristbands Tested to Enforce Lockdown—BBC News. Available online: https://www.bbc.co.uk/news/technology-52409893 (accessed on 26 February 2021).
42. Munawar, H.; Khan, S.; Qadir, Z.; Kouzani, A.; Mahmud, M. Insight into the Impact of COVID-19 on Australian Transportation Sector: An Economic and Community-Based Perspective. *Sustainability* **2021**, *13*, 1276. [CrossRef]
43. Gray, R.S. Agriculture, transportation, and the COVID-19 crisis. *Can. J. Agric. Econ.* **2020**, *68*, 239–243. [CrossRef]
44. Muthuramalingam, S.; Bharathi, A.; Kumar, S.R.; Gayathri, N.; Sathiyaraj, R.; Balamurugan, B. Iot based intelligent transportation system (iot-its) for global perspective: A case study. In *Intelligent Systems Reference Library*; Springer Science and Business Media LLC: Berlin/Heidelberg, Germany, 2019; Volume 154.
45. Darsena, D.; Gelli, G.; Iudice, I.; Verde, F. Safe and reliable public transportation systems (SALUTARY) in the COVID-19 pandemic. *arXiv* **2020**.
46. Sutar, S.; Koul, R.; Suryavanshi, R. Integration of smart phone and IOT for development of smart public transportation system. In Proceedings of the 2016 International Conference on Internet of Things and Applications (IOTA), Pune, India, 22–24 January 2016; pp. 73–78.
47. Al-Dweik, A.; Muresan, R.; Mayhew, M.; Lieberman, M. IoT-based multifunctional Scalable real-time Enhanced Road Side Unit for Intelligent Transportation Systems. Proceedings of 30th annual IEEE Canadian Conference on Electrical and Computer Engineering (IEEE 2017 CCECE), Windsor, ON, Canada, 30 May–3 April 2017.
48. Puiu, D.; Bischof, S.; Serbanescu, B.; Nechifor, S.; Parreira, J.; Schreiner, H. A public transportation journey planner enabled by IoT data analytics. In *2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)*; Institute of Electrical and Electronics Engineers (IEEE): New York, NY, USA, 2017; pp. 355–359.
49. Schurtze, A. Cold Chain Doubts Delay COVID-19 Vaccinations in Some German Cities | Reuters. Available online: https://www.reuters.com/article/health-coronavirus-europe-vaccines-germa/cold-chain-doubts-delay-covid-19-vaccinations-in-some-german-cities-idINKBN2910G8 (accessed on 3 March 2021).
50. Nadeak, B. The effectiveness of distance learning using social media during the pandemic period of covid-19: A case in universitas kristen Indonesia. *Int. J. Adv. Sci. Technol.* **2020**, *29*, 1764–1772.
51. Makransky, G.; Thisgaard, M.W.; Gadegaard, H. Virtual Simulations as Preparation for Lab Exercises: Assessing Learning of Key Laboratory Skills in Microbiology and Improvement of Essential Non-Cognitive Skills. *PLoS ONE* **2016**, *11*, e0155895. [CrossRef]
52. Ilieva, G.; Yankova, T. IoT in Distance Learning during the COVID-19 Pandemic. *TEM J.* **2020**, *9*, 1669–1674. [CrossRef]
53. Awais, M.; Raza, M.; Singh, N.; Bashir, K.; Manzoor, U.; Islam, S.U.; Rodrigues, J.J.P.C. LSTM based Emotion Detection using Physiological Signals: IoT framework for Healthcare and Distance Learning in COVID-19. *IEEE Internet Things J.* **2020**, 1. [CrossRef]
54. Exposure Notifications: Helping Fight COVID-19—Google. Available online: https://www.google.com/covid19/exposurenotifications/ (accessed on 3 March 2021).
55. Self Checkout Systems in 2021: Comprehensive Guide. Available online: https://research.aimultiple.com/self-checkout/ (accessed on 28 March 2021).
56. Panchal, J. How IoT-Enhanced Warehouses Are Changing the Supply Chain Management—Part 1—IoT Now News—How to Run an IoT Enabled Business. Available online: https://www.iot-now.com/2019/01/07/91762-iot-enhanced-warehouses-changing-supply-chain-management/ (accessed on 3 March 2021).
57. Gregory, J. The Internet of Things: Revolutionizing the Retail Industry. Available online: https://www.accenture.com/_acnmedia/Accenture/ConversionAssets/DotCom/Documents/Global/PDF/Dualpub_14/AccentureTheInternetOfThings.pdf (accessed on 21 April 2021).
58. De Vass, T.; Shee, H.; Miah, S.J. Iot in supply chain management: A narrative on retail sector sustainability. *Int. J. Logist. Res. Appl.* **2020**, 1–20. [CrossRef]
59. Bashir, A.; Izhar, U.; Jones, C. IoT Based COVID-19 SOP Compliance Monitoring and Assisting System for Businesses and Public Offices. Available online: https://ecsa-7.sciforum.net/ (accessed on 22 April 2021). [CrossRef]
60. Reimer, J. How IoT Can Help Us Get Moving Post-COVID. Available online: https://360.here.com/iot-technology-covid-19 (accessed on 26 February 2021).
61. Jain, A. A Smart Gym Framework: Theoretical Approach. *2015 IEEE Int. Symp. Nanoelectron. Inf. Syst.* **2015**, 191–196. [CrossRef]
62. Petrovic, N.; Kocic, D. IoT-based System for COVID-19 Indoor Safety Monitoring. *IcETRAN* **2020**, *2020*, 1–6.

63. Statista Research Department. IoT Market Size Worldwide 2017–2025 | Statista. 22 January 2021. Available online: https://www.statista.com/statistics/976313/global-iot-market-size/ (accessed on 26 February 2021).
64. Hung, M. Leading the IoT—Gartner Insights on How to Lead in a Connected World. *Gart. Res.* **2017**, *1*, 1–5.
65. Domb, M. Smart Home Systems Based on Internet of Things. In *IoT and Smart Home Automation [Working Title]*; IntechOpen: London, UK, 2019; pp. 25–37.
66. HTF Market Intelligence Consulting. IOT In Logistics Market May See a Big Move | Cisco Systems, IBM. Available online: https://www.openpr.com/news/2134501/iot-in-logistics-market-may-see-a-big-move-cisco-systems-ibm (accessed on 26 February 2021).
67. IoT Business News. IoT News—Cisco Predicts Rapid Growth in The IoT Logistics Market—IoT Business News. Available online: https://iotbusinessnews.com/2020/08/19/06126-cisco-predicts-rapid-growth-in-the-iot-logistics-market/ (accessed on 26 February 2021).
68. Morrish, J. Global IoT Market to Grow to $1.5trn Annual Revenue by 2030—IoT Now News—How to Run an IoT Enabled Business. Available online: https://www.iot-now.com/2020/05/20/102937-global-iot-market-to-grow-to-1-5trn-annual-revenue-by-2030/ (accessed on 26 February 2021).
69. Horwitz, L. Internet of Things (IoT)—The Future of IoT Miniguide: The burgeoning IoT Market Continues—Cisco. Available online: https://www.cisco.com/c/en/us/solutions/internet-of-things/future-of-iot.html (accessed on 26 February 2021).
70. Medberry, P. Industrial IoT: Top 3 Trends for 2021—Cisco Blogs. Available online: https://blogs.cisco.com/internet-of-things/industrial-iot-top-3-trends-for-2021 (accessed on 26 February 2021).
71. Uma, M.; Padmavathi, G. A survey on various cyber attacks and their classification. *Int. J. Netw. Secur.* **2013**, *15*, 5.
72. Abomhara, M.; Køien, G.M. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *J. Cyber Secur. Mobil.* **2015**, *4*, 65–88. [CrossRef]
73. Hoque, N.; Bhuyan, M.H.; Baishya, R.; Bhattacharyya, D.; Kalita, J. Network attacks: Taxonomy, tools and systems. *J. Netw. Comput. Appl.* **2014**, *40*, 307–324. [CrossRef]
74. Canongia, C.; Mandarino, R. Cybersecurity: The new challenge of the information society. In *Crisis Management: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2013; Volume 1–3.
75. Injac, O.; Šendelj, R. National security policy and strategy and cyber security risks. In *Identity Theft: Breakthroughs in Research and Practice*; IGI Global: Hershey, PA, USA, 2016.
76. What Is Cyberspace? Definition from WhatIs.com. Available online: https://whatis.techtarget.com/definition/cyberspace (accessed on 4 March 2021).
77. Varga, P.; Plosz, S.; Soos, G.; Hegedus, C. Security threats and issues in automation IoT. In Proceedings of the 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), Trondheim, Norway, 31 May–2 June 2017; pp. 1–6.
78. Michael, K.; Abbas, R. Behind COVID-19 Contact Trace Apps: The Google–Apple Partnership. *IEEE Consum. Electron. Mag.* **2020**, *9*, 71–76. [CrossRef]
79. New Technologies and Challenges for Personal Identity—The Digital Health Society. Available online: https://thedigitalhealthsociety.com/new-technologies-and-challenges-for-personal-identity/ (accessed on 5 March 2021).
80. Farooq, U.M.; Waseem, M.; Mazhar, S.; Khairi, A.; Kamal, T. A Review on Internet of Things (IoT). *Int. J. Comput. Appl.* **2015**, *113*, 1–7. [CrossRef]
81. Leloglu, E. A Review of Security Concerns in Internet of Things. *J. Comput. Commun.* **2017**, *5*, 121–136. [CrossRef]
82. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017, Kona, HI, USA, 13–17 March 2017.
83. Huh, S.; Cho, S.; Kim, S. Managing IoT devices using blockchain platform. In Proceedings of the International Conference on Advanced Communication Technology, ICACT, Phoenix Park, PyeongChang, Korea, 19–22 February 2017.
84. Nawaf, L. Optimizing IoT Security by Implementing Artificial Intelligence—Infosecurity Magazine. Available online: https://www.infosecurity-magazine.com/next-gen-infosec/optimizing-iot-ai/ (accessed on 15 March 2021).
85. Nawaf, L.F.; Allen, S.M.; Rana, O. Optimizing Infrastructure Placement in Wireless Mesh Networks Using NSGA-II. In *20th International Conference on High Performance Computing and Communications, 16th International Conference on Smart City and 4th International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2018*; IEEE: New York, NY, USA, 2019.
86. Yousefi, A.; Jameii, S.M. Improving the security of internet of things using encryption algorithms. Proceedings of IEEE International Conference on IoT and Its Applications (ICIOT 2017), Nagapattinam, India, 19–20 May 2017.
87. C. M. & S. Department for Digital. Code of Practice for Consumer IoT Security—GOV.UK. Available online: https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security (accessed on 26 February 2021).
88. National Telecommunications and Information Administration. Communicating IoT Device Security Update Capability to Improve Transparency for Consumers. Available online: https://www.consumer.ftc.gov/topics/online-security (accessed on 26 February 2021).
89. TISAX Association. *Trusted Information Security Assessment Exchange*; ENX Association: Boulogne-Billancourt, France, 2021.

90. IET; NCSC. Code of Practice: Cyber Security and Safety: IET. Available online: https://electrical.theiet.org/guidance-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-and-safety/ (accessed on 21 April 2021).
91. Hewage, C. Opportunities, Challenges and Strategies for Integrating Cyber Security and Safety in Engineering Practice. *Eng. Technol. Open Access J.* **2021**, *3*, 1–5. [CrossRef]