CHAPTER 4: INTERNET OF THINGS

BRYAN ORACION

ALVIE SHANYL PAGOD

REA ANN TOLEDO

TITO ABANDA

OVERVIEW OF IOT

- **What is IoT?**

The Internet of Things (IoT) refers to the interconnected network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, and connectivity which enables these objects to connect and exchange data. IoT allows for the seamless collection and exchange of data, enabling a more automated and efficient world.

HISTORY OF IOT

- The concept of the Internet of Things has its roots in the early 1990s when Kevin Ashton, a British technology pioneer, first used the term "Internet of Things." However, the development of IoT can be traced back to the advent of wireless technology, the internet, and microelectronics. Over time, with the advancements in technology and the increasing number of connected devices, the concept of IoT has evolved and become more widespread. In recent years, IoT has grown rapidly, with the number of connected devices expected to reach tens of billions by the end of the decade. IoT is being used in various fields such as healthcare, manufacturing, retail, transportation, and smart homes, among others, to improve efficiency and enhance the quality of life.

IOT ADVANTAGES:

- **Increased efficiency and automation:** IoT devices can communicate with each other and share data, allowing for more automated and efficient systems.
- **Improved decision making**: IoT devices generate large amounts of data that can be analyzed to make informed decisions and solve problems.
- **Enhanced customer experience:** IoT technology can be used to improve customer service and experience in various industries, such as retail and hospitality.
- **Better monitoring and control:** IoT devices can be used to monitor and control various systems, such as heating and lighting, from a remote location.
- **Cost savings**: IoT technology can help companies save money by reducing waste, increasing productivity, and improving resource allocation.
- **New business opportunities**: IoT creates new business opportunities by enabling the development of new products and services that leverage the capabilities of connected devices.
- **Improved safety**: IoT can be used to enhance safety in various industries, such as transportation and healthcare.

IOT DISADVANTAGE

- **Security and privacy concerns:** As more devices become connected, the risk of hacking and cyber attacks increases, putting sensitive information and personal data at risk.
- **Complexity:** IoT systems can be complex and difficult to manage, especially as the number of connected devices grows.
- **Interoperability issues**: Different IoT devices and systems may not be compatible with each other, leading to difficulties in integration and communication.
- **Limited battery life**: Many IoT devices rely on battery power, and their limited battery life can be a hindrance to their widespread adoption.
- **Cost**: The cost of implementing an IoT system can be high, especially for small and medium-sized businesses.
- **Data overload**: The large amount of data generated by IoT devices can be overwhelming and difficult to manage, leading to difficulties in extracting valuable insights.
- **Dependence on connectivity**: IoT devices rely on a constant internet connection, and disruptions in connectivity can impact their functionality.

CHALLENGES OF IOT

- **Security and privacy**: Ensuring the security of sensitive data and personal information transmitted over IoT networks is a major challenge. Cyber threats, such as hacking and data theft, are growing concerns in the IoT landscape.
- **Interoperability:** IoT devices from different manufacturers may not be compatible with each other, making it difficult to integrate and exchange data between devices.
- **Scalability**: Managing the increasing number of connected devices and ensuring that the infrastructure can support the growing volume of data is a challenge.
- **Reliability**: Ensuring the reliability of IoT devices and networks is crucial to their widespread adoption, as even minor disruptions can have a significant impact.
- **Standards:** The lack of universal standards for IoT devices and networks makes it difficult for them to work together effectively, and creates challenges for interoperability and integration.
- **Data Management**: The large amounts of data generated by IoT devices can be overwhelming, and managing and analyzing this data to extract valuable insights is a challenge.
- **Network coverage**: Ensuring adequate network coverage and connectivity, especially in remote areas, is a challenge that needs to be addressed to support the widespread adoption of IoT.

HOW DOES IT WORK? ARCHITECTURE OF IOT

- **Devices**: IoT devices are physical objects that are embedded with sensors, electronics, and software, allowing them to collect and exchange data. These devices include smart home appliances, wearable devices, and industrial equipment, among others.
- **Network:** IoT devices communicate with each other and with other systems through a network. This can be a local area network (LAN), a wide area network (WAN), or a combination of both.
- **Cloud**: IoT devices typically transmit data to a cloud-based server for storage and processing. The cloud provides scalable computing resources for data analysis and application development.
- **Gateway**: The gateway acts as a bridge between the IoT devices and the cloud, allowing data to be transmitted between the two. The gateway also performs data processing and protocol translation, ensuring that the data is in a format that can be used by the cloud.
- **Analytics:** IoT data is analyzed to extract insights and inform decision-making. This can be done using advanced analytics tools, such as machine learning algorithms and predictive analytics.
- **Application**: The final component of the IoT architecture is the application layer, which allows users to interact with the IoT system and access the data generated by the devices. Applications can be web-based or mobile, and can be developed for a wide range of use cases, including industrial automation, smart homes, and wearables.

DEVICES AND NETWORKS

- **IoT Devices**: IoT devices are physical objects that are embedded with sensors, electronics, and software, allowing them to collect and exchange data. These devices can range from smart home appliances, such as thermostats and security systems, to wearable devices, such as fitness trackers, to industrial equipment, such as machinery and vehicles.
- **Network**: The network is the communication infrastructure that enables IoT devices to exchange data. There are several types of networks used in IoT, including:
- **Local Area Networks (LANs):** LANs are used to connect IoT devices within a small geographic area, such as a home or office.
- **Wide Area Networks (WANs):** WANs are used to connect IoT devices over large geographic distances, such as across cities or countries.
- **Wireless networks**: Wireless networks, such as Wi-Fi and cellular networks, are used to transmit data between IoT devices and the cloud.

3. **Protocols:** IoT devices and networks use communication protocols to exchange data. Some of the most commonly used protocols in IoT include:

- **MQTT (Message Queuing Telemetry Transport):** A lightweight publish/subscribe protocol used for small devices with limited computing power.
- **CoAP (Constrained Application Protocol):** A lightweight protocol for resource-constrained devices, such as sensors.
- **HTTP (Hypertext Transfer Protocol):** The standard protocol used for exchanging data on the World Wide Web.
- **XMPP (Extensible Messaging and Presence Protocol):** An open standard for real-time communication used in IoT applications, such as instant messaging and online gaming.

IOT TOOLS AND PLATFORM

- **AWS IoT:** Amazon Web Services (AWS) IoT is a cloud-based platform for connecting and managing IoT devices. It provides services for device management, data analytics, and application development.
- **Azure IoT:** Microsoft Azure IoT is a cloud-based platform that provides a suite of services for building and managing IoT solutions, including device management, data analytics, and application development.
- **Google Cloud IoT:** Google Cloud IoT is a cloud-based platform for managing and analyzing data from IoT devices. It provides services for device management, real-time data streaming, and data storage.
- **IBM Watson IoT:** IBM Watson IoT is a cloud-based platform that provides a suite of services for building and deploying IoT solutions, including device management, data analytics, and application development.
- **Thing Worx:** Thing Worx is an IoT platform that provides tools for device management, data analytics, and application development. It is used by organizations in a variety of industries, including manufacturing, healthcare, and transportation.
- **Node-RED:** Node-RED is an open-source visual programming tool for wiring together IoT devices and services. It can be used for prototyping and building IoT solutions.
- **Raspberry Pi:** The Raspberry Pi is a small, low-cost computer that can be used as the basis for building IoT devices and solutions. It is widely used in education, hobby projects, and commercial applications.

IOT BASED SMART HOME

- A smart home based on the Internet of Things (IoT) is a home equipped with a network of connected devices that can be controlled and monitored remotely through a smartphone or a central control unit. These devices can range from smart thermostats, lighting systems, and security systems, to smart appliances, such as refrigerators, washing machines, and ovens.

IOT BASED SMART CITY

- Smart cities offer numerous benefits, including improved quality of life, reduced environmental impact, and increased efficiency. However, there are also challenges associated with building and maintaining a smart city, including the cost of implementing and maintaining the technology, the need for reliable and secure networks, and the potential for privacy and security breaches. To overcome these challenges, it is important to carefully plan the deployment of IoT devices, to ensure that they are secure, and to involve all stakeholders in the planning process.Bottom of Form.

IOT BASED SMART FARMING

- Smart farming offers numerous benefits, including increased efficiency, productivity, and profitability. It can also help farmers make more informed decisions about resource use, reduce waste, and protect the environment. However, there are also challenges associated with implementing IoT in agriculture, including the cost of deploying the technology, the need for reliable networks, and the potential for privacy and security breaches. To overcome these challenges, it is important to carefully plan the deployment of IoT devices, to ensure that they are secure, and to involve all stakeholders in the planning process.