M T W T F S S
Page No. YOUVA
Date

Internet of Things -

(1) IoT -

- It stands for Internet of Things.
- It refers to the network of physical objects or 'things' embedded with sensors, software and other technologies that enable them to connect and exchange data with other devices and systems over the internet.
- These objects can range from everyday items such as household appliances, wearable devices and vehicles to industrial machines and infrastructure components.
- The concept behind IoT is to create a connected ecosystem where devices can communicate & interact with minimal human intervention.
- This connectivity enables the collection of data, remote monitoring & control and the automation of various tasks & processes.

It can range from simple sensors to complex systems such as -

1. smart home devices - security cameras, smart locks
2. wearable devices - smartwatches, fitness tracker
3. Industrial devices - sensors in manufacturing plants, logistics tracking
4. connected vehicles - cars with internet connectivity, GPS tracking
5. Smart city infrastructure - intelligent traffic management systems, smart meters
6. Healthcare devices - Remote patient monitoring systems, smart pill dispensers.

Characteristics of IOT -

① Dynamic and self adapting -
- IOT devices and systems should be able to dynamically adapt to changing environment conditions or requirements.
- They can reconfigure themselves, update their software and adjust their behaviour based on real-time data & feedback.
- This self adaptation allows IOT systems to optimise their performance, energy efficiency and responsiveness to changing situations.

② Self-configuring -
- IOT devices should have the capability to self-configure, automatically discovering and connecting to available networks, services or other devices.
- They can negotiate communication protocols, establish secure connections and integrate themselves into existing systems with minimal human intervention.
- Self configuration simplifies the deployment and maintenance of IOT networks, reducing the need for manual configuratn & improving scalability.

③ Interoperable Communication protocols –

- IoT devices & systems often need to communicate with a variety of other devices, platforms & systems, requiring interoperable communⁿ protocols
- Standard protocols like MQTT, HTTP are commonly used to ensure interoperability & seamless commⁿ
- These protocols facilitate data exchange, device discovery & command execution across IoT ecosystems

④ Unique Identity –

- Each IoT device should have a unique identifier such as MAC address, IP address, allowing it to distinctly recognized within the network
- Unique identities enable secure authentication, authorization and communicatⁿ bet devices as well as efficient device management and data attribution
- They also help in tracking, monitoring & controlling individual devices within large scale IoT deployments

⑤ Integrated into Information Networks –

- IoT devices are designed to be integrated into larger information networks, allowing them to commun with cloud services, servers, databases & other IT sy
- This integration enables data aggregation, analysis and decision-making based on the collective data from multiple IoT devices
- IoT devices can leverage the computing power, storage & analytical capabilities of info n/w extending their functionality beyond their local resources

Components of IoT-

(1) Devices / Things - These are physical objects or things that are equipped with sensors, actuators, processors and communication capabilities. Eg - smart home devices, wearables, connected vehicles

(2) Sensors & Actuators - Sensors are devices that detect and measure physical or environmental conditions, such as temperature, humidity, motion. Actuators, are devices that can take actions based on the data received from sensors or commands from control systems.

(3) Communication Technologies - IoT devices communicate with each other & with other systems using various communication technologies such as wifi, bluetooth, cellular network (4G/5G) & wired connections like ethernet.

(4) Cloud platform - cloud platforms are used to manage, monitor and control IoT devices, as well as to store and process the data they generate. These platforms often provide services like device management, data storage, analytics & integration with other applicat

(5) Data processing & analysis - IoT data needs to be processed, filtered & analyzed to extract valuable insights. done through ML, predictive analysis & data visualisation tools

(6) User Interfaces & Applications: UI such as mobile apps dashboards or web app, allows users to interact with IoT devices, control behaviour.

(7) Internet - plays a crucial role as a component in the IoT ecosystem, enables interconnectn & communicatn between IoT devices, gateways cloud platforms & other components. provides connectivity, data transmission, remote access & control.

Ecosystem —

(1) IoT devices collect data from their environment using sensors & transmit it to sensor bridge or directly to IoT services or data analytics problem.
(2) Sensor bridges recieve data from multiple IoT devices, perform local processing if required & forward the data.
(3) Device managers monitor and manage the IoT devices, handling task such as provisioning, updates.
(4) Data analytics platforms process & analyze the incoming IoT data applying techniques like ML, PA & Data visuli.
(5) IoT servicesprovide various functionalities such as device management, data storage, processing & integration.
(6) Controllers & users interact with IoT ecosystem through UI, dashboards, apps.

M T W T F S S
Page No.
Date
YOUVA

Layered Architecture –

① Device Integration layer :-
- this device includes various types of IOT devices and sensors that collect data from the physical world.

It acts as a translator, interpreting sensor data and commands from different language & protocol.

It is responsible for –
① reading sensor data
② interpreting device commands
③ translation

Device management layer –
It is responsible for managing and controlling the IOT devices connected to the system.
this layer receives device registrations & sensor measurement from device integratn layer.
t checks where the status of an actuators changes, lidates the change, translates it to actuators.

Data management layer –
ores all the data collected from IoT devices in entral database.
t as central data hub for entire IoT system
structure depends on the specific requirement

④ Context management Layer –
- This layer represents central business logic and decision making component of IOT system.
- It defines goals & objectives of the IOT system.
- It evaluates situations against the defined goals & trigger actions based on rules or logic.

⑤ Thing Integration layer –
- This layer is responsible for discovering & communicating with other 'things' (devices, systems, apps) in IOT env.
- It verifies if communication with a new 'thing' is possible & handles the registration mechanism.
- It ~~two~~ focuses on communication & collaboration between different devices & systems

⑥ Application Integration layer –
- This layer connects the end user to the IOT system.
- It provides UI, services, API for interacting with IOT system.
- This can ~~include~~ involve data visualization dashboards, controls for sending commands etc.

- physical design of IOT –

① IOT devices – physical devices, sensors, actuators, processors, connectivity

② Communication protocols – lang. devices use to communicate with each other

③ Network infrastructure – connecting devices to cloud or local servers, gateways

Logical design of IOT –

(1) Functional blocks –
Device layer, communicat" l., data manage l., security l & appl" l.

(2) Communication Models –
define how data flows between devices, servers and applications

(1) Request-response model (client-server) –
(1) This is a familiar model where a device (client) initiates communicat" by sending a request for specific data to a server.
(2) The server then processes the request, retrieves the data & sends a response back to device.
(3) This model is suitable for scenarios where devices need to retrieve specific info from central server.

(2) Publish-subscribe model –
(1) this model involves a central message broker that acts as a hub for data exchange.
(2) devices that have data to share (publishers) publish their data to specific topics on broker.
(3) Other devices interested in that data (subscribers) subscribe to those topics.
(4) The broker then delivers published data to all subscribed devices.
(5) efficient for real-time data distribution where multiple devices need to recieve same data simultaneously.

M T W T F S S

Page No. | YOUVA

Date

(3) Push-pull model -

(1) This model involves a more direct exchange between devices & server.

(2) The server can push data to devices based on pre-defined rules.

(3) Devices can pull data from server as upon req.

(4) This model is useful for scenarios where devices need to receive immediate updates.

M2M -

stands for machine to machine communicatn, refers to the direct exchange of data & info. betn devices without human interaction. It forms the foundatn of communicatn within IOT ecosystem.

M2M communicatn -

- core function - enables devices to exchange data and perform action autonomously.
- Benefits -

(1) improved efficiency - automates data collectn & comm. saving time & resources.

(2) Real-time insights - enable real time data exchange for faster decision making & improved responsiveness

(3) Scalability - M2M systems can easily accomodate a growing no. of devices

(4) Reduced costs - automated tasks & eliminates the need for manual intervention, leading to cost savings

M T W T F S S
Page No.
Date
YOUVA

M2M Architecture -

(1) Device layer -
- It consists of physical devices like sensors, actuators & controllers embedding within objects
- Sensors collect data from environment
- actuators perform action based on received instruct
- controllers process sensor data & send commands to actuators

(2) Connectivity layer -
- This layer provides the network infrastructure for devices to communicate with each other.
- Common technologies include cellular networks, wifi, bluetooth & LPWAN

Application layer -
This layer focuses on specific appl^n logic of M2M syst
It defines how data collected from devices will be used to generate insights, triggered actions.
Appl^n can reside on local ~~device~~ servers, cloud platforms.

Difference

Feature	M2M commun	IOT
① Focus	direct data exchange between devices	network of interconnected devices sharing data
② Scope	limited to specific appl^{n}	broader range of devices connect diverse systems
③ Commun^{n}	mostly device-to-device	user interact^{n} through interfaces & app's.
④ user interact^{n}	limited or no direct user interact^{n}	more complex
⑤ Architecture	Simpler	

IP Addressing in IOT –
helps in uniquely identifying devices on the n/w enabling communication & data exchange.

- Unique Identificat^{n} – An IP address acts like a digital address for each device on the network allows devices to recognize & communicate w each other
- Data Routing – when a device sends data its IP address helps route the data to the intended recipient device or server.
- Remote access – IP addresses enable remote access to devices over the internet.

Page No. | YOUVA
Date

Types of IP addresses in IOT:-

(1) Static IP address - These addresses are fixed & manually assigned to devices. used for critical devices that require identificat^n for access.

(2) Dynamic IP address :- addresses are automatically assigned to devices by a dynamic host configurat^n protocol (DHCP). They are more common in home & small business IOT networks

IPv4	IPv6
1) 32 bits (4 octets)	128 bits (16 octets)
2) limited address space	vast address space (unlimited)
3) decimal notation	hexadecimal notat^n
4) No built in security features	supports built in security feat for authenticat^n & encrypt^n

IPv4 served us well for decades, but the internet is growing at an unprecedented pace. IPv6, with its virtually limitless address space enhanced security features and efficient addressing scheme, is the foundation for the internet of future. As the world embrace the IOT and connects a multitude of devices, IPv6 will ensure every device has its own unique address for secure communication channel.

DNS –

- Domain name system acts like the phonebook of the internet. It translates human readable domain names into numerical IP addresses that computers use to locate and connect to websites.
- DNS makes the internet more accessible by allowing us to use memorable domain names.

SDN –

- software defined networking is an approach to network management that offer greater flexibility control and programmability compared to traditional network architectures.

use cases – data center networks, cloud computing, security automation

Benefits –

1. provides a single point of control for the entire network, simplifying configuration & management task.
2. SDN can easily manages a large number of network devices.
3. centralised policy enforcement and network visibility can enhance overall network security.
4. SDN allows for custom appl" for specific n/w needs, leading to more dynamic n/w behaviours.

Sensors – The eyes & ears of IoT –
sensors are the fundamental building blocks of the IoT. They act as the eye & ear of the system capturing real time data about the physical world around us. This data can be anything from temperature & pressure to motion, light & even air quality. By collecting data and analysing it, IoT systems can gain valuable insights, automate tasks.

Characteristics –
1) Sensors are designed to detect and quantify specific physical phenomena or environmental condn
2) Sensors convert the detected data into an electrical signal that can be processed by electronic device
3) Sensors have the ability to detect small changes in the environment
4) IoT sensors need to be compact and lightweight for easy installatn & integratn
5) Most IoT sensors incorporate wireless communic capabilities such as bluetooth, wifi, LPWAN.
6) Depending on the appln, IoT sensors needs to provide accurate and precise measurement with high sensivity.
7) IoT sensors may incorporate security features like data encryption, secure communication protocols and access control mechanisms to protect the collected data.

Classification -
① By operating principles - focuses on the physical phenomenon the sensor utilises to detect.
② By output signal - Analog, digital (based on type of electrical signal they produce)
③ By application - environmental, industrial, medical, security sensors.

Types -
① Environment Sensors -
- Temperature sensors - These sensors measure temperature variations using various principles, such as resistance, voltage, infrared radiation
- Thermostats, industrial process control, weather monitoring, medical devices, food safety monitoring automotive engine temp. monitoring

② Proximity sensors - detect the presence or absence of nearby objects without physical contact using various technique such as capacitance, inductance, infrared light.
- Collision avoidance in robots, automatic door opening systems, (inventory management) touchless controls in electronics, security system

③ Pressure sensors - pressure sensors measure pressure variations in gases or liquid using physical principles such as capacitive sensing, etc.
- weather stations, altitude & measurement in airplanes blood pressure monitors, automotive tire pressure

(4) optical sensors - detect light variations or properties using techniques such as photodiode, light emitting diode (LEDs)
- camera light metering, smoke detectors, barcode scanners.

(5) Humidity sensors - measure relative humidity, moisture content or dew point using physical properties such as capacitance, resistance, etc
- controlling humidity levels in building, greenhouses, storage facilities, weather monitoring

feature	IOT	WOT
focus	connectivity & communicatn bet^n IOT devices	Integratn of IOT devices with web
Appln	smart homes, healthcare, smart cities	web based IOT appln integratn with web
protocols	MQTT, CoAP, HTTP	HTTP, REST, JSON
Communt^n	device-to-device	Device-to-web
Example	Network of smart thermostats communicating with a central hub	Smart home devices from different brands communicating with a central app

Actuators -

Actuators are the muscle of IoT system, translating electrical signals into physical signals/actions that manipulate the environment.
They are electromechanical devices that convert electrical energy into mechanical motion or other forms of physical output.
They receive control signals from IoT controllers based on sensor data.
This allows for automation, remote control & real time responses to changes in the environment.

Applications -

1) Smart homes - control thermostats, adjust lighting, lock & unlock doors, operate blinds.
2) Industrial automation - control motors in production lines, regulate pipelines, activate alarms.
3) Wearable technology - enable feedbacks in smartwatches, adjust lenses in smart glasses.
4) Connected cars - manage engine parameters, control brakes and steering, deploy airbags in case of accidents, adjust car seats.
5) Smart cities - control traffic lights, manage parking meters, activate streetlights, adjust building temperature

Network function Visualisation -
with NFV, instead of each device having its own separate hardware, they can share resources and use software to do the same tasks. It's like having a bunch of apps on your phone instead of separate devices for each task.
It's more flexible, efficient and cost effective.

NFV in IoT Network -

(1) virtualised platform - A central software platform (hypervisor) replaces the physical hardware infrastructure. This platform provides the resources to run virtualised network functions (VNF)

(2) Virtualised network functions - The functionalities previously performed by dedicated hardware are now software programs running on the virtualised platform.

(3) IoT Device communication - IOT devices continue to send data to the network

(4) Data flow & VNF processing - As data flows through the network, it encounters the VNF -
(1) Firewall VNF (2) Load balancer VNF
(3) Data transformation VNF

(5) Management & Orchestration - A central management system oversees the entire NFV environment. manages this lifecycle, & ensures smooth operation.

IEEE 802.15.4 –
It is a widely used standard for creating low-rate wireless personal area network (LR-WPAN). It defines the communication protocols for devices to exchange data over short distances, typically within 10-meter range.

- IEEE 802.15.4 specifies the rules for how devices transmit & receive data wirelessly. It ensures devices from different manufacturer can communicate.

Key features –
1. Low power consumption - optimised for battery-powered devices.
2. Low Data Rate – designed for transmitting small amount of data, ideal for sending sensor reading
3. Simple network formatn - Devices can easily join a network with minimal configuratn
4. Security features – provides basic security mechanisms to protect data from unauthorised access.

Applications –
1. Wireless sensor network –
environmental monitoring, Smart agriculture.
2. Smart Homes –
thermostats, light bulbs, door locks.
3. Wearable devices –
fitness trackers or Smartwatches
4. Building automation systems –
controlling lighting, heating, ventilation air conditioning

- Wireless sensor networks -
- WSN are type of network consisting of spatially distributed, battery powered sensors that communicate wirelessly to collect data and transmit it to a central location.
- They play a vital role in IoT by enabling the connection and monitoring physical conditions.

→ Components -

(1) Sensor nodes - small intelligent devices equipped with sensors to detect and measure parameters like temperature, pressure, humidity, light.

(2) Communicat protocol - like zigbee, 6LOWPAN or Bluetooth low energy used for efficient data exchange between sensor nodes & other n/w components.

(3) Gateway - This act as a bridge between sensor n/w and external world. It collects data from sensor nodes, pre-process it & forwards to central server.

(4) Central server / Cloud platform - This is central location where the collected data is stored, processed, analyzed & visualised.

→ Benefits -

(1) Real time monitoring
(2) Remote data access
(3) cost effective
(4) scalability

Applications -

(1) environmental monitoring
(2) smart cities
(3) Building automation
(4) Health monitoring