Internet of Thinks: The Internet of Things (IoT) is a network of interconnected devices that communicate and share data with each other over the internet, enabling them to perform tasks and provide valuable insights without human intervention.
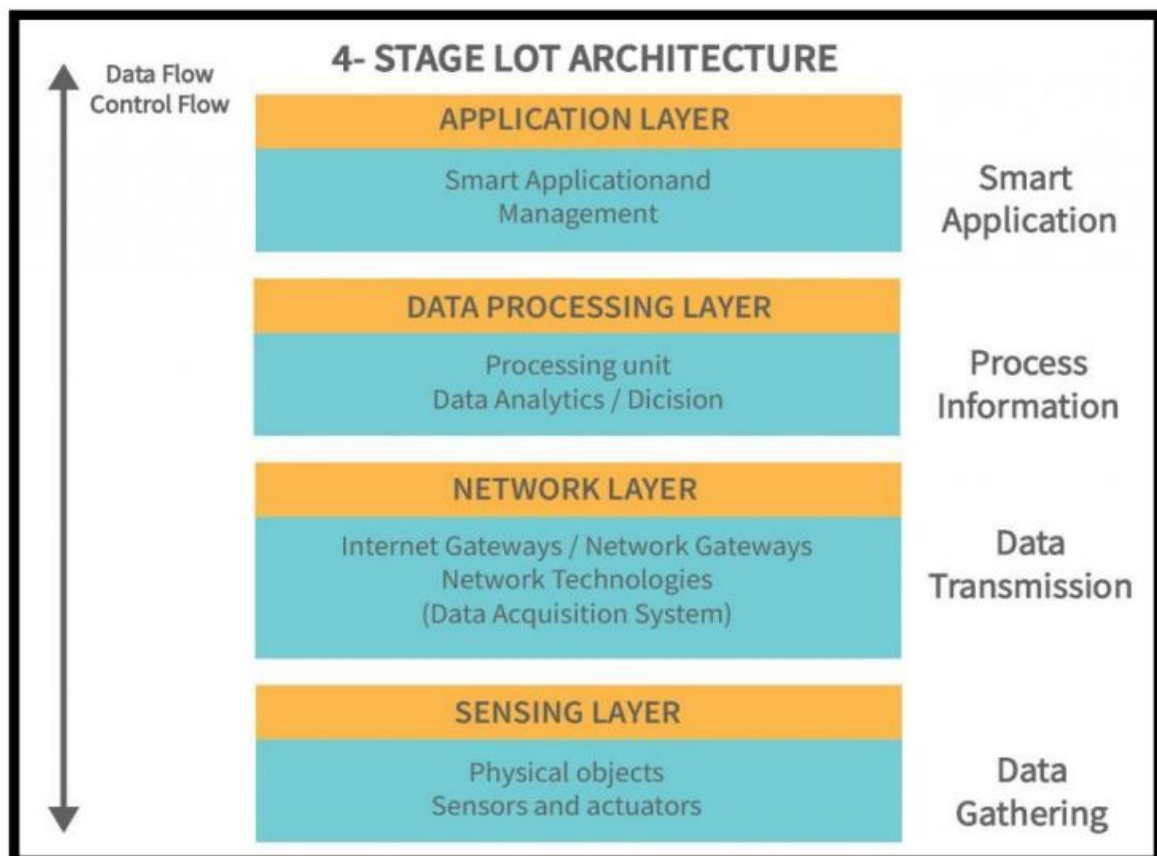
Characteristics of IoT :-

- Connectivity
- Uniuqe Identity
- Scalability
- Dynamic Nature
- Architecture
- Self Adapting
- Self Configuring
- Remote Accessibility
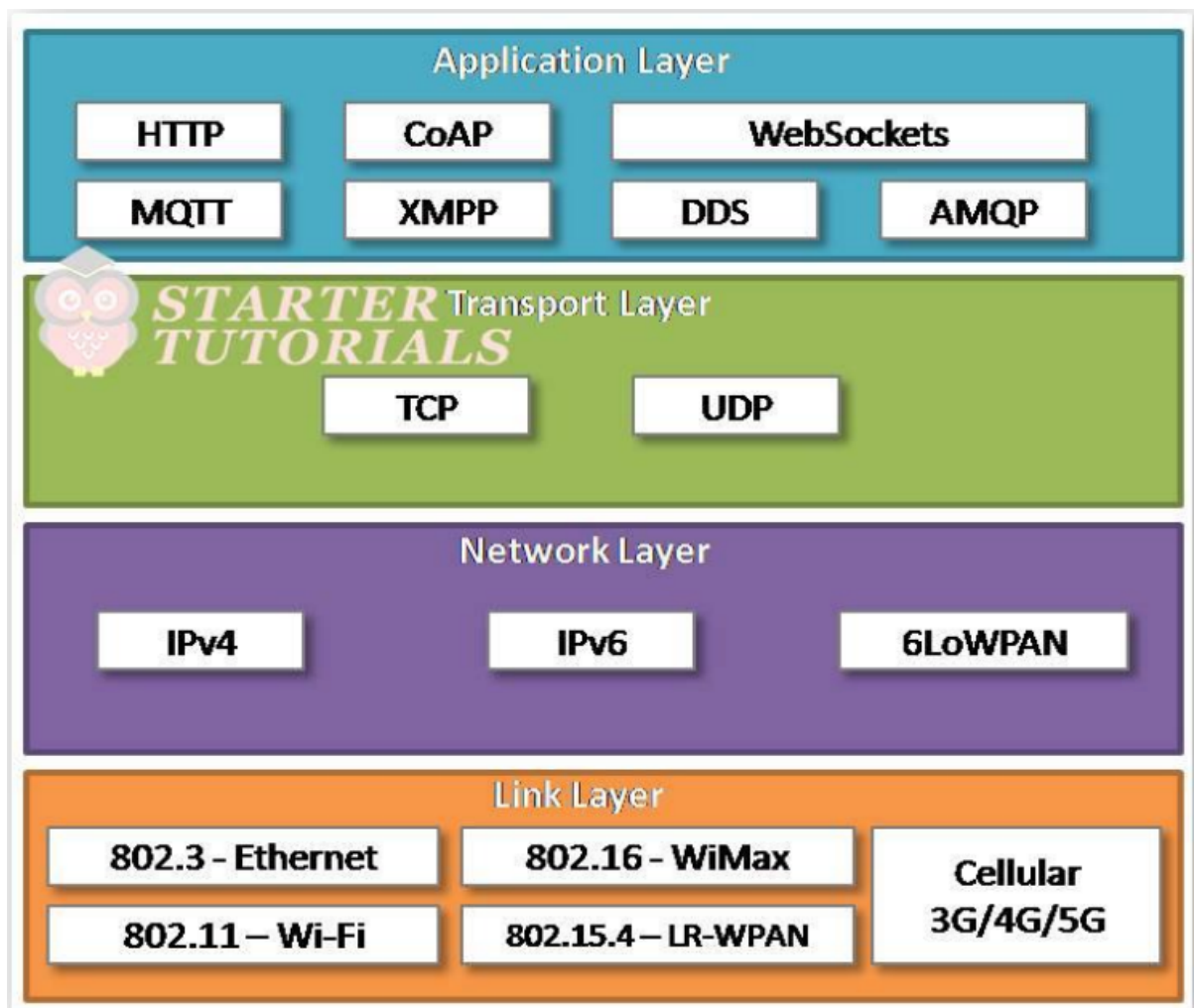- Security and Privacy
- Energy Efficiency

Component of IOT:

- Control Unit
- Sensor
- Communication Modules
- Power Sources

IoT Architecture:
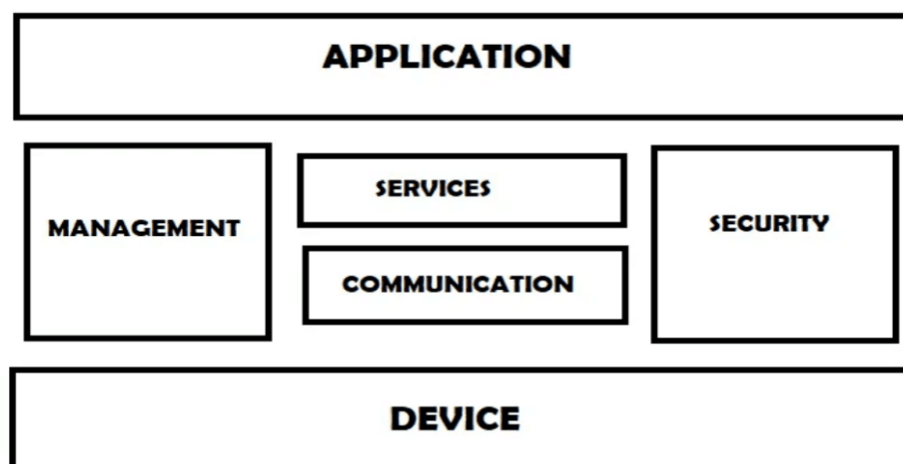
IoT Protocols:

IoT Functional Block:

IoT Communicational Model :

- o Request-Response Communication Model
- o Publish-Subscribe Communication Model
- o Push-Pull Communication Model
- o Exclusive Pair Communication Model

UNIT – 2

M2M : Machine-to-Machine (M2M) communication refers to the exchange of data and information between autonomous devices, machines, or systems without human intervention. It enables interconnected devices to communicate, collaborate, and coordinate actions seamlessly, often in real-time, to achieve specific objectives or perform tasks efficiently.

Security in IOT:
1) CIA Triad:

The CIA triad provides a framework for understanding and implementing security measures to protect information assets effectively. By considering confidentiality, integrity, and availability, organizations can develop comprehensive security strategies to safeguard their data and systems against various threats and risks.

> **A) Confidentiality**
>
> **B) Integrity**
>
> **C) Availability**

2. AAA Framework:

> **a. Authentication:**
>
> **b. Authorization**
>
> **c. Audit Trial**

1. Confidentiality: This refers to the protection of sensitive information from unauthorized access or disclosure. Confidentiality ensures that only authorized individuals or systems can access certain data or resources. Measures such as encryption, access controls, and user authentication help maintain confidentiality.

2. Integrity: Integrity ensures that data remains accurate, consistent, and trustworthy throughout its lifecycle. It involves protecting data from unauthorized modification, deletion, or alteration. Measures such as checksums, digital signatures, and access controls help maintain data integrity and prevent unauthorized changes.

3. Availability: Availability ensures that information and resources are accessible and usable when needed by authorized users. It involves preventing or minimizing disruptions to services, systems, or data. Measures such as redundancy, backups, disaster recovery plans, and network resilience help ensure availability by mitigating the impact of outages, failures, or attacks.

Authentication: Authentication is the process of verifying the identity of a user or system attempting to access a network or resource. It ensures that users are who they claim to be before granting them access. Authentication methods may include passwords, biometrics, security tokens, certificates, or multifactor authentication (MFA).

Authorization: Authorization determines the actions or resources that an authenticated user or system is permitted to access. Once a user's identity has been authenticated, authorization mechanisms enforce policies that define what specific resources or operations the user can perform. Authorization controls may be based on roles, permissions, access control lists (ACLs), or other criteria.

Accounting: Accounting, also known as auditing or accountability, involves tracking and logging the actions of authenticated users or systems. It records details such as who accessed which resources, when the access occurred, and what actions were performed. Accounting information is valuable for monitoring and auditing purposes, compliance with regulations, detecting security incidents, and analyzing usage patterns.

Big Data Analysis :

Types of Big Data Analytics :
- Descriptive Analysis (summarizing historical data)
- Diagnostic Analysis (determine why certain events occurred)
- Predictive Analysis (Forecasting future trends)
- Prescriptive Analysis (What actions should we take to achieve a specific goal?)

Tools :
- MongoDB
- Hadoop
- Python and R
- Spark
- Talend

Embedded System :

As its name suggests, Embedded means something that is attached to another thing. An embedded system can be thought of as a computer hardware system having software embedded in it. An embedded system can be an independent system or it can be a part of alarge system. An embedded system is a microcontroller or microprocessor based system which is designed to perform a specific task. For example, a fire alarm is an embedded system, it will sense only smoke.

UNIT – 3

Sensor is a device used for the conversion of physical events or characteristics into the electrical signals. This is a hardware device that takes the input from environment and gives to the system by converting it. For example, a thermometer takes the temperature as physical characteristic and then converts it into electrical signals for the system.

Environment ———→>— Sensor ———→ Input Conditioning Unit of System
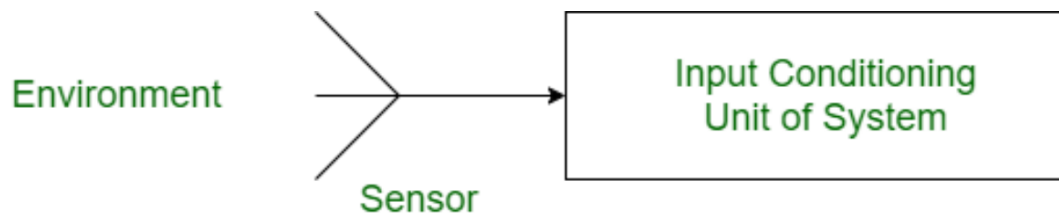
Unit – 4

Basic Building blocks of an IoT Device :

- Sensors
- Internet or Network
- Microcontroller or processor
- Power source
- Actuators
- Memory
- Security feature
- Software
- User Interface (Optinoal)

Raspberry PI :

Application Areas :

- Education
- Home Automation
- Robotics
- Gaming
- Weather Stations
- Security Systems
- IoT (Internet of Things)

Components of Raspberry pi :

- CPU
- GPU
- HDMI PORT
- RAM
- STORAGE
- ETHERNET PORT
- SD CARD SLOT
- Power Source
- USB Ports (Universal Service Bus)

Advantages :

- o Affordability
- o Low power consumption
- o Small Size

- Versatility
- Easy to use
- Community Support

Disadvantages:

- Limited Performance
- Limited size of RAM and Storage
- Generate Lots of heat
- Security Considerations
- Software Compatibility
- Limited connectivity Options

Arduino :

Arduino is an open-source electronics platform designed for creating interactive projects and prototypes. It consists of both hardware and software components that allow users to build a wide range of electronic devices, from simple blinking LED lights to complex robots and automation systems.