Unit 1

Introductory Concepts: What is the IoT and why is it important? Elements of an IoT ecosystem, Technology drivers, Business drivers, Trends and implications, Overview of Governance, Privacy and Security Issues.

—----------

IoT: The internet of things, or IoT, is a network of interrelated devices that connect and exchange data with other IoT devices and the cloud. IoT devices are typically embedded with technology such as sensors and software and can include mechanical and digital machines and consumer objects.

Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, deliver enhanced customer service, improve decision-making and increase the value of the business.

With IoT, data is transferable over a network without requiring human-to-human or human-to-computer interactions.

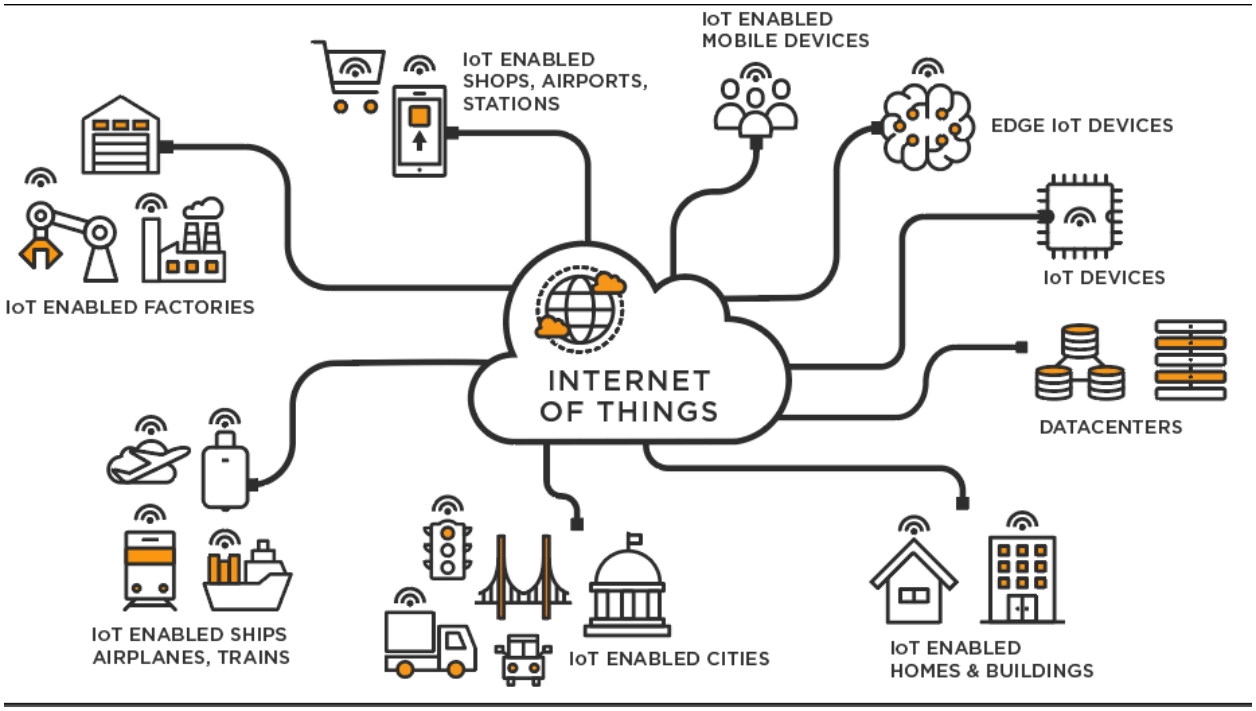
A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low, or any other natural or man-made object that can be assigned an Internet Protocol address and is able to transfer data over a network.

IoT − Key Features

The most important features of IoT include artificial intelligence, connectivity, sensors, active engagement, and small device use. A brief review of these features is given below:

- AI – IoT essentially makes virtually anything “smart”, meaning it enhances every aspect of life with the power of data collection, artificial intelligence algorithms, and networks. This can mean something as simple as enhancing your refrigerator and cabinets to detect when milk and your favorite cereal run low, and to then place an order with your preferred grocer.
- Connectivity – New enabling technologies for networking, and specifically IoT networking, mean networks are no longer exclusively tied to major providers. Networks can exist on a much smaller and cheaper scale while still being practical. IoT creates these small networks between its system devices.
- Sensors – IoT loses its distinction without sensors. They act as defining instruments which transform IoT from a standard passive network of devices into an active system capable of real-world integration.
- Active Engagement – Much of today's interaction with connected technology happens through passive engagement. IoT introduces a new paradigm for active content, product, or service engagement.

- Small Devices – Devices, as predicted, have become smaller, cheaper, and more powerful over time. IoT exploits purpose-built small devices to deliver its precision, scalability, and versatility.



Characteristics of IoT

- Massively scalable and efficient
- IP-based addressing will no longer be suitable in the upcoming future.
- An abundance of physical objects is present that do not use IP, so IoT is made possible.
- Devices typically consume less power. When not in use, they should be automatically programmed to sleep.
- A device that is connected to another device right now may not be connected in another instant of time.
- Intermittent connectivity – IoT devices aren't always connected. In order to save bandwidth and battery consumption, devices will be powered off periodically when not in use. Otherwise, connections might turn unreliable and thus prove to be inefficient.

Desired Quality of any IoT Application

- **Interconnectivity:** It is the basic first requirement in any IoT infrastructure. Connectivity should be guaranteed from any devices on any network then only devices in a network can communicate with each other.

- **Heterogeneity:** There can be diversity in IoT enabled devices like different hardware and software configuration or different network topologies or connections, but they should connect and interact with each other despite so much heterogeneity.
- **Dynamic in Nature:** IoT devices should dynamically adapt themselves to the changing surroundings like different situations and different prefaces.
- **Self-adapting and self configuring technology:** For example, surveillance camera. It should be flexible to work in different weather conditions and different light situations (morning, afternoon, or night).
- **Intelligence:** Just data collection is not enough in IoT, extraction of knowledge from the generated data is very important. For example, sensors generate data, but that data will only be useful if it is interpreted properly. So intelligence is one of the key characteristics in IoT. Because data interpretation is the major part in any IoT application because without data processing we can't make any insights from data. Hence, big data is also one of the most enabling technologies in IoT field.
- **Scalability:** The number of elements (devices) connected to IoT zones is increasing day by day. Therefore, an IoT setup should be capable of handling the expansion. It can be either expand capability in terms of processing power, storage, etc. as vertical scaling or horizontal scaling by multiplying with easy cloning.
- **Identity:** Each IoT device has a unique identity (e.g., an IP address). This identity is helpful in communication, tracking and to know status of the things. If there is no identification then it will directly affect security and safety of any system because without discrimination we can't identify with whom one network is connected or with whom we have to communicate. So there should be clear and appropriate discrimination technology available between IoT networks and devices.
- **Safety:** Sensitive personal details of a user might be compromised when the devices are connected to the Internet. So data security is a major challenge. This could cause a loss to the user. Equipment in the huge IoT network may also be at risk. Therefore, equipment safety is also critical.
- **Architecture:** It should be hybrid, supporting different manufacturer's products to function in the IoT network.

IoT Application

1. **Smart Homes:** Developing smart homes has caused a revolution in designing residential homes. The smart home products would save energy, time and money. A Smart Home would enable the owner to control household jobs at the house even from a remote location. For example, switching on the air conditioner or heaters minutes before reaching home, switching on / off the lights, controlling the washing machine, etc.

Although such smart homes have been implemented, the cost of establishing such homes is still a major restriction that limits its usage.

2. **Wearable Devices:** Wearable devices include wrist watches or glasses that are installed with sensors and software which collect and analyze data. Companies like Google and Samsung have invested heavily in building such devices. These devices broadly cover fitness, health and entertainment requirements. A major challenge for developing such systems is that it should be lightweight, small in size and should have very low power consumption.
3. **Traffic Monitoring:** Vehicles should be capable of optimizing its operation, fuel consumption, pollution control, maintenance and comfort of passengers. A breakthrough will be achieved if such smart traffic could be developed as it would drastically reduce road accident casualties. By installing sensors and using web applications, citizens can also find free available parking slots across the city.
4. **Industrial Internet:** Industrial Internet is the new buzz in the industrial sector, also termed as Industrial Internet of Things (IIoT). It is empowering industrial engineering with sensors, software and big data analytics to create brilliant machines. IIoT holds great potential for quality control and sustainability. Applications for tracking goods, real time information exchange about inventory among suppliers and retailers and automated delivery will increase the supply chain efficiency.
5. **Smart Cities:** Smart city is another buzzword gaining immense interest from the public. Smart surveillance, automated transportation, smarter energy management systems, water distribution, urban security and environmental monitoring all are examples of internet of things applications for smart cities. It will solve major problems faced by the people living in cities like pollution, traffic congestion and shortage of energy supplies etc. Products like cellular communication enabled Smart trash will send alerts to municipal services when a bin needs to be emptied.
6. **Agriculture:** With the continuous increase in world's population, demand for food supply is extremely high. Governments are helping farmers to use advanced techniques and research to increase food production. Smart farming is one of the fastest growing fields in IoT. Farmers are using meaningful insights from the data to yield better return on investment. Sensing for soil moisture and nutrients, controlling water usage for plant growth and determining custom fertilizer are some simple uses of IoT.
7. **Healthcare:** The concept of a connected healthcare system and smart medical devices bears enormous potential not just for companies, but also for the well-being of people in general. Research shows IoT in healthcare will be massive in coming years. IoT in healthcare is aimed at empowering people to live healthier life by wearing connected devices. The collected data will help in personalized analysis of an individual's health and provide tailor made strategies to combat illness.

Importance of IoT

1) More data means better decisions: With added sensors, these devices are able to collect a large amount of data on many different areas.
For example, in addition to the practical elements of being able to know which foods are going out of date in your smart refrigerator, this enhanced household item will be able to give you additional information on its power consumption, temperature, average time of the door spent open and much more. A greater flow of information means that the company behind the device can analyze large trends in the data to better improve the features of the device.

2) Ability to track and monitor things: As well as tracking data for a company to use, it also greatly benefits the user. These devices would have the ability to keep an eye out on the current quality of goods at home. Knowing the state of your items will allow a homeowner to know when they need to replace an item, without them having to consistently check the quality themselves.

3) Lighten the workload with automation: Having a device doing most of the work for you means that you can save more time and cost. Imagine having your fridge order a new carton of milk to be delivered when it reaches a certain level of expiry?
This greatly reduces human efforts. It also results in devices being created that need little to no human intervention, allowing them to operate entirely on their own.

4) Increases efficiency by saving money and resources: As well as saving time for the device owner, it can also result in cost savings. For example, if lights automatically turn themselves off the moment you leave the room, you could save a lot of money on electricity bills.

5) Better quality of life: In the end, all the benefits lead to an increased quality of life. IoT can track devices and orders things, turn light switches off, and help manage important tasks.

Improvements to your lifestyle, health benefits and improved wellness are also part of the IoT future. For example, those that exercise regularly can utilize wearable technology to help them track their heart rate,body temperature, and hydration to stay in shape and monitor their health.

6) Better Decision Making: Since devices have multiple sensors, they can acquire considerable data from numerous sources, giving them more information to work with when acting on data received.

A great example is smartphones. The device automatically tracks your behaviors on its interface and makes suggestions based on your activity, location, and age.

The phone can also keep tabs on various activities. This includes the amount of screen time users spend each day, power consumption, and sleeping patterns. Massive amounts of data are being collected and sent back to smartphone companies each day to improve features on their devices.

With the constant influx of big data, companies begin to see trends in the usage of their devices and can immediately pinpoint their strengths and weaknesses. This insight would not be possible without the help of embedded sensors and processors which analyze the data.

7. Real-time Tracking and Monitoring: The potential for web-based tracking and monitoring systems is enormous. IoT tracking provides an efficient means to track and monitor anything from vehicle fleets, stolen goods, or shipping containers.

Particular devices can even detect changes in the environment. There are multiple industries where IoT trackers can immensely improve the efficiency of companies. A malfunction in these products can lead to enormous losses for the company.

IoT-based trackers need to be reliable to provide the best services. These devices should provide the following:

- **Real-time data analytics:** Fast, accurate data is required in the industry to allow for quick, informed decision-making when assets or changes in the environment are being monitored.
- **Secure communication:** Companies usually track and monitor high-value assets. It is essential that the shared data is protected and not under the threat of hackers.
- **Stable connectivity:** The device should securely provide helpful information on asset locations, machine functionality, and temperatures. This is required at all times and from anywhere on the planet.

8. Automation: A big reason for the invention of IoT is convenience. Smart devices that automate daily tasks allow humans to do other activities. These devices ultimately lighten people's workload. Smartphones allow us to connect with people from all over the world. We can schedule when to send messages and even use dictation to avoid typing ourselves.

Then there are smart fridges. Imagine having one that can detect when foods are about to expire and notify the owner to eat that food before it's too late. Perhaps the smart fridge could even register that the milk is nearly finished and automatically order more.

Another example is a self-driving car, connecting to the Internet to find the quickest route to a destination. This is the ultimate convenience for humans. The room for innovation within IoT is massive.

9. **More Efficient Personal and Business Tasks:** Web-based devices save people money and time. This includes planning work schedules, time tracking, effective communication, and setting reminders for daily tasks.

Disadvantages of IoT

- Security concerns and potential for hacking or data breaches.
- Privacy issues related to the collection and use of personal data.
- Dependence on technology and potential for system failures.
- Limited standardization and interoperability among devices.
- Complexity and increased maintenance requirements.
- High initial investment costs.
- Limited battery life on some devices.
- Concerns about job displacement due to automation.
- Limited regulation and legal framework for IoT, which can lead to confusion and uncertainty.

IoT Ecosystem

When we talk about an ecosystem, we are talking about a complex system of interconnected components and the environment in which they exist and with which they interact.

In fact, all components are connected by energy flow, certain cycles (e.g. nutrient cycles in biology) and their environment. So, the point of connection between all these elements and the environment is very important in an ecosystem. It distinguishes a system from an ecosystem. I.e. the system forms a complex and unified whole, while an ecosystem is closely connected to its environment.

We can use the term IoT ecosystem instead of IoT system because IoT devices have no value without their existing environment. The main benefit that IoT devices bring to people is data. These data are related to environmental conditions or external phenomena but also something within the system. Regardless of the relationship with the environment, all devices are connected to each other. So, the data's final destination is always the people who use it.

These three facts (environment, data, people) lead us to the definition of an Internet of Things ecosystem – a network of interconnected devices existing in a specific environment that collects

data and transmits it to people who use modern technologies. To analyze them to achieve a clear goal like building a smart home.

While different groups of people create different IoT applications for their needs, IoT software development creates many IoT ecosystems. These ecosystems can be a simple network with 20 connected devices like a smart home or a multi-level structure with a complex and extensive network of devices that requires a sophisticated platform to manage all the layers.

The Key Elements of an IoT Ecosystem

IoT devices collect data and transmit it securely to an internet-connected gateway that compresses the data and sends it to them. This data is sent to the cloud for further analysis and then displayed within the app to provide users with meaningful information.
Therefore, we have listed the seven major components of an IoT ecosystem:

- IoT devices
- Security
- Network
- Gateway
- The cloud
- Application
- User

1. IoT Devices: IoT devices are actually the layer of sensors, actuators and smart objects that collect data about the environment and measure physical parameters. Sensors are the perception of the IoT system, whose main function is to extract information from the environment and convert it into data.
In the internet of things ecosystem, it is rare to find only one type of sensor or actuator. Because there are many types of sensors, each type has its subcategories.

So, we want to mention two of the most common and two of the most important sensors for improving the ecological state of the earth:

- Temperature sensors: They are one of the most common and popular. A wide range of industries can use these sensors to measure the temperature of industrial machinery to monitor its condition, to monitor the temperature of a patient continuously, or to monitor the condition of a farmer’s soil. **Subcategories:** Thermocouples, RTDs, Infrared Sensors, etc.

- Proximity sensors: They are a popular IoT device because they save light in thousands of homes with these sensors when no one is around. **Subcategories:** Inductive sensors, Photoelectric sensors, Ultrasonic sensors.
- Water quality sensors – They are particularly important due to ocean pollution. Because these sensors can help monitor water conditions and detect sources of pollution in real time! Sub-categories: residual chlorine sensor, turbidity sensor, pH sensor.
- Chemical sensors – these monitor chemical changes in the air, which is extremely important in large cities where air pollution problems continue to worsen. These sensors are also useful in industrial environmental monitoring, hazardous chemical detection and radioactive detection. **Subcategories:** Chemical Field Effect Transistor, Hydrogen Sulfide Sensor, Potentiometric Sensor.

2. Security: It is the part that includes all the other parts, provides security for data transfer and prevents unauthorized connections outside the Internet of Things ecosystem.
In recent years, we also see that the number of IoT-based DDoS attacks has skyrocketed. Therefore, every IoT system needs a strong level of security that at least protects against the most common vulnerabilities.

The security level has a wide range of responsibilities, such as:

- **Access control to the IoT network:** Anyone who connects to the network has access to all its devices, making broken authentication problems particularly acute. Moreover, IoT devices can also trust the local network so that no further authentication is required.
- **Prevention of data loss during data transfer over the network:** The data must be encrypted through the IoT system using protocols such as AES, DES, DSA and others.
- **Look for malicious software:** Software bugs can sometimes trick attackers into executing their code on the IoT device. Hence the software versions need to be corrected when a vulnerability is found.

The Internet of Things ecosystem is also safeguarded by a number of firmware and security providers, including Azure Sphere, LynxOS, Mocana, Spartan, Forescout, Symantec, etc.

But unfortunately, most Internet of Things vendors and IoT device manufacturers also need to pay more attention to basic security guidelines. They are:

- The device boot process should be protected from running inappropriate pieces of code.
- Cryptographic keys must be used to execute all commands on devices. This is especially important when managing IoT updates.
- All commands and control information must pass through a gateway to avoid direct access to the device outside the network.

- All IoT devices must install security patches whenever a new security flaw is detected.

3. Network: The network is the logistical heart of the Internet of Things ecosystem. The network is also known as the connectivity layer. It is responsible for all communications within the IoT system: connecting smart objects, transferring data and commands between IoT stages, and connecting to the cloud.

There are two means of communication:

1. **The first mode of communication:** Occurs locally in a local area network (LAN) between IoT devices and smart gateways via short-range wireless communication protocols. This communication mode is optional because the sensors can connect directly to the cloud via the Internet using the TCP / IP protocol.
   However, connecting via non-IP protocols consumes less power because the devices connect to local smart gateways instead of trying to access the main server in the cloud.
   So, the most popular short-distance protocols for IoT architecture are:
   - Wireless internet access (WiFi)
   - Bluetooth and Bluetooth Low Energy (or Bluetooth LE for less powerful devices that generate less data)
   - ZigBee – a universal solution that connects all smart devices
   - Near Field Communication (NFC)
   - Radio Frequency Identification (RFID)
   - Sigfox
   - LoRaWAN

If the system needs to cover long distances in the range of miles, it can use Low Power Wide Area Network (or LPWAN) designed for long-distance wireless data transfer.

2. **The second mode of communication:** Occurs when the data of things are transferred to the cloud in cases where there is no smart gateway or in cases of communication between the smart gateways and the cloud. The network layer establishes a connection between the local network and the Internet. The basic protocol here is the IPv6 protocol.

4. Gateways: IoT Gateway is a physical or virtual platform that mediates between IoT devices and the cloud.

There are several main functions of IoT gateways:

- Control the flow of data in the Internet of Things ecosystem. The data flow goes through the gateway from the devices to the cloud and in the opposite direction.

- Ensure the security of the transmission of information in both directions. Also, transmit commands from the cloud to IoT devices.
- Preprocess data before sending it to the cloud. Gateways filter, aggregate, synthesize, and aggregate traffic from different devices.
- Save energy from IoT devices as communication over the internet is energy-intensive, unlike low-energy technologies such as Bluetooth Low Energy (it is a wireless personal area network technology designed and marketed by the Bluetooth Special Interest Group aimed at novel applications in the healthcare, fitness, beacons, security, and home entertainment industries).
- Reduce response latency to IoT devices. Some devices require a real-time response from the system.

5. The Cloud: The cloud is a computing resource responsible for storing, analyzing, and managing data. In other words, it is a group of computers that people access over the Internet to use their computing power for a particular purpose.

The cloud is where a large pile of raw sensor data is converted into neat little piles of valuable information. The cloud can be powered by analytics software, visualization tools, AI, and machine learning for in-depth data analysis and processing. And the most popular cloud computing providers are Microsoft Azure and AWS IoT.

Surprisingly one of the main advantages of the cloud solution is that it is easily scalable. It is an essential requirement for building an effective IoT system.

6. Application: When software development companies build software products for the IoT ecosystem, they will cover all seven components. And will create a system that covers all the requirements at every level.

Application is used to interact with the users with the Internet of Things ecosystem. This interaction is only made possible by the graphical user interface, where the users can consult analyses reports, control the system and manage devices.

The list of technologies used in the development includes:

- Programming languages: C/C++, Python, Ruby, JavaScript
- Development frameworks: Node.Js (Node-Red for rapid prototyping), OT, IoT.js, Device.js, Eclipse IoT (Kura, SmartHome), AngularJS
- Third-party APIs: Google Assistant, Google Home (Actions on Google), Google Vision, Apple HomeKit, MI Light, Cortana, Alexa Voice Service, Philips Hue, Android Things

7. Users: Its users are the most important component among the seven components of the Internet of Things ecosystem.

Here, users have two roles:

They use an IoT ecosystem for their needs. Here, the possibilities offered by the Internet of Things ecosystem are becoming a valuable database for all types of users. For example, sensors and IoT applications can become professional healthcare assistants that measure the patient's biometry. This will help to make a more accurate diagnosis.
Secondly, the Internet of Things ecosystems should serve people. And meet their needs, and provide information that assists them in achieving their goals. Moreover, focusing on people's needs, the IoT ecosystem was built by and for people. So, the users determine what the IoT ecosystem will do and won't.

Users can be:

- People who use IoT gadgets for personal use
- Researchers
- Personnel (doctors, warehouse workers, carriers, engineers, etc.)
- Stakeholders and top managers

Technology Drivers

Its potential to redefine our lives is simply unexplainable. For instance, heart patients continuously need to visit their cardiologist so they can record their heart rate and perform related tests. However, with IoT, these patients can quickly provide their physician with hourly updates even without needing to make a trip to the clinic. They can wear an IoT-connected heart monitor that allows their physician to assess the information periodically and suggest the right course of treatment.

For such to happen and for IoT to assume its position as a potent force, it needs support from various technological developments. What these technologies need to do primarily is not to necessarily support the IoT, but instead as they advance, they are subsequently going to massively boost IoT innovation as a whole.

Herein are five different technologies that are driving the development of IoT.

1. **Cloud Computing**: IoT is set to produce a significant data volume, and as such, you will need some considerable space to not only process but also store this data, and this is where Cloud computing comes into play.
   Cloud computing is the only technology that boasts the potential to quickly and faultlessly process such a significant volume of data. For instance, where numerous smart devices transmit crucial health data to physicians from across the globe, enormous data volumes are produced. Unsurprisingly, only the cloud can process such masses of data effectively.
   Several significant developments in innovation have rendered cloud computing among the most potent IoT drivers. Identity management platforms are one such solution to offer data security.
   What's more, the cloud is gradually becoming more scalable and efficient. In efforts to leverage these benefits, there are numerous cloud-based platforms under development. This will ensure easier exchange of data between multiple platforms since IoT is not exclusively confined to desktops, laptops or even mobile devices.

2. **Marketing Automation:** IoT has the potential to offer a substantial volume of information on customers, such as their hobbies, preferences or even what devices they use. International companies can find such data more than valuable as it can help them customize and sell their products and services to fit their market. IoT can also effectively help such firms to generate customer-focused items.
   Currently, software developers are working to produce marketing automation software which can automate marketing procedures such as customer segmentation, integration of customer data, as well as campaign management. Moreover, there is a massive investment going towards creating intelligent marketing automation systems which can utilize the vital information provided by IoT devices.
   IoT is well-equipped to provide actionable and vital customer data needed by intelligent (marketing automation) applications. Both IoT and marketing automation can be defined as mutually dependent.

3. **App Technology Boom:** App technology is yet another critical component in the development of IoT solutions. The recent emergence of app innovation has drastically been scaling up the rate at which IoT is developing.
   Generally, apps allow data exchange between various devices. In essence, they offer virtually everything that IoT offers. Apps have been vital for the development of IoT, and their relevance can best be captured through several examples including:
   - Parking apps that can check all available parking spaces within a city.
   - Noise monitoring apps that identify certain sound decibels in otherwise sensitive areas like hospitals and schools.

- Structural assessment apps, which can monitor the state of materials and vibrations in both buildings and bridges.

4. **IPv6:** IoT will facilitate the interconnection of millions of devices. Undoubtedly, all these devices will need IP addresses. IPv4, which is currently the most popularly used internet protocol, cannot cope with the subsequent demand surge for IP addresses. Furthermore, IPv4 has particular concerns that can hinder the progress of IoT, as can other security threats. IPv4 is not the most secure internet protocol, and considering the volume of confidential data that will be shared through IoT, it can be a risky option.
   But with IPv6, which is IPv4's newer successor protocol, all these concerns are adequately addressed. Besides this, it also comes with multiple added benefits including the fact that to address a device, it offers four times more bits on the internet. With these extra bits, you can enjoy about 3.4×1038 address combinations. As such, it can accommodate virtually all space allotment requirements.
   Furthermore, IPv6 enables direct connection between hosts over the internet although it depends on the firewall policies and security of an organization. With IPv6, devices can remain connected via the same IP address notwithstanding whether it is roaming in another area. Finally, IPv6 comes with an optional feature known as IPSec for more secure connection between devices.

5. **Sensors:** Several factors make IoT outstanding, and one of such is inter-device interaction notwithstanding their technological affiliations. Sensors which are fitted in these devices allow them to interact with multiple devices smoothly and effortlessly.
   Sensors are among the core components of IoT. For instance, to unlock your main door, the key's sensor can open it, which instantly transmits a message for your lights to switch on and your thermostats to regulate the temperature in the house. All these activities happen simultaneously.
   The science behind IoT sensor design is similar to how microprocessors work. They use the lithography procedure that ensures that various sensor copies are rolled out concurrently. However, IoT can only perform a particular task. You can subsequently pair a microprocessor and a typical IoT sensor and attach it to wireless radios to communicate.
6. **Blockchain:** One of the key technologies that are driving the development of IoT solutions is blockchain. Putting together IoT solutions along with blockchain technology can be highly beneficial for organizations and their customers as it ensures that data is reliable, authentic, and genuine. For instance, IoT devices are used by supply chain and logistics companies for tracking goods, each product/component may be assigned a digital id which helps in smooth movement and transportation of goods. In addition to this, with the help of the unique digital id, they can maintain tamper-proof and secure blockchain repositories maintaining a proper history about the product. Organizations and

customers can be assured that the products are exactly as described and the information is not tampered with. It is important for organizations to integrate both the technologies to gain a competitive advantage in the industry and an IoT development company could help your organization with this integration.

7. Artificial intelligence: Now that we understand that IoT solutions are focused on connectivity and sensors, we also understand that these technologies generate a huge amount of data which would require advanced data analytics. Artificial intelligence combined with IoT solutions would help businesses analyze the huge amount of data collected by IoT apps and devices and would help in generating important insights.

   Internet of things was a relatively new concept sometime back and there were various speculations around how it will be implemented across industries but during the outbreak of the global pandemic, we witnessed how IoT helped businesses across industries to operate and grow simultaneously. These technologies that we discussed not only are driving IoT development but also help in expanding the scope of these IoT solutions and pushing it to greater heights. IoT solutions are picking up pace across the industries and future advancement in these solutions will play an important role in the coming wave of digital transformation.

Business Drivers for IoT

The Internet of Things (IoT) has become a transformative force across various industries, driven by a range of business needs and opportunities. Here are some key business drivers for adopting IoT:

- **Operational Efficiency:**
  - IoT enables real-time monitoring, automation, and optimization of processes, leading to increased operational efficiency.
  - Businesses can streamline workflows, reduce downtime, and improve resource utilization through the deployment of IoT devices.
- **Cost Reduction:**
  - By leveraging IoT for predictive maintenance and monitoring, businesses can reduce maintenance costs and avoid unexpected downtime.
  - Energy efficiency gains and optimized resource utilization contribute to overall cost savings.
- **Data-Driven Decision Making:**
  - IoT generates vast amounts of data that can be analyzed to gain valuable insights.
  - Businesses can make informed decisions based on real-time data, improving strategic planning and operational responsiveness.
- **Improved Customer Experience:**

    - IoT enables the development of smart, connected products and services, enhancing the overall customer experience.
    - Personalized offerings, remote monitoring, and proactive issue resolution contribute to increased customer satisfaction.
- **Innovative Business Models:**
    - IoT facilitates the creation of new revenue streams through innovative business models.
    - Subscription services, pay-per-use models, and data monetization opportunities arise from IoT-enabled products and services.
- **Supply Chain Optimization:**
    - IoT provides visibility and traceability across the supply chain, improving inventory management, logistics, and demand forecasting.
    - Enhanced supply chain visibility reduces lead times and minimizes disruptions.
- **Quality Improvement:**
    - IoT sensors and devices can monitor and ensure the quality of products in real-time.
    - Early detection of defects or deviations from quality standards leads to improved product quality and reduced waste.
- **Compliance and Safety:**
    - IoT helps businesses monitor and enforce compliance with safety regulations and industry standards.
    - Enhanced safety features and real-time monitoring contribute to a safer working environment.
- **Asset Tracking and Management:**
    - IoT enables businesses to track and manage their physical assets more effectively.
    - Improved asset visibility, utilization, and maintenance lead to better resource management.
- **Environmental Sustainability:**
    - IoT supports sustainable practices by optimizing resource consumption, reducing waste, and promoting energy efficiency.
    - Businesses can demonstrate environmental responsibility and meet regulatory requirements.
- **Market Differentiation:**
    - Adoption of IoT technologies can set businesses apart from competitors, providing a competitive advantage.
    - Offering smart, connected products can enhance brand perception and attract tech-savvy consumers.
- **Predictive Analytics and Maintenance:**
    - IoT enables the implementation of predictive analytics to anticipate equipment failures and schedule maintenance proactively.

    - This helps in reducing downtime, extending equipment life, and optimizing maintenance costs.
- **Remote Monitoring and Management:**
    - IoT allows businesses to remotely monitor and manage assets, facilities, and operations from anywhere in the world.
    - This capability is especially valuable for businesses with distributed operations.
- **Partnerships and Ecosystems:**
    - IoT fosters collaboration and partnerships between businesses, creating ecosystems where interconnected devices and services work together for mutual benefit.
    - Collaborative ecosystems enable innovative solutions and value creation.
- **Digital Transformation:**
    - IoT is a key enabler of digital transformation, helping businesses evolve and adapt to the digital age.
    - Embracing IoT is often a fundamental part of broader digital transformation initiatives.

Ultimately, the specific drivers for adopting IoT will vary across industries and individual businesses, but the overarching goal is often to leverage connected technologies to drive efficiency, innovation, and competitive advantage.

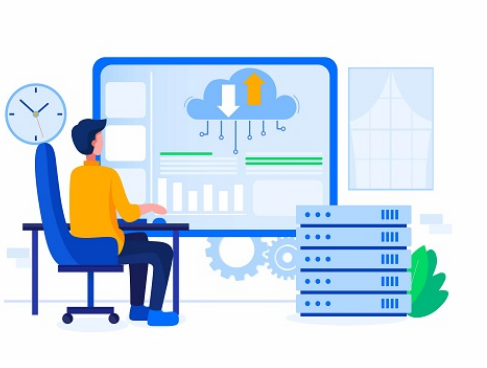
Trends And Implications Of IoT

1. **Blockchain:** One of the latest Internet of Things (IoT) trends is the increased adoption of blockchain technology. It can help in ensuring data security in IoT devices and enables thriving interaction between various network nodes and assures safe record keeping, and that is the reason Blockchain is a great fit for IoT applications as they are also distributed by nature.

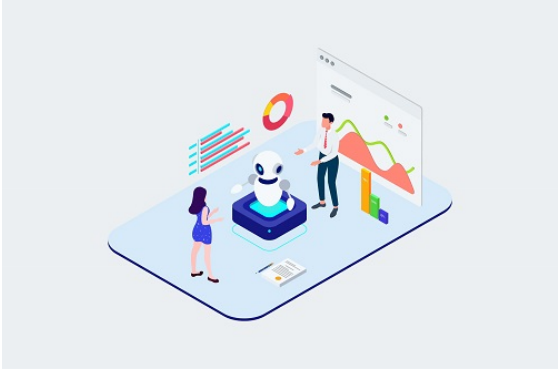
2. **Smart Cities:** When talking about emerging technologies in the internet of things (IoT), smart cities always take a leap ahead. Several governmental institutions in the past five years have begun IoT technology projects that will reshape whole cities.
   The government will be capable of implementing different intelligent solutions using enormous amounts of data for varied issues like citizen safety, energy utilization, traffic congestion, sustainable development, and more.

3. **IoT Powered with 5G Technology:** 5G technology is not only a new age of wireless technology, but it is also a foundation to deliver the full potential of IoT, therefore transforming technological growth.
   No doubt 5G technology is one of the most significant internet of things (IoT) emerging technologies in the year 2022 because strong connectivity will result in more trustworthy performing IoT devices. Lower latency, network slicing, real-time data processing, extensive coverage, and real-time data processing are some things that 5G will bring to the table.

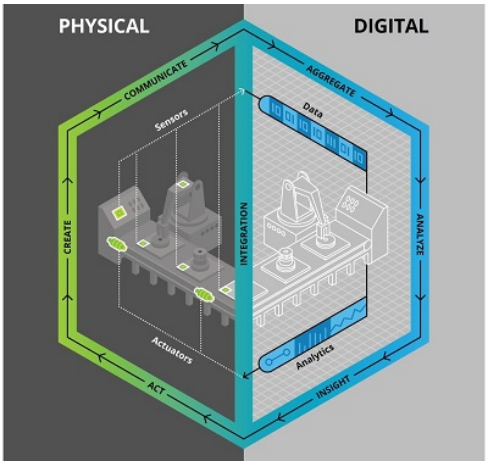
4. **Traffic Management:** Modern internet of things (IoT) trends suggest that IoT technology is relevant to address challenges like traffic and blockage issues globally. Many organizations these days are giving arrangements and solutions that utilize IoT-installed technology in traffic systems and vehicles to sketch more smart traffic networks, presumed to reduce unnecessary traffic and congestion.



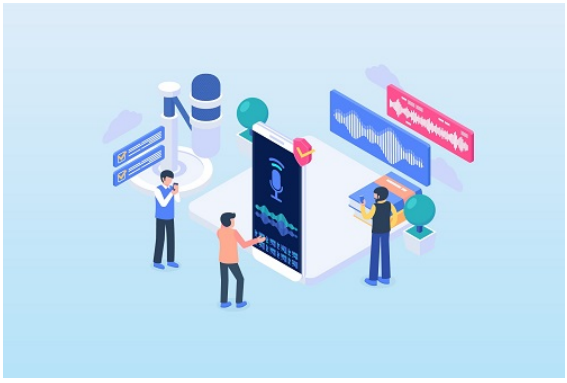
5. **IoT-Empowered AI Applications:** The internet of things (IoT) and artificial intelligence (AI), these two quite different technologies, can together present commercial solutions. In order to deliver reliable results, AI algorithms presently need very limited data. Industries using these two technologies can help automate several processes and reduce operating costs, reduce downtime, increase productivity and facilitate predictive maintenance.



6. **Digital Twins:** Recognized in 2020, a digital twin is a virtual representation that serves as the real-time digital equivalent of a physical object or process. It can be exercised for varied things such as diagnosing, optimizing, monitoring, and controlling asset utilization and performance. The projected combined annual growth rate of the digital twins market will be several folds by 2025.



7. **Voice Activated IoT Devices:** Artificial Intelligence-powered virtual assistant – Google Assistant, virtual assistant AI technology developed by Amazon – Amazon Echo, and virtual assistant by Apple – Siri, have taken voice-based user interfaces to another level. With the developing technologies, voice interactions will be used in other applications in multiple industries in the forthcoming new age that will allow people to give commands, change settings and receive results from smart devices.
   Voice biometry is another exciting development in voice recognition technology. Voice biometry lets organizations build a digital profile of someone's voice, after analyzing a set of specific characteristics such as pitch, intensity, tone, dominant frequencies, dynamics, etc. Businesses are confident that this method will be more reliable than the methods that are presently in place.



8. **IoT Security:** Security is one of the major concerns these days when it comes to the extensive level of connectivity that we are involved in. The increased intervention of technology in the lives of people has highlighted the continued threat to unsecured connected devices/things.
   As a consequence, security is an evolving IoT trend and several businesses around the world are developing IoT security solutions using diverse technologies.

9. **Edge Computing:** Due to distant work and the COVID-19 pandemic, Edge Computing is presumed to rise dramatically by the end of the year 2021. This innovation helps new kinds of business to emerge in the competitive world.
   According to a report, end-of-life marketers may keep a sizable proposal in the public cloud market prompted by the way that notable retailers, like, Dell, IBM, and HPE are creating solutions for edges with cloud-like features. In a burgeoning workforce, edge computing grants organizations to assist clients in new areas and back control and flexibility.

IoT Governance

As IoT usage becomes more widespread, the physical network of IoT devices grows larger and more complicated to manage, with approximately 13.1 billion IoT devices in operation today according to Statista. An IoT governance model is an effective way to address data security and privacy concerns, as well as legal, ethical, and public relations matters. It establishes the policies, procedures, and practices that define how a company will design, build, deploy, and manage an IoT system.

IoT governance models also outline how the system will comply with industry, local, and global data security and privacy laws. These laws define how an IoT device should collect, store, manage, use, and discard data. The type of data an IoT device collects is another contributing factor. IoT devices that collect sensitive PII – i.e. full name, home address, driver's license, medical record – must manage this data in accordance with data protection laws, such as the GDPR in EU member states. Failure to do so can result in significant fines.

Should organizations that collect sensitive data be allowed to sell and monetize it? What happens if a government entity or court order demands that such data be handed over? What security measures should be in place to protect the IoT network from unauthorized access? IoT governance models can help answer these questions. Google, for instance, has a policy against users sending PII to Google when collecting Analytics data.

The Three Main Criteria of an IoT Governance Model

A good IoT governance model should serve as a roadmap to follow, addressing the most pressing IoT concerns, including data security, data management, privacy, and technological requirements. The more comprehensive an IoT governance model is, and the more areas of concern it covers, the more effectively it will overcome challenges and deliver successful results. Therefore, companies can make more informed decisions, maintain customer confidence, and avoid paying penalties due to non-compliance.

No two IoT governance models are alike. But there are three areas that any model should cover. These include Technical Architecture, Data Management, and Information Security. Each area covers different facets of the IoT governance model. And they each involve the input of different decision makers and subject matter experts. After all, creating an IoT governance model should be a collaborative effort, one that involves several brainstorming sessions, consisting of feedback from people from all walks of life, from programmers to designers to product owners to legal consultants.

Here is a quick breakdown of the three areas that an IoT governance model should cover:

1. **Technical Architecture:** Technical architecture is the blueprint to follow to design an IoT system and related software. There may already be a technical architecture standard in place before the creation of the IoT governance model. This standard may be used as is or modified to suit the unique requirements of the IoT governance model. It may need modifying based on the volume of IoT devices that are added or interacted with, the technical limitations of the physical IoT device, and the type of data the IoT device will collect. Given the nature of the subject, matters surrounding technical architecture are largely established by technical experts such as coders, programmers, and project managers.

2. **Data Management:** Data management is one of the most complex and challenging components of an IoT governance model. That is because there are more than technical considerations to be made. How a company collects, stores, and uses data is a major legal and ethical hurdle to overcome. Data scientists, data analysts, and data engineers play a huge role in outlining the data management components of an IoT governance model. For example, the data analyst may outline what data should be collected and how it should be analyzed, while a data engineer will propose the tools to be used for easy data access and interpretation.

   Legal consultants and advisors with experience in data security and privacy may also be of assistance, making sure the company's governance model is compliant with industry, local, and global standards.

3. **Information Security:** Information security refers to how secure an IoT device is. Following the recommended manufacturer guidelines is the best way to secure an IoT device. And those configurations should be reviewed when changes occur, such as when IoT devices are added or removed from the network. Information security also refers to the data collection process, including the type and volume of data collected. If an IoT device collects Personally Identifiable Information (PII), strict security measures should be in place to protect that data. These include requiring users to provide additional proof of identity with MFA, and encrypting sensitive PII during transmission from one IoT device to another device.

Security & Privacy Issues In The Internet Of Things (IoT)

The concept of the Internet of Things (IoT) has completely transformed the way we perceive connectivity. With IoT, we have seen devices, apart from personal computers, connecting to the internet. IoT has enabled the possibility for embedding internet connectivity and relevant functions in various types of devices.

The world has witnessed rapid growth in the connectivity of televisions, cars, refrigerators, air conditioners, hairbrushes, and many other devices to the internet. At the same time, the concerns regarding security and privacy in IoT have also gained prominent attention as the world recognizes the true potential of IoT.

Understanding the Concept of Security in IoT

The Internet of Things landscape is gradually becoming more diverse with legacy computing systems and modern computing devices. As a result, IoT easily becomes vulnerable to a wide range of security risks in different approaches.

If a poorly secured device connects with the IoT landscape, then it could affect the security and resilience of IoT. With a large number of homogenous devices deployed in IoT, the IoT users and developers must ensure that they are not exposing other users to potential harm.

One of the most prominent factors to draw attention towards security in IoT would refer to authentication. The authentication mechanisms used in existing IoT ecosystems are restricted only to offering safeguards against limited threats such as replay attacks or Denial of Service (DoS) attacks. It is also important to consider the role of information security as one of the highly vulnerable domains of IoT authentication.

The abundance of risky applications which enable a natural multiplicity of data collection could present formidable information security risks. In addition, the importance of security becomes clearly evident with the prevalence of man-in-the-middle attacks. Third-party agents could intercept communication channels for impersonating identities of vulnerable nodes associated with network exchange.

Understanding the Concept of Privacy in IoT

The next notable aspect in discussions on privacy and security in IoT refers to the way consumers view privacy. People are likely to perceive the usefulness of IoT in accordance with its effectiveness in safeguarding their privacy goals. The common assumptions regarding privacy issues in IoT and the potential security issues could become formidable setbacks in IoT adoption.

The aspects of user privacy and the rights of privacy are basic requirements for developing the trust and confidence of users in IoT, connected devices, and associated services. At the same time, the developments in IoT are focusing largely on addressing privacy issues in a completely new way.

One of the most important concerns in understanding the issues of privacy in IoT would draw attention towards reasons for privacy concerns. The IoT ecosystem has intelligent artifacts present almost everywhere with flexibility for sampling process and information distribution from any location.

In addition, the ubiquitous connectivity in IoT through the internet also plays a crucial role in amplifying privacy concerns. Without a unique mechanism for privacy protection, the ubiquitous connectivity of IoT could enable flexible access to personal information from any corner of the world.

Security Issues in IoT

With a clear impression of the significance of security and privacy in IoT, it is important to find out the issues. Businesses could reap credible benefits from the capabilities of the Internet of Things (IoT). However, the threats to security could present notable setbacks for the effective adoption of IoT-enabled solutions. On the other hand, a clear impression of the IoT security issues could help in developing suitable strategies for mitigation. Let us take a look at some of the notable issues for security in IoT.

1. **Inadequate Password Protection:** Hard-coded and embedded credentials in IoT devices provide an easy target for hackers to compromise the devices directly. Default passwords may enable hackers to enter the machine without any obstacles. One of the examples of such an attack refers to the Mirai malware, which infected IoT devices such as routers, video recorders, and video cameras. The Mirai malware was successful in logging in by using 61 general hard-coded usernames and passwords. Subsequently, the malware brought almost 400,000 connected devices in its control and resulted in the world's first 1Tbps DDoS attack. The Distributed Denial of Service of DDoS attack affects some parts of Amazon Web Services and its clients such as Twitter, Netflix, Airbnb, and GitHub. Now in 2021, a Mirai-type malware, known as Mozi, is the most active botnet.

2. Limited Compliance from IoT Manufacturers: Another important factor affecting the security factor in privacy and security in IoT refers to the lack of compliance from IoT manufacturers. Many fitness trackers with Bluetooth generally remain visible after pairing. Your refrigerator could give out your Gmail login credentials.
   As manufacturers continue the development of devices with limited security, the concerns of security in IoT would definitely witness an upward turn. IoT device manufacturers have started introducing internet connectivity in their devices without paying attention to the 'security' aspect in the product designing process. Some of the notable security risks for IoT which are due to manufacturers include,
   - Hardware issues
   - Lack of security in data transfer and storage

- Hard-coded, weak, or guessable usernames and passwords

3. Device Update Management: The concerns of security and privacy in IoT could also refer to security issues due to device update management. Insecure firmware or software could generally lead to IoT security risks. Even if a manufacturer offers a device with the most recent software update, you will encounter new vulnerabilities.

   Therefore, updates are highly important for ensuring security on IoT devices, which should be updated immediately after the discovery of new vulnerabilities. The use of IoT devices without necessary updates could escalate the threats to their security. In addition, update management can be risky due to the fact that devices will send backups to the cloud. Without appropriate encryption for the connection and protection for updated files, any malicious agent could access sensitive information.

4. Lack of Secure Interfaces: The answers to 'Why security is important in IoT?' become clear with the security issues due to insecure interfaces. All IoT devices are involved in the processing and communication of data. The IoT devices need apps, protocols, and services for communication, and the insecure interfaces are responsible for various IoT vulnerabilities.

   You can find insecure interfaces in web, API, cloud, mobile, and application interfaces with possibilities for compromising the device and data. The most common concern of security in IoT interface is the lack of device authorization and authentication mechanism and weak or no encryption mechanism.

Privacy Concerns in IoT

While the challenges to security are quite prevalent in IoT, the concerns of privacy are also another critical factor. Many people also want to find out 'What are the privacy concerns in IoT?' and the answers could help in improving IoT for large-scale adoption. Let us take a look at some of the common privacy concerns in IoT which you can find today.

1. **Abundance of Data:** The data generated by IoT devices is radically staggering for all the right reasons. According to the Federal Trade Commission, less than 10,000 households could create almost 150 million discrete data points daily. Therefore, you can clearly notice the increased possibilities for breaches of privacy in IoT. You have more entry points for hackers while leaving sensitive information and your IoT devices vulnerable.
2. **Eavesdropping:** IoT users would also have to find eavesdropping as one of the ominous answers to 'What are the privacy concerns in IoT?' for specific reasons. Imagine a hacker using one of your smart home appliances to snoop in your personal life. As a matter of fact, hackers and even manufacturers could use a connected device to basically invading an individual's home.

For example, researchers have been successful in eavesdropping in IoT by intercepting unencrypted data from a smart meter device. The unencrypted data helped in identify the television show an individual was watching at the particular instance of time.

3. **Unwanted Public Exposure:** The next and probably the most important entry among privacy issues in IoT would refer to unwanted public exposure. IoT device manufacturers often have long documentation for terms of service, and there is barely anyone who reads the document thoroughly. According to the Federal Trade Commission, manufacturers and enterprises could leverage data offered willingly by consumers for making employment decisions.

   For example, an insurance company could collect information from an individual regarding their driving habits through a connected car. Similarly, health or life insurance providers could also use data from fitness trackers for calculating the insurance rates of different individuals.