UNIT-1

INTRODUCTION TO INTERNET OF THINGS

1.1 INTRODUCTION OF IOT

IoT stands for Internet of Things. The term 'Internet of Things' was coined in 1999 by the computer scientist Kevin Ashton. There are multiple ways to define IoT, but basic of all the definitions remains the same. It refers to the interconnection of physical devices, such as appliances and vehicles, that are embedded with software, sensors and connectivity which enables these objects to connect and exchange data.

IoT is not a single technology but it is a combination of technologies and domain knowledge. As a result, engineers from different domain have to work together in order to build complete IoT product. IoT can be used to build applications for home automation, agriculture, defence, education, healthcare, pharmaceuticals, transportation, retail and manufacturing industry, etc.

The term "Things" in the Internet of Things refers to anything and everything in day to day life which is accessed or connected through the internet. A thing in the IoT 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. In other words, any other natural or man-made object that can be assigned an Internet Protocol (IP) address and is able to transfer data over a network can be considered as a thing.

For example, in IoT Based Home Automation System following can be considered as "things":

- Light Control and Automation Devices
- Ventilation devices
- Air Conditioners
- Security Cameras
- Smart Lock
- Smart Switches
- Air Purifiers, etc

In IoT all the things can be put into 3 categories:

1) Sensors that collect information and then send it.
2) Computers that receive information and then act on it.
3) Things that do both.

- **Sensors that collect information and then send it:**

  Sensors can measure temperature, motion, moisture, air quality, light and almost anything else you can think of. Sensors, when paired with an internet connection, allow us to collect information from the environment which, in turn, helps make better decisions. On a farm, automatically getting information about soil moisture can tell farmers exactly when crops need to be watered. Instead of watering too much or too little (either of which can lead to bad outcomes), the farmer can ensure that crops get

exactly the right amount of water. Just as our senses allow us to collect information, sensors allow machines to make sense of their environments.

- **Receiving and Acting on Information:**
  We're all very familiar with machines acting on input information. A printer receives a document and then prints it. A garage door receives a wireless signal and the door opens. It's common place to remotely command a machine to act. So, what? The real power of IoT arises when things can both collect information act on it.
- **Doing Both:**
  Consider the example of farming. The sensors collect information about soil moisture. Now, the farmer could activate the irrigation system or turn it off as appropriate. With IoT-enabled systems, you don't actually need the farmer for that process. Instead, the irrigation system can automatically act as needed, based on how much moisture is detected. You can take it a step further too. If the irrigation system receives information about the weather from its internet connection, it can also know when it's going to rain and decide not to water the crops when they'll be watered by the rain anyways. And it doesn't stop there! All this information about the soil moisture, how much the irrigation system is watering the crops and how well the crops actually grow can be collected and sent to supercomputers in the cloud that run algorithms to that analyse all this information, leading to models that could be used to predict future conditions and prevent losses.

IoT Protocols:

Communication between various things in IoT takes place with help of various protocols and standards. Below mentioned are some most commonly used protocols in IoT:

1) MQTT (Message Queuing Telemetry Transport) Protocol
2) DDS (Data Distribution Service) Protocol
3) AMQP (Advanced Message Queuing Protocol)
4) Bluetooth Protocol
5) Wi-Fi Protocol
6) Zigbee Protocol
7) Cellular Protocol
8) LoRa WAN (Long Range Wide Area Network) Protocol
9) CoAP (Constrained Application Protocol)
10) XMPP (Extensible Messaging and Presence Protocol)

1.2 CHARACTERISTICS OF IoT

1) Connectivity:

Connectivity is an important requirement of the IoT infrastructure. Things of IoT should be connected to the IoT infrastructure. Anyone, anywhere, anytime can connect, this should be guaranteed at all times. IoT can connect through several wireless devices like sensors, mobile phones, trackers, etc.

2) Intelligence and Identity:

The extraction of knowledge from the generated data is very important. For example, a sensor generates data, but that data will only be useful if it is interpreted properly. Each IoT device has a unique identity. This identification is helpful in tracking the equipment and at times for querying its status.

3) Scalability:

The number of elements connected to the IoT zone is increasing day by day. Hence, an IoT setup should be capable of handling the massive expansion. The data generated as an outcome is enormous and it should be handled appropriately.

4) Dynamic and Self Adapting:

IoT devices should dynamically adapt themselves to changing contexts and scenarios. Assume a camera meant for surveillance. It should be adaptable to work in different conditions and different light situations (morning, afternoon and night).

5) Architecture:

The architecture of IoT is designed in a way that it is capable of supporting various devices, technologies and protocols. Its main work is to confirm whether each connected device does not interfere with the other. This way, the safety and security of each device's data are maintained.

6) Security:

With the increasing number of IoT devices, issues regarding the security of personal data have arisen. There might be a chance of data leakage as a large amount of data is collected, exchanged and generated. There is a chance of personal data being transferred without approval, which is a matter of concern.

To overcome this challenge, IoT has created networks, systems and devices wherein privacy is well maintained. Maintaining safety and security is a big dare for IoT. However, it still handles it without any disruption.

7) Self-Configuring:

This is one of the most important characteristics of IoT. IoT devices are able to upgrade their software in accordance with requirements with a minimum of user participation. Additionally, they can set up the network, allowing for the addition of new devices to an already-existing network.

8) Interoperability:

Interoperability is one of the key characteristics of the Internet of Things (IoT). It refers to the ability of different IoT devices and systems to communicate and exchange data with each other, regardless of the

underlying technology or manufacturer. To achieve interoperability, IoT devices and systems use standardized communication protocols and data formats.

9) Autonomous Operation:

Autonomous operation refers to the ability of IoT devices and systems to operate independently and make decisions without human intervention.

10) Data Driven:

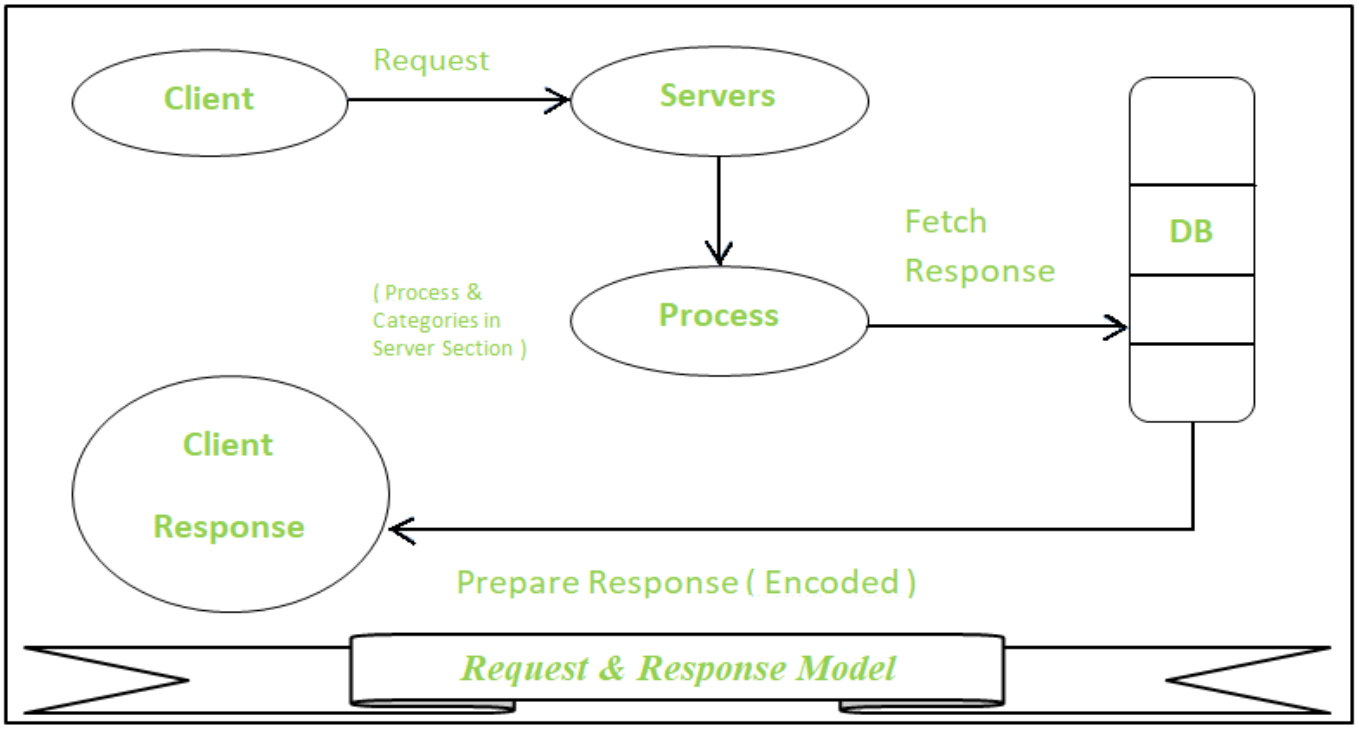
Data-driven is a key characteristic of the IoT. IoT devices and systems collect vast amounts of data from sensors and other sources, which can be analysed and used to make data-driven decisions.

1.3 MODELS OF IoT

1) Request & Response Model

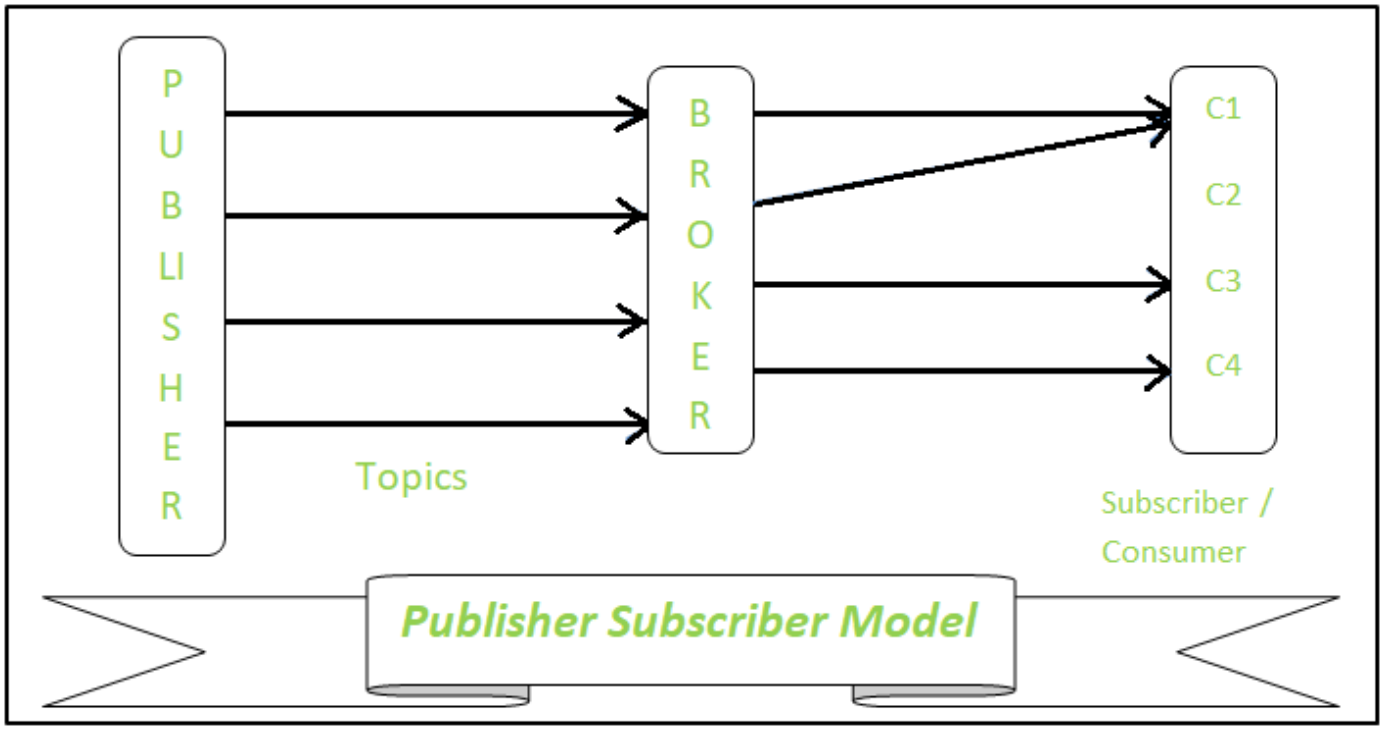
This model follows a client-server architecture.

The client, when required, requests the information from the server. This request is usually in the encoded format**.** This model is stateless since the data between the requests is not retained and each request is independently handled. The server categories the request and fetches the data from the database and its resource representation. This data is converted to response and is transferred in an encoded format to the client. The client, in turn, receives the response. On the other hand, in Request-Response communication model, client sends a request to the server and the server responds to the request. When the server receives the request, it decides how to respond, fetches the data retrieves resources and prepares the response and sends it to the client.



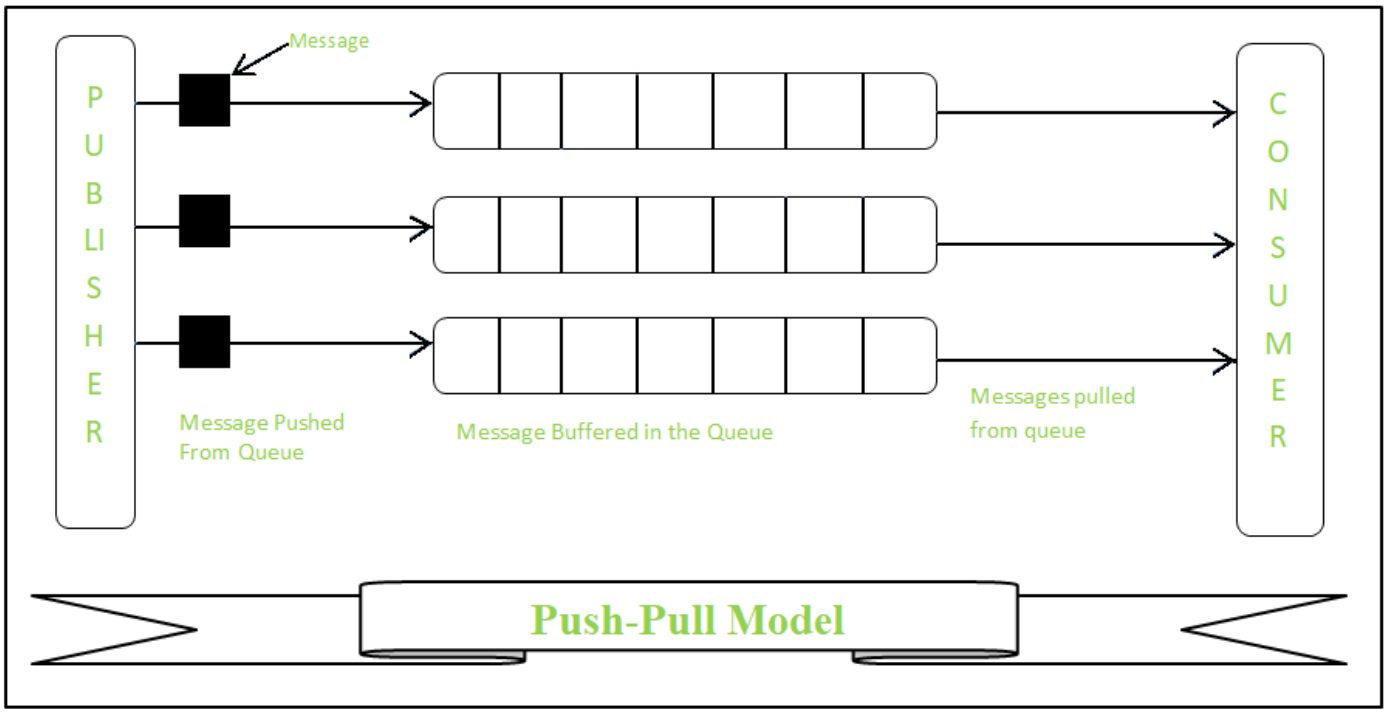
2) Publisher-Subscriber Model

This model comprises three entities: Publishers, Brokers, and Consumers. Publishers are the source of data. It sends the data to the topic which are managed by the broker. They are not aware of consumers. Consumers subscribe to the topics which are managed by the broker. Hence, Brokers responsibility is to accept data from publishers and send it to the appropriate consumers. The broker only has the information regarding the consumer to which a particular topic belongs to which the publisher is unaware of.



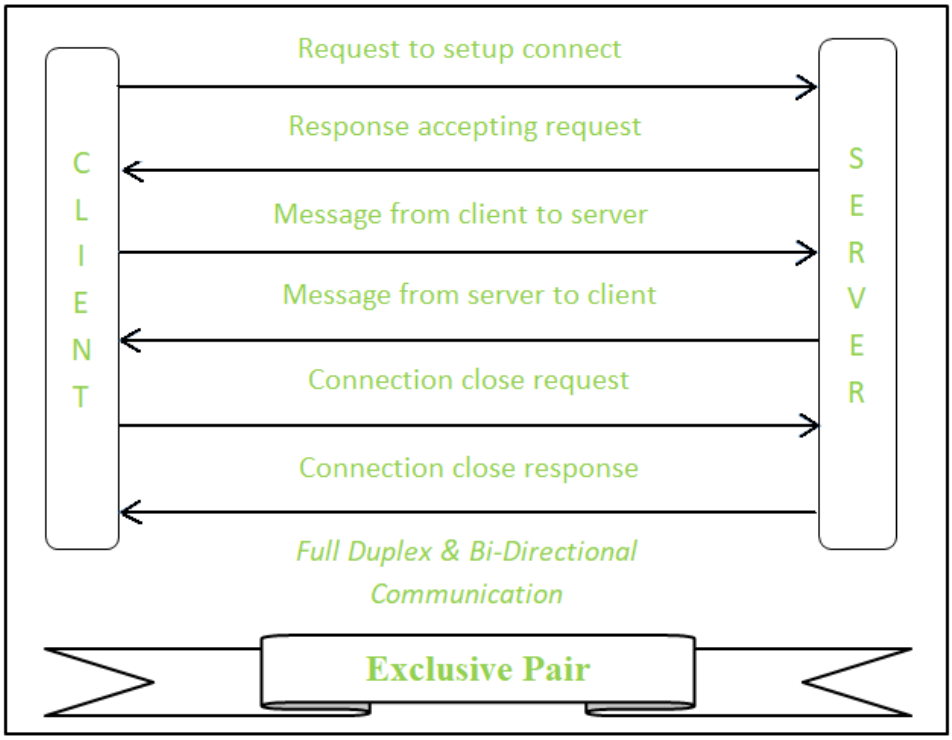
3) Push-Pull Model

The Push-Pull model constitutes data publishers, data consumers and data queues. Publishers and Consumers are not aware of each other. Publishers publish the message/data and push it into the queue. The consumers, present on the other side, pull the data out of the queue. Thus, the queue acts as the buffer for the message when the difference occurs in the rate of push or pull of data on the side of a publisher and consumer. Queues help in decoupling the messaging between the producer and consumer. Queues also act as a buffer which helps in situations where there is a mismatch between the rate at which the producers push the data and consumers pull the data.



4) Exclusive Pair

Exclusive Pair is the bi-directional model, including full-duplex communication among client and server. The connection is constant and remains open till the client sends a request to close the connection. The Server has the record of all the connections which has been opened. This is a state-full connection model and the server is aware of all open connections. WebSocket based communication API is fully based on this model.



1.4 TECHNOLOGY ROADMAP

Creating a technology roadmap specifically for IoT involves considering the unique challenges and opportunities presented by the Internet of Things. Here's a tailored approach for developing an IoT technology Roadmap:

1) Assessment of Current State and Readiness:

- Evaluate existing IoT infrastructure, devices, sensors and connectivity mechanisms.
- Assess data handling, security measures and analytics capabilities specific to IoT.

2) Define IoT Objectives and Use Cases:

- Clearly outline the business objectives and use cases for IoT implementation (e.g., predictive maintenance, smart monitoring, supply chain optimization).
- Prioritize use cases based on their potential impact on the business.

3) Stakeholder Engagement and Requirements Gathering:

- Involve stakeholders from various departments to understand their specific IoT needs and challenges.
- Gather requirements to ensure that the IoT roadmap aligns with business goals.

4) Identify Key IoT Technologies:

- Evaluate and select the appropriate IoT technologies (sensors, connectivity protocols, edge computing, platforms) needed to support the defined use cases.
- Consider scalability, interoperability, security and data management capabilities of these technologies.

5) Data Management and Analytics Strategy:

- Develop a strategy for managing the vast amount of data generated by IoT devices.
- Plan for real-time or near real-time data processing, analytics and deriving actionable insights.

6) Security and Privacy Measures:

- Incorporate robust security measures to protect IoT devices, networks and the data transmitted and stored.
- Implement privacy controls and compliance with relevant regulations.

7) Integration and Interoperability:

- Ensure that IoT systems can integrate with existing IT infrastructure and other applications within the organization.
- Focus on interoperability standards to facilitate seamless communication between devices and systems.

8) Pilot Projects and Proof of Concepts (POCs):

- Initiate small-scale pilot projects or POCs to validate selected IoT technologies and use cases.
- Gather feedback and refine strategies based on the results.

9) Scaling and Expansion:

- Plan for scaling up successful IoT initiatives across the organization or into new areas.

- Consider the infrastructure, resources, and potential challenges associated with scaling IoT deployments.

10) Continuous Evaluation and Improvement:

- Regularly evaluate the performance, efficiency and ROI of implemented IoT solutions.
- Incorporate feedback, lessons learned and technological advancements into the roadmap for continuous improvement.

1.5 BENEFITS OF IoT

1) It can assist in the smarter control of homes and cities via mobile phones. It enhances security and offers personal protection.
2) By automating activities, it saves us a lot of time.
3) Information is easily accessible, even if we are far away from our actual location and it is updated frequently in real time.
4) Electric Devices are directly connected and communicated with a controller computer, such as a cell phone, resulting in efficient electricity use. As a result, there will be no unnecessary use of electricity equipment.
5) Personal assistance can be provided by IoT apps, which can alert you to your regular plans.
6) It is useful for safety because it senses any potential danger and warns users. For example, GM OnStar, is an integrated device that system which identifies a car crash or accident on road. It immediately makes a call if an accident or crash is found.
7) It minimizes human effort because IoT devices connect and communicate with one another and perform a variety of tasks without the need for human intervention.
8) Patient care can be performed more effectively in real time without the need for a doctor's visit. It gives them the ability to make choices as well as provide evidence-based care.
9) Asset tracking, traffic or transportation tracking, inventory control, delivery, surveillance, individual order tracking, and customer management can all be made more cost-effective with the right tracking system.

1.6 IMPACT OF IoT ON THE BUSINESS LANDSCAPE

The Internet of Things (IoT) has had a significant impact on the business landscape across various industries. Following are some key ways in which IoT has influenced and continues to shape businesses:

1) Operational Efficiency:

- Automation: IoT enables businesses to automate various processes, reducing the need for manual intervention. This leads to increased operational efficiency and cost savings.
- Real-time Monitoring: Businesses can monitor equipment, assets and processes in real-time, allowing for better decision-making and proactive maintenance.

2) Data-driven Insights:

- Big Data Analytics: The vast amount of data generated by IoT devices provides valuable insights. Companies can analyse this data to make informed decisions, optimize processes and identify new business opportunities.
- Predictive Analytics: IoT data allows businesses to predict maintenance needs, demand patterns and other critical factors, helping them stay ahead of potential issues.

3) Improved Customer Experience:

- Personalization: IoT enables businesses to offer personalized products and services based on customer behaviour and preferences.
- Enhanced Interactivity: Smart devices and connected systems enhance customer engagement through interactive experiences, creating new ways to connect with consumers.

4) Supply Chain Optimization:

- Visibility and Traceability: IoT provides real-time visibility into the supply chain, allowing businesses to track the movement of goods and monitor conditions such as temperature and humidity.
- Inventory Management: Smart sensors help optimize inventory levels, reducing waste and ensuring that products are available when needed.

5) Cost Savings and Resource Optimization:

- Energy Efficiency: IoT devices can help monitor and control energy consumption, leading to cost savings and a reduced environmental impact.
- Resource Allocation: Businesses can optimize the use of resources such as equipment, personnel, and space based on real-time data, minimizing waste and maximizing efficiency.

6) Security and Risk Management:

- Cybersecurity Measures: As more devices become interconnected, cybersecurity becomes crucial. Businesses need to implement robust security measures to protect sensitive data and prevent unauthorized access.
- Risk Mitigation: IoT enables businesses to identify and address potential risks in real time, reducing the likelihood of disruptions and losses.

7) New Business Models:

- Subscription Services: IoT facilitates the shift from traditional product-based business models to service-based models, where companies offer ongoing services and support.
- Ecosystem Collaboration: Businesses can create new partnerships and collaborations within the IoT ecosystem, leading to innovative solutions and mutually beneficial relationships.

8) Regulatory Compliance:

- Data Privacy: With the increased collection and processing of personal data, businesses must comply with evolving data protection regulations. Implementing privacy measures is essential to maintain trust with customers and meet legal requirements.

Overall, the integration of IoT technologies has reshaped how businesses operate, offering opportunities for increased efficiency, innovation and competitiveness in the evolving digital landscape.