# Assignment No: 3

Q.1. Explain Actuator Role in IOT in brief?

→

- An IoT device is made up of physical object ("things") + controller ("brain") + sensors + Actuator + Network (Internet).
- An Actuator is a machine component or system that moves or controls the mechanism of the system.
- Sensor is the device sense the environment, then control signal are generated for the actuators according to the actions needed to perform.
- A servor motor is an example of an Actuator they are linear or rotatory actuators, can move to a given specified angular or Linear position.
- We can use servor Motors for IOT application and make the Motor rotate on 90 degrees 180 degrees as per our need.

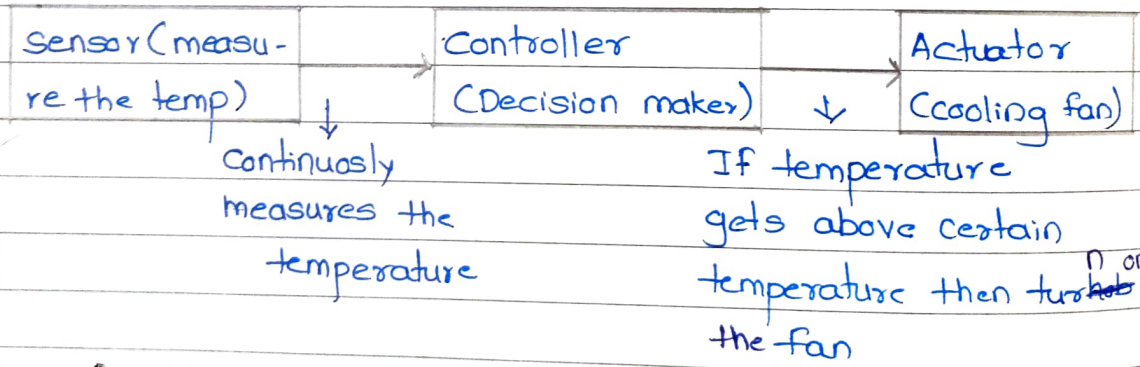


fig. Working of IOT devices & use of Actuators.

- The control system acts upon an environment through the actuator.
- It requires a source of energy and a control signal.
- When it receives a control signal, it converts the source of energy to Mechanical operation.

• Types of Actuator.

1] Hydraulic Actuator.

2] Pneumatic Actuator.

3] Electrical Actuator.

1) Hydraulic Actuator-

- A Hydraulic Actuator uses Hydraulic power to perform a mechanical operation.

- They are Actuated by cylinder fluid motor.

- The Mechanical Motion is converted to rotary, linear, or oscillatory motion according to the need of IOT device.

- Ex- construction equipment uses Hydraulic actuators because Hydraulic actuators can generate a large amount of force.

2) Pneumatic Actuator-

- A pneumatic Actuators user energy formed by vacuum or compressed air at high pressure to convert into either linear or rotary motion.

- Example - used in robotics, use Sensors that work like human fingers by using compressed air.

3) Electrical Actuator-

- An Electrical Actuators uses electrical energy is usually actuated by a Motor that converts electrical energy into Mechanical torque.

- An example of An electrical Actuator is a solenoid based electrical bell.

Q.2 Explain zigbee Architecture in IOT ?

→

- Zigbee is a wireless communication technology designed for low-Power, low-date rate, and short-range communication in the realm of the Internet of things (IOT).

- Its Architecture comprises various elements that enables devices to connect and communicate efficiently in a zigbee network.

- Here's an overview of the zigbee Architecture.

1) Zigbee Coordinator.

- The zigbee network requires one coordinator to initate and manage the network.

- It's typically the root device and controls the overall network setup, including channel selection, securily and addressing.

2) Zigbee end devices.

- These are the devices that operate on the network and are typically sensor or Actuators.

- They have limited capabilities and usually communicate with a zigbee co-ordinator or a router to exchange a bdata.

3) Zigbee Router's

- Routers facilitate communication between end device and the co-ordinator.

- They extend the network's range by passing data between devices and can also functions as an intermediate link for the other devices.

4) Zigbee coordinator & Device communication.

- The coordinator forms the network and assign addresses to devices.
- It manages the network by controlling data transmission, security & addressing schemes.
- Devices can communicate directly with the co-ordinator or through routers.

5) Zigbee protocol stack.

- The zigbee protocol stack comerises Multiple layers.

• Application layers.

-This layer defines the Application-specific functionality and how devices intereact and forming the network topology.

• Network layer.

- Responsible for routing Data within the network, managing device associations and forming the network topology.

• Physical layer.

- Deals with the actual transmission of data through physical medium, specifying the frequency modulation and other physical aspects of communication.

• MAC ( media Access control layer).

- Manages access to physical radio medium and handles the channel selection, device, addressing data.

6) Mesh Networking.

- Zigbee networks often utilize mesh topology enabling device to communicate which Multiple paths.
- This help in extending coverage, improving

reliability & overcoming obstacles that might interfere with direct communication.

7) Low power consumption.
- Zigbee is designed to be power-efficient, allowing devices to operate for extended periods on limited power sources like batteries.

8) Security.
- zigbee offers various security features to protect the network, including encryption, authentication and the ability to setup secure connection between devices

Q.3. Explain WSN characteristic, communication models, security consideration, challenges and Emerging models
→.

- Wireless Sensor Network (WSN) are composed of a collection of sensor nodes that communicate wirelessly to gather data from an environment.
- Following is an overview of their characteristics, communication Models, security consideration challenges and Emeging models.

• Characteristics of WSN:

1) Limited Power.
- Sensor nodes often operate on battery power, necessitating energy-efficient protocol and algorithms.

2) Distributed Deployment.
- Nodes are typically deployed randomly or in a predetermined pattern across an area of interest.

3) Resource Constraints -

- Nodes have limited Memory, processing capability and communication Range, affecting the overall network performance.

4) Dynamic Topology.

- Nodes may move or fail, causing the network topology to change frequently.

5) Data Aggregation.

- Aggregating Data at nodes help in reducing redundant information and conserving energy during transmission.

• Communication Models.

1) flat model -

- All sensor nodes communicate directly with base station.
- It simple's but may lead to high energy consumption closer to the base station.

2) Hierachical Model -

- Nodes are organized into clusters with a hierachy (e.g. cluster heads).
- It helps in reducing energy consumption and improving scalablity.

3) Mesh model.

- Nodes communicate with nearbby nodes, forming a mesh network.
- This model enhances reliability and extends the network coverage.

• Security considerations -

1) Data confidentiality and Integrity -

- Encryption techniques Secure data during transmission and storage to prevent unautorized access or tempering.

2) Authentication.

- Ensuring that only authenticated nodes can enjoy join network to prevent attacks by malicious nodes.

3) Secure Routing protocols.

- Protecting a Routing information and ensuring paths for data transmission to prevent attacks like Pampering or eavesdropping.

• Challenges.

1) Energy Efficiency.

- Maximizing network lifetime by developing energy efficient protocol for data transmission, routing and data aggregation.

2) .

- Developing robust security mechanisms to protect against various attacks due to open & distributed nature of WSNs.

3) fault tolerance.

- Creating mechanisms to handle node failures & maintain network connectivity.

4) Scalability.

- Designing protocols that can handle an increasing number of nodes without a significant drop in performance.

• Emerging Models.

1) Machine Learning in WSNs.

- Integrating Machine learning algorithms to enhance data processing, optimize energy consumption, and improve network performance.

2) Software Define WSNs.

- Employed software-defined networking principle to enhance flexiblity and manageability in WSNs.

3) Blockchain-based security-

- Exploring the use of blockchain technology to enhance security, immutability and trust in WSNs by providing a decentralized and temper resistant framework.

4) Congitive Radio Sensor Network-

- utilizing congitive radio technology to optimize spectrum usage and improve communication Reliablity in WSNs.

Q.4. Explain RFID communication modes, security consideration, Application, challenges?

→

- RFID (Radio frequency Indentification) is a technology that uses Radio waves to identify object or individuals automatically.

- There are different communication modes in RFID, primilarly categorized into 3 main types.

1) Active RFID
2) Passive RFID
3) Semi-Passive RFID.

1) Active RFID-

- In this mode, the RFID tag has it own power source (battery) and can Actively broadcast its signal.

- Active RFID tags can typically transmit signal over longer distance and have higher data transmission rates compared to passive tags.

2) Passive RFID-

- Passive RFID tags do not have an internal power source and instead rely on the electromagnetic energy transmitted by an RFID reader to power the tag and enable communication.

3) Semi-Passive RfID.

- These tags have a small battery to power certain functionalities like the on board sensor or extended communication range.

- They use energy from the RfID reader to power the communication but also have a limited battery life.

• Security consideration in RFID

- RfID systems face various security challenges that need to be addressed to protect data and prevent unauthorized access.

- Some security consideration include:

1) Privacy Concerns.

- Unauthorized Access to RfID Data can lead to privacy breaches, especially when RfID tags contains sensitive information.

- Encryption and Access control Mechanisms help mitigate these risks.

2) Data Integrity -

- Ensuring the Data stored or transmitted by RfID tags is accurate and has not tempered with curical.

- Authentication protocols and Data encryption techniques are employed to maintain data integrity.

3) cloning and Spoofing -

- Unauthorized claning of RfID tags or spoofing the communication between tags and Readers can

leads to security threats.

4) Physical security -

- Protecting the physical infrastructure of RfID systems, including readers and tags, from tempering or unauthorized access is essential to maintain overall security.

• Application of RfID.

1) Supply chain Management -

- RfID is widely used for inventory management tracking goods in supply chain, reducing errors and improving efficiency.

2) Access control and security -

- RfID cards or tags are used for Access control in buildings, parking lots and restricted areas.

3) Retail -

- RfID tags on products enable efficient inventory management reduce theft and improve the shopping experience.

4) Asset Tracking -

- Tracking high-value assets, such as equipment in hospitals, IT Assets in bussinesses, or tools in construction, using RfID technology or efficient monitoring.

• Challenges in RfID Implementation.

1) Cost -

- Implementing RfID system can be costly especially for large-scale application.

2) Interoperability -

- Ensuring the RfID systems from different

manufacturers can work together seamlessly can be challenge.

3) Read Range & Interferance -

- Signal Interferance and limitations in read Range can affect the Reliability and accuracy RFID System.

4) Data Security and Privacy -

- Protecting the Data and ensuring the privacy of Information stored on RfID tags is a continuous challenges due to evolving security threats.

Q.5. Explain all electronic communication protocols?

→

- Electronic communication protocols are set of Rules and Conventions that define how dat is transmitted and Recieved between electronic device.

- These protocol enable device to communicate ensuring seamless and standardized information exchange across networks.

- There are various types of electronic communication protocols used in different Application & here are explanation of some prominent ones.

1) Transmission control protocol / Internet protocol.

- TCP / IP is the foundational protocol suite for the Internet.

- It comprises to Main protocols - Tcp manages the assembly and disassembly of packets, ensuring data transmission reliablity, while IP handles addressing and Routing of data across networks.

2) Hypertext Transfer Protocol (HTTP).

- HTTP is used for transfering hypertext documents on the web.
- It defines how web browser Request web pages from servers and how server respond to the request.
- HTTP is evolved in HTTP/2 and HTTP/3 to improve performance and security.

3) file transfer protocol (FTP).

- FTP is standard network protocol used for transferring files between client & server. on a computer network.
- It provide a way to access, manipulate & transfer file securely.

4) Simple Male Transfer Protocol (SMTP).

- SMTP is a protocol used for sending & Relaying email Message between servers.
- It defines the Rules for how email clients communicate with email Servers to send emails.

5) Post office protocol (POP) and Internet Message Access protocol (IMAP).

- These protocol are used by email clients to retrieve email from a server.
- POP downloads email to a local device while IMAP allow users to Manage email directly on the server.

6) Bluetooth.

- Bluetooth is a wireless technology standard

used for short-range communication between devices.

- It enables device like smartphones, laptops & peripherals to establish connections for data transfers & communication.

7) Wi-Fi (IEEE 802.11)-

- Wifi is a wireless networking Technology that allow devices to connect a local area Network (LAN) wirelessly.

- It operates based on the IEEE 802.11 standards and enables internet access and local network communication.

8) Ethernet -

- Ethernet is widely used standard for wired area networks.

- It specifies how data is transmitted over lan using cabels and defines protocols for device to communicate within a local network.