IoT

Contents

Evaluations

- Theory (CCEE) - 40 Marks
- Lab exam - 40 Marks
- Internal exam - 20 Marks

IoT

- collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves
- The Internet of Things integrates everyday “things” with the internet
- The cost of integrating computing power into small objects has now dropped considerably
- these smart objects can automatically transmit data to and from the Internet.
- All these “invisible computing devices” and the technology associated with them are collectively referred to as the Internet of Things.
- A typical IoT system works through the real-time collection and exchange of data.
- An IoT system has three components:
    - Smart devices
        - a device that has been given computing capabilities
        - It collects data from its environment, user inputs, or usage patterns and communicates data over the internet to and from its IoT application.
    - IoT application

        - a collection of services and software that integrates data received from various IoT devices
        - It uses machine learning or artificial intelligence (AI) technology to analyze this data and make informed decisions
        - These decisions are communicated back to the IoT device and the IoT device then responds intelligently to inputs

    - A graphical user interface

        - IoT device can be managed through a graphical user interface
        - eg. mobile applications, web applications

Features

- Artificial Intelligence
    - IoT essentially makes virtually anything “smart”
    - it enhances every aspect of life with the power of data collection artificial intelligence algorithms
- networks
    - Connectivity
    - 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 without sensor can not do anything
    - They act as defining instruments which transform IoT from a standard passive network of devices into an active system capable of real-world integration
- Devices
    - IoT exploits purpose-built small devices to deliver its precision, scalability, and versatility

Advantages

- Improved Customer Engagement
    - Current analytics suffer from blind-spots and significant flaws in accuracy; and as noted, engagement remains passive
    - IoT completely transforms this to achieve richer and more effective engagement with audiences
- Technology Optimization
    - The same technologies and data which improve the customer experience also improve device use, and aid in more potent improvements to technology
- Reduced Waste
    - IoT makes areas of improvement clear
    - IoT provides real-world information leading to more effective management of resources
- Enhanced Data Collection
    - IoT makes data collection easier
    - With the collected data we can accurately analyse the world we want
    - It allows an accurate picture of everything

Disadvantages

- Security
  - IoT creates an ecosystem of constantly connected devices communicating over networks
  - The system offers little control despite any security measures
  - This leaves users exposed to various kinds of attackers
- Privacy
  - The sophistication of IoT provides substantial personal data in extreme detail without the user's active participation
- Complexity
  - Some find IoT systems complicated in terms of design, deployment, and maintenance
- Flexibility
  - Many are concerned about the flexibility of an IoT system to integrate easily with another
  - They worry about finding themselves with several conflicting or locked systems
- Compliance
  - Its complexity makes the issue of compliance seem incredibly challenging

pros and cons of IoT

Some of the advantages of IoT include the following:

- Enables access to information from anywhere at any time on any device.
- Improves communication between connected electronic devices.
- Enables the transfer of data packets over a connected network, which can save time and money.
- Collects large amounts of data from multiple devices, aiding both users and manufacturers.
- Analyzes data at the edge, reducing the amount of data that needs to be sent to the cloud.
- Automates tasks to improve the quality of a business's services and reduces the need for human intervention.
- Enables healthcare patients to be cared for continually and more effectively.

Some disadvantages of IoT include the following:

- Increases the attack surface as the number of connected devices grows. As more information is shared between devices, the potential for a hacker to steal confidential information increases.
- Makes device management challenging as the number of IoT devices increases. Organizations might eventually have to deal with a massive number of IoT devices, and collecting and managing the data from all those devices could be challenging.
- Has the potential to corrupt other connected devices if there's a bug in the system.
- Increases compatibility issues between devices, as there's no international standard of compatibility for IoT. This makes it difficult for devices from different manufacturers to communicate with each other.

Multuple Access Techniques

- multiplexing techniques that provide communication services to multiple users in a single-bandwidth wired or wireless medium
- Communication channels (wireless spectrum segments or cable connections), they are expensive.
- Communication service providers must engage multiple paid users over limited resources to make a profit
- Access methods allow many users to share these limited channels

- There are five basic access or multiplexing methods
    - Frequency Division Multiple Access (FDMA)
    - Time Division Multiple Access (TDMA)
    - Code Division Multiple Access (CDMA)
    - Orthogonal Frequency Division Multiple Access (OFDMA)

Frequency Division Multiple Access (FDMA)

- one channel or bandwidth is divided into multiple individual bands and each is assigned to single user
- Each individual band or channel is wide enough to accommodate the signal

Time Division Multiple Access (TDMA)

- Divides a single channel or band into time slots
- Each time slot is used to transmit one byte or another digital segment of each signal in sequential serial data format

Code Division Multiple Access (CDMA)

- CDMA is another pure digital technique.
- It is also known as spread spectrum because it takes the digitized version of an analog signal and spreads it out over a wider bandwidth at a lower power level
- The digitized and compressed voice signal in serial data form is spread by processing it in an XOR circuit

Orthogonal Frequency Division Multiple Access (OFDMA)

- used in Long-Term Evolution (LTE) cellular systems to accommodate multiple users in a given bandwidth.
- a modulation method that divides a channel into multiple narrow orthogonal bands
- Each band is divided into hundreds or even thousands of 15-kHz wide subcarriers.
- The data to be transmitted is divided into many lower-speed bit streams and modulated onto the subcarriers

Carrier Sense Multiple Access with Collision Detection (CSMA-CD)

- access method used in Ethernet local-area networks (LANs)
- It allows multiple users of the network to access the single cable for transmission
- All network nodes listen continuously.
- When they want to send data, they listen first and then transmit if no other signals are on the line.
- For instance, the transmission will be one packet or frame. Then the process repeats.
- If two or more transmissions occur simultaneously, a collision occurs.
- The network interface circuitry can detect a collision, and then the nodes will wait a random time before retransmitting.
- A variation of this method is called carrier sense multiple access with collision avoidance (CSMA-CA).
- a special scheduling algorithm is used to determine the appropriate time to transmit over the shared channel.
- CSMA-CD technique is most used in wired networks

- CSMA-CA is the preferred method in wireless networks.

PAN (Personal Area Networ)

- A personal area network (PAN) is a computer network for interconnecting electronic devices within an individual person's workspace.
- A PAN provides data transmission among devices such as computers, smartphones, tablets and personal digital assistants.
- A PAN may be wireless or carried over wired interfaces such as USB.
- A wireless personal area network (WPAN) is a PAN carried over a low-powered, short-distance wireless network technology such as
    - IrDA
    - Wireless USB
    - Bluetooth
    - Zigbee.
- The reach of a WPAN varies from a few centimeters to a few meters.
- IEEE 802.15 has produced standards for several types of PANs

IEEE 802.15

- IEEE (Institute of Electrical and Electronics Engineers)
- specifies wireless personal area network (WPAN) standards.
    - IEEE 802.15.1: WPAN / Bluetooth *
    - IEEE 802.15.2: Coexistence
    - IEEE 802.15.3: High Rate WPAN
    - IEEE 802.15.4: Low Rate WPAN *
    - IEEE 802.15.5: Mesh Networking
    - IEEE 802.15.6: Body Area Networks
    - IEEE 802.15.7: Visible Light Communication
    - IEEE P802.15.8: Peer Aware Communications
    - IEEE P802.15.9: Key Management Protocol
    - IEEE P802.15.10: Layer 2 Routing
    - IEEE 802.15.13: Multi-Gigabit/s Optical Wireless Communications

Zigbee

- Zigbee is an IEEE 802.15.4-based specification
- Designed for small scale projects which need wireless connection.
- Hence, Zigbee is a
    - low-power,
    - low data rate, and
    - close proximity (i.e., personal area) wireless ad hoc network.
- intended to be simpler and less expensive than other WPANs like Bluetooth, WiFi
- Key 802.15.4 features include:
    - real-time suitability by reservation of Guaranteed Time Slots (GTS).
    - collision avoidance through CSMA/CA.
    - integrated support for secure communications.
    - power management functions such as link speed/quality and energy detection.

    - Support for time and data rate sensitive applications because of its ability to operate either as CSMA/CA or TDMA access modes.

Architecture

- Zigbee system structure consists of three different types of devices as Zigbee Coordinator, Router, and End device
- Every Zigbee network must consist of at least one coordinator which acts as a root and bridge of the network
- The coordinator is responsible for handling and storing the information while performing receiving and transmitting data operations
- Zigbee routers act as intermediary devices that permit data to pass to and fro through them to other devices
- End devices have limited functionality to communicate with the parent nodes such that the battery power is saved
- The number of routers, coordinators, and end devices depends on the type of networks such as star, tree, and mesh networks

Protocol architecture

- only the lower layers are defined in the standard
- an IEEE 802.2 logical link control sublayer accessing the MAC through a convergence sublayer
- Implementations may rely on external devices or be purely embedded, self-functioning devices.

Physical layer

- bottom layer in the OSI, protocols layers transmit packets using it
- The physical layer (PHY) provides the data transmission service
- provides an interface to the physical layer management entity,
- which offers access to every physical layer management function and
- maintains a database of information on related personal area networks.
- the PHY manages the physical radio transceiver, performs channel selection along with energy and signal management functions.
- It operates on one of three possible unlicensed frequency bands:
    - 868.0–868.6 MHz: Europe, allows one communication channel
    - 902–928 MHz: North America, originally allowed up to ten channels
    - 2400–2483.5 MHz: worldwide use, up to sixteen channels

MAC layer

- The medium access control (MAC) enables the transmission of MAC frames through the use of the physical channel
- It offers a management interface and itself manages access to the physical channel and network
- Controls frame validation, guarantees time slots and handles node associations.

Network Layer:

- This layer takes care of all network-related operations such as network setup, end device connection, and disconnection to network, routing, device configurations, etc.

Application Support Sub-Layer:

- This layer enables the services necessary for Zigbee device objects and application objects to interface with the network layers for data managing services.
- This layer is responsible for matching two devices according to their services and needs.

Application Framework:

- It provides two types of data services as key-value pair and generic message services.
- The generic message is a developer-defined structure, whereas the key-value pair is used for getting attributes within the application objects.
- Zigbee Device Objects (ZDO) provides an interface between application objects and the Application Support Sublayer (APS) layer in Zigbee devices.
- It is responsible for detecting, initiating, and binding other devices to the network.

6LowPAN

- 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks)
- a low power wireless mesh network where every node has its own IPv6 address
- This allows the node to connect directly with the Internet using open standards
- reated with the intention of applying the Internet Protocol (IP) even to the smallest devices

Advantages of 6LoWPAN

- Uses Open IP Standards
  - It works great with open IP standard including TCP, UDP, HTTP, COAP, MATT and web-sockets.
- Offers End-To-End IP Addressable Nodes
  - It offers end-to-end IP addressable nodes. There's no need for a gateway, only a router which can connect the 6LoWPAN network to IP.
- Offers Self-Healing, Robust and Scalable Mesh Routing
  - It supports self-healing, robust and scalable mesh routing.
  - Offers one-to-many & many-to-one routing.
  - The 6LoWPAN mesh routers can route data to others nodes in the network.
- Leaf Nodes Can Sleep For a Long Duration of Time
  - In a 6LowPAN network, leaf nodes can sleep for a long duration of time.
- Offers Thorough Support For The PHY Layer
  - It also offers thorough support for the PHY layer which gives freedom of frequency band & physical layer, which can be used across multiple communication platforms like Ethernet, WI-Fi, 802.15.4 or Sub-1GHz ISM with interoperability at the IP level.
- It is a Standard: RFC6282

6LoWPAN basics

- The 6LoWPAN technology utilises IEEE 802.15.4 to provide the lower layers for this low power wireless network system.
- In order to send packet data, IPv6 over 6LowPAN, it is necessary to have a method of converting the packet data into a format that can be handled by the IEEE 802.15.4 lower layer system.

- IPv6 requires the maximum transmission unit (MTU) to be at least 1280 bytes in length. This is considerably longer than the IEEE802.15.4's standard packet size of 127 octets which was set to keep transmissions short and thereby reduce power consumption.
- To overcome the address resolution issue, IPv6 nodes are given 128 bit addresses in a hierarchical manner.

6LoWPAN application

- General Automation
  - There are enormous opportunities for 6LoWPAN to be used in many different areas of automation.
- Home automation
  - There is a large market for home automation.
  - By connecting using IPv6, it is possible to gain distinct advantages over other IoT systems.
- Smart Grid
  - Smart grids enable smart meters and other devices to build a micro mesh network and they are able to send the data back to the grid operator’s monitoring and billing system using the IPv6 backbone.
- Industrial monitoring
  - Automated factories and industrial plants provide a great opportunity for 6LoWPAN and using automation, can enable major savings to be made.
  - The ability of 6LoWPAN to connect to the cloud opens up many different areas for data monitoring and analysis.