**Chapter 2**

**IoT Applications in the Future: Opportunities and Challenges**

# Introduction

The emergence of the internet of things (IoT) has impacted and revolutionised computing and information systems. IoT is a computer idea in which everyday physical items would identify themselves by connecting to the internet. IoT brings together physical items integrated with software, sensors, actuators, radio-frequency identification, and smart objects to collect and exchange data. The Internet of Things is predicted to bring about radical changes and answers to the majority of real-world daily issues. As a result, IoT offers connection at all times for everyone and everything. The Internet of Things (IoT) imbues items linked to the Internet with intelligence that enables them to share information, make choices, carry out activities, and offer extraordinary services.

It has a crucial societal and economic influence on how information, network, and communication technology is built in the future. The Internet of Things (IoT) is anticipated to connect numerous technologies in the future years to open up new applications and help intelligent decision-making by linking physical things.

Global navigation satellite systems (GNSS) have become a crucial component of major contemporary technological developments, particularly the Internet of Things (IoT), Big Data, Smart Cities, and Multimodal Logistics. GNSS is the most efficient and cost-effective source of positioning and timing information in outdoor environments.

More than 20 billion IoT devices will be connected by 2020, and the market for these devices might be worth $1.5 trillion. IoT's predicted effects on the Internet and economy are astounding; some estimate that by 2025, there could be up to 100 billion linked IoT devices and a $11 trillion worldwide economic impact.

By prohibiting abuse of market power, safeguarding users and Internet networks, and promoting efficient markets and the general welfare, regulators can play a role in fostering the growth and acceptance of the IoT. Regulators can think about and choose various actions to promote IoT growth. Encourage the development of 5G and LTE-A wireless networks, and continue to assess the demand for IoT-specific spectrum.

Governments adopting IPv6 universally across all of their services and purchases, as well as providing various incentives to the private sector. giving people a right to simple access to their personal data and enhancing interoperability through competition legislation. Encourage the adoption of global standards and the use of remotely provided SIMs to increase machine-to-machine rivalry. Regulators will need to pay close attention to IoT privacy and security concerns, which are essential for fostering public confidence in and adoption of the technology.

In particular, this book focuses on the fundamental technologies that make it possible to implement the Internet of Things and its general layered architecture, the market for IoT and GNSS technologies and how they affect the global economy, the IoT application domain, and finally the policy and regulatory implications and best practises.

Due to built-in computational intelligence that processes data extremely effectively and will combine enhanced connection, cloud-based storage, and a variety of connected devices and services, this new era of 5G promises speeds of 1–10 Gbits/s, greater data bandwidth, and fewer delays. A mobile IoT will become possible with extensive processing capacity and virtual system architecture[1,2]. Advances in health care, transportation, agriculture, environmental monitoring, education, resource management, and many other fields will be made possible by a system that connects billions of devices and sensors.

Noting that 5G is an all-encompassing technology that moves communications to a computer platform is crucial. From a point-to-point system, 5G symbolises an upgrade to one that gathers data from billions of devices and uses the suitable processing platform to deliver communication packets to the correct device effortlessly.

People will be able to take advantage of more individualised, immersive, and improved experiences whenever and wherever they are thanks to connected gadgets. Because gadgets and sensors are becoming much more affordable, connection will be pervasive and inconspicuous. People will have systems that behave based on their predefined preferences, so they won't have to make a deliberate decision to send a computational command.

We are headed towards a civilization where everything and everyone will be connected thanks to technological innovation. The Internet of Things (IoT) is seen as the Internet's next evolution, enabling machine-to-machine (M2M) learning. The fundamental goal of IoT is to enable data interchange and communication between applications and devices used in the real world in an autonomous and safe manner. The Internet of Things (IoT) connects the physical and digital worlds in real life [3].

The number of devices linked to the Internet is growing quickly. Personal computers, laptops, tablets, smart phones, PDAs, and other portable embedded devices are some of these gadgets.

The majority of mobile devices have various sensors and actuators that can perceive, process data, make wise judgements, and send valuable information gathered via the Internet. Utilising a network of such devices with various sensors can result in a vast array of remarkable applications and services that can have a positive impact on one's life on a personal, professional, and financial level [3].

The Internet of Things is made up of physical things, sensor technology, network infrastructure, computing power that may be stored in the cloud, and systems for making decisions and triggering actions. The items are uniquely recognised, have certain distinctive traits, and can be accessed over the Internet. The smart sensor devices can detect the Radio-Frequency identifying (RFID) tags or other identifying bar-codes that are attached to these physical things.

Over the Internet, the sensors send the computational and processing unit object-specific data. Smart services may be designed using a variety of various sensors. The decision-making and action-invoking system uses the processing result to decide whether to execute an automated action. There are many items or objects that are present everywhere in the human environment, as shown in Figure.1's overall overview of the development of the internet with many IoT services[4]. The viewpoints, issues, and possibilities around a future Internet that fully supports "things" are discussed in this book, along with how things can aid in the creation of a more synergistic future Internet.

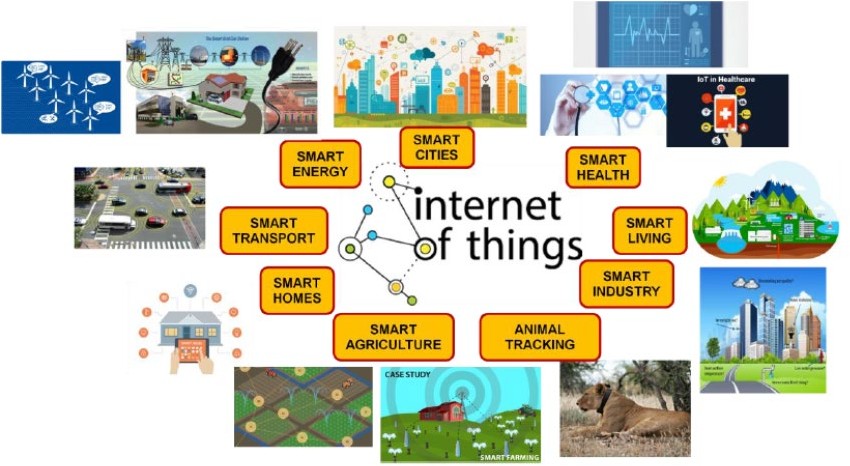


Figure.1: The IOT generic scenarios

# Market

The possible effects of IoT on the Internet and the economy over the next several years have been the subject of a broad variety of estimates from a number of businesses and academic institutions. By comparison, Morgan Stanley expects 75 billion networked gadgets by 2020[6], while Cisco projects more than 24 billion Internet-connected things by 2019 [5]. In a longer-term outlook and with bigger stakes, Huawei projects 100 billion IoT connections by 2025[7]. According to the McKinsey Global Institute, by 2025, the Internet of Things may have a $11.1 trillion financial impact on the world economy. According to estimates, users of IoT (businesses, other organisations, and consumers) might take advantage of 90% of the value that IoT applications provide. For instance, the cost of improving the health of people with chronic diseases by remote monitoring might reach $1.1 trillion annually by 2025[8].

By 2020, it is anticipated that the 5G network would accommodate 212 billion linked sensors, 50 billion connected devices, and 44 zettabytes of data. This will include everything from smartphones and tablets to smartwatches, automobiles, equipment, home appliances, and remote surveillance tools. These will all provide a tremendous amount of "useful data" that can be examined. In fact, according to academics, this interconnected ecosystem will make it feasible to use a far higher percentage of digital data (35%) than was previously conceivable (5%). The volume of traffic that gadgets produce is anticipated to increase noticeably as the number of Internet-connected devices increases. For instance, Cisco predicts that the percentage of Internet traffic produced by non-PC devices would increase from 40% in 2014 to slightly less than 70% in 2019[9]. Cisco predicts that "M2M" connections will increase from 24% of all connected devices in 2014 to 43% in 2019. This prediction includes connections in the industrial, residential, healthcare, automotive, and other IoT sectors. These patterns suggest that over the next 10 years, the general understanding of what it means to be "on the Internet" may change.

The installed base of GNSS devices is expected to rise from 5.8 billion in use in 2017 to roughly 8 billion in 2020 as the global GNSS industry continues to see steady expansion. The global installed base of GNSS devices continues to be dominated by smartphones, with 5.4 billion and 380 million units in use, respectively, in 2017[10], supported by a burgeoning mobile economy and rising buying power. Millions of people around the world use GNSS devices on a daily basis, whether it be by utilising GNSS-synchronized telecommunications networks, using efficiently coordinated transport networks, or enjoying the fruits of sustainable and cost-effective agriculture, despite the fact that the number of GNSS devices used for professional applications is much lower than that of their mass-market counterparts. These downstream sectors are in turn allowing services that provide consumers with extra value by utilising GNSS technology, including several smartphone apps and fleet management programmes for the transportation industry. In turn, the introduction of 5G, Automated Driving, Smart Cities, and the IoT is expected to lead to an even greater proliferation and diversification of GNSS-enabled added-value services, and their annual revenues will reach € 195 bln in 2025, more than 2.5 times higher than the anticipated GNSS device and service revenues[10]. A window of opportunity for hybrid and cross-cutting applications as well as the emergence of new customer wants and requirements is created by emerging technological paradigms like the Internet of Things (IoT) or Smart Cities that connect together established GNSS business sectors.

# Generic Architecture

1. The long-proposed TCP/IP protocol stack is still in use today on the Internet to enable communication between network sites. The IoT links billions of items, but this will result in considerably more traffic and need much more data storage. IoT development therefore depends on the advancement of technology and the creation of numerous new applications. As seen in Figure 2, the IoT framework is often separated into four tiers. Below[11] is a quick description of these strata.
2. ***Perception Layer****:* 'Device Layer' is another name for the perception layer. It is made up of both physical things and sensing technology. Depending on how an object is identified, the sensors may be RFID, 2D barcode, or infrared. This layer primarily deals with the identification and gathering of information about specific objects via sensing devices. The information can be about position, temperature, direction, motion, vibration, acceleration, humidity, chemical changes in the air, etc., depending on the type of sensor used. The network layer receives the information collection after which it transmits it securely to the information processing system.
3. ***Network Layer****:* 'Transmission Layer' is another name for the network layer. This layer transmits data from sensor devices to the information processing system in a safe manner. Depending on the sensor devices, the transmission method can be cable or wireless and the technology can be 3G, UMTS, LTE, 4G, Wi-Fi, Bluetooth, infrared, or ZigBee. As a result, the Network layer transmits data from the Middleware layer to the Perception layer.
4. ***Middleware Layer****:* Between the application and network layers, the middleware layer abstracts. In addition to offering services to clients, this layer also stores data from lower layers in databases. Visualization approaches have become more important as IoT creates massive amounts of data and focuses on giving information to users through data analytics and storage. It processes data, does ubiquitous computation, and then automatically decides depending on the outcomes.
5. ***Application Layer****:* The uppermost layer in the IoT architecture, the application layer, contains application management, which is based on the data processed and gathered from the middleware layer. IoT may be used for a variety of purposes, including e-health, smart homes, smart cities, intelligent transportation, retail, agriculture, supply chain management, security, and emergency preparedness, as well as factory, culture and tourism, environment, and energy.

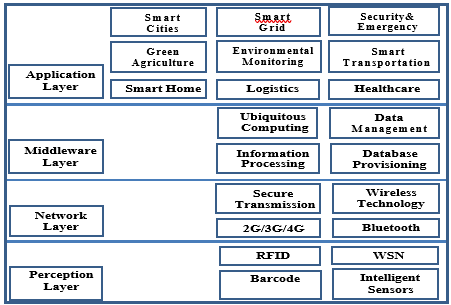


Figure.2: Basic IoT layers.

# IOT Applications

# The IoT application scenario is quite fragmented and includes many different types of applications, some of which are listed below.

# Smart Cities

The IOT enables Smart Cities to manage resources more effectively, increase their resilience to short-term failures and calamities, and promote efficient behaviour. Using the IoT to address today's urban difficulties includes using smart and weather-adaptive lighting, monitoring water and gas leaks, smart parking with dynamic pricing, and automated parking recommendations. By spotting potential threats and providing vital data on crowd behaviour and citizen requirements, ubiquitous vision can provide a degree of safety and security that has never before been possible. In addition to providing all-encompassing and enhanced surveillance, IoT vision enables physical augmentation to social media and human activity monitoring to improve the dynamic match between demand and supply of services.

Similar to this, it may be used to localise noise occurrences for safety assurance and generate real-time noise urban maps to reduce noise pollution at crucial moments [3]. Another niche where the IoT might have an influence is smart irrigation of parks and green areas. The IoT will also help smart infrastructures in terms of security (such as automatic detection of abandoned luggage and suspicious behaviour) and safety (such as structural monitoring of bridges). The IoT architecture for smart metering and monitoring will assist to obtain precise automated metre readings and the issue of energy, gas and water invoices to the consumers.

Having a street light that has sensors for spotting automobiles or people moving about allows it to be dynamically switched on when there is activity in the area and off otherwise. By minimising the creation of dark zones around people, it can help the city conserve electricity (and money) while preserving security [12]. In addition to already existing factual information on locations, smart tourism promises to give visitors the ability to have an immediate understanding of the city, such as the availability, crowdedness, or quietness of different places, and to receive dynamic recommendations on tours that adapt to their disposition. While identifying possibly hazardous and unsuitable garbage that would need to be disposed of using a different technique, waste management may be made more effective.

# Healthcare

Numerous IoT applications are possible in the healthcare industry. They can be utilised to improve the present assisted living options, on the one hand. In order to continually monitor parameters including body temperature, blood pressure, heart rate, blood glucose level, and blood oxygen level, patients would wear medical sensors [4]. Data from additional sensors will be utilised to track patient behaviours in their homes. Information will be collected locally and sent to distant medical facilities so they can do enhanced remote monitoring and, if necessary, take quick action. When such heterogeneous sensors are connected, a complete picture of health data might be produced, allowing medical personnel to intervene when situations are detected that could lead to

Additionally, the accessibility of big data gathered from a large number of patients provides an unmatched chance to investigate connections, create models and tools for early detection and therapy, and improve the efficiency and effectiveness of drug discovery. Similar reasons apply to the aged and the disabled since continuous, unobtrusive monitoring enables better, more responsive/predictive treatment, preserves patient independence, and relieves hospital resources. Additionally, remote supervision makes it easier to share experts with more people and patients, which reduces the cost of care [3].

* 1. **Transportation system:** Utilising cutting-edge sensor, information, and network technologies, the intelligent transportation system will offer effective transportation control and management. Transportation law enforcement, mobile emergency command and scheduling, vehicle rule violation monitoring, reducing environmental pollution, anti-theft system, avoiding traffic jams, reporting traffic incidents, smart beaconing, minimising arrival delays, and many other interesting features can be found in intelligent transportation.

All kinds of metropolitan transport, including automobiles, trains, buses, and bicycles, are increasingly outfitted with sensors and/or actuators, creating a network of mobile sensors. Transported commodities, as well as the roads and railroads they travel on, are all outfitted with tags and sensors that provide vital data to traffic control centres. This enables not only the tracking of the progress of the products being carried, but also the development of novel solutions, such as improved traffic routing for transportation vehicles or giving tourists the necessary transit information.

Furthermore, external sensor devices that track particular physical characteristics like temperature, humidity, and pollution may be added to cars. Thus, the idea of "smart vehicles" begins to take shape. If data is correctly gathered and provided, it can help to make road transit more intelligent, safe, and environmentally friendly [3]. Driving advice that focuses on eco-efficiency for public transport and lowering fuel consumption and pollution levels, for instance, can be given. Users' data is used by mobile applications like Google Traffic to track traffic conditions. Smart traffic signal systems can be utilised to make driving and cycling in cities safer and more convenient for drivers and passengers. For instance, integrating information from riders' smartphones and traffic information received from various types of sensors placed in the traffic light infrastructure of a city may allow for an intelligent traffic light orchestration.

# Retail and Logistics

Implementing IoT in retail/supply chain management offers various benefits, including tracking products for traceability reasons and monitoring storage conditions along the supply chain, as well as processing payments based on location or time for activities like riding public transportation or visiting theme parks. IoT offers a variety of applications in the store itself, including automated check-out using biometrics, fast payment options, the ability to identify potential allergens in a given product, and the ability to rotate products in shelves and warehouses to automate the restocking process. The IoT in logistics includes tracking every step of the physical movement of goods from suppliers to demanders to ensure their quality of shipment conditions, item location, fleet tracking, container openings for insurance purposes, search for individual items in large surfaces like warehouses, and warning emission on containers storing flammable goods close to others containing explosive material [3].

**Smart Energy**

A more modern type of intelligent power system known as the "smart grid" can increase energy efficiency, lessen environmental effect, increase the safety and dependability of the electrical supply, and cut down on grid-wide electricity transmission. Through the installation of energy sensors, the integration of IoT technology in smart grids may assist in implementing fault detection and monitoring as well as consumption monitoring [13]. Other sets of similar solutions plan to regulate the heat and energy in buildings and houses to achieve a goal of energy savings. The energy efficiency and competitiveness of manufacturing firms at the level of energy production may be enhanced by using IoT technology to gather data on energy usage.

**Facilities Energy Management**: This programme, which combines operational technology, information systems, and sophisticated metering, can track, report, and notify operational employees in real time. These management systems have a large capacity for enabling dynamic visibility into the functioning of buildings and other facilities. Additionally, they can offer dashboard views for different levels of energy usage, different levels of granulation, and allow data flows from a variety of building equipment and other subsystems.

**Home Energy Management(HEM):** Using energy management, a room's temperature and lighting may be adjusted according to the occupancy, the time of day, the weather outside, and the cost of the utility. It optimises the generation and use of domestic energy. Applications that analyse energy consumption levels are included in the HEM system, as well as energy management sensors that are linked to a home area network and react to a fluctuating power supply to optimise energy. A combination of these strategies can help lower total energy use and greenhouse gas emissions from residences. The Internet of Things is also beneficial in identifying and preventing thefts [3] and may be used to remotely operate household equipment.

**Smart Agriculture**

A network of various sensors may gather data, process it, and alert the farmer via communication infrastructure, such as text message on a mobile phone, about the area of the farm that needs special care.

۷

Smart packaging for seeds, fertiliser, and pest control products that reacts to particular local conditions and signals activities may fall under this category. By having the information of the land conditions and climatic variability, intelligent farming systems will aid agronomists in having a better grasp of the plant development models and having effective farming practises. By avoiding the unsuitable farming circumstances, this will considerably boost agricultural production. The Internet of Things (IoT) plays a role in water management by analysing whether water from rivers and the sea is suitable for use in agriculture and as drinking water, detecting liquid presence outside tanks and pressure fluctuations throughout pipes, and monitoring changes in water level in rivers, dams, and reservoirs.

# Environmental Monitoring

Using of wireless identifiable devices and IoT technologies in environmental conservation and other green applications are one of the top most promising market segments in the future. There will be an increased usage of these devices in environmental friendly programs in worldwide, like bio-monitoring, remote sensing, soil monitoring, water monitoring and air quality monitoring. IoT can be used to advance environmental programs, including the collection of recyclable materials for the reuse, the disposal of electronic waste (RFID used to identify electronic subcomponents of personal computers, mobile devices and other consumer electronics products to increase the re usage of these sub parts and to reduce e-waste). The control of CO2 emissions from companies, pollution from autos, and poisonous gases produced by farmers are all highly essential IoT applications. Monitoring combustion gases and anticipating fire conditions to establish alarm zones are two methods of detecting forest fires. Weather monitoring: keeping an eye on factors including pressure, temperature, humidity, and wind speed, Early earthquake detection, Water quality monitoring can help reduce water pollution by keeping tabs on the discharge of garbage and dangerous chemicals into rivers and the ocean. It can also help preserve the quality of water supplied for drinking. River Floods: Monitoring changes in water levels in rivers, dams, and reservoirs on days when it rains, Wildlife protection: GPS/GSM tracking collars are being used to find, monitor, and SMS-communicate the coordinates of wild animals.

# Security & Emergencies

IoT technologies are becoming increasingly prevalent in the fields of security and emergency. A few examples include perimeter access control, liquid presence, radiation levels, and explosive and dangerous gases. The perimeter access control is used for a variety of tasks, including monitoring places, keeping track of people and assets, maintaining infrastructure and equipment, alerting, and more. In order to avoid breakdowns and corrosion, liquid presence is used to detect liquids in data centres, warehouses, and sensitive building grounds.

The final IoT application is used to detect the gas levels and leaks in industrial settings, around chemical industries, and inside mines. The radiation levels application is used to measure the radiation levels in nuclear power stations surrounds to create leakage warnings. By detecting vibrations or other natural catastrophes, the integration of sensors and their autonomous coordination and modelling will assist to anticipate the onset of earthquakes and tsunamis and to take the necessary precautions in advance [3].

**Practical System in IoT**

The Tsunami Detection System is a real-world IoT application that is described [3]. This device helps with early tsunami warning by continuously monitoring the water level in Japan. In this system, a significant number of buoys with sensors and miniature earth stations will be placed all across Japan. While the tiny ground stations transmit the sensor data to the satellite, the sensors are utilised to measure the variation in wave height. The deployment of multiple sensor terminals is required to cover the whole country of Japan and detect a tsunami as early as feasible.

Due to the base station's remote location, it is challenging for ground-based wireless networks to communicate the sensor data collected directly to the base station when the sensor terminals are widely dispersed.

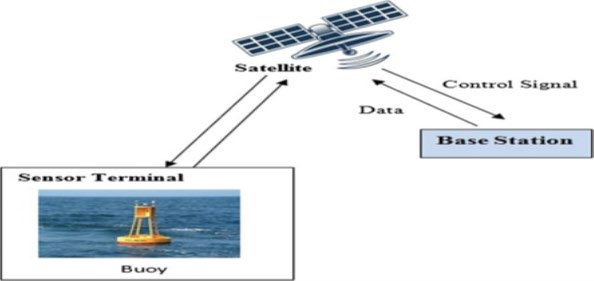


Figure. 3: Tsunami detection system

As a result, in this system, data is transmitted by satellite from the sensor terminals to the base station. It is feasible to gather data from sensor terminals placed all across Japan since the satellite has a wide coverage area. Figure 3 depicts the building of the tsunami detecting system. In this system, the GPS is utilised to measure how the Z-axis location has changed using the sensors. The shifting of the Z-axis suggests a shifting of the sea level. To differentiate the tsunami from regular waves, the recorded data is transmitted by satellite to the base station, where it is analysed. As a result, the base station is capable of detecting tsunamis.

# Challenges and Opportunities

Regardless of a user's location, area, or level of economic development, we think that the Internet should be a source of empowerment for everyone and that the whole set of skills and values that underpin our existence and the success of the Internet hold true everywhere. The same can be reasonably anticipated to apply to the IoT's prospective advantages and difficulties. The Internet of Things (IoT) poses several new legal and regulatory issues in addition to perhaps escalating current Internet-related problems. Developing rules and regulations must prioritise fostering people' capacities for communication, innovation, sharing, choice, and trust. But in this part, we give a brief introduction of key subjects that are commonly brought up in connection with IoT: security, privacy, interoperability, and standards, as well as legal, regulatory, and rights issues. We start by analysing these challenges, outlining critical elements of each one, and putting out a number of discussion-worthy topics.

# The IoT Security Challenge

In order to facilitate the widespread use of IoT technology and applications, security is a crucial component. The key stakeholders are unlikely to embrace IoT solutions widely without assurances about system-level secrecy, authenticity, and privacy[13]. People are less likely to utilise the Internet if they don't think their linked gadgets and personal information are suitably safe from abuse or danger. In fact, the industry should consider guaranteeing security in IoT devices and services a key priority. There are more chances to take advantage of possible security flaws as we link items to the Internet on a larger scale. IoT devices with weak security might be used as entry points for cyberattacks since they make it possible for hackers to reprogram or break a device.

Devices with poor design might leave data streams unprotected, making user information vulnerable to theft. Device failure or malfunction can potentially lead to security flaws. The IoT's small, affordable, and pervasive smart gadgets face the same or even more severe issues as the computers that have historically served as the Internet's connection endpoints. IoT device makers have technological and cost-competitive limitations that make it difficult to include proper security measures into these devices, potentially leading to security and long-term maintainability vulnerabilities that are worse than those of traditional computer systems.

The significant growth in the quantity and variety of IoT devices might expand the opportunity for attack in addition to any security design flaws. Every insecure device linked to the Internet has the potential to damage the security and resilience of the Internet globally, not just locally, given the highly interconnected nature of IoT devices. We need IoT devices to be safe as we grow more connected and reliant on them for vital services, but we also understand that no device can be completely secure. Some IoT devices are likely to be installed in locations where achieving physical security is challenging or impossible. IoT gadgets might be physically accessible to attackers.

The way security issues are identified and addressed has an impact on the IoT's overall security and resilience. The chance that a gadget will be hacked determines how secure it is. This risk assessment and mitigation calculation is influenced by a number of variables, such as having a clear understanding of both the current and potential future security risks, the estimated financial and other costs of harm that would result from the risk realisation, and the estimated cost to mitigate the risk.

Experts recommend a few internet of things security solutions. The IoT devices that require direct connection to the internet should first be divided into separate networks with limited access. It will then be simpler to keep an eye out for any unusual traffic on a device's network section. Companies must enhance their data privacy and security practises. At the corporate level, security infrastructure provision should be funded. The security risk may be significantly reduced by teaching regular people and corporate workers how to secure their IoT devices.

# IoT Privacy

Privacy outlines the conditions under which information about specific users may be accessed. The primary factors that make privacy a key IoT need are the technology employed and the envisioned IoT application areas. The most notable application area for IoT technology is in the field of health care, where a lack of proper privacy protections for sensitive and/or personal data has accelerated IoT growth. Additionally, wireless communication technologies will play a significant part in the IoT concept. The widespread use of wireless technology for data exchange may create new privacy-related problems. In fact, the remote access capabilities of wireless channels make them more likely to be violated since they might leave the system open to eavesdropping and disguising attacks[13].

Additionally, the characteristics of IoT devices and how they are utilised reframe the privacy argument since they significantly alter how personal data is gathered, examined, used, and protected[14]. When the people being tracked by IoT devices have different privacy expectations than the data collector regarding the scope and use of that data, IoT data collection and usage becomes a privacy concern. The user might not be aware that an IoT device is obtaining information about them and perhaps disclosing it to outside parties. Devices used by consumers, such as smart televisions and video gaming consoles, are increasingly using this form of data collecting.

These devices contain speech recognition or vision features that continually listen to conversations or look for movement in a space and then transfer that information selectively to a cloud service for processing, which occasionally involves a third party. Unaware that their activities or conversations are being recorded, a person may be in the vicinity of these types of devices. A user who is aware of these capabilities may find them useful, but others who are uninformed of the devices' presence and have no significant control over the way that information is utilised may be concerned about their privacy.

These instances demonstrate the importance of these personalised data streams for businesses and organisations looking to gather and profit from IoT information, regardless of whether the user is aware of and consents to having their IoT data gathered and analysed. The need for this information highlights the statutory and regulatory difficulties that data protection and privacy regulations face.

People generally understand that their privacy is fundamentally valued and have expectations around the kind of information that may be gathered about them and the potential uses for that information. This broad principle of privacy is valid for data gathered by IoT devices, but such technologies may make it more difficult for users to express and enforce their privacy choices. Therefore, privacy is a genuine unresolved issue that might hinder the growth of the IoT.

# IoT Interoperability/ Standards

Device interoperability may promote innovation and provide producers of IoT devices efficiency, boosting the market's total economic value. The most fundamental core value of the internet is interoperability; the first need for Internet connectivity is that "connected" devices must be able to "talk the same language" of protocols and encodings. Internet users may not be able to connect, converse, share, and innovate—all essential components of interoperability—if barriers are purposefully built to prevent the sharing of information.

Any IoT device would be able to connect to any other device or system and share information as needed in a completely interoperable ecosystem. IoT device and system interoperability occurs to differing degrees at various stages of the communications protocol stack between the devices. The core of the IoT interoperability debate is the standardisation and acceptance of protocols that define these communication specifics, including where it is ideal to have standards. The consequence of a lack of standards and best practises documentation goes beyond only restricting the potential of IoT devices.

Lack of these standards might, in a passive manner, encourage undesirable behaviour in IoT devices. The networking resources they link to on the Internet as a whole, as well as these devices, may suffer if they are poorly designed and configured[14]. In addition to the technological considerations, interoperability has a huge impact on the potential economic impact of IoT. Incentives for innovation and cost savings for IoT device makers may be gained by well-functioning and well specified device interoperability, raising the market's total economic value. Additionally, the use of current standards and, if appropriate, the creation of new open standards, remove entry barriers, enable new business models, and promote economies of scale.

# Technical and cost constraints

Innovative processing and communications technologies may now be fitted into extremely small things thanks to manufacturing advancements. This, together with improved computer costs, has accelerated the development of compact, low-cost sensor devices, which power many IoT applications. IoT device adoption is growing, and with it is the amount of traffic that these devices produce. In order to store the enormous quantity of data needed for analysis and further ultimate storage, network capacity must be increased, which presents another difficulty. The collection, correlation, and analysis of enormous amounts of data are made possible by new algorithms and the rapid advancements in computer power, data storage, and cloud services; these massive and dynamic datasets open up new possibilities for knowledge extraction.

Technical, time-to-market, and financial restrictions are built into IoT device design from the outset when manufacturers create these connected objects. Technical limitations on some devices, such as low internal processing power, memory requirements, or power consumption requirements, place restrictions on their functionality. Similar pressure is placed on manufacturers to minimise the cost per unit of the device by reducing the expenses associated with part and product design. When deciding whether to implement standards, manufacturers conduct cost-benefit studies to determine whether the increased expenses and potential reduction in product performance are worthwhile. It can be more expensive in the short run to incorporate interoperability features into a product and test it to ensure that it complies with a standards specification.

In some situations, using exclusive protocols and systems may be the cheapest route to market. However, this needs to be contrasted with the advantages provided by interoperability for the long-term product lifetime. The IoT requires billions of batteries to function, which poses a serious risk to the environment because many gadgets won't be properly disposed of after usage. As an alternative, energy harvesting, which turns environmental energy sources into electrical energy (such as vibration, light, and temperature), might replace current energy-efficient technology standards. These gadgets could serve as long-term replacements because they have recently been proved to function just as well as their battery-powered equivalents.

# Regulation and Policy Issues

IoT device applications provide a wide range of regulatory and legal difficulties and questions that require careful study. In addition, technology is developing more quickly than the corresponding legal and policy frameworks. The IoT raises a wide range of legal, regulatory, and rights challenges. IoT devices both magnify and generate a number of new legal and regulatory issues that weren't previously there. For instance, IoT device accessibility requirements for people with disabilities provide new issues when new categories of IoT devices are introduced while still being compliant with current accessibility standards and guidelines.

On the other side, the enormous number of wireless IoT devices and the radio frequency interference and noise they cause is an illustration of how IoT devices exacerbate the problem of currently controlling the usage of the RF spectrum. IoT devices are facing new legal and regulatory hurdles as a result of concerns about intellectual property issues, environmental concerns (like disposing of gadgets), and legal ownership of devices. Determining where in an IoT system architecture is the ideal location to accomplish the desired objectives is in addition to the difficulty of choosing the right regulatory or policy measures for IoT concerns.

More and more, consumer protection laws and regulations, as well as general, technology-neutral legal perspectives, are used to analyse IoT device restrictions. Informing judgements on privacy and security, among other things, may be done by analysing the legal implications of IoT devices from the standpoint of prohibiting unfair or deceptive practises against customers. IoT devices can occasionally give rise to new legal, regulatory, and civil rights problems that did not previously exist[15].

# IOT Data Protection

IoT devices may not be restricted from sending data across national boundaries. The Internet, which crosses all levels of territorial boundaries, is the communication medium used by these gadgets. IoT devices generally have minimal or no technological hurdles for collecting data on individuals in one country and transmitting that data to another territory for data storage or processing. If the information gathered is considered to be sensitive or personal information and is covered by data protection rules in several different countries, for instance, this might rapidly turn into a legal issue. These circumstances are referred to as cross-border data flows, and they raise concerns regarding the potential applicability of legal restrictions. Which legal system, then, regulates both the equipment collecting the data and the storage and use of the data collected? A few questions are also raised by this circumstance. Can these regulations be changed to lessen the amount of Internet fragmentation they bring about while still upholding user rights? Should a territory be allowed to impose its stricter data protection regulations on other jurisdictions in order to handle and transmit specific IoT-enabled data? These gadgets will eventually be able to automatically link to other gadgets and systems and communicate data across boundaries without the user's awareness.

This might lead to circumstances in which a user is held responsible for cross-border data flow obligations without being aware of them. As technology continues to advance faster than legislation, these are complicated problems that will only get more so[15].

# IoT Device Liability

IoT devices operate in a more complex way than a simple stand-alone product, which suggest more complex liability scenarios need to be considered. For example: IoT devices are likely to be used in ways never predicted by the manufacturer. An IoT device manufacturer cannot reasonably perform product assurance testing on all possible use cases of IoT devices. There is the potential for IoT devices to connect and interact with other IoT devices in untested and unforeseen ways. As interoperability of these devices increases, they may be able to form ad hoc network connections among themselves. Therefore, it is difficult for a manufacturer or user to account for all potentially harmful scenarios in advance of deploying these devices.

IoT devices will be integrated into autonomous systems like driverless cars, which incorporate adaptive machine-learning algorithms to control their behavior based on sensor inputs from IoT devices. The actions of these systems cannot be fully known and tested in advance[15].

These scenarios and others raise questions. If harm results from one of these scenarios, do existing liability laws adequately address legal responsibility and clarify the liability exposure of parties involved? Do liability laws need reconsideration for intelligent IoT devices that learn from their environment and modify themselves over

time? If autonomous systems are instructed by the end user rather than by their internal algorithms, what happens in cases of user error? Should IoT devices be smart enough to have a “do what I meant” instruction? To what extent will current liability laws for conventional products extend to products that become Internet-enabled? What can we as a community do to better inform legislators and policy makers, so that they are not as susceptible to the vast amounts of misinformation and biased advice they are receiving?

# Conclusion

The IoT describes the billions of connected devices that exist in an increasingly networked society, pervading smart homes, workplaces, healthcare, logistics and retails, Transportation, industries and smart cities. The opportunities afforded by this technology are huge, connecting machine to machine, humans to their environments and allowing analysis of the world at new levels of detail. Whilst these opportunities are significant, they are accompanied by risks to society and its infrastructure. This book covered several key points related to IOT including technology, security, privacy, interoperability and standardizations, regulations and legal policy, and global issues. Cyber-attacks on IoT devices are inevitable and the resilience of devices and networks must be carefully considered. Separation of valuable network assets may be the best way to protect them from attacks.

In a constantly developing world of apparent ubiquity and a pervasive network of interconnected things, the development of new techniques and enablers in the area of communication/middleware systems, high-performance embedded and computing technologies and WSNs amongst others will be necessary. The standardization of the IoT communication protocols and technology enablers cannot be exaggerate.

More importantly, the issues of security, privacy, vulnerability management and interoperability should be prioritized in any IoT design, build and implementation as this is, without any doubt, the biggest concern with the proliferation of the IoT in the modern era.

The legacy of devices is important when they are placed into environments for long periods. They must be resilient in terms of security, power supplies, software and hardware, but also remain interoperable with IoT devices of the future. Devices should be ‘secure by default’. Owners of IoT devices, the networks they are hosted on and the data they generate need to be accountable when problems occur, especially as artificial intelligence and machine learning becomes more commonplace. Device users should understand the choice they make when they agree to providing their data to service providers.

Society needs to reconsider legislation and regulation in a networked society to take account of the data generated by IoT devices and the power it gives to those that possess it. More transparency of who collects data and what it is used for should be provided to device users. Industry is likely to drive for standards in the IoT faster than government can legislate. The public sector may drive the creation and adoption of standards through procurement policies. The dynamic nature of IoT has challenges and concerns to be addressed. We also get an indication of the important aspects that need to be further studied and developed for making large-scale deployment of IoT a reality.

# References

1. Darrell M. West, “How 5G technology enables the health internet of things”, Center for technology innovations at Brookings, July 2016.
2. D. Warren, C. Dewar, , "Understanding 5G: Perspectives on future technological advancements in mobile", GSMA Technology GSMA Intelligence Dec.2014.
3. D.P. Acharjya, M. K. Geetha, “Internet of Things: Novel Advances and Envisioned Applications”, Springer International Publishing AG 2017.
4. Keyur K Patel, Sunil M Patel, “ IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges”, International Journal of Engineering Science and Computing, Volume 6 Issue No. 5, May 2016 .
5. “Cloud and Mobile Network Traffic Forecast- Visual Networking Index” *Cisco, 2015*.<http://cisco.com/c/en/us/solutions/service-provider/visual-networking-> indexvni/index.html
6. T. Danova, “Morgan Stanley: 75 Billion Devices Will Be Connected to The Internet of Things by 2020.”, *Business Insider*, October 2013.
7. “Global Connectivity Index.” Huawei Technologies Co., Ltd., 2015. Web. 6 Sept.2015. <http://www.huawei.com/minisite/gci/en/index.html>
8. J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin and D. Aharon, “The IoT: Mapping the Value Beyond the Hype” McKinsey Global Institute,

June2015

1. “Cisco Visual Networking Index: Forecast and Methodology, 2014-2019.” Cisco, May 27, 2015. <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-> ngn-ip-next-generation-network/white-book-c11-481360.pdf
2. GSA, “GNSS Market Report Issue 5,” European GNSS Agency Publications, 2017.
3. T. S. Sri, J. R. Prasad, Y. Vijayalakshmi, “A review on the state of art of Internet of Things”, International Journal of Advanced Research in Computer and Communication Engineering(IJARCCE), Vol. 5, Issue 7, July 2016.
4. C. X. Mavromoustakis, G. Mastorakis, J. M. Batalla , “Internet of Things (IoT) in 5G Mobile Technologies”, Springer International Publishing Switzerland 2016.
5. D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac, “Internet of things: Vision, applications and research challenges”, [Ad Hoc Networks](https://www.sciencedirect.com/science/journal/15708705) [Volume 10, Issue](https://www.sciencedirect.com/science/journal/15708705/10/7) [7](https://www.sciencedirect.com/science/journal/15708705/10/7), September 2012, Pages 1497-1516.
6. D. Bandyopadhyay, J. Sen, “ Internet of Things: Applications and Challenges in Technology and Standardization”, Wireless Pers Commun (2011) 58:49–69, DOI 10.1007/s11277-011-0288-5.
7. K. Rose, S. Eldridge, L. Chapin, “The Internet of things: An Overview understanding the Issues and challenges of a more connected world”, Internet Society(ISOC), Oct.2015.