Internal Assessment Test 1

Solution

Sub:	Internet of Things					Sub Code:	BCS701	Branch:	CSE
Date:		Duration:	90 mins	Max Marks:	50	Sem / Sec:	3 A,B,C		

Question number

1. a) With a neat diagram explain the physical design of an IOT device.

answer

1. a) **Physical Design of IoT :**

The "Things" in IoT usually refers to IoT devices which have unique identities and can perform remote sensing, actuating and monitoring capabilities.

IoT devices can:

● Exchange data with other connected devices and applications (directly or indirectly), or

● Collect data from other devices and process the data locally or

● Send the data to centralized servers or cloud-based application back-ends for processing the data,

● Perform some tasks locally and other tasks within the IoT infrastructure, based on temporal and
space constraints

Generic block diagram of an IoT Device

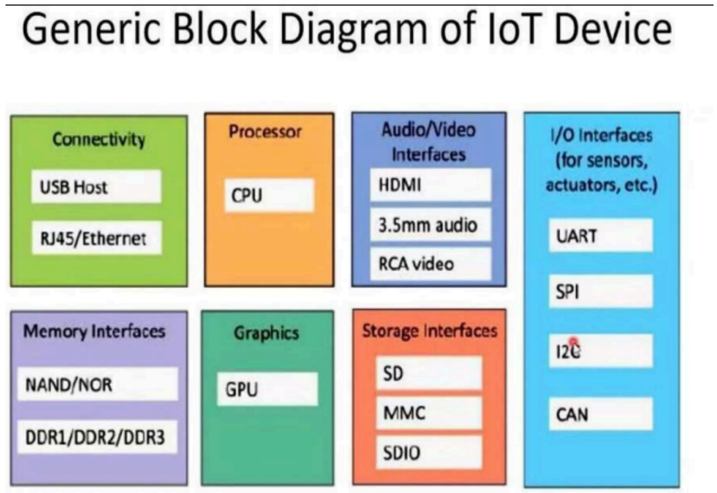
• An IoT device may consist of several interfaces for connections to other devices, both wired and wireless.

• I/O interfaces for sensors

• Interfaces for Internet connectivity

• Memory and storage interfaces

• Audio/video interfaces



HDMI: High definition multimedia Interface.
•
3.5mm: Audio Jack with headphone adapter.
•
RCA: Radio Corporation of America.
•
UART: Universal Asynchronous Receiver Transmitter.
•
SPI: Serial Peripheral Interface.
•
I2C: Inter integrated circuit
•
CAN: Controller Area Network used for Micro-controllers and devices to communicate.
•
SD: Secure digital (memory card)
•
MMC: multimedia card
•
SDIO: Secure digital Input Output
•
GPU: Graphics processing unit.
•
DDR: Double data rate

1.b) With an example describe an IOT service that uses Publish-Subscribe communication model.

A **Smart Weather Monitoring System** collects data (like temperature, humidity, air pressure, and rainfall) from multiple IoT sensors deployed across different locations and shares the information with different users or applications — such as weather dashboards, mobile apps, or alerting systems.

This system uses the **Publish–Subscribe model** for efficient and scalable communication.

1. Publishers (Data Senders)

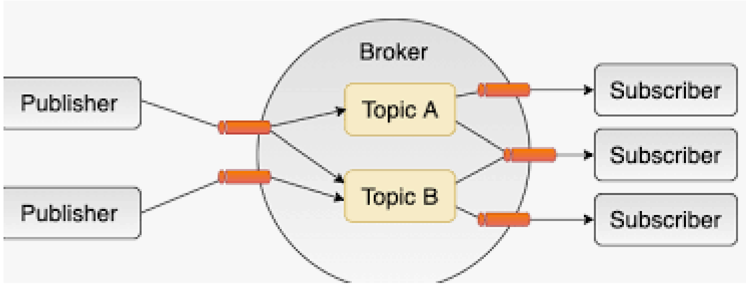
- Devices like **temperature sensors**, **humidity sensors**, and **rainfall gauges** act as **publishers**.
- Each sensor publishes data to a specific **topic** on a **message broker** (like MQTT broker – e.g., *“city1/temperature”*, *“city1/humidity”*).

2. Broker (Message Server)

- A **message broker** (such as **Mosquitto MQTT Broker** or **Google Cloud IoT Core**) receives the data from publishers.
- It **stores and forwards** the messages to all **subscribers** interested in that topic.
- The broker decouples publishers and subscribers — they don’t need to know each other directly.

3. Subscribers (Data Receivers)

- Various applications or devices **subscribe** to topics of interest.
- Example subscribers:
    - A **weather display board** subscribes to `city1/temperature`.
    - A **mobile app** subscribes to `city1/#` (to get all weather parameters).
    - An **alert system** subscribes to `city1/rainfall` to trigger flood warnings.



2.a)What are wireless sensor networks, describe the role of coordinator in wireless sensor networks.

Ans-

Wireless sensor network (wsn) comprises distributed devices with the sensor which are used to monitor the environmental and physical conditions. A WSN consists of a number of end nodes and routers and a coordinator. End nodes have several sensors attached to them. End node can also act as a router. Routers are responsible for routing the data packet from end nodes to the coordinator.

The coordinator node collects the data from all the node coordinates and also acts as a gateway that connects the WSN to the internet. IoT systems are described as follows-

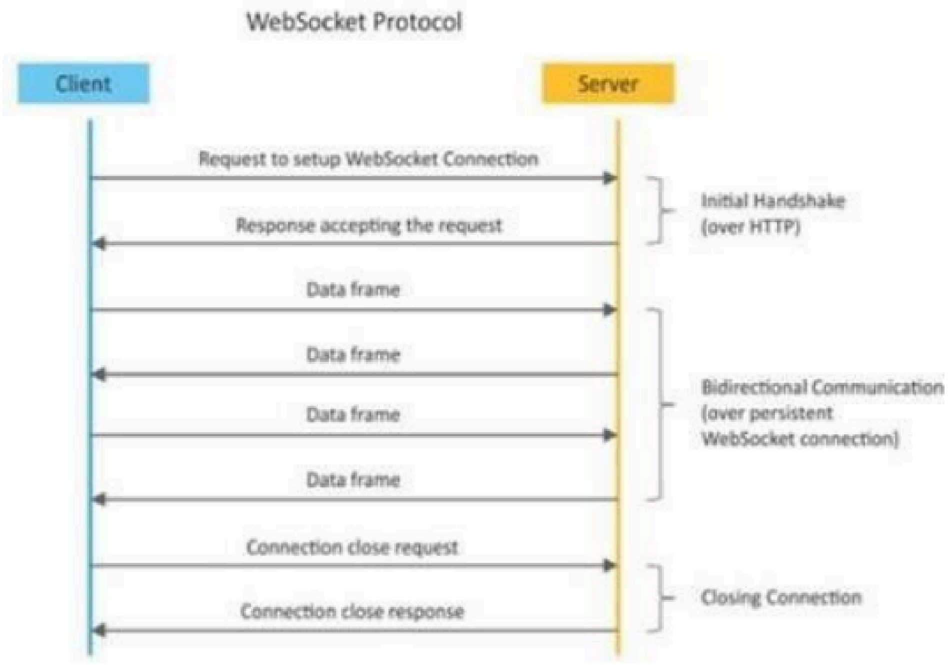
- Weather monitoring system using WSN in which the nodes collect temperature, humidity and other data which is aggregated and analyzed .
- Indoor air quality monitoring system using WSN to collect data on the indoor air quality and connections of various gases.
- Soil moisture monitoring system using WSN to monitor soil moisture at various locations.
- Surveillance systems use WSN for collecting surveillance data(motion detection data)
- Smart grids use wireless sensor networks for monitoring the grid at various points.
- Structural health monitoring systems use WSN to monitor the health of the structure by writing vibration data from sensor nodes deployed at various points in the structure.

2.b) Write short notes on web socket-based communication API.

Ans-

WebSocket Based Communication APIs:

WebSocket APIs allow bi-directional, full duplex communication between clients and servers. WebSocket APIs follow the exclusive pair Communication model


WebSocket Protocol
Client
Server
Request to setup WebSocket Connection
Response accepting the request
Initial Handshake (over HTTP)
Data frame
Data frame
Data frame
Data frame
Bidirectional Communication (over persistent WebSocket connection)
Connection close request
Connection close response
Closing Connection

3. a) Describe IOT level for designing smart health monitoring system
Ans-
IoT system has multiple end nodes and one coordinator node. The end nodes that perform sensing and or actuation. Coordinator node collects data from the end node and sends it to the cloud. Data is stored and analyzed in the cloud and applications are cloud based.
Level 5 IoT system are suitable for solutions based on wireless sensor networks, in which data involved is big and analysis requirements are computationally intensive.
A **Smart Health Monitoring System** continuously tracks patients' vital parameters using sensors and IoT devices, analyzes the data, and alerts doctors or caregivers in case of abnormalities.
It provides real-time health updates and predictive analysis through cloud and AI technologies.

Perception Layer (Sensing Layer)

Function: Collects physiological data from the human body.

Components:

- Sensors: Heart rate, temperature, blood pressure, ECG, SpO_2 (oxygen level), glucose sensors
- Devices: Smartwatches, fitness bands, or wearable health patches

Network Layer

Function: Transfers sensor data to cloud or edge devices for further processing.

Technologies Used:

- Bluetooth, Wi-Fi, ZigBee, 4G/5G, or LoRaWAN
- Communication between sensor → smartphone → cloud server

Processing Layer (Middleware Layer / Edge Computing Layer)

Function: Processes and filters raw data before sending it to cloud analytics.

Components:

- Microcontrollers or gateways (Raspberry Pi, ESP32)
- Edge computing for preliminary analysis (reduces latency)

Application Layer

Function: Provides user-friendly applications and dashboards for visualization and monitoring.

Components:

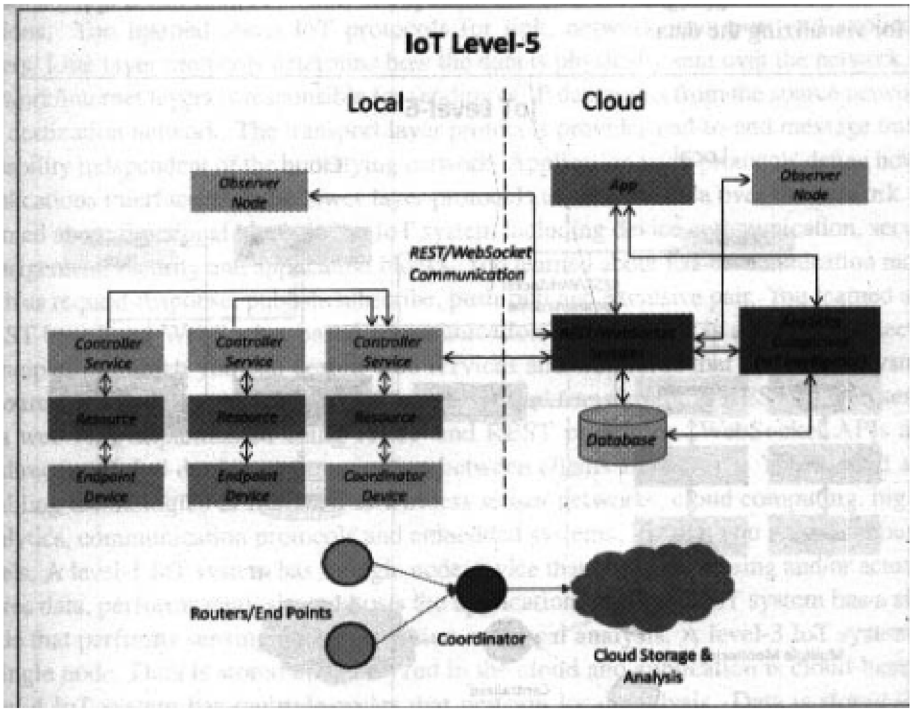
- Mobile apps, hospital monitoring dashboards, or web-based portals
- Displays reports, graphs, and real-time notifications

Business Layer

Function: Manages overall IoT system operations, analytics, and decision-making.
It turns data into **actionable insights** using AI and cloud analytics.

Components:

- Cloud servers and data analytics tools
- Machine learning models for disease prediction and trend analysis
- Decision-making systems for healthcare professionals



3.b)Explain the role of communication block in an IOT system
Ans-
The **communication block** plays a **central role** in any IoT system — it is the **bridge** that connects devices, sensors, gateways, and cloud platforms, allowing data to flow seamlessly from the physical world to the digital world.

The communication **block** in an IoT system is responsible for **transmitting data** collected by sensors (perception layer) to other devices or cloud servers where it can be processed, analyzed, and visualized.

It ensures **reliable, secure, and efficient data exchange** between all IoT components.

Main Functions of the Communication Block

1. **Data Transmission**
    - Transfers sensor data from devices to gateways, servers, or cloud platforms.
    - Ensures low-latency and lossless communication.
2. **Network Connectivity**
    - Establishes connections between IoT devices using wired or wireless technologies.

    - Examples: Wi-Fi, Bluetooth, ZigBee, 4G/5G, LoRa, or Ethernet.

3. **Protocol Management**
    - Uses communication protocols to define how data is formatted, transmitted, and received.
    - Common IoT protocols: **MQTT**, **CoAP**, **HTTP**, **AMQP**, **DDS**.
4. **Device-to-Device / Device-to-Cloud Communication**
    - Enables direct or indirect interaction:
        - **Device-to-Device:** Smartwatch to smartphone
        - **Device-to-Cloud:** Sensor sending data to ThingSpeak or AWS IoT
5. **Data Routing and Synchronization**
    - Handles how data packets move across the network.
    - Ensures synchronization between multiple devices in real time.
6. **Security and Encryption**
    - Protects transmitted data from unauthorized access using encryption and authentication techniques (TLS/SSL).

4. a)Describe the architecture of SDN

Ans-

Software defined Networking(SDN)

SDN stands for Software Defined Network which is a networking architecture approach. It enables the control

and management of the network using software applications. Through Software Defined Network (SDN)

networking behavior of the entire network and its devices are programmed in a centrally controlled manner

through software applications using open APIs.

To understand software-defined networks, we need to understand the various planes involved in networking.

1. Data Plane

2. Control Plane

Data plane:

All the activities involving as well as resulting from data packets sent by the end-user belong to this plane.

This includes:

- Forwarding of packets.
- Segmentation and reassembly of data.
- Replication of packets for multicasting.

Control plane:

All activities necessary to perform data plane activities but do not involve end-user data packets belong to

this plane. In other words, this is the brain of the network. The activities of the control plane include:

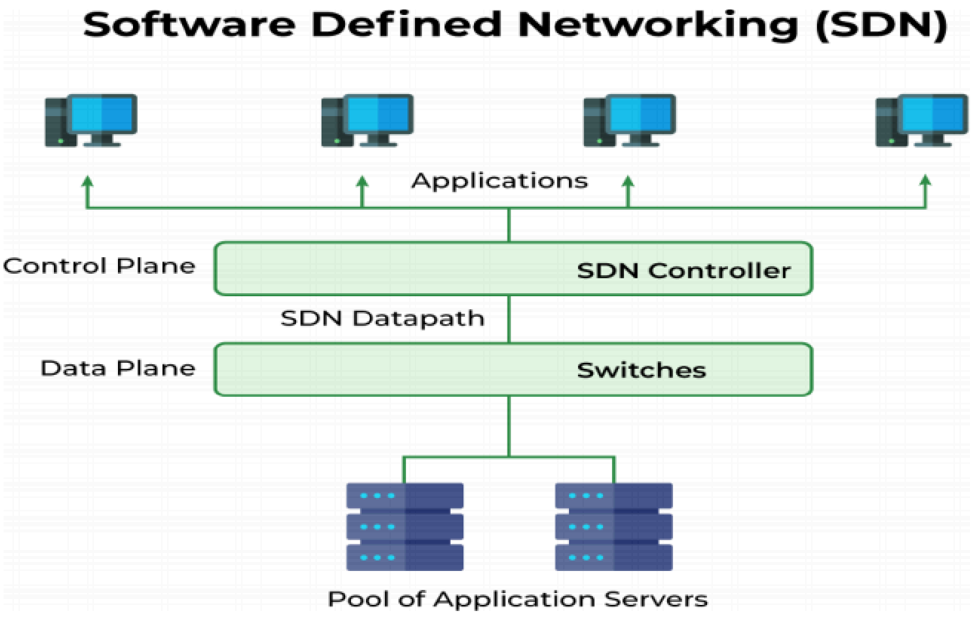
- Making routing tables.
- Setting packet handling policies.

SDN provides —-

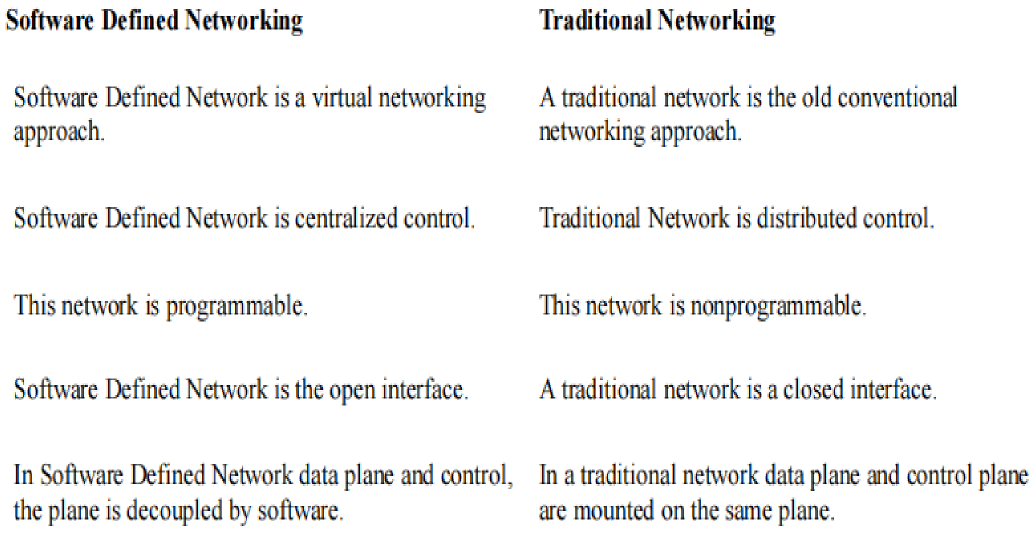
Better Network Connectivity: SDN provides very better network connectivity for sales, services, and internal communications. SDN also helps in faster data sharing.

- **Better Deployment of Applications:** Deployment of new applications, services, and many business models can be speed up using Software Defined Networking.
- **Better Security:** Software-defined network provides better visibility throughout the network. Operators can create separate zones for devices that require different levels of security. SDN networks give more freedom to operators.
- **Better Control with High Speed:** Software-defined networking provides better speed than other networking types by applying an open standard software-based controller.

In short, it can be said that- SDN acts as a “Bigger Umbrella or a HUB” where the rest of other networking technologies come and sit under that umbrella and get merged with another platform to bring out the best of the best outcome by decreasing the traffic rate and by increasing the efficiency of data flow.



4. b) How is SDN different from traditional networking,



Software Defined Networking	Traditional Networking
Software Defined Network is a virtual networking approach.	A traditional network is the old conventional networking approach.
Software Defined Network is centralized control.	Traditional Network is distributed control.
This network is programmable.	This network is nonprogrammable.
Software Defined Network is the open interface.	A traditional network is a closed interface.
In Software Defined Network data plane and control, the plane is decoupled by software.	In a traditional network data plane and control plane are mounted on the same plane.

5.a) Explain the general architecture of M2M systems
Ans-

Machine-to-Machine (M2M) refers to networking of machines (or devices) for the purpose of remote monitoring and control and data exchange. Figure shows the end-to-end architecture for M2M systems consisting of M2M area networks, communication network and application domain. An M2M area network comprises machines (or M2M nodes) which have embedded hardware modules for sensing, actuation and communication. Various communication protocols can be used for M2M local area networks such as ZigBee, Bluetooth, ModBus. These communication protocols provide connectivity between M2M nodes within an M2M area network. The communication network provides connectivity between remote M2M area networks. The communication network can use either wired or wireless networks (IP-based). While the M2M area networks use either proprietary or non-IP based communication protocols, the communication network uses IP-based networks. Since non-IP based protocols are used within M2M area networks, the M2M nodes within one network cannot communicate with nodes in an external network. To enable the communication between remote M2M area networks, M2M gateways are used.

Figure 3.2 shows a block diagram of an M2M gateway. The communication between the M2M nodes and the M2M gateway is based on the communication protocols which are native to the M2M area network. M2M gateway performs protocol translations to enable IP-connectivity for M2M area networks. M2M gateway acts as a proxy performing translations from/to native protocols to/from Internet Protocol (IP). With an M2M gateway, each node in an M2M area network appears as a virtualized node for external M2M area networks

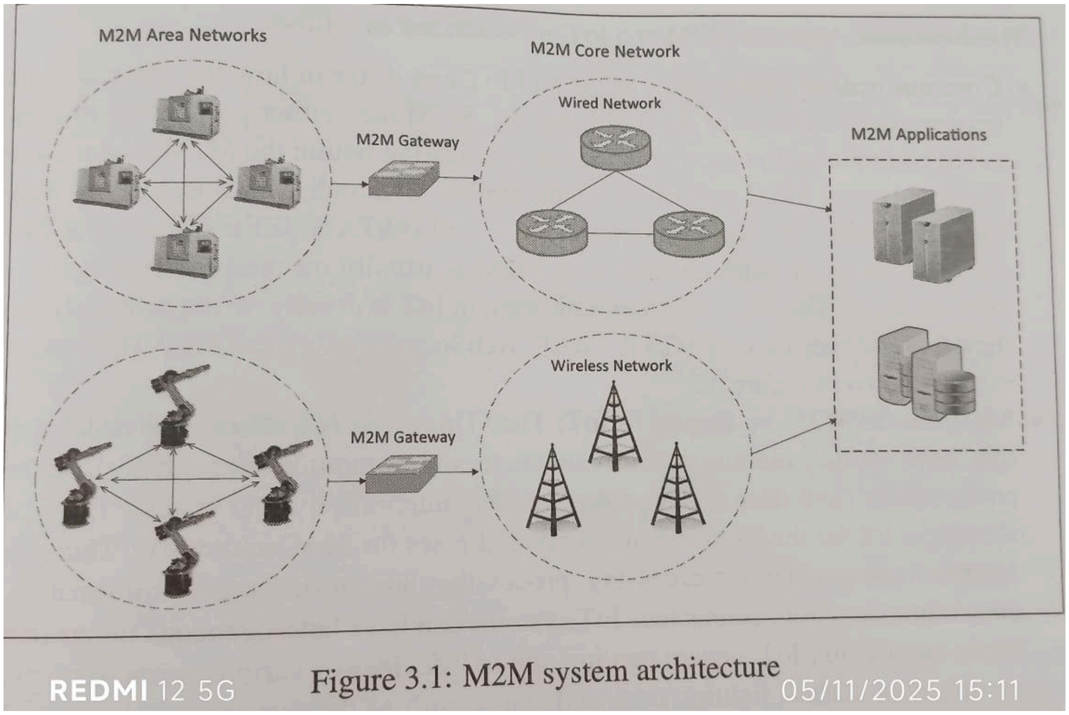
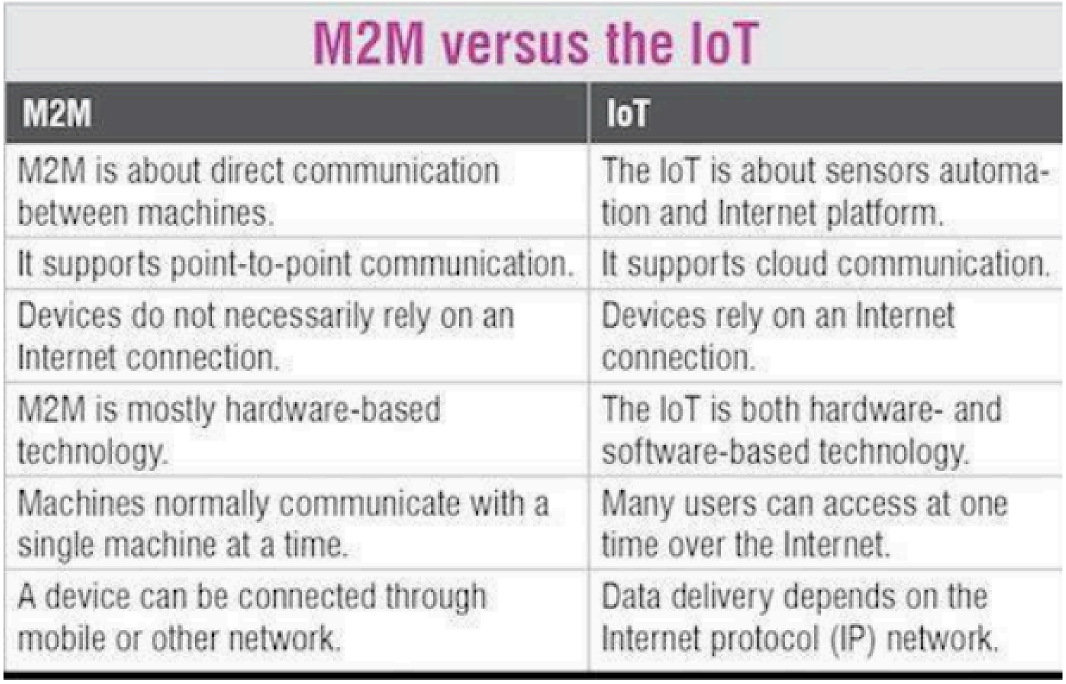


Figure 3.1: M2M system architecture

5. b) Explain how data collection and analysis approaches differ in M2M and IOT
Ans-



M2M versus the IoT

M2M	IoT
M2M is about direct communication between machines.	The IoT is about sensors automation and Internet platform.
It supports point-to-point communication.	It supports cloud communication.
Devices do not necessarily rely on an Internet connection.	Devices rely on an Internet connection.
M2M is mostly hardware-based technology.	The IoT is both hardware- and software-based technology.
Machines normally communicate with a single machine at a time.	Many users can access at one time over the Internet.
A device can be connected through mobile or other network.	Data delivery depends on the Internet protocol (IP) network.

6.a) Describe how NPV can be used for virtualization of IOT devices

Ans- Network Function Virtualization

Network Function Virtualization (NFV) is a technology that leverages virtualization to consolidate the heterogeneous network devices onto industry standard high volume servers, switches and storage. NFV is complementary to SDN as NFV can provide the infrastructure on which SDN can run. NFV and SDN are mutually beneficial to each other, but not dependent. Network functions can be virtualized without SDN, similarly, SDN can exist without NFV.

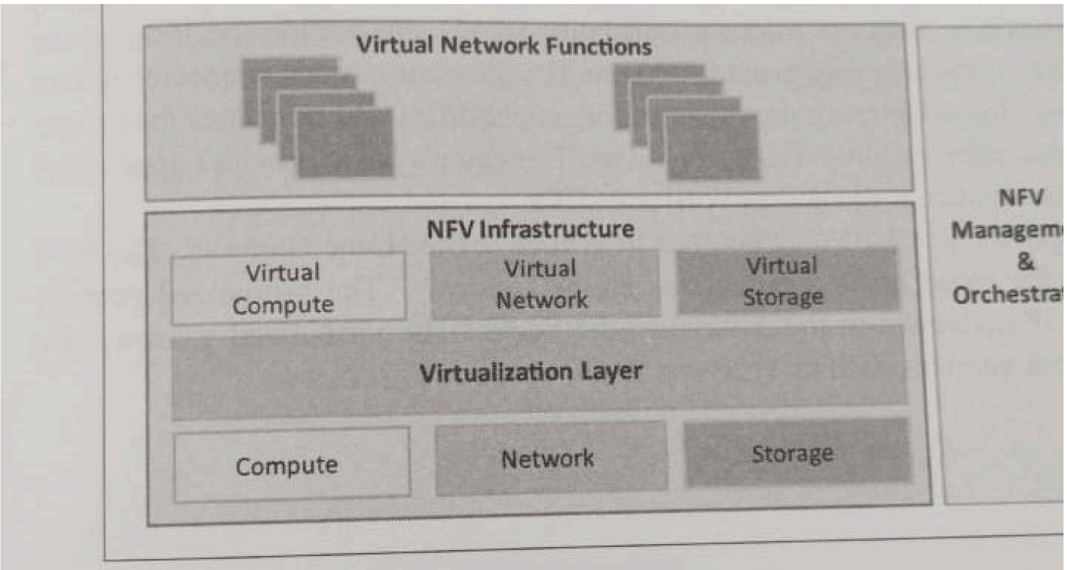


Figure 3.11: NFV architecture

Figure 3.11 shows the NFV architecture, as being standardized by the European Telecommunications Standards Institute (ETSI) [82]. Key elements of the NFV architecture are as follows:

- **Virtualized Network Function (VNF):** VNF is a software implementation of a network function which is capable of running over the NFV Infrastructure (NFVI).

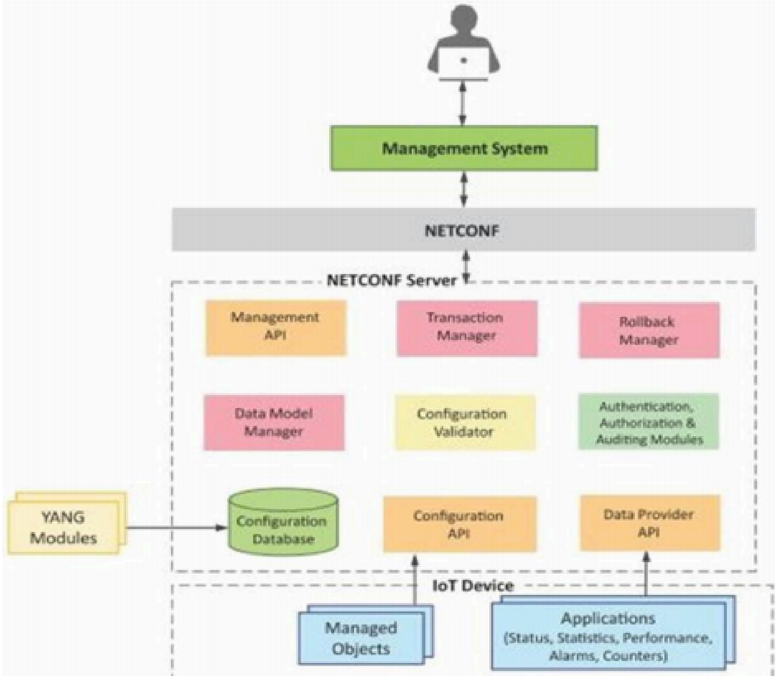
- **NFV Infrastructure (NFVI):** NFVI includes compute, network and storage resources that are virtualized.

- **NFV Management and Orchestration:** NFV Management and Orchestration focuses on all virtualization-specific management tasks and covers the orchestration and life-cycle management of physical and/or software resources that support the infrastructure virtualization, and the life-cycle management of VNFs.

NFV comprises network functions implemented in software that run on virtualized resources in the cloud. NFV enables separation of network functions which are implemented in software from the underlying hardware. Thus network functions can be easily tested and upgraded by installing new software while the hardware remains the same. Virtualizing network functions reduces the equipment costs and also reduces power consumption

b) Describe the role of NETCONF-YANG modules in device management

Ans-YANG is a data modeling language used to model configuration and state data manipulated by the NETCONF protocol.
ThegenericapproachofIoTdevicemanagement with NETCONF-YANG.
Roles of various components are:
1) ManagementSystem
2) ManagementAPI
3) TransactionManager
4) RollbackManager
5) Data ModelManager
6) ConfigurationValidator
7) ConfigurationDatabase
8) ConfigurationAPI
9) Data ProviderAPI



1) **Management System :** The operator uses a management system to send NETCONF messages to
configure the IoT device and receives state information and notifications from the device as
NETCONFmessages.
2) **ManagementAPI :**allowsmanagementapplicationtostartNETCONFsessions.
3) **Transaction Manager:** executes all the NETCONF transactions and ensures that ACID properties
hold true for the transactions.

	4) **Rollback Manager :** is responsible for generating all the transactions necessary to rollback a current configuration to its original state. 5) **DataModelManager:** KeepstrackofalltheYANGdatamodelsandthecorresponding managed objects. Also keeps track of the applications which provide dataforeach part of a datamodel. 6) **Configuration Validator :** checks if the resulting configuration after applying a transaction would be a valid configuration. 7) **ConfigurationDatabase:**containsbothconfigurationandoperastionaldata 8) **Configuration API :** Using the configuration API the application on the IoT device can be read configuration data from the configuration datastore and write operational data to the operational datastore. 9) **DataProviderAPI:** Applications on the IoTdevice can register for callbacks events using the Data Provider API. Through the Data Provider API, the applications can report statistics and operational data.