# PRIVACY AND SECURITY CHALLENGES DURING AND BEYOND COVID-19

Abirami A, Jayasuriya J, Mohanaprabhu D, Divith S,

Department of Information Technology,

Bannari Amman Institute of Technology,

Sathyamangalam-638401, Erode Dt.,

Tamilnadu, India.

**Abstract:** During the Coronavirus, many individuals experience physical, mental health, and privacy issues. Coronavirus also assesses the healthcare-associated with wearing a mask, flares, and maintaining distance between people to prevent from it, and also, we've developed various kinds of digital monitoring systems such as drone-grounded systems, contact tracing systems, etc. The automated system of contact tracking brings vexation among the physical labor and manual workers who are most affected due to the improvement of the automated systems. The contact tracking applications lack in safety and security of the user's data, which is considered as the step to attract hackers to attack the host. The lack of public awareness about the use of mobile drives and the improvement of drone surveillance also attract people who give importance to their privacy and security in the technical era. In this chapter, we looked at the future development and design of IoT applications with their corresponding protocols in and around the world. All sectors that give their share in the mass adjustment are treated and remedies are given with the necessary solution. Sectors like social and profitability were discussed in this chapter. A number of independent operations are suggested, such as drone-grounded monitoring systems and contact tracing systems. In addition, this composition outlines implicit exploration directions that better performance with preserved privacy and security for the coming-generation IoT operation and digital surveillance system, as well as wider adaptation by the large population.

**Keywords:** COVID-19; Internet of Things; Digital Surveillance System; Privacy and Security Challenges; Cyber Security; Contact Tracing Systems; Drone-grounded Monitoring;

**Table of Content:**

## 1. INTRODUCTION:

The Iot technology (IoT) is a way of linking numerous commodities and gadgets across a network, which can be interconnected. IoT (internet of things) innovation has recently become very popular as it is used for a multitude of purposes, including communication, transportation, education, and commercial growth. The Internet of Things gave rise to the notion of hyper connection, that enables people and organisations to interact with others from afar. The phrase "Internet of Things" was invented by Kevin Ashton in 1999 to promote the RFID (Radio Frequency Identification) idea, which comprises embedding sensing devices. However, the original concept was introduced in the 1960s. Around that time, the method became known as interconnected devices or integrated Internet. Ashton advocated the Internet of Things (IoT) as a solution to optimise supply chain procedures. The IoT's numerous uses, on the other hand, helped it acquire significant notice throughout the summer of 2010. The Chinese government gave IoT strategic significance with the creation of a five-year strategy. There are approximately 26.66 billion Sensor nodes on the planet now. In 2011, the tremendous rise was sparked by smart things, wearable technologies, and smart power metres. In a number of different ways, the fast rise of IoT has enhances the performance and enhanced competitive analysis and corporate strategy. Similarly, by providing automated services, the Iot has enhanced people's lives. However, such some out development has sparked new confidentiality worries.

The global effect of Coronavirus Disease 2019 (COVID-19) has been tremendous capitalist model by isolating individuals from normal industrialization. Because there is currently no vaccination or treatment for COVID-19, the simplest way to avoid becoming infected is to avoid being exposed to it. Coughing, sneezing, or even conversing close to other people can significantly increase the probability of inhaling respiratory particles from irritated people. Current research has shown that asymptomatic persons should silently disseminate the virus not evoking concern, therefore social separation must be maintained among everybody.

Inadvertent password abuse, refusal to update identities, and a dearth of tools improvements have compounded cybersecurity vulnerabilities, allowing ransomware to access confidential material on Connected systems. Off-the-beaten-path safety approaches increase the risk of data breaches and other risks. Many security analysts recall IoT as a weak factor for phishing efforts due to fragile security processes and standards. Despite the development of numerous preventative methods to safeguard Iot technologies from botnet, cybersecurity recommendations are not widely distributed. As a result, end-users will no longer be able to adopt shielding techniques to protect themselves from data breaches. Since the evening of 2008, cybercriminals have developed unique sorts of spyware to infiltrate IoT devices. They devised a number of online frauds to get workers or individuals to provide sensitive data. As a consequence of high attacks, business computers and devices are routinely subjected to data breaches. If tool makers and security experts do thorough investigations into cybersecurity risks, they may be able to improve a greener screening system to save you or neutralise cyber hazards.

Iot has been employed in professional courses for a variety of reasons, including cost savings. The applications help these businesses obtain an edge over its competitors. Protection and data breach have become a big concern with most enterprises as a result of the widespread acceptability of many smart gadgets that share and aggregate information, since it disturbs the circulation of art, activity, and society offerings. Experts are required to battle these risks and to expand thorough authentication techniques and norms in order to preserve corporate company assets and assure the continuing of services. Creative cooking and cleaning, for example. Iot links devices to the local area network, which might be a route of access for fraudsters attempting to get entry towards the business and/or private info, as well as control and disrupt corporate processes. Every day, new technology emerges or current technology is improved. Take a look at the most current advancements in the 5G world. 5G is discovered to play a critical function in IoT systems and applications. Its high bandwidth has piqued the interest of researchers while also raising worries about possible cybersecurity problems. However, because of the wavelengths shorter, the infrastructure changes, requiring more cell towers to cover same area as earlier wi-fi systems. This new kind, which consists of phoney ground stations, poses a greater threat. It is vital to be aware of the dangers to one's protection as well as the potential solutions. In this graphic, we intend to present an assessment of IoT projects, benefits, and potential risks. Furthermore, by enforcing and assessing current schemes or inventing new ones, to give a framework for evaluating and increasing accepted standard precautions. Based on our findings, we provide advice for minimizing such risks and fixing any security issues. This painting will enable regulatory frameworks in maintaining tight criteria, as well as instructing terminal and corporations, as well as other IoT participants, to grow and conform to more tolerable data security protections.

Because the approach is somewhat arduous to execute manually, this social distance prompts primary health professionals and individuals to join forces with team of workers to implement virtual surveillance structures (DSSs) to exhibit persons digitally. Automated hand mapping is one of the most often used DSSs (ACT). ACT architecture automating the usual guide interview with the affected individuals, which is performed by the physical officials, in order to find persons who have recently came into contact to COVID-19 high standard persons. ACT constructs its use of cellular telephone applications(apps) might have been an excellent opportunity that has been introduced, developed, or even deployed in a few countries. Instead of collecting the contacts the affected man or woman would have with different people for the previous 2-three weeks through extensive interviews, ACT structures the use of mobile phone applications(apps) may be an exquisite opportunity that has been introduced, formed, or even mobilised in a few nations. Also, it's difficult for individuals to recall their previous two to three weeks after they've had an impact on many strangers in public areas. Furthermore, these interviews need a professional group of professionals with ongoing, intensive training, which is occasionally no longer possible. Also with ACT app stores that use mobile phones and their location debugging through the global positioning system (GPS), wireless-fidelity (Wi-Fi), and integrated Headset interface to communicate with and construe nearness with neighbouring mobile phones, the privacy and security difficulties are rising to an uncomfortable level. The apps should be repurposed to better serve their consumers. Several security issues, such as

jammer, development of energy drain assaults, proactive and reactive snoopers, and stealing video surveillance used in ACT applications, are only a few of them.

We built our variant using Amazon Web Service (AWS) as proof of concept, which was eventually converted into real-life sensor network architectures that mimicked desired IoT topologies. By creating the system, we will be able to install and test one-of-a-kind security measures by creating realistic scenarios and metrics. We presented our own perspective on the widely adopted and extended IoT version, as well as its privacy and security issues. A virtualized evidenced IoT edition was built and investigated, consisting of a cloud-based machine (sensors), an aspect node (Raspberry Pi), and cloud services (AWS). This setup was created to evaluate the version of the paper that we presented parts. Our work does not include information on unique Iot systems (smart health, smart cities, supply chain, transportation, and so on. ); their features, benefits, and problems, or the potential security risks or attacks among those programs. Such information may be found in abundance in the journals. We wanted to provide a preferred evaluation with proof of concept in this painting, as well as establish the groundwork for future evaluations and studies. The following is the modification of this paper: The next phase includes a literature review, which is followed by an examination of IoT security and privacy issues. The fate of the Iot technology is discussed in Section 4. The suggested cloud/aspect supported IoT layered models are described in Section 5: broadly vast and expanded with privateness and security supplements, as well as layered recognition. This stage also shows how the planned version would be implemented using AWS cloud and aspect platforms, as well as the Raspberry Pi 4 kit. This artwork comes to a close with Section 6. Drone-based fully completely direct observations are just another fantastic DSS. Drones are a type of unmanned aerial vehicle (UAV), and they are by far the most common UAV on the market today. A vehicle's command authority can be classified into three categories: some length off flight engineer control, in which the drone is completely controlled manually with the assistance of an operator; some distance off supervised regulation, in which the copter can undertake a specified function autonomously while also allowing for human interference if needed .; and identity regulation, in which the drone performs a defined task on its own. Drone surveillance, on the other hand, may result in a breach of privacy if the image structure or video recording is uploaded with the aid of an intruder, pix or movement snap photos of a person are taken from a drone, and the Joint Photographic Experts Group (JPEG) image graph format, which comprises data about the location and time of an event comes into the wrong hands. Furthermore, drone-based entirely completely surveillance technologies may be impacted by hijacking, GPS signal spoofing, control signal hacking, and making so many more wireless network attempts.

## 2. LITERATURE SURVEY:

The security of the customer computer has been jeopardised by a number of threats, including blocking and mimicking attacks, along with data theft. There are numerous solutions that can help a person enforce cybercrime components that can help their IoT devices stay stable. Various privacy threats have emerged recently, and that they might become able to compromise IoT technologies and networks. It's challenging to keep the security of The network devices in organizations and subgroups under control. Organizations must undertake

surveillance and measurement checks for all Connected systems in order to discover any privacy problems and attempt to reduce the danger of being compromised. Detection and study of different cyberattacks are aided by planes and analysis software.

On current developments in IoT security, several research and applications have now been undertaken. Additional services having proposed different Connected technologies and their administrators with a range of tough situations or attack vectors. Several models, designers, and the provision of numerous components that may check this suitable protocol can also assist in the creation of a way for distinctive IoT security. It is true that research on Internet networks has progressed quickly, and numerous simulated hardware and designers have funded this study. The repercussions of IoT device failure might be devastating.

Although the Internet of Things has provided users with several benefits, it also has a number of challenging scenarios that must be considered. Cybersecurity and privacy threats are the most often mentioned concerns. As a result of these measures, many businesses and government agencies are in a huge quandary. Recent record cyberattacks have exposed the vulnerabilities of IoT devices. This is because the interconnectedness of connectivity on the inside of the Iot technology allows access to the dishonest and anonymous Online, needing novel security measures. When it comes to the IoT protection apparatus's regulations, on the other hand, it's vital to emphasise the IoT Cybersecurity Strategy's aims and core concepts. According to, one of the most important processes to remember is terminating a contract that comprises several devices with various wireless communications. Variety in technology allow for the performance of autonomous operator treaties, which are vital components of any Web of Things counterterrorism form. In order to secure the dependability of IoT infrastructure within the cybercrime area, he affirmed that a few modest measures must be made to assist reduce the hard situations of IoT cybersecurity. Furthermore, the privacy Iot new application's effectiveness depends on its flexibility. According to experts, the Internet of Things ecosystem must be adaptable enough to accommodate a billion Internet-connected devices as well as cyberwarfare threats. Furthermore, according to the magazine, the IoT digital security environment must also enable dependability, such as unit tests, part experimenting, procedure experimenting, and features that allow, in order to totally decrease tough situations scenarios and risks.

Many recent IoT security enhancements function in a similar setting. With the aid of the service, some basic encryption techniques are established, and it is noted that providing good solutions is not always beneficial for the supplier. Regulators are unlikely to improve the right response for Iot application protection.

As a result, it was critical to investigate and examine numerous possible threats in the IoT. One of the key goals of IoT security would be to provide anonymous and protection, as well as that each client has comprehensive support, equipment, and a commitment for the treatment of drugs companies via the Iot ecosystem. As a result, studies in developing Iot security is gaining pace with the use of various design instruments and a few computing architectures.

## 3. RELATED WORKS:

The COVID-19 outbreak has boosted a number of forecasts for the future. The Internet of Things is expected to play a significant role in the new normal. This article examines, analyses, and analyses IoT-stimulated responses in many industries throughout the epidemic, as well as difficulties and opportunities beyond the outbreak. The IoT's vast array of networked devices, which may play music and notify users to various types of illness, aid in the development of a smart community for fitness control systems. Patient data is collected without the need for human contact, which can influence the decision. There are a variety of portable luminous IoT devices that might be used to reduce the spread of infectious viruses like COVID-19 and improve medical care.

With the help of IoT devices, several indications may be easily monitored. If traces of the virus are discovered, the technology may alert each customer as well as the nearby fitness centre. IoT may also function as a monitoring network, indicating areas with a high population density or areas with a high incidence of occurrences and a higher risk of infection. This will improve fitness branch performance in detecting and storing individuals in critical situations (e.g., the patient is unable to reach the exercise branches at the appropriate time owing to indicators) and sharing information with other agencies to offer faster treatment and keep citizens alive. It is significantly less challenging to check for signs from a considerable distance utilising technology such as 4G /5G and the cloud, particularly for those who find it difficult to reach or get access to medical care institutions.

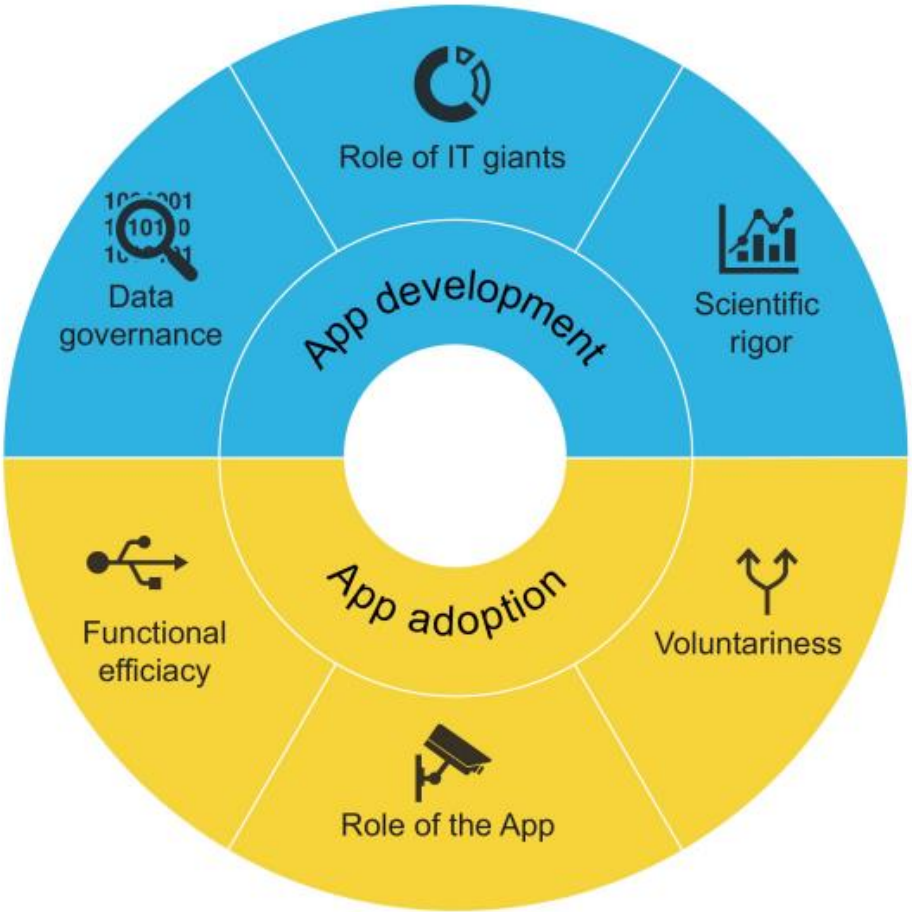


Figure 1

Additional benefit of IoT devices in the medical industry is the reduction in human mistake, which is more prevalent than machine or AI faults. Given that unfortunate incidents are likely to repeat, IoT can provide more diagnose and patient tracking. IoT generation plays an important role in identifying the virus by using fever screenings to spot some of the virus's symptoms, limiting its spread by enforcing social distance, and working with far-flung fitness monitoring, pollutants and air quality management, habitation control, and smart. Fever detection eliminates the need for individuals to touch each other and allows for the identification of many goals. Shade temperature scales and pictures are provided by sensing devices. The first line of defence against the disease is well before of personnel, disaster evacuees, or patients. This does not guarantee viral detection, but it may be used to determine if the problem also has indicators of the virus, and more inspections are performed for a final diagnosis. Fever monitoring is common in places like airports, schools, warehouses, and other busy places. Figure 1 depicts the temperature screening output of a commercially available technology.


Figure 2

The Internet of Things (IoT) has the potential to overcome all of COVID-19's difficulties. It can be used as a notification system, a warning system, a punishment mechanism, or a mix of these to help control the epidemic. The procedures may be divided into three stages, with notifying becoming the first and punishment being the third. At the notifying stage, IoT

can notify users if, for example, a location has a dense population, instances are present in a certain region, or if a closure is imminent. The caution and punishment degrees are combined in this picture. Individuals who arrive from another town, for example, may be warned not to leave their homes for 14 days, and if the cautions are disregarded, a charge may be imposed. These processes can limit the virus's spread and help manage the outbreak. Increasing engagement, on the other hand, necessitates more non-public records and permits (or consent) from the customer, which has an effect on the user's online privacy. There is a war going on between gaining access to records in order to deliver better services and protecting customer privacy. Due to the obvious necessity of explicit approval from users, the volume of data collected from IoT devices puts people at risk because they become more clearly recognizable with the use of profiles, tracing, and unauthorised processing, which could violate records safety legal guidelines such as the General Data Protection Regulation (GDPR). Valid hobbies, on the other hand, can play a significant role in limiting a worldwide epidemic, such as COVID19.

Throughout an outbreak, Home automation innovation can be put to further use at a lower cost and with a faster identification of illness. With in fitness business, for example, the ADAMM Asthma Screen detects bronchial allergy attacks and the Smart Continuous Glucose Monitoring (CGM) are excellent examples of Iot scenarios. In these critical times, IoT might be a huge help to the elderly, who are more susceptible to the disease than other age categories. They are also more general as a result of the increase in average lifespan. Portable IoT devices that can-do biometric analysis and activity monitoring, such as the Apple smart fitness watch and the Omron blood pressure monitor, can help people keep track of their health online. Magnificent care is also a useful technology that allows elderly people to speak with their loved ones and might be useful for domestic tracking. A study was carried out using eight suggested device learning systems to determine probable COVID cases early on. Five of these methods have an accuracy of greater than 90% when it comes to predicting capability occurrences. In order to determine the virus's nature, the architecture also examines the patient's response to treatment and true surveillance. This high level of precision can aid in the early detection of various diseases and the prompt application of appropriate treatment. IoT is capable of producing great outcomes and personalised attention and benefits to the afflicted individual via the use of innovation technologies.

## 4. COVID-19 OUTBREAK AND PANDEMIC:

COVID 19 was initially discovered in late 2019 in China, and it quickly spread across the globe. The World Health Organization (WHO) was obliged to declare a pandemic as a result of this. Researchers discovered that this viral is more powerful and causes serious respiratory difficulties after additional investigation. To control the over spreading of the COVID 19 many countries decided to move with lockdown, which restricted the public freedom and the economy of the common folks of the countries around the world. This also restricted the useless and unwanted travel inside and around the country and their economic and societal impact remains low. When government began to move with partial lockdown it

made an urge to grow a suitable exit which would avoid the further wave of the virus which would increase the infection and end in more healthy care systems. So the government began with safety precautions like frequent sanitation and maintaining social distance among the public. And the huge task for the government is to tracing and securing the people who show positive towards the virus.

## 5. COVID TRACING APPLICATION:

As COVID 19 grows, it's more important than ever to find a viable path to digital surveillance. The traditional method of surveillance is to track down the person who is ill and the people who have come into contact with him or her. Digital touch mapping, on the other hand, extends on this by using mobile devices such as GPS, Bluetooth, or QR codes to digitally music and tell consumers about their contact with an enraged person. This provides agencies with a more cost-effective and easily scalable solution than traditional tracing. Many worldwide places have or are in the process of building simulated fingertip tracking cell technologies as a result of this benefit. Asian foreign places such as China and Singapore quickly rose to the forefront, utilising their sophisticated digital facilities to install contact tracking applications and other virtual easy surveillance technologies. The Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) consortium was one of the first to form alliances to work on device technologies in Europe. Most of the first foreign venues in Europe to download a realistic device programme were in Austria. Since March 25, 2020, their "Stop Corona App," produced by the Austrian Red Cross, has been accessible. On June 16, 2020, the Robert Koch Institute in Germany published their "Corona-Warn-App". Swiss- Covid-App" proceeded via two Swiss federal institutions of technology (EPFL and ETH) around the same period, and was then noticed on June 25th. In contrast to other international sites (such as Taiwan, Singapore, and Poland), which employ virtual touch tracing applications to implement quarantine measures, these German-speaking international places use virtual touch tracing as a device solely to aid abatement and isolation. Digital touch trying to trace: Difficulties and Opportunities The academic networks surprisingly responded to this increase in virtual a little technology. Critics stated that such apps raise a slew of ethical and technological issues. The precision of the approach was initially questioned by the students. Experts emphasised the low quality of facts and the unreliability of Bluetooth and wi - fi for vicinity tracing, as well as the fact that combining citizen self-prognosis with legitimate validated checks propagates phoney positives. Furthermore, despite the fact that a large majority of the population wishes to participate for efficacy, adoption rates in countries like as Singapore have been below 20%. The opt-in method can thus reduce efficacy due to a loss of critical mass, but making it mandatory would jeopardise autonomy. Moreover, there are challenges with observation over short and extended periods of time, as well as privacy concerns. Virtual touch tracking, according to critics, incorporates a large-scale monitoring mechanism that may outlast the epidemic. Everyone else is concerned about possible information leakage, the dubious reliability of steganography, country-by-country variances in data security and privacy standards, as well as the flaws of centralised file system. Despite countless concerns, advocates argue that online is the way to go.

## 6. METHODOLOGY OF IOT:

In order to answer questions about IoT Technology's use and impact before and after the election, COVID-19 and the following study objectives are worded as follows:

(a) Figuring of major Internet of Things (IoT) technologies that influenced COVID-related management. a thorough study of the literature on the pandemic

(b) An assessment of the social and economic consequences, the technology's maturity, and the timeframe for implementation broader use.

(c) Policy, privacy, and security concerns are examined and discussed, and then a solution is proposed. frication and analysis of IoT technology best practises and codes of conduct

The following research approach was used to fulfil the research goals listed above. This study adheres to it. The study was based on secondary data that was made available to the public. sources of information on a variety of topics.

IoT technology are used in a variety of industries. This review used the SCOPUS collection, the Academic databases reference network, the ACM library, IEEE Xplore, Google Scholar, and other datasets. A number of keyword searches were carried out. In order to answer to our research questions, we needed to find relevant papers and reviews. The most prevalent keyword combinations were "COVID-19," "Coronavirus," "Internet of Things," "Internet of Everything," and "Internet of Everything." IoT, IoMT, and other keywords connected to the Internet of Things There was no criterion for exclusion. The quantity of search results that appeared for all keyword combinations in the review procedure were used to choose important IoT areas for the evaluation. The areas to focus on this evaluation were picked using tutorials, surveys, and reviews, in conjunction to the writers' keyword search and past study ideas. The details of each Iot platform were examined, classified, and presented. The study looked at Iot systems that were categorised by sector and industry. Then it's time to take a big breath. Each sector's Tech was evaluated separately. Each and every essential software It was also given a score based on its possible social and financial consequences.

These decisions have been made data obtained from each program. Moreover, the data is used to anticipate the timeframe for further implementation of each Iot ( internet of things). based on the data received in relation to the specific application Finally, there's the Capability Maturity Level. Each IoT software's present measurement models is displayed. In order to determine The TRL values were obtained using the European Government's nine-category TRL approach. Issues concerning safety and confidentiality, as well as best - practice for IoT, were also examined using data gathered from the research. It is vital to conduct a comprehensive inquiry. developed to discover the most important challenges and opportunities for every technology study area based in a particular sector

## 7. CHALLENGES OF IOT

There is a shortage of cyber defence expertise and information, according to a poll on cyber related and their category. This had a big impact on a lot of individuals. Organizations and people are exposed to these attacks as a result of new immoral advances. People misuse others via the use of technologies in the fields of internet and connectivity spring to mind as two examples. According to the researchers, a thorough comprehension of Individuals and corporations both require cyber-attacks. According to a study conducted by, a better understanding of the dangers is needed. and that cyber safeguards against assaults on IoT infrastructure are required Because it is integrating with our communities and personal lives, we must take it seriously. It is mentioned by Hoque. It's critical that we have one. To fight and prevent network attacks, a broad grasp of contemporary systems and technologies available in the public domain is required. A systematic examination of contemporary techniques that can assist is also included in the research. Issues about the three tiers in which IoT functions are highlighted by the author: application layer, network layer, and perception layer are three sorts of tiers. Protection was divided into two categories: universal and particular. Each layer is concerned with own number of security issues. The IoT's varied nature enables categorising it challenging. Data breaches include vices, power use, adaptability, and networked nature. challenges, such as:

• Gadgets with various capacities, providers, intricacy, and models, as well as their purposes, are interconnected.

• The Internet of Things (IoT) landscape is constantly changing.

• To assure delivery and maintenance, principles such as the Terms and Conditions (SLA) are in place.

• Reliability, Honesty, and Secrecy are all important factors to consider (CIA).

Additional obstacles, such as Wi-Fi signal power, IoT sensor network acquisition, and so on, are caused by additional assaults and risks produced from each layer. Mechanisms of authentication the existence of internet has resulted in a variety of cybercrimes. It is described as Networks and computers provide a nonphysical world in which people interact in various Methods. Information systems, telecommunication networks, embedded processors and brains, the World wide web, and microcomputer and control logic make up the interconnected network infrastructure [75]. Cyberspace is defined as a domain in which electromagnetic spectrum is used. and technology to share, store, and modify data, as well as the physical infrastructure that goes with it Ture and systems that are connected Hacking will develop sooner rather than later in IoE or Using in. sooner rather than later

### 7.1 Privacy, Policies, and Security Issues:

With both the increased use of IoT in the pandemic and the predicted increase post-COVID-19, confidentiality challenges must be resolved adequately. Because of confidentiality, IoT technology development will be restricted absent pledges of safe. Developers must adhere to certain guidelines. To create secure apps or frameworks, use secure and privacy design

principles. In In addition, personal data obtained by IoT should be protected with care. solutions. Data controllers are susceptible to penalties under GDPR in the case of a data breach (4 percent of annual global turnover). Yearly Revenue or $20 million, which is larger) or other personal data protection technology regulations from around the globe, this report looks at the confidentiality ramifications of Colourful, and even the issues they confront. There is a higher risk of cyber-attacks, privacy breaches, and security issues as the number of IoT applications grows. Any security threat to critical IoT devices Implantable Medical Devices (IMDs) and smart cars are examples of technologies that can put people's lives in danger. Can lead to significant financial losses According to the report, "vendors of IoT devices “Most organisations and users lack awareness of privacy and security," according to the report, and " need not maintain or repair their gadgets unless the client requests them. IoT devices aren't always up to speed on security issues, and they can have a lot of flaws.

In the IoT, the automation area faces significant risks and problems. IoT, according to the authors of [77], Instead of being a technology within itself, is an idea for transferring iot to WSN. Scalability, security, and interoperability all influence the architecture and interoperability of IoT systems. Convenience, genuine speed, and power equipment are all important factors. Hazards are classified into two groups. The level of sensing devices is one of the layers involved (along with the protocol stack, process control layer, communication layer, and so on). The detectors and controllers’ layer, for instance, might be vulnerable to hacking. A tangible alteration to the shows the locations or the gadget itself is required. A biosensor is a smaller version of something. They can also be a system threat by causing DDoS attacks (Distributed Denial of Service). ( Threats on the service) In the robotics IoT, any effect on the system might be dangerous.

This page defines several operations, and also as Distributed denial of service and Man-in-the-Middle threats, as well as wiretapping, repeat strikes, and router airstrikes. Most of these attacks may be readily prevented utilising multiple techniques, however fences and protections are hard to implement owing to memory and connection limits, as well as the restricted CPU capacity of devices. principles. Systems that are light, computation, and reduced are sought. It's probable that guesswork might be risky for assaults on the computational level, such as spyware, psychological manipulation, and credential guesses. To limit the risk of the epidemic propagating and worsening, screening tools are being utilised to identify the virus's presence, and some nations are creating connection monitoring applications. Google and Apple's apps use a distributed system design. and save user connections within the software rather than on a centralised server the government's and IT industry's reactions to the COVID-19 outbreak have been conflicting. There have previously been statements made about the privacy consequences of using contact tracking tools. Like during the COVID-19 epidemic Seclusion should be used to explore the impact of communication monitoring applications; face detection equipment, bracelets, and government aerial drones must all be evaluated. Public monitors using biometric technology, for instance, have been utilised by the Chinese government to catch, humiliate, and penalise people. Using similar technology, citizens who went somewhere without face masks were recognised. Those who seemed to be contaminated with the virus were quarantined.

Based on the president's and technology sector's reactions to the COVID-19 epidemic, questions are already raised about the implications of using contact tracking technologies on anonymity during and after the epidemic. Apps that track contacts have such a big impact. Additionally, the impact of face detection cameras should be investigated individually. Wearing bracelets and using police aerial drones Apprehending, punishing, and issuing fines individuals has just been done with the use of public camera and biometric scanners technology in China, for example. Residents walking around without surgical masks, and even identifying them with similar instruments. Those who seemed to be afflicted were placed under rigorous isolation.

As per a source, S. Korea has also put in place a robust surveillance system, with the Korean administration relying heavily on data obtained from CCTV video, payment card records, and smartphone data to counteract the growth. The findings of the studies Moreover, the UK claims to have deployed drones to follow persons who disobeyed COVID-19 social guidelines. Distancing yourself from others is a must. In one case, these IoT-inspired methods violate public privacy. in some way Despite the fact that technology has the potential to help solve problems, when a pandemic occurs, private rights are jeopardised. Our most serious issue is face is imagining the extent of surveillance and the potential for shocks. When confronted with a People are more likely to prefer health over privacy if given the opportunity, However, it is preferable that they use both. The Internet of Things is fast growing, but with the deployment of IPv6 and 5G (and now 6G), this should keep delivering new possibilities and solutions to the country's most urgent problems. However, there are indeed confidentiality risks with the Iot technology. Because of the network's heterogeneity, vendors' equipment and patches aren't updated on a regular basis. Website (IoT) gadgets are indeed a type of Sensor node (IoT Wearables and intelligent automobiles, for example, are examples of mobile IoT devices that frequently switch from one to the next. It is vulnerable to network attacks since it connects from one network to another. Alternatively, IoT devices, on the other hand, may already be infested with malware and distributing it.

Data access to improve services and consumer privacy are at odds. Individuals are at risk as a result of the volume of data acquired by IoT devices, as they become more easily identified through profiling, tracing, and unwanted pro-active surveillance. Because of the necessity, cessing may be in violation of data protection rules such as GDPR. users' unambiguous consent There is a clear discrepancy between the data and the conclusions. IoT Practices and GDPR Minimization Principle Because IoT companies engage in gathering that much data and information in order to get conclusions and archiving it for a lengthy moment, they believe in collecting as much data as possible. More data, in theory, will lead to more knowledge and benefits for enterprises and society as a whole. As a result, enforcing data minimizations will limit the amount of information that may be collected. Some IoT applications have been a huge hit. Personal information could also be safeguarded. On the other hand, one could argue that adopting procedures like pseudonymization is ineffective. Attempting to accomplish pseudonymization by deleting identifiers may jeopardise the quality of the data. Because the data would be tampered with, the results would be tainted.

The collection of large volumes of data through IoT may only be justified if the advantages outweigh the risks, such as privacy and security of personal data. Personal identity protection has become a serious issue in such an atmosphere. A challenge in the presence of a growing threat The idea that we've been all one and the same is an ugly reality. We are always under monitoring, either we are inside or outdoors, and if we are really using our devices. Using one's own vehicle or taking advantage of public transportation. There is further work to be done in this area. Concerns about privacy and security are being addressed by the Internet of Things. Some of the most useful recommendations the following subsections explore this cause.

7.2. IoT Privacy and Security Threat Mitigation Research:

Developing a cybersecurity strategy to handle the issues and possible threats associated with IoT technologies. A general layering scheme is as follows:

1. The perception layer, which comprises RFID and various sensors for item identification;
2. The network layer (Internet and mobile network) is in charge of data transmission.
3. The middleware layer, which processes, stores, and links various types of data; and finally, the application layer.
4. The application layer is where real-world applications can be found. Each layer has its own set of elements.

Wireshark and dangerous code implantation on the protocol stack, as well as unauthorised access to tagging and tag copying at the user devices, Malware on the network topology, and computer hacking to tagged and tag duplicating at the higher layers. Layer of the application Hash and encryption mechanisms are used to address these issues. The security goals were confidentiality, integrity, and availability. Confidentiality ensured that data from sensor nodes was not divulged, integrity ensured that data was The information wasn't really tampered with this in any form, and its accessibility insured that it was visible.

A blockchain technology method has the potential to be even more reliable and provide stronger privacy benefits. This technique has an impact on processing time, traffic, and energy consumption, but these drawbacks are minor in comparison to the privacy benefits it provides. brings. A local block chain is used to maintain track of communication in this process. as well as data transfer between devices to provide services, each device requests specific information. Additionally, the delays are minor and have no bearing on the smart home device's availability. This approach avoids DDoS assaults by inspecting all incoming and outgoing traffic. Ensure that the device has given permission for the data to be sent. It also protects against linked assaults by employing a one-of-a-kind identifier. Each communication between the devices requires a unique key. Another study [83] proposed a blockchain IoT system to solve the obstacle of using a current server-client approach, which has some drawbacks and limitations, when thousands of IoT devices are connected. Ethereum is distinct from other cryptocurrencies. Because it is a distributed computing platform, the server-client model and data transactions are separate. attackers can't figure out or tamper with. stored using adversaries can't readily discover out or meddle with a consensus mechanism This method protects

networks against Based DDos assaults. Ethereum is volatile, which is one of its weaknesses. Transactions require time; therefore, it's not suited for activities that need to be done quickly. The second concern is the amount of storage that small Connected systems will require, which may be substantial.

The author recommends further study on using methods and approaches to improve the effectiveness of Security controls, notably the protection of finisher, with an emphasis on heuristic methods that can yield amazing results. Non-profit companies are used. The Completely controlled Sorting Optimizer (NSGA-II) offers accurate alternatives to the dominating sorts issue. The location of Wireless Mesh Network (WMN) equipment is challenging to optimise. For Optimization techniques are an useful tool for determining a set of useful solutions. When dealing with IoT security issues, this should be considered. An encrypting data approach for data confidentiality, consistency, and non-repudiation in IoT technologies. The Internet of Things (IoT) is a new network that makes use of RFID to enable smart data analytics, dependable data transport, and user observation. Smart sensor connectivity and cybersecurity creates a variety of challenges. A few of the subjects covered are interaction, internet propagation, RFID, processing information, and confidentiality. The recommended solution uses cryptosystem since it takes less space. cryptography at a high rate. To produce a decryption key, the procedure begins with encryption process, which is accompanied by an uneven method to secure the data. The message is decrypted by the absorber who possesses an encryption key using a secret key and an uneven process. Al-Qaeda is a terrorist organisation. In this algorithm, the Advanced Encryption Standard (AES) and the NTRU techniques are integrated. To boost protection, the key is generated using AES and NTRU cryptosystem.

## 8. PROPOSED SOLUTIONS:

Health restrictions (local and national lockdowns) that safeguarded people's safety had a significant impact on a variety of sectors. The researchers wanted to know how Sensor products are employed and also how they influence COVID-19. The listing of specializations and key industries below is by no means complete. It was picked as a consequence of the experts' initial investigation and suggestions, and the needed information for the analysis was acquired with the support of the writers' previous scientific investigation. The approaches given in Section 3 cover a variety of uses and key industries. During COVID-19, researchers observed that IoT-based technologies were used from the start. The number one search outcomes for offer a unique opportunity variant are shown in Table 1. Based on the number of recommendations and keywords. Furthermore, multiple sectors were integrated in order to

more accurately measure its use effect of the majority of users.

| 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 |

Table 1

While many of the businesses included in this essay, such as medicine, have been included in almost every previous study, others have not. There will not be a lot of research done on this. In adding to the fields mentioned above, IoT could be used in a diversity of other fields. Farming and hospitality are good instances of such industries [29–31]. The phrase, on the other hand, has not been widely used. Those industries have been evaluated in response to the solutions chosen for this research.

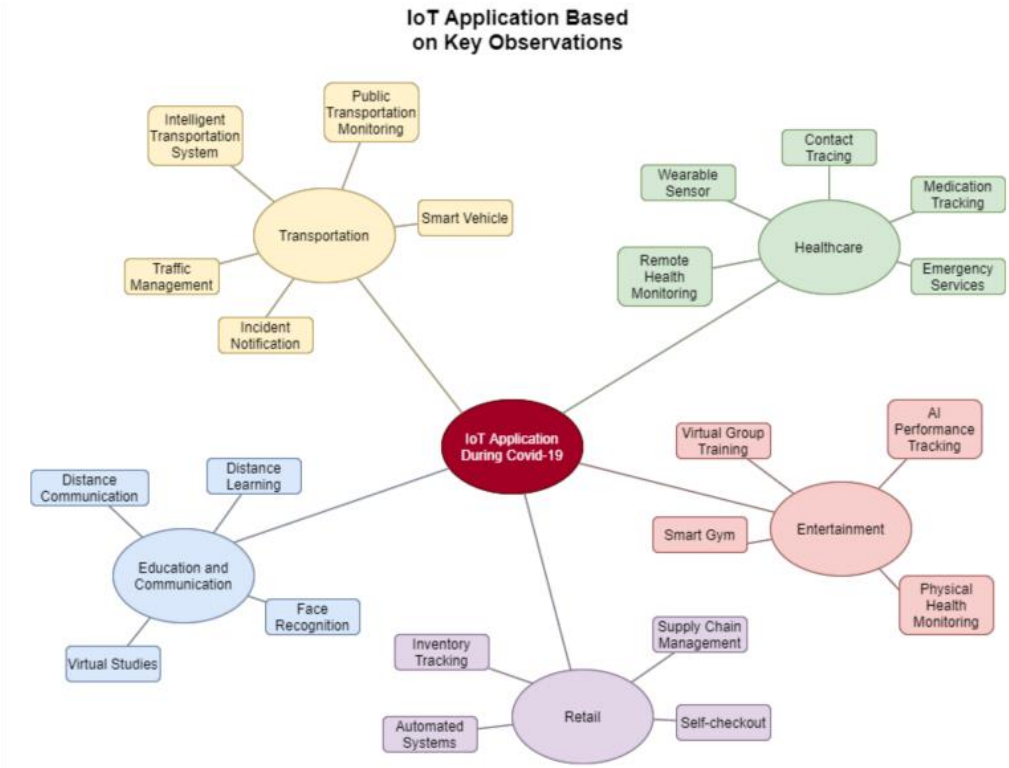


Figure 1

8.1 IOT in health care sector.

In HealthCare, the Internet (IoT) Health was one of the key businesses that benefited from Sensor solutions during the COVID-19 epidemic. Portable remedies for individuals with disabilities are only a few instances of these. EMS (emergency medical services) and other ambulance crews Even while certain IoT solutions aren't yet commercially accessible, they were old but need to be employed on a bigger scale throughout the campaigns and showed potential. pandemic. This accreditation will influence the creation and verification of these applications as a result. used in a bigger context with trust. COVID-19 is an infection caused by the SARS-CoV-2 virus, that affects the respiratory system. The study suggests a wearing temperature sensor that analyses the user's ventilation machine's range and rate of breathing. These instruments, which use the Internet of Medical Things (IoMT) to adjust and monitor patients' breathing conditions, can regularly replace anxious cardiologists who are concerned about the patient's respiratory status. This also saves time because it is much easier for the concerned medical specialists to make appropriate suggestions remotely. The author of [33] offers a portable IoT-based completely gadget for detecting anxiety levels.

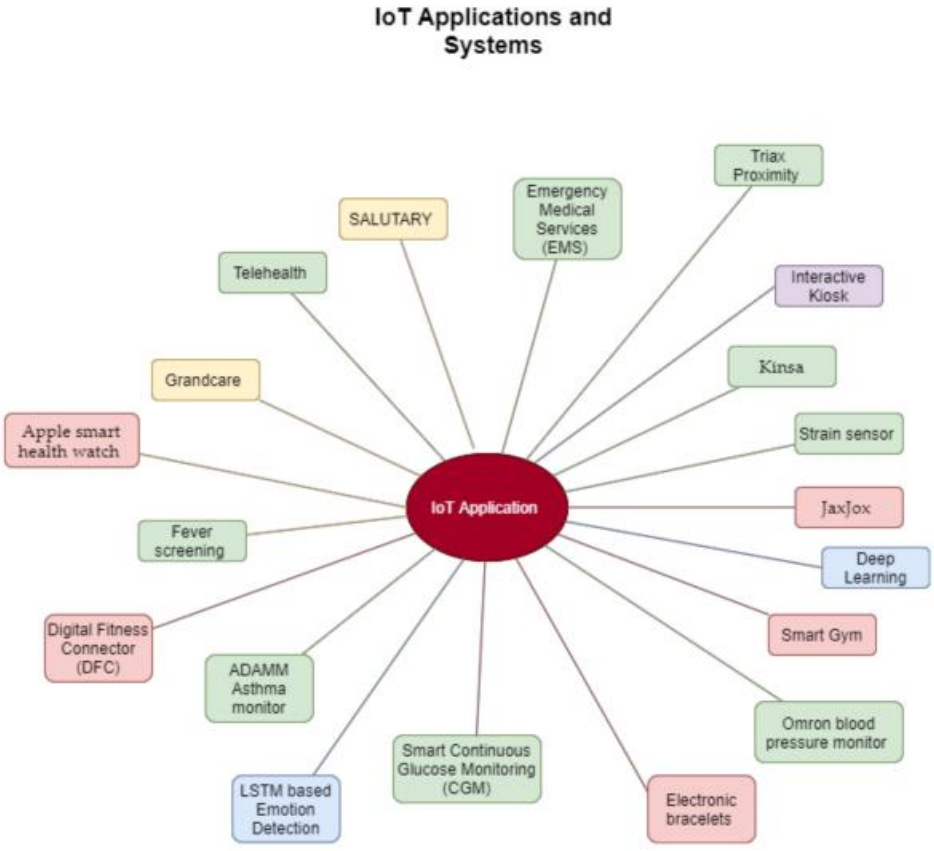


Figure 3

During the COVID-19 pandemic, mapping of contacts proven to be an effective method of protecting personal information while keeping people safe. Triax Proximity Trace, for example, is a wearable light IoT gadget that uses touch tracing to address societal issues. It's distancing because it warns users when they're getting too close. Departure of the Enterprisements can distribute wearable gadgets that assure compliance with safety rules without the need for any additional hardware. Downloads or mobile phones Tags are delivered

using Bluetooth technology, which eliminates the need for wires. It's necessary to keep track of a user's current location. Furthermore, anonymous Every 15 minutes, the keys change are utilized. utilised to secure your privacy even more. Contact tracing has been used in Alberta. COVID-19 is an application. The app confirms favourable results and alerts Canadians.

Stanford People's health Clinic was able to grow from being seen 20 persons per day to seeing around 650 through such a two-way, live telemedicine, or "virtually contact," interaction [35]. Online activities, such as audio and video, are used to facilitate conversation. without the necessity for patients to meet face to face with their specialist or medical specialist, which is an alternative to a community meeting in a doctor's office with a dangerous weapon. Swine flu is a chance.

Kinsa, a clever thermometer, is yet another great alternative for monitoring devices at home. Fever and illness may be tracked on a cell phone, allowing users to respond more promptly to their surroundings. It also records a family's medical and health histories, as well as their medicines. It also offers youngster capabilities and helps in creating reminders. The device establishes an internet connection. The Kinsa Apps can supply further data to a central party gather via Bluetooth. Hospital professionals work for ambulance crews are subjected to extremely difficult conditions during an epidemic. IoT-assisted ambulance technology provides time-saving options by enabling expert to advise personnel on how to handle a scenario. EMS service enabled by the Internet of Things (IoT) are wonderful for critically ill patients. In life-threatening instances, mechanisms to save lives are required, according to the authors, who propose a strategy that provides actual statistics on the number of accessible beds and high blood pressure.

There are a variety of issues to consider, including blood type availability and doctor availability. Actual statistics from the ambulances can be collected during serious crashes with multiple victims.

| | 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 |

Table - 2

Table 2 outlines the most important IoT applications in this domain, as well as the expected economic and social impacts. Technology Readiness Levels, social impact, and expected timescale for widespread adaptation (TRLs) of the programme in order to make it more widely available.

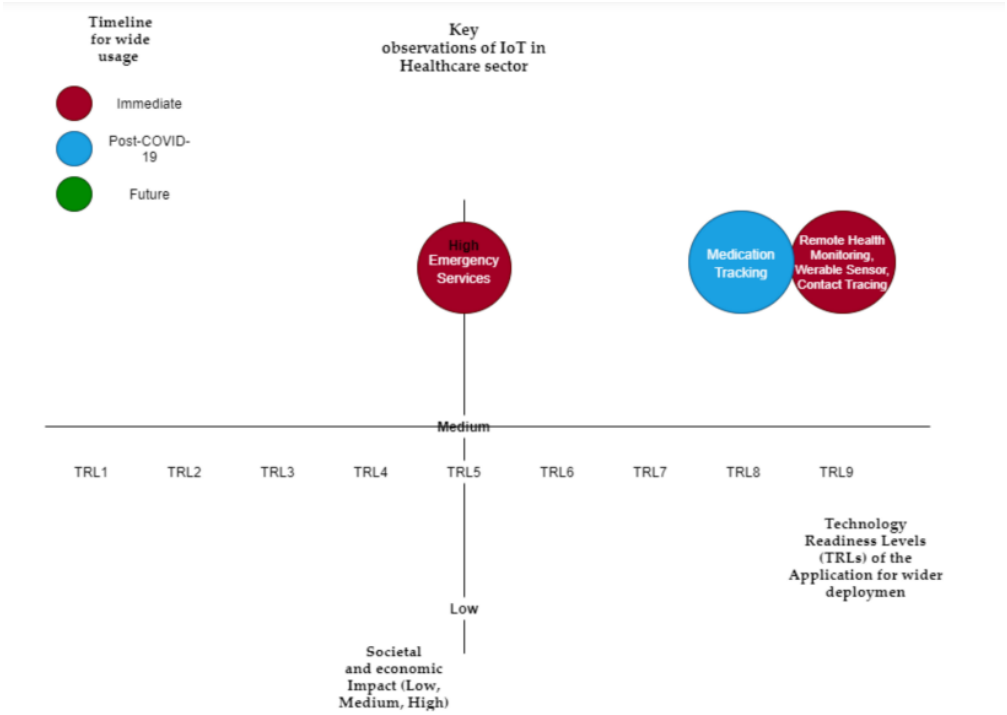


Figure 4

Figure 1 depicts wellness IoT technology in 3 directions (social and economic benefit, Timetable for Broad Usage, and Implementation Technology Adoption Levels (TRLs) for Expanded Rollout), as stated in Table 1. You'll have more alternatives as a result of this. The effects of technology, as well as its timeline and TRL, are all illustrated.

8.2 IOT in transportation sector:

COVID-19 has had a significant impact on the rail industry. The implementation of COVID avoidance techniques has resulted in decreased road transport, which has since influenced other sectors such as agriculture supply chains [43]. Payment and registration booking platforms, gps monitoring and GIS plotting, controller and guiding devices, inventory control solutions devices, and intelligent vehicle managed services devices are all examples of IoT applications. Throughout an epidemic, technology can aid in the reduction of crowded areas and the spread of pathogens. With your help, import and selling products is a lot easier. Internet of Things-based transportation engineering Automated can enhance roads, trains, the water, and the air. Minimize physical interaction to limit the chance of infection while still allowing for the exchange of information.

SALUTARY is a reliable and secure transportation system that aims to reduce traffic jams in public transport services (bus stations, metro platforms, tramway, vehicles, train, and track) [45]. The system specifies the amount of users of the service to predict traffic. Users will be notified, and system operations, such as routing and times, will be altered. Combining the technology with the smart Transport (ITS) could provide new opportunities. There is crowd detection as well as services such as online ticketing, bookings, and car access. management to keep the flow of traffic at check To overcome the issues, Sutar offered a method based on

Internet of things, GPS, and Android. given the growing number of cars on the road and the need for better traffic control for mass transit.

## 9. IMPLICATIONS AND FUTURE DIRECTIONS:

The authors found sufficient evidence in this review to support the critical role performed by IoT-based totally programs and technologies throughout COVID-19. It was also revealed that many projects are ready for widespread implementation and have a significant impact on society, but others produce similar R&D and verification before being launched. However, the writers agree that more research and development should be forced to remedy privacy and security problems, as mentioned in this section. This could be a critical factor in deciding whether or not to mass-produce IoT devices in the future. According to [71], researchers should concentrate more on how to ensure that people are well-informed enough to approach the future without risk. This is because there may be a scarcity of data and documents on cyber security. Furthermore, a more comprehensive understanding of IoT dangers is required [72], as there are likely to be fewer research on green techniques for delivering important and challenging records to clients. The Consumer IoT Safety Code of Ethics [87] is an example of this. These codes of conduct are available to the general public, but customers are significantly less likely to hunt for them on their own. The medical sector is currently undergoing extensive research and provision of effective. As discussed in the essay, IoT has the potential to make a significant difference in a variety of industries. However, more research is needed to transition this generation into other industries, such as tourist, food and banquets, mines, infrastructure, and government services.

Researchers can apply the systematic analysis provided in this work to understand IoT-based totally utility use during COVID-19 and beyond. Furthermore, it provides sufficient information about specific IoT technology in a variety of industries. Readers can use this assessment to learn more about the societal and financial implications, as well as the time to market and technological preparedness. In addition, this text expands on major challenges and opportunities in the areas of privacy and security, which can be addressed in future studies and development. Finally, this work provides readers with sufficient information about the importance of codes of conduct in this sector as well as emerging best practises for IoT in general.

## 10. CONCLUSIONS:

COVID-19 enables new IoT applications to be tested in a range of application domains, as described in this review research. Some IoT-based solutions aided in the management of the COVID-19 pandemic (for example, contact tracing), whilst other IoT-based solutions aided in the management of the COVID-19 epidemic. To test new technology, pilots and experiments are utilised. It's evident that some of these technologies aren't quite ready for widespread use. There are also a few Various IoT application potential were discovered throughout the outbreak (for example, SALUTARY, Triax Proximity, and IoT-based Standard Operating Procedure). Although IoT-based technology has the potential to revolutionise the way we live following COVID-19, as stated in the paper, additional research and validation is required before

widespread adoption and deployment. In this review, the key topics were summarised. TRL, as well as IoT application fields, estimated socioeconomic benefit, and de-risking timetable employment In addition, the application concerns were discussed in this evaluation. domains that place a heavy priority on privacy and security In addition, standards and emerging codes of practise for IoT-based applications were explored in this study. The Internet of Things enabled better healthcare services and clinical judgments during the pandemic. IoT, like healthcare, has a significant opportunity to improve our lives, and it already has the capability to do so. Especially in light of the COVID-19's new normal.

**REFERENCE:**


1. Khvoynitskaya, S. The History and Future of the Internet of Things. 2020.25 March 2020.
2. Conti, M.; Dehghantanha, A.; Franke, K.; Watson, S. Internet of Things security and forensics: Challenges and opportunities. Future Gener. Comput. Syst. 2018, 78, 544–546. [CrossRef]
3. Monther, A.A.; Tawalbeh, L. Security techniques for intelligent spam sensing and anomaly detection in online social platforms. Int. J. Electr. Comput. Eng. 2020, 10, 2088–8708.
4. Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of threats to the Internet of things. IEEE Commun. Surv. Tutor. 2018, 21, 1636–1675. [CrossRef]
5. Meng, Y.; Zhang, W.; Zhu, H.; Shen, X.S. Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures. IEEE Wirel. Commun. 2018, 25, 53–59. [CrossRef]
6. Siby, S.; Maiti, R.R.; Tippenhauer, N.O. Iotscanner: Detecting privacy threats in IoT neighborhoods. In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, Abu Dhabi United Arab Emirates, 2 April 2017; pp. 23–30.
7. Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. Comput. Netw. 2019, 148, 283–294.
8. Leloglu, E. A review of security concerns in Internet of Things. J. Comput. Commun. 2016, 5, 121–136. [CrossRef]
9. Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe, W. A security framework for the internet of things in the future internet architecture. Future Internet 2017, 9, 27. [CrossRef]
10. Ali, S.; Bosche, A.; Ford, F. Cybersecurity Is the Key to Unlocking Demand in the Internet of Things; Bain and Company: Boston, MA, USA, 2018.
11. Y. Gvili, “Security Analysis of the COVID-19 Contact Tracing Specifications by Apple Inc. and Google Inc,” in Cryptology ePrint Archive: 2020/428, International Association for Cryptologic Research (IACR).
12. L. Reichert, S. Brack, and B. Scheuermann, “A Survey of Automatic Contact Tracing Approaches,” in Cryptology ePrint Archive: 2020/672, International Association for Cryptologic Research (IACR).
13. Ministry Of Health Saudi Arabia, 2020. MOH: «Tatamman» Smart Bracelet a Must for Citizens Returning from Abroad [Online]. Available at: <

https://www.moh.gov.sa/en/Ministry/MediaCenter/News/Pages/News -2020-05-22-002.aspx > [Accessed 23 May 2020]
14. “Driving the future of drones since the pre-drone era,” Draganfly. [Online]. Available: https://draganfly.com/. [Accessed: 30-Jun-2020].
15. S. Kashyaap, “This drone start-up is taking on coronavirus with thermal detection headgear,” YourStory.com, 19-May-2020. [Online]. Available: https://yourstory.com/2020/05/drone-startup-indianrobotics-solution-coronavirus-thermal-headgear. [Accessed: 30-Jun 2020].
16. Dieter Moormann, “DHL parcelcopter research flight campaign 2014 for emergency delivery of medication,” In Proceedings of the ICAO RPAS Symposium, 2015.
17. Thierer, A.D. The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation. 2015. Available online: http://jolt.richmond.edu/v21i2/article6.pdf (accessed on 6 March 2020).
18. Available online: https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html (accessed on 17 March 2020).
19. Available online: https://www.tecmint.com/protect-hard-and-symbolic-links-in-centos-rhel/ (accessed on 26 May 2020).
20. Available online: https://docs.aws.amazon.com/iot/latest/developerguide/iot-message-broker.html (accessed on 25 May 2020).
21. Sethi, P.; Sarangi, S. Internet of Things: Architectures, Protocols, and Applications. J. Electr. Comput. Eng.2017, 1–25. [CrossRef]
22. Liyanage, M.; Braeken, A.; Kumar, P.; Ylianttila, M. IoT Security: Advances in Authentication; John Wiley & Sons: West Sussex, UK, 2020.
23. “Hacking a Drone - Is it Possible?,” UMV School, 12-Dec-2019. [Online]. Available: https://umvschool.com/hacking-a-drone-is-it-possible/.[Accessed: 29-Jun-2020].
24. Y. Zhi, Z. Fu, X. Sun, and J. Yu, “Security and Privacy Issues of UAV: A Survey,” Mobile Networks and Applications, vol. 25, no. 1, pp. 95–101, 2019.
25. Horstmann KT, Buecker S, Krasko J, Kritzler S, Terwiel S. Who does or does not use the “Corona Warn-App” and why? psyarxiv preprint. 2020. https://doi.org/10.1093/eurpub/ckaa239 PMID: 33340328
26. Bf Statistik. SwissCovid-App Monitoring Swizterland: Schweizerische Eidgenossenschaft; 2020 [cited 2020 September 20]. Available from: https://www.experimental.bfs.admin.ch/expstat/de/home/ innovative-methoden/swisscovid-app-monitoring.html.
27. Renner A, Kohler A, Thier J, Skinner B. Bis Infizierungen in der SwissCovid-App gemeldet werden, ist es oft zu spa¨t. Neue Zu¨rcher Zeitung. 2020.
28. Thier J. Die «beste Corona-App» ist auf dem Boden der Realita¨t angekommen. Neue Zu¨rcher Zeitung. 2020.
29. Studie: Stopp-Corona-Apps funktionieren in o¨ffentlichen Verkehrsmitteln nicht richtig. Der Standard. 2020.
30. Institute RK. Kennzahlen zur Coronawarnapp. In: Institute RK, editor. 2020.
31. Cross AR. Datenschutzinformation zur Stopp Corona App Roteskreuz; 2020 [cited 2020 20 September]. Available from: https://www.roteskreuz.at/site/faq-app-stopp-corona/datenschutzinformation-zurstopp-corona-app/.

32. Institut F. Stopp corona-App Austria: Marketing Research Ges.m.b.; 2020 [cited 2020 20 September]. Available from: https://www.focusmr.com/wp-content/uploads/2020/08/stopp-corona-app-focusaugust-2020-1.pdf.
33. Camerer CF. Behavioral game theory: Experiments in strategic interaction: Princeton University Press; 2011.
34. Cappelen A, Mæstad O, Tungodden B, editors. Demand for childhood vaccination–insights from behavioral economics. Forum for development studies; 2010: Taylor & Francis.
35. Rooke C, Amos A. News media representations of electronic cigarettes: an analysis of newspaper coverage in the UK and Scotland. Tobacco Control. 2014; 23(6):507–12. https://doi.org/10.1136/ tobaccocontrol-2013-051043 PMID: 2388401