IOT

Introduction to IOT:

The IoT is a concept which enables the communication between internetworking device and appliances whereby physical objects or things communicate to internet. The concepts of IoT begin with things as identity communication device.

RFID – Radio frequency identification device is an example of identity communication device.

IOT Defination: IOT means network of physical ~~visible~~ things sending receiving or communicating information using the internet or other communication technology and network just as a computers, tablets and mobile which enables monitoring, co-ordinating or controlling process across the internet for another data network.

Ex: Smart watch, washing machine.

IOT life cycle:

Collect

① Devices ⟶ communicate ⟶ Analyse ↓ Act

② Sensors

NFC → near field comm^{n}.

① Collection: Devices & sensors are collecting data everywhere.

② Communication :- Different technology, NFC, private data center, zigbee, cloud platform sending data and events trough network to same destination.

③ Analyse: Building reports, creating visiulise the data, filtering → graph / table form

④ Act : Communicate with one machine to another machine, sending information.

IoT Vision: IoT is a vision where things (variable watches, alarm clock, home-device) becomes smart and function like living entities by sending, computing and communication through embeded device which interact with remote objects (Servers), clouds, applines, services and process or persons through the internet or near field communication (NFC).

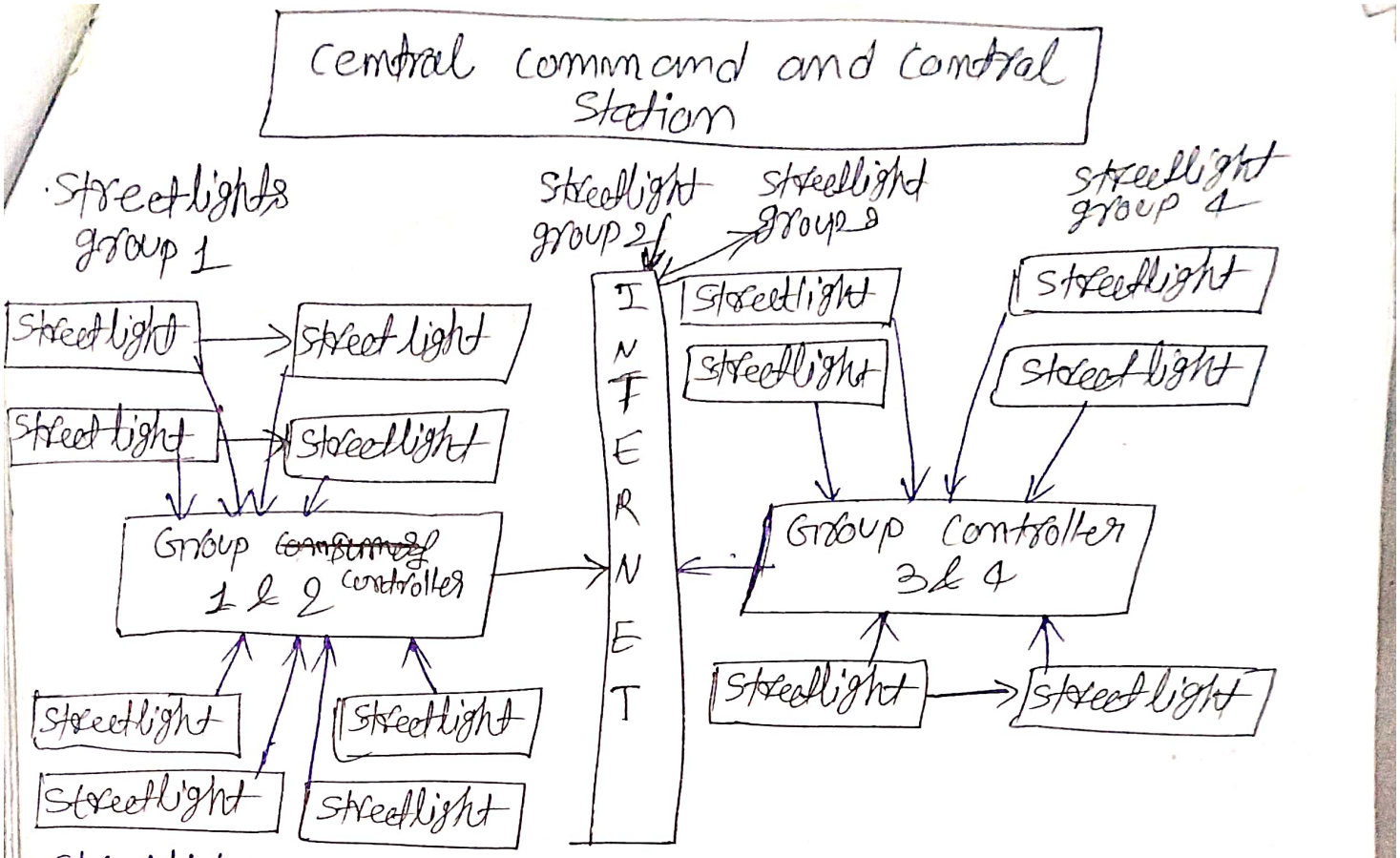
Ex: umberalla can be made to function like a living entity by installing a tiny embeded device which interact with a web based weather Service and a device owner through the internet. A website regularly publish the weather report, the umberalla recives these reports each morning and analyse the data and issues reminder to the owner at his/her office going time.

→ ~~Bluetho~~ Bluetooth, sms, → technology are used.

→ the message can be

① Protect yourself, from rain, it's going to rain, Bring your umberalla.

② Protect yourself from sun, it's going to be hot ~~today~~ today don't forget to bring umberalla.



Streetlight in a city can be made to function like living entities through sensing and computing using tiny embedded devices that communicate and interact with the central control and command station through the internet. Assume that each ligh in a globe of 32 streetlights deals with a sensing, computing and communication circuit. each group connects towards group controller to Bluetooth or zigbee, each controller further connects to central command & control ~~salat~~ station through the internet The station receives information about each street light in each group in the city at period intervals. The information received is related to the functioning of 32 lights, faulty lights, about the presence or absence of traffic in groups, weather cloudy, dark or normal day light.

The station remotely programs the group controller which automatically takes an appropriate action as per the condition of traffic and light level

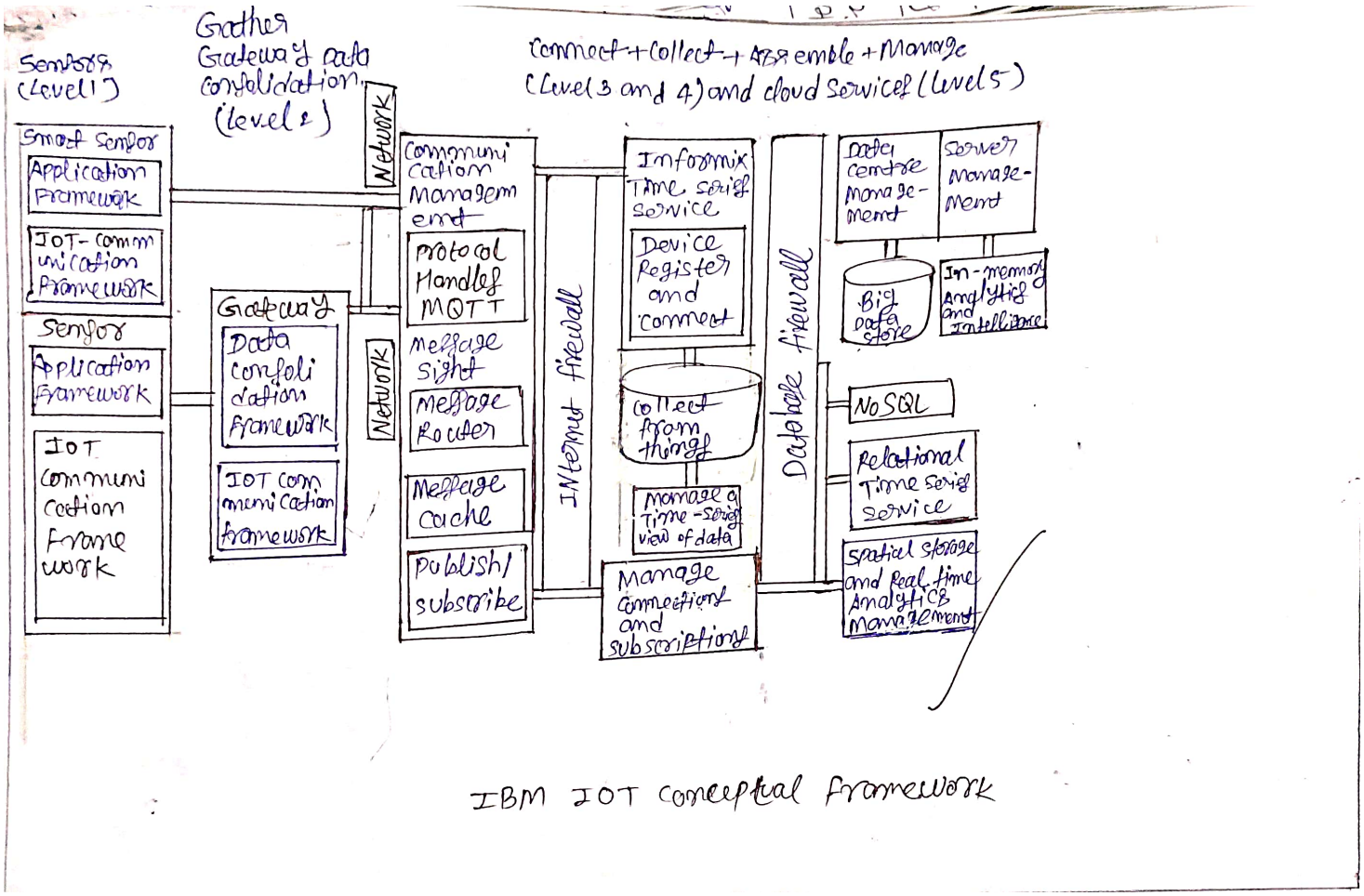
Smart and Hyper Connected devices :

Hyper/constantly Connectivity means use of multiple systems and devices to remain constatly connected to social networks network and streams of information.

Smart devices: Smart devices are devices with computing & communication capabilities that can constantly connected to the networks is known as Smart device.

Example:

* Hyper Connected RFID's: An RFID's or Smart labours is tag to all consignment, this way many confinment send from a place can be constantly back.



IBM IOT conceptual framework

equation 1 : physical object + controller, sensor & actuators + internet
= IOT give by IBM

equation 1st conceptualy describes the internet of umbrella of comprising of an umberalla, controller, sensor & actuator and the internet for connectivity to a web service and a mobile service provider forming an IOT.

equation 2 → gather + enrich + stream + manage + Aquire + organize & analyse = IOT with connectivity to data center or cloud server.
given by oracle

equation second the steps are of follow

① at Level 1 Data of the devices using sensors for the things gether the predata from the internet

L2 → A Sensor Connected to a gateway femetions of smart Sensor ie Smart Sensor refers to a Sensor with compiting and comm^n capacity". the data them enrich at level 2 for example by transcoding ie transpoding means coding or decoding befor data transfer b/w 2 emdities ".

L3 → A communication management subsystem sends and receives data streams. at level 3

L4 → Device management, access management subsystem recieve the device data at level 4

L5 → Aquire → Data store for database aquires the data at level 5

oral & only : Data routing routed from the device & things organise & analyse at level 6.

Gather + Consolidate + connect + collect + Assemble + manage + analyse = IoT with connectivity to cloud Service

Equation 3:

equation 3rd represent a complex conceptual framework for IoT using cloud platform based process and services the steps are as follows.

(i) Level 1 and Level 2 consist of a sensor network to gather and consolidate the data. 1st level gathers the data of the things using sensor circuits. The sensor connects to a gateway. Data from consolidate at the second level. for example transformation at the gateway at level 2.

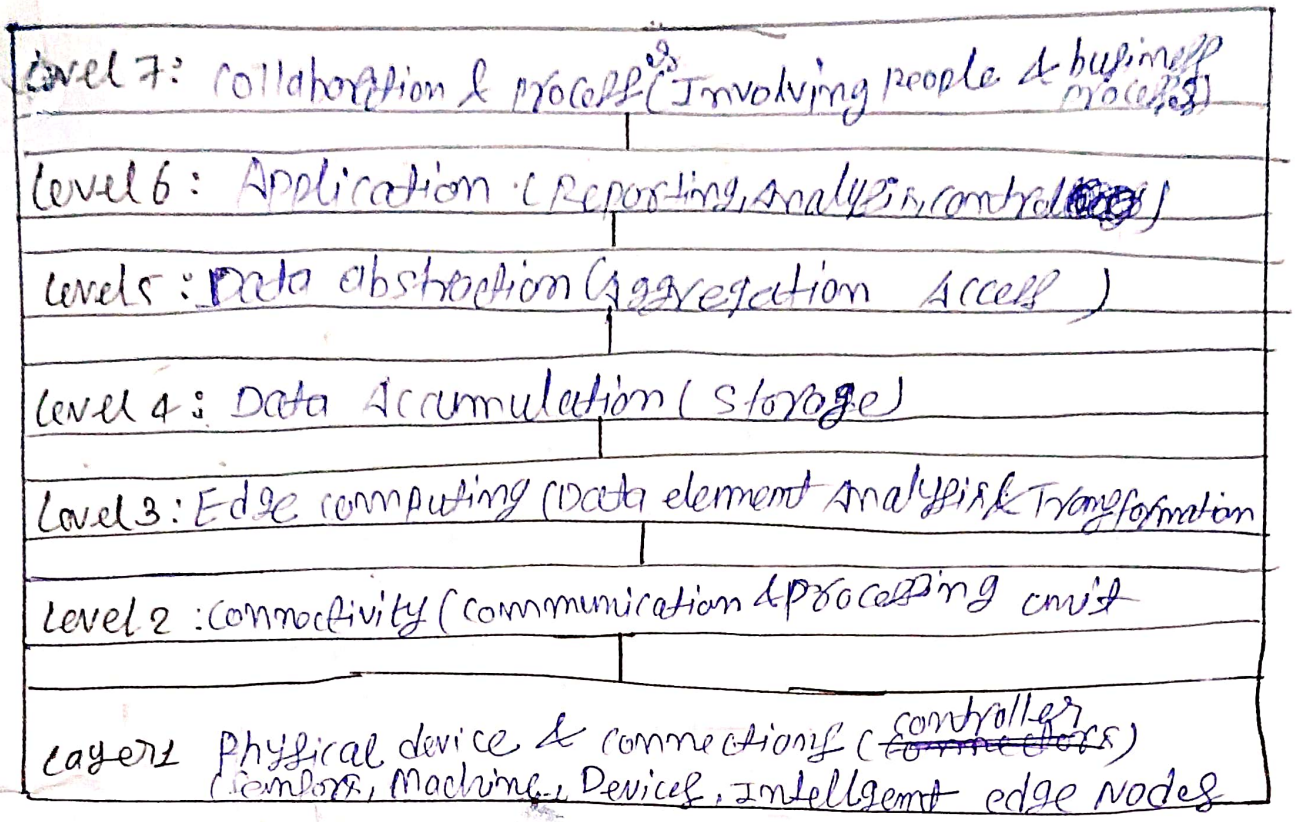
(ii) The gateway at level 2 communicate the data streams between levels and levels 3. The system level 3. uses of communication - management subsystem at

(iii) An information service consist of connect, collect, assemble and manage subsystem at level 3 and 4. The service render from level 4.

(iv) Realtime series analysis, data, analytics and intelligence subsystem are also at level 4 & 5. A cloud infrastructure, a data store or database aquires the data at level 5.

IOT Architecture view (Main components used)

CISCO : seven layered reference model

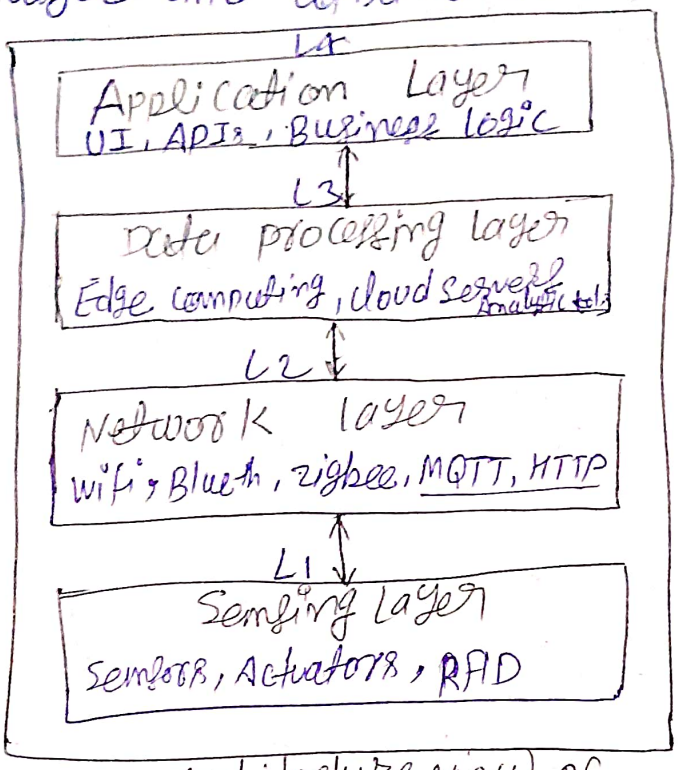


An IOT system has multiple levels. These levels are also known as tiers. A model enable conceptualization of a framework. A reference model can be used to depict the building blocks, successive interactions and integration. An example is CISCO representation of a reference model has seven levels.

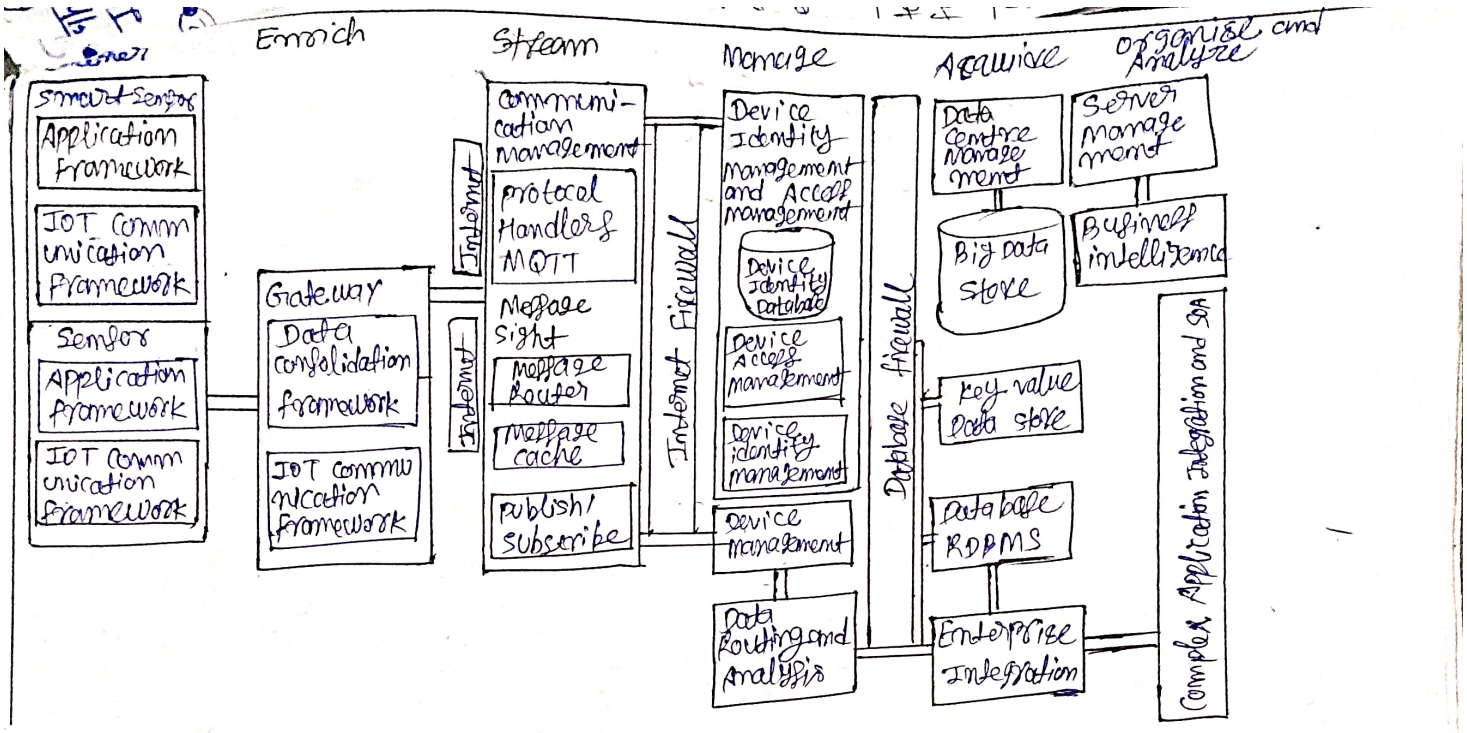
A reference could be identified to specify reference architecture.

Pg 10 List the major components involved in an IoT architecture. Provide a simple overview of architectural view of an IoT system.

An IoT system architecture typically consists of multiple layers and components that work together to collect, process, analyze and utilize data for interconnected devices.



Architecture view of IOT



IOT Architecture by oracle

An Architecture has the following features

- The architecture serves as a reference in applications of IOT in services and business processes.

(2) • A set of sensors which are smart, capture the data, perform necessary data element analysis and transformation as per device application framework and connect directly to a communication manager.

(3) • A set of sensor circuits is connected to a gateway processing separate data capturing, gathering, computing and communication capabilities. The gateway recieves the data in one form at one end and sends it in another form to the other end.

(5) • The management communication subsystem has functionalities for devices identity database, device identity management and ~~per~~ access management.

(6) • Data routes from the gateway through the internet and data centre to the application server or enterprise server which acquires that data.

(7) • Organisation and analysis subsystem enable the services, business processes, enterprise integration and complex processes.

(4) • The communication-management subsystem consists of protocol handlers, message, routers and message cache

Technology Behind IOT

The following entities provide a diverse technology environment

- Hardware : Arduino, Raspberry pi, intel Galileo, intel Edison.
- IDE (Integrated Development Environment) for developing device software, firmware and APIs.
- protocols : RPL, CoAP, RESTful HTTP, MQTT, XMPP (extensible messaging and presence pro
- Communication : powerline Ethernet, RFID, NFC, 6LoWPAN, ~~Bluetoo~~ Bluetooth, WiFi, ZigBee, WiMax, 2G/3G/4G/5G
- Network backbone : IPV4, IPV6, UDP and 6LoWPAN.
- Software : RIOT OS, Contiki OS, Eclipse IOT.
- Internetwork cloud platform : Nimbits, Azure, Semle, Xively, AWS IOT, CISCO IOT, TCS CUP.
- Machine learning algorithm and software : An example of machine learning software is GROK ~~from Numenta~~ that uses machine intelligence to analyse the streaming data from clouds and environment factors. that ~~helps~~ has ability to learn continuously from data and ability to drive action from the output of GROK's data models.

* Technology behind IOT: IOT is the combination of technologies that enable devices to communicate and interact with each other. key technologies are:

(1) Hardware Technologies: Sensors, Actuators, Arduino, Raspberry, MP, MC.

(2) Communication Technologies: wife, zigbee, bluethooth, cellular

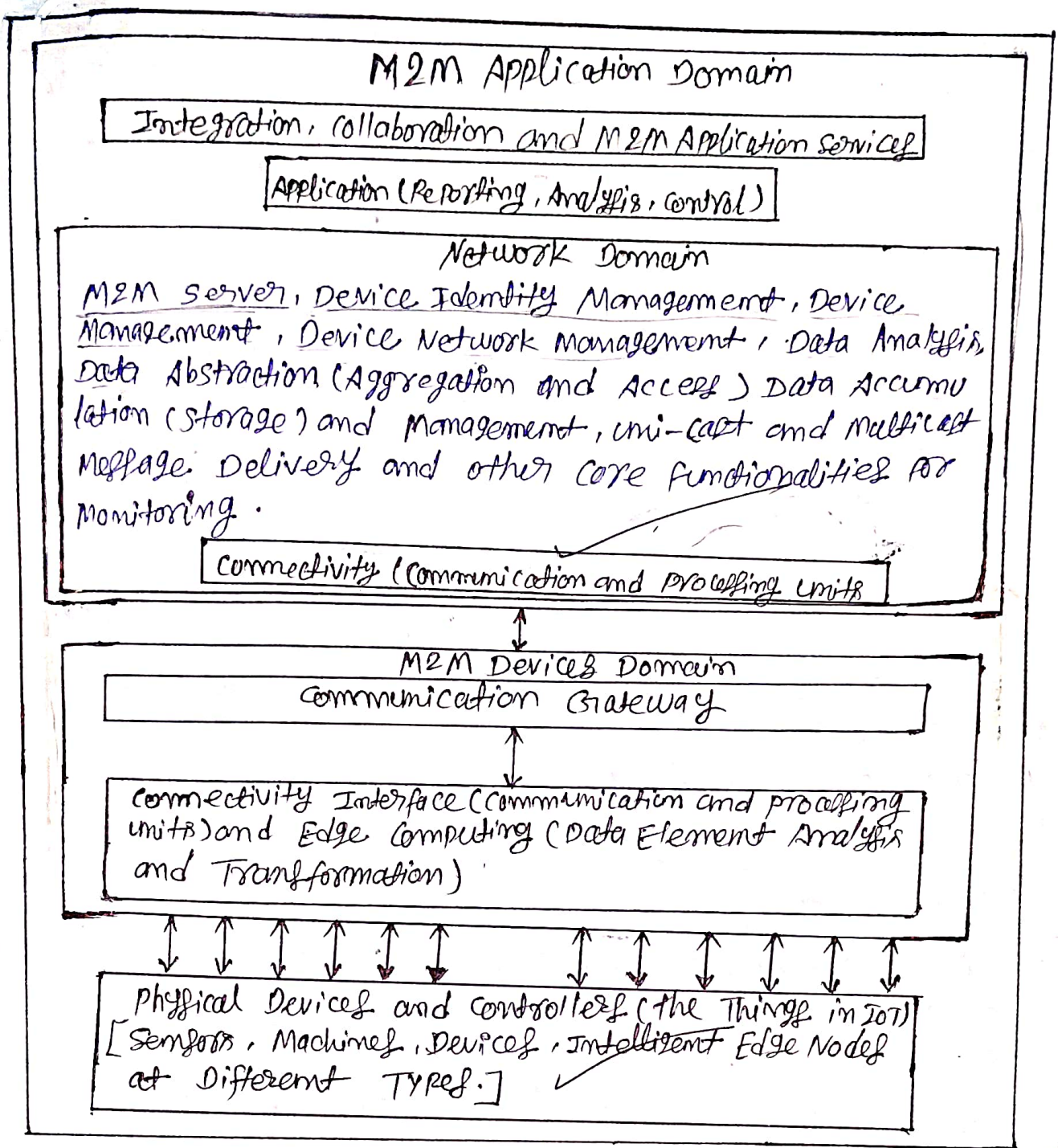
(3) Communication protocols: MQTT, HTTP, ~~IPV4, IPV6~~, XMPP

(4) Cloud computing: AWS IOT, Google cloud IoT, Microsoft Azure IOT.

(5) Software Technologies: operating system: RIOT, contiki OS, TinyOS

(6) Network Technologies: IPV4, IPV6, 6lowPAN, UDP Eclipse IoT

M2M Architecture



M2M refers to the process of communication of ~~with~~ physical object or device at machine with others of the same type mostly for monitoring. but also for control purpose. Each machine in M2M system embeded the smart devices. The device sends the data and status of the machine

and perform the computation protocols & communication function. A device communicate via a wired or wireless system. The communication protocols are 6LoWPAN & LWM2M, MQTT & XMPP, each communication device is assigned IPV6 (48-bit address).

M2M to IOT

M2M technology enables direct communication between devices without using the internet, primarily for tasks like coordination, monitoring, and control. It has application in industry automation, logistics and smart grids. IOT expands on M2M by integrating the internet, allowing devices to communication over networks, analyze data, and provide services through cloud-based applications. while M2M focuses on devices-to-devices communication, IOT incorporates broader connectivity and data-driven processes across various industries.

M2M Architecture

M2M architecture consists of three domains

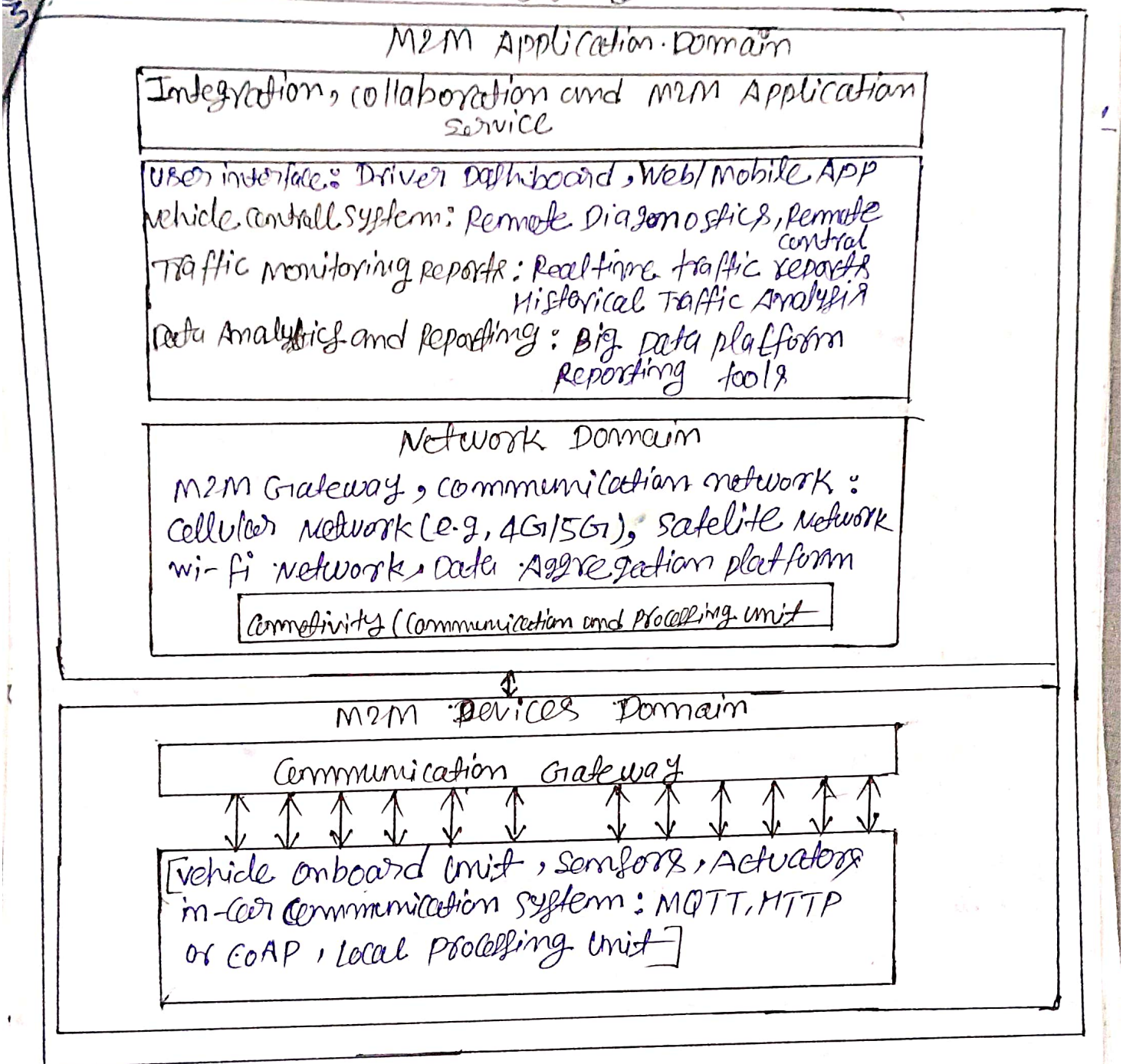
1. M2M device domain
2. M2M network domain
3. M2M application domain

1. M2M device domain: M2M device communication domain consists of three entities: physical devices, communication interface and gateway. communication interface is a port or a subsystem, which receives the input from one end and sends the data received to another.

2. M2M Network domain: M2M Network domain consists of M2M Servers, device identity Management, data analytics and data and device Management Similar to IOT architecture (Connect + Collect + Assemble + analyse) level.

Application domain: M2M application domain consists of solution for services, monitoring, analysis and controlling of devices networks.

Case-Study on traffic reports, central monitoring



1. M2M Device Domain:

Components:

(i) Vehicle onboard unit (OBU): Embedded systems in the car that include sensors and communication modules.

(ii) Sensors: Gather data such as speed, location (GPS), fuel levels, engine diagnostics, and traffic conditions.

(iii) Actuators: Control systems for functions like braking, acceleration, and lights.

- In-Car Communication system: It connects the OBU to the M2M network, supporting protocols like MQTT, HTTP or CoAP
- Local processing unit: Processes data locally to reduce latency and perform immediate actions.

functions: • Data Collection: collects data from various sensors in the vehicle.

• local processing: Analyze data to make immediate decisions (eg. alert driver of maintenance needs)

• Communication: Sends data to the M2M network and receives commands.

(2) M2M Network Domain

Components:

M2M Gateway: Interfaces b/w vehicle local network and external networks. It handles data routing.

Communication Network:

- Cellular Network: Transmits data from the vehicle to the cloud and receives updates or commands.
- Satelite Network: Optional, for areas without cellular coverage.
- Wifi Network: For communication within range of wi-fi access points
- Data Aggregation platform: Aggregates data from multiple vehicles and manages network communication.

Functions:

- Data Transmission: facilitates communication b/w the vehicle and the application domain.
- Data Aggregation: collects Data from multiple vehicles and processes it.
- Network management: Ensures reliable and secure communication.

M2M Application Domain
components

- Traffic Monitoring System: Collects and Analyzes traffic data to provide insights and reports.
  (i) Real-time Traffic Reports: offers updates on traffic conditions
  (ii) vehicle control system
- Remote Diagnostics: Allows remote monitoring and diagnostics of vehicle health.
  (i) Remote control: Enables remote actions (eg: locking doors, engine control)
- User Interface:
  (i) Driver Dashboard: provides real-time updates and alerts to the driver.
  (ii) Web/Mobile App: Allows users to interact with vehicle data, control features, and view traffic reports.
- Data Analytics and Reporting:
  (i) Big Data platform: Analyzes large volumes of data for insights and trend analysis.
  (ii) Reporting Tools: Generates reports on vehicle performance, traffic conditions, and more.

functions:

- Traffic Management: provides real-time traffic data and insights for better route planning.
- vehicle monitoring: monitors vehicle health and provides remote diagnostics and control.
- user interaction: provides interfaces for drivers to interact with vehicle and traffic data.
- Data Analysis: processes and analyzes collected data to provide actionable insights.

M2M application domain: M2M application domain consists of application for services, monitoring, analysis and controlling of devices networks.

Example of M2M software and development Tools:

(i) Mango: mango is an open source M2M software
(ii) MainSpring.
(iii) Devicehive.

Question type: Draw the Architecture view of M2M application for a car, for trafficing report, controll and monitoring. (Case Study).

Unit-2

Design principles for connected devices

A No of international organization have taken action for IOT design and standardization.

(i) IETF → IETF An information body that initiated actions for addressing and workings on the recommendation for engineering specification for the IOT.

(ii) ITU-T : International telecommunication union for - Telecommunication : ITU-T suggested a reference model. for IOT domain, network, and transport capabilities for the IOT services and Application forth layer.

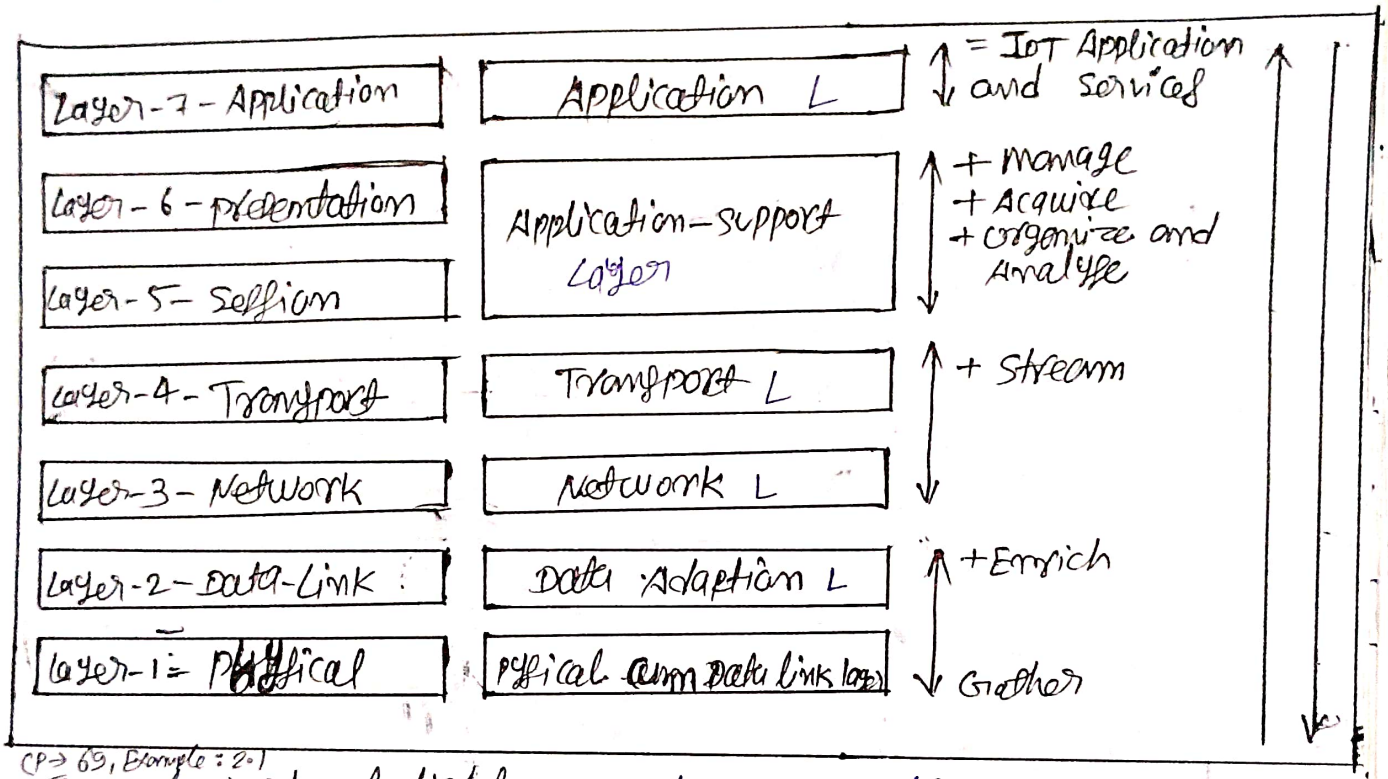
(iii) ETSI : European Telecommunication standard Institute : ETSI initiated the development of a set of standard for a network, device and Gateway domains for the communication b/w M2M.

* Modified OSI Model for IoT (How old OSI diff from modified)

OSI protocol means a family of information exchange standards developed jointly by the ISO and ITU-T. The seven layer OSI model is a standard model. It gives the basic outline for designing communication network. various models for data interchanges consider the layers specified by the OSI model and modify it simplicity according to the requirement.

Figure shows a classical 7-layer OSI model and the modification in that model proposed by IETF. Data communicates from device end to application end. Each layer processes the received data and creates a new data stack which transfers it to the next layer.

Gather + Enrich + Stream + Manage + Acquire + Organise + Analyse = IOT Applications and Services.



CP → 69, Example : 2.1

Example : Street light : consider a model for streetlights L1 : It consists of smart sensing and data-link circuits with each streetlight transfering the sensed data to L2.

L2 : It consists of a group-controller with receives data of each group through Bluetooth or zigbee, aggregates and compacts the data for communication to the internet, and controls the group streetlights as per the program commands from a central station.

L3: It communicates a network stream on the internet to the next layer.
L4: The transport layer does device identity management identity registry and data routing to the next layer.
L5: The application-support layer does data managing, aquiring, organizing and analyzing and functionalities of standard protocols such as COAP, UDP and IP.
L6: The Application layer enables remote programming and issue of control station directions to switch on-off and commands of services to the controllers along with monitoring each group of streetlights in the whole city.

- ITU-T Reference model:

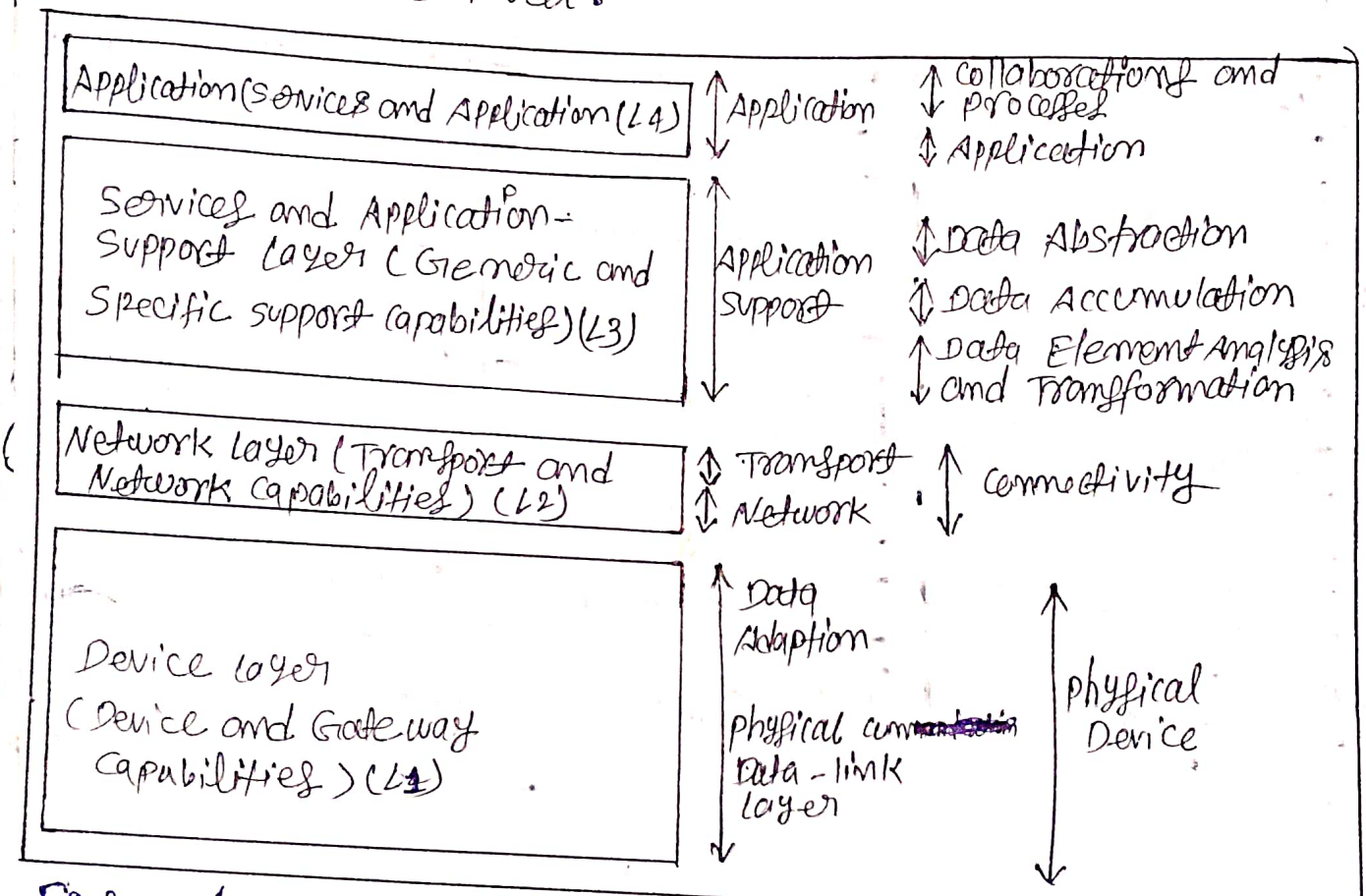


Figure shows the ITU-T reference model RM1. It also shows correspondence of the model with six layers modified OSI model.

- Lowest layer, L1, is the device layer and has device and gateway capabilities.
- Next layer, L2, has transport and network capabilities.

- Next layer, L3, is the Services and application-support layer. The support layer two types of capabilities - generic and specific service or application-support capabilities.
- Top layer, L4, is for applications and services

Example: Consider a model for internet of RFIDs.

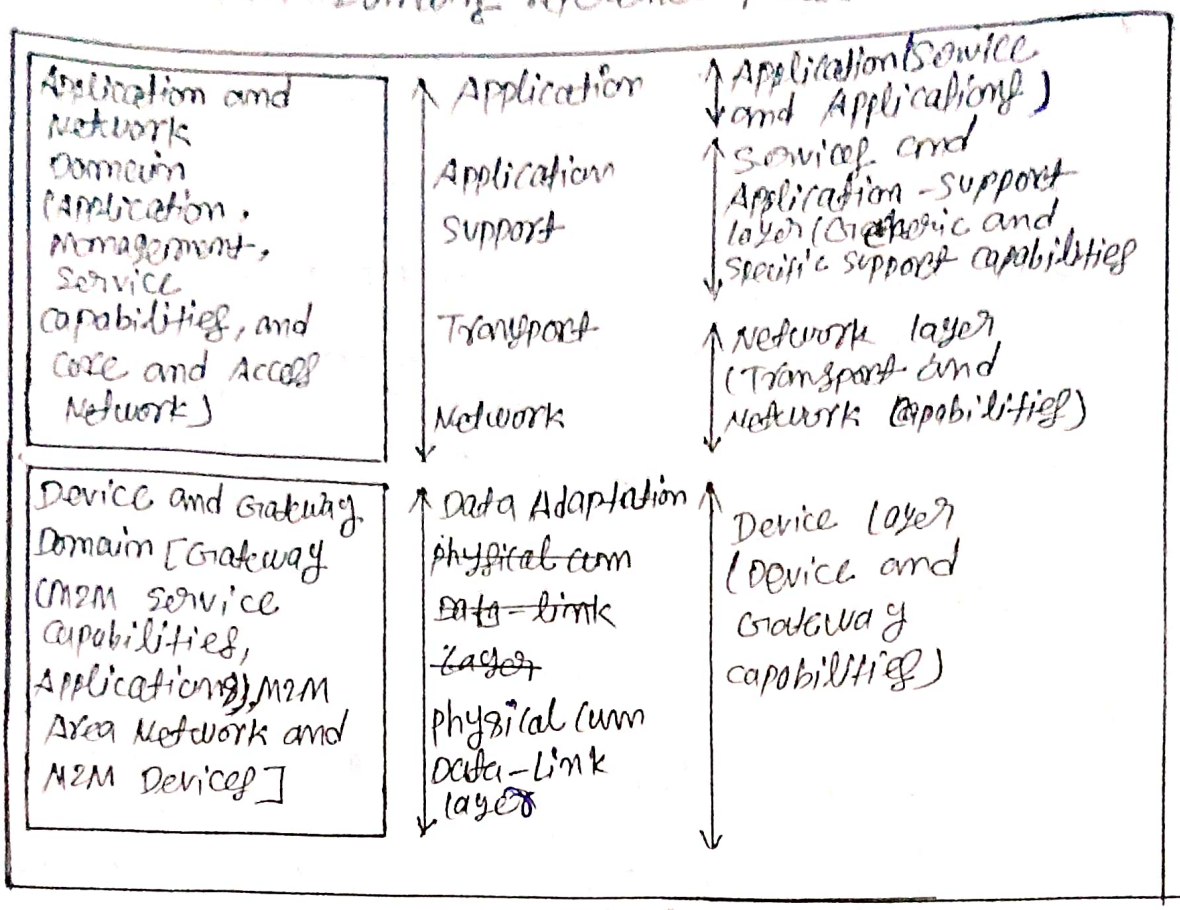
1. Layer 1 (Device and Gateway): This layer includes the RFID physical devices and readers that capture ID data and send it wirelessly to an access point.

Layer 2 (Transport and Network): This layer involves the access network, including access points and internet connectivity, which transports the data to servers.

Layer 3 (Services And Application support): This layer is responsible for managing RFID device registeries, ID management, data routing, and analyzing RFID data.

Layer 4 (Services and Applications): This layer supports applications like tracking, inventory control, and managing business processes such as supply-chain management.

* ETSI M2M Domain reference Model



The ETSI M2M (Machine-to-Machine) architecture is divided into different domains, each focusing on specific functions. The architecture to both the modified OSI model's six layer and ITU-T reference model's four layer. The main capabilities and functions within the ETSI network domain include:

1. M2M Applications: These are the actual service that support M2M applications.
2. M2M Service capabilities: These provide services that support M2M applications.
3. M2M Management functions: ~~These handle the management of the network itself.~~ These manage the M2M services and devices.
4. Network Management functions: These handle the management of the network itself.
5. Core Network: This includes networks like, 3G, IP networks

and controls how different networks connect with each other.

6. Access Network: This includes types of networks that provide access, such as LPWAN, Wi-Fi, and WiMax.

Example:
In the ETSI high-level architecture for applications and services in the internet of ATM machine, there are two main domains.

1. Device and Gateway Domain: This domain includes the ATM machines and the cards used in them. The ATM gateway manages ATM services and applications, handles card and banking data and controls the exchange of information between the ATM and the bank's server. It also monitors cash dispensing and other ATM services, all connected through a network. The gateway ensures that the data is processed and transmitted correctly according to the network protocol.

2. Applications and Network Domain: This domain handles the management of ATM operations and the network they use. It includes banking applications and services that supports ATM functions. The domain connects to the bank's core network, which links all the ATM gateway's access networks, ensuring smooth communication and operation across the entire system.

Design principle for web connectivity

An IOT M2M Device network gateway need connectivity to web server, A communication gateway enables web connectivity, while IOT/M2M specific protocols and methods enable web connectivity for a connected device network. A server enables IoT device data accumulation. Application, collaboration service and processes use this data.

Assignment No. 1

Sub: IOT
Name: Raufhan Kumar
CRN: 2221139
URN: 2203757
Section: IT(B2)

16

Q1. Compare and contrast the various ⓐ wired & wireless communication medium for Internet application and services.
ⓐ NFC ⓑ BTLE ⓒ Zigbee ⓓ Wi-fi

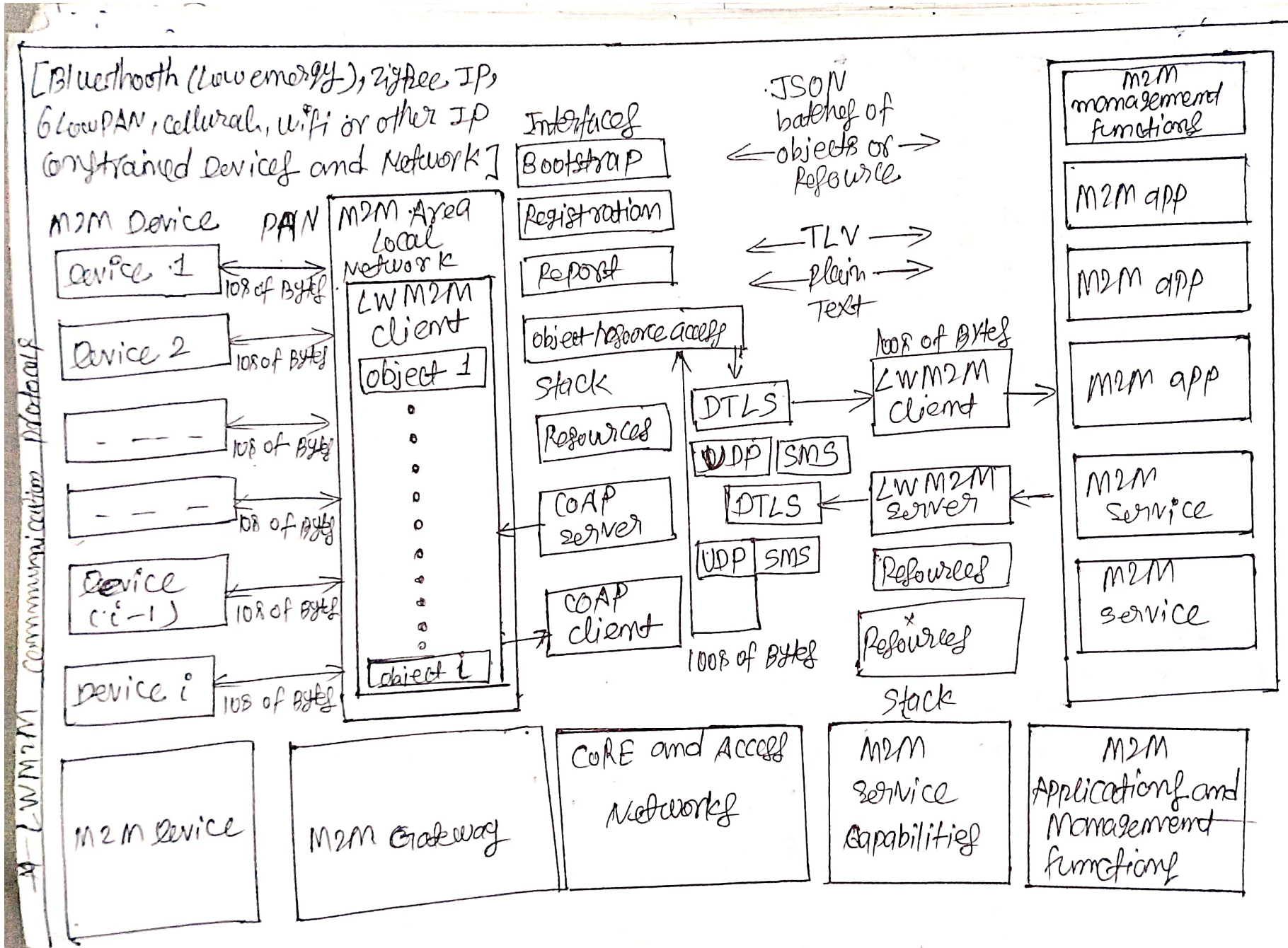
Property	NFC	BTLE Bluethooth low Energy	Zigbee	Wifi (WLAN 802.11)
Definitions	NFC (Near field communication) A short range wireless communication technology that allows device to exchange data over a distance of about 10-20cm	A wireless communication protocol optimized for low power consumption, used primarily in personal devices and IOT applications.	A low power, low-data-rate wireless communication standard typically used in smart home device and industrial automation system.	A wireless networking technology that allows devices to connect to the internet and with one another wirelessly over a local area Network
Example	contactless payment system like Googlepay	fitness trackers like fitbit.	smart lighting systems like philips Hue.	Home wi-fi networks provided by routers.
IEE Protocol	802.15.1	802.15.1	802.15.4	802.11
MAC Layer	CSMA/CA	LE 2.4 GHz	CSMA/CA	CSMA/CD
Data transfer rate	106 kbps	1 Mbps	250 kbps	11Mbps/54mbps
Range	10-20 cm	10m	larger than BTLE	large
Power consumption	Very low	lower than zigbee and wifi	low	Higher than zigbee and BTLE

Network Topology	Point-Point	Star	Mesh	LAN
Broadcast/ Multicast/ unicast	unicast	unicast	unicast/ multicast	unicast

(*) Compare and contrast the various wired communication mediums for internet application and services.

Parameters	Ethernet	Coaxial cable	Fiber optic cable
Definition	A cable used to connect devices in a local network typically using twisted pair.	A cable with a central conductor insulation layer, and a shield, used for signal transmission	A cable that transmits data as light pulses through thin glass fibers.
Example	Connecting computers to a LAN network.	Cable TV connections older internet connections	High speed internet, telecom networks
Speed	100 Mbps - 10 Gbps	up to 1 Gbps	1 Gbps to 100 Gbps or more
Uses	offices, homes, data centers	TV, broadband connections	long-distance internet,
~~Advantage~~ distance	High speed over short distance	Good bandwidth over longer distance	Extremely high speed over long distance.
Cost	cheaper	moderate	Expensive
Installation	Easy to install	Easy to install	difficult to install
Durability	Less Durable	More than ethernet	High Durable
Transmission medium	Electrical signal	Electrical signal	Light signals
~~Speed~~	~~up to 100 meters~~	~~up to 500 meters~~	~~up to 100s kms~~
Bandwidth	Moderate	Moderate	High

5. Core Network: This includes network use,


[Bluethooth (Low energy), Zigbee, IP, 6LowPAN, cellural, wifi or other IP constrained Devices and Network]
Interfaces
Bootstrap
Registration
Report
object/resource access
JSON
TLV
Plain Text
M2M management functions
M2M app
M2M app
M2M app
M2M Service
M2M service
M2M Device
PAN
Device 1
Device 2
Device (i-1)
Device i
108 of Bytes
M2M Area Local Network
LWM2M client
object 1
object i
Stack
Resources
COAP server
COAP client
DTLS
UDP
SMS
LWM2M client
LWM2M server
Resources
Resources
Stack
LWM2M Communication protocols
M2M Device
M2M Gateway
CoRE and Access Networks
M2M Service Capabilities
M2M Applications and Management functions

The lightweight machine to machine communication (LWM2M) protocol is a simple, efficient protocol used for communication between devices (like IoT devices) and servers in machine to machine applications. It is developed by the open Mobile Alliance (OMA) and mainly helps manage and monitor devices in networks like cellular or sensor networks.

The "lightweight" aspect means it uses minimal system resources and transmits smaller data formats, such as binary data or JSON, which are easier for constrained devices to handle. LWM2M is often paired with the CoAP protocol for efficient communication. This protocol is specially designed for constrained environments, making it ideal for IoT applications. It allows devices to communicate using small, efficient data packets.

Working:

① Device connecting: M2M device (like sensors) connect to a gateway using local networks like Bluetooth, wifi, zigbee or cellular data.

② LWM2M client: Each device uses an LWM2M client, which follows OMA standards, to communicate with a central server.

③ Efficient data Transfer: The client sends and receive small data packets (10B to 100B of bytes) in formats like JSON, plain text, or binary TLV.

④ Communication Protocols: It uses protocols like CoAP, DTLS, and UDP or SMS for secure and lightweight message exchanges.

⑤ function: The LWM2M client performs functions like bootstrapping, registering, updating and reporting data to the server.

Server interaction: The server manages services and device data, enabling remote control and management.

Lightweight Design: The protocol is optimized for low power, constrained devices, minimizing the use of resources and data.

JSON (Javascript object notation): JSON is simple, text-based format used to transmit data b/w a server and a web application. It is human-readable, easy to understand, and uses attribute value pairs to represent data. JSON was derived from Javascript but is now language-independent, meaning it can be used in any programming languages like Java, or C to parse and generate data.

Example:
```
{ "0" : { "id" : 0,
          "name" : "LWM2M",
          "mandatory" : true.
        }
}
```
etc.

* Tag-length-value format: TLV format is a simple format used to transfer data. In TLV the first two bytes identify the parameter (Tag), the next byte indicate the length of the data, and the actual data (value) follows immediately after.

Example: CoAP (protocol) with code "2.06". The engine RPM is assigned ID = 125, the velocity is assigned ID = 126

in TLV formate

- The engine is represented as:
<engine>; Engobj; id = "100"; ct = "200".
- The RPM is represented as:
<engine/rpm>; Engobj; id = "125".
- The velocity is represented as:
<engine/velocity>; Engobj; id = "126".

MST-1

(10) Interpret the following statement:
~~The statement describes the~~
"Internet of Things is a vision where things become "smart", and function like living entities by sensing, computing and communicating through embedded devices which interact with remote objects, or persons through the internet or Near-field communication (NFC) etc.

ans ⇒ The statement describes the Internet of Things (IOT) as a concept in which everyday objects, devices are embedded with sensors, computing capabilities, and communication technologies. These devices become "smart" by being able to collect data, process information, and communicate with other devices or people over the internet through technologies like (NFC) Near field communication. The idea is that these interconnected devices can function autonomously, making decisions and performing tasks similar to how living entities would, enhancing convenience, efficiency and

Usage in web connectivity: TLV is used in various communication protocols, including some IoT protocols, smart cards, and telecommunication systems. It is particularly useful in environment where the data structures need to be extensible or where different types of data need to be transmitted together in a single stream.

- IMEI: (International Mobile Equipment Identity): IMEI is a unique identifier assigned to mobile devices in telecommunication for identifying and tracking devices.

Structure: The IMEI Number is typically divided into several parts

(i) TAC (TYPE Allocation Code): The first 8 digits, identifying the device model and origin.

(ii) SNA (Serial Number): The next 6 digits, unique to each device

(iii) Check Digit: The final digit, used for error-checking the IMEI number.

Example: IMEI: 490154203237518 → for error-checking
(TAC: 49015420, unique: 323751, check digit: 8)

Usage in web connectivity: The IMEI is primarily used by mobile networks to identify devices and manage their access to the network. for instance, if a device is reported stolen, the IMEI can be used to block that device from accessing any network, effectively "blacklisting" it.

4. Explain M2M Architecture, IOT Architecture and WSN in details.

formation in daily life

1. Interpret the following Statement

Machine to Machine Communication refers to communication of machines with others of the same type, mostly for monitoring and also for control purpose using M2M Architecture.

(a) Machine to Machine (M2M) communication refers to the direct exchange of data between devices or machines of the same type, typically without human intervention. These machines communicate with each other to monitor and control systems, using an M2M architecture that supports automation and real-time data exchange. The communication is mainly used for applications such as remote monitoring, industrial automation and smart devices where machines share information to enhance efficiency or performance.

(b) Describe the features of the Apple smart watch

(b)

(i) Health and fitness Tracking: includes heart rate monitoring, ECG, blood oxygen measurement and activity tracking (calories burned, steps taken etc).

(ii) Notifications & Communication: Users can receive calls, texts, and notifications directly on the watch. It can also integrate with iphone apps.

(iii) GPS & cellular connectivity: Built-in GPS and optional cellular connectivity allow tracking and communication without needing a phone nearby.

(iv) Water Resistance: Designed for water related activities like swimming.

(v) Siri integration: Voice commands via Siri for setting reminders, sending messages or controlling smart home devices.

(vi) Fall Detection and Emergency SOS: Automatic detection of falls and the ability to alert emergency services in case of an emergency.

Q How to find IP address

Step 1: Press win + R, type cmd, and press Enter to open the command prompt.

Step 2: TYPE ipconfig and press Enter.

Step 3: Look for the IPV4 Address under the appropriate network adapter. This is your IP address.

(A) Analyze the IoT Data to be pushed in the cloud using JSON.

Format (Code):

```
Location = "F0E"
room = "CR2046"
user_id = x
sensors = ["DHT11", "BMP180"]
DHT11_Humidity = 57
DHT11_temperature = 23
BMP180_pressure = 1009.
```

Note Replace x with your full student ID (10 digits)

```
{ "location" : "FOE",
  "room" : "CR20046",
  "user-id": "1234567890",
  "sensors": [
     { "DHT11",
       "BMP180"
     ],
  "readings" : {
      "DHT11" : {
        "humidity" : 57,
        "temperature" : 23
      },
      "BMP180" : {
        "presure" : 1009
      } } }
```

Components used in like: Resistance, Led bulb, Push button etc.

LED Code for lab:

```
#define LED_PIN 8
#define BUTTON_PIN 5
void setup(){
 pinMode(LED_PIN, OUTPUT);
 pinMode(BUTTON_PIN, INPUT);
} void loop(){
 if(digitalRead(BUTTON_PIN == HIGH)
 { digitalWrite(LED_PIN, HIGH);
 }else{
     digitalWrite(LED_PIN, LOW);
 } }
```

Q Diff b/w DHT11 & DHT22

DHT11	DHT22
① A basic temperature and humidity sensor with a limited range and accuracy	An improved sensor compared to the DHT11, offering better accuracy, a wider range
② Example: suitable for simple project, where high precision is not required, such as basic weather station	Example: Suitable for complex project, where high precision is required, such as environmental monitoring
③ price: cheaper	price: more expensive
④ size: smaller	size: slightly larger

* Data collection, storage and computing using a cloud platform.

* Introduction to cloud computing: Cloud computing mean using services like storage, computing power, and applications over the internet without needing to know how everything works behind the scenes. It's similar to how we use electricity - we just turn on the lights without worrying about the power plant that generated the electricity. Example: when we use Google Drive to store files, you don't need to know where the data is stored and how google managed it, you just upload your files, and google handles everything else, like saving the data on its servers, which may be located anywhere in the world. You similarly use the service without needing to understand the complex infrastructure behind it.

Definition of cloud computing

* cloud computing: cloud computing is the delivery of a variety of computing services such as servers, storage, database, networking, software, analytics and intelligence over the internet. The goal of cloud computing is to provide faster innovation, flexible resources, and economies of scale, which helps to organizations to reducing their operating costs, improve efficiency and scale up their business needs.

* Types of cloud computing

There are three types of cloud computing

(i) public cloud (ii) private cloud (iii) Hybrid cloud

(i) public cloud: A public cloud is owned and operated by a third party cloud service provider, which delivery computing resources like servers, storage and software over the internet. The provider manages the infrastructure and maintains the hardware and software. Customers can access these services through a web browser

Examples: Amazon web services (AWS), Microsoft Azure, Google cloud.

(ii) private cloud: A private cloud is used by a single organization, either hosted on-site at the company's data center or by a third party service provider, unlike the public cloud, the infrastructure and services in a private cloud are dedicated to one organization, providing greater control and security.

Example: AWS outposts

(3) Hybrid cloud: A hybrid cloud combines both public and private cloud environments with technology enabling data and applications to move between them. This allows businesses to take advantage of the benefits of both deployment models. Like flexibility, optimized use of existing infrastructure and enhanced security, Better cost management.

Example ⇒ Microsoft Azure Hybrid cloud

* cloud computing: cloud computing means storing and accessing the data and programs on remote servers that are hosted on the internet instead of the computer's hard drive or local server. cloud computing is also referred to as internet-based computing, it is a technology where the resource is provided as a service through the internet to the user. The data that is stored can be files, images, documents or any other storable document.

The following are some of the operations that can be performed with cloud computing.

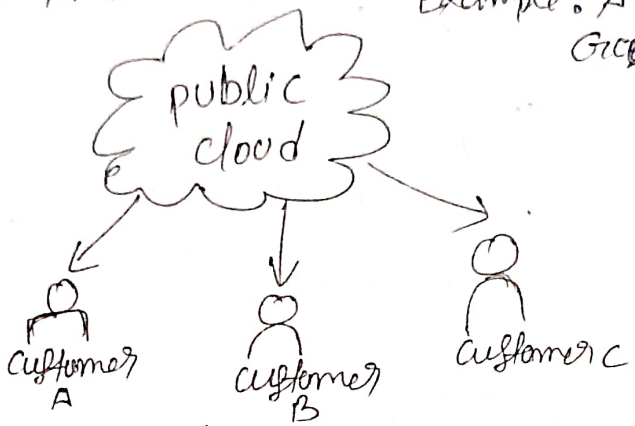
- Storage, backup, and recovery of data
- Delivery of Software on demand
- Development of new applications and services
- Streaming ~~video~~ videos and audio.

* Cloud computing Deployment Models

(i) public cloud
(ii) private cloud
(iii) Hybrid cloud

(1) Public cloud: The public cloud is a model of cloud computing where cloud services and resources are made available to the public over the internet, managed by cloud service providers (such as Amazon, Azure); these services are available to a wide audience, including businesses and individuals.

Example: AWS, Microsoft Azure, Google cloud platform



Advantage of the public cloud Model

(i) Minimal investment: costs are based on usage

(ii) No setup costs: The entire infrastructure is fully provided by cloud service providers. No need of set up any hardware

(iii) No infrastructure management: The provider manages and maintains

(iv) pay-as-you-go: you only pay for the resources you use.

(v) worldwide Access: Access your data and applications anywhere in world

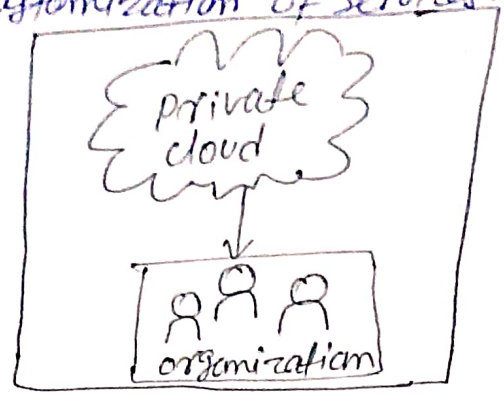
DisAdvantages

(i) Security concerns: Since resources are shared among multiple users, security may be lower compared to private environment

(ii) Limited customization: public cloud services are standardized, which can limit customization options to meet specific requirements

(2) private cloud: The private cloud is a cloud computing model that provides a dedicated environment to a single organization. The private offers exclusive access to ~~reso~~

resources within a protected network, managed either by the organization or a third-party provider. This gives the organization greater control over data, security and customization of services. Example: VMware cloud



* Advantages of the private cloud model

(i) Dedicated Resources: All resources are exclusively for one organization

(ii) Customization: Better customization according to their organizations needs.

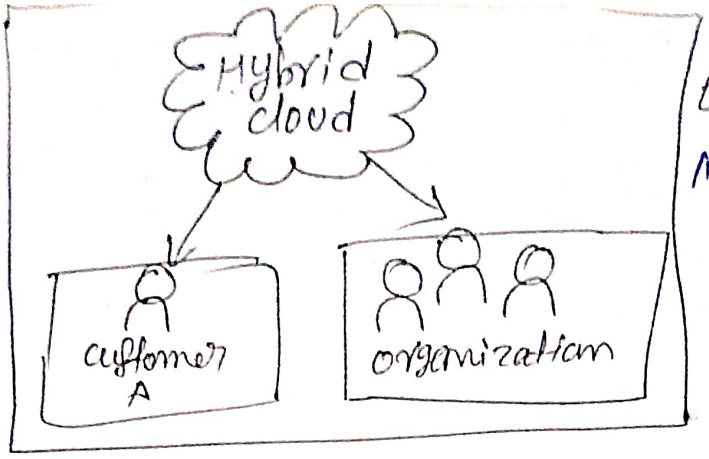
(iii) Enhanced Security: Due to resources are dedicated to a single organization, security and privacy is enhanced.

Disadvantages:

(i) Less Scalable: private clouds are scaled within a certain range as there is less no of clients

(ii) costly: private clouds are more costly.

(3) Hybrid cloud: The Hybrid cloud model combines both public and private clouds, enabling organizations to take benefits of both environments. Through a hybrid approach, companies can keep sensitive data in a private cloud while utilizing the public cloud for other workloads. This model offers flexibility, enabling organizations to balance security, performance, and cost-effectiveness.



Example:
Microsoft Azure Stack.

Advantages

(i) Flexibility and Scalability: Easily scale resources up or down to meet changing demands.

(ii) Cost effectiveness: Optimize costs by ~~running~~ paying only for the extra capacity if you require it.

(iii) Enhance Security: protect sensitive data by keeping it on-premises while using public cloud for less sensitive data.

Disadvantages of the Hybrid cloud

(i) Difficult to manage: Hybrid clouds are difficult to manage as it is a combination of both public and private cloud.

(ii) Slow data transmission: Data transmission in the hybrid cloud takes place through the public cloud so latency occurs.

* cloud service models

(i) Software as a Service (SaaS)
(ii) platform as a service (PaaS)
(iii) Infrastructure as a service (IaaS)
(iv) Everything as a service (XaaS)

(1) Software as a service (SaaS): SaaS provides software applications over the internet on a subscription basis, users access these applications via a web browser without needing to install or maintain them on their device.

Examples: Microsoft 365

Advantage:

Accessibility: Accessible from any device with internet access.

Cost Effective: Reduces the need for hardware purchases.

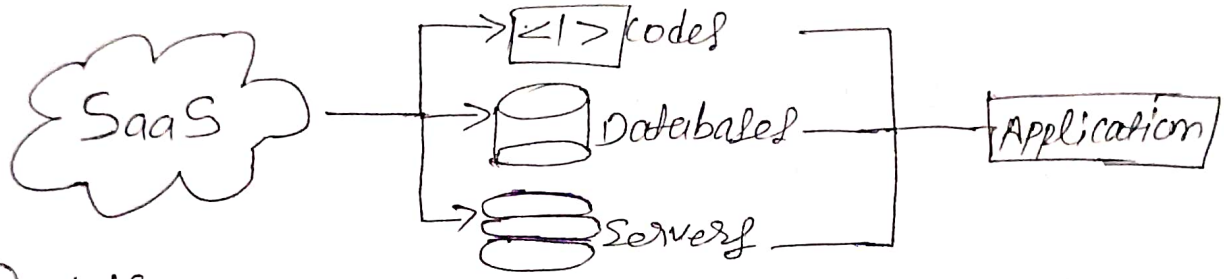
Automatic updates: Software updates are managed by the provider. Provider ; ensuring users always have the latest version.

Disadvantage:

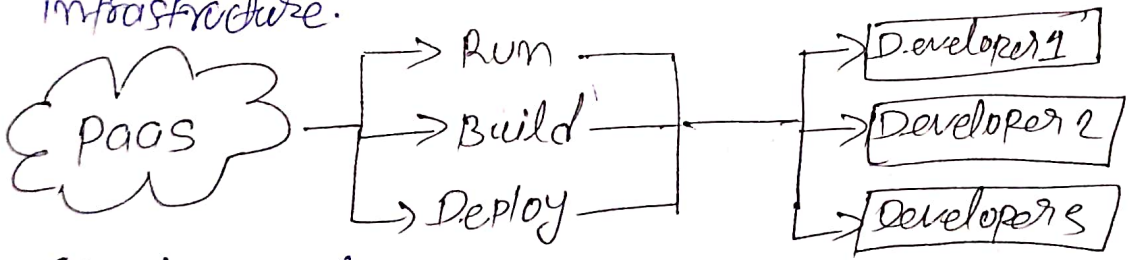
Limited customization: Users may have limited ability to customize software to their specific needs.

Dependency on internet: Requires a reliable internet connection.

Data Security: Storing sensitive data on third party servers raises concerns about data privacy and security.



(2) Platform as a Service (PaaS): platform as a service provides a platform allowing developers to build, deploy, and manage applications without dealing with the underlying infrastructure.



Example: Google App Engine

(1) Advantages: Development Focus: Developers can concentrate on coding without worrying about infrastructure management.

(2) Integrated Development Tools: Offers built-in tools for

development, testing, and develop deployment ~~testing~~ and, speeding up the development process.

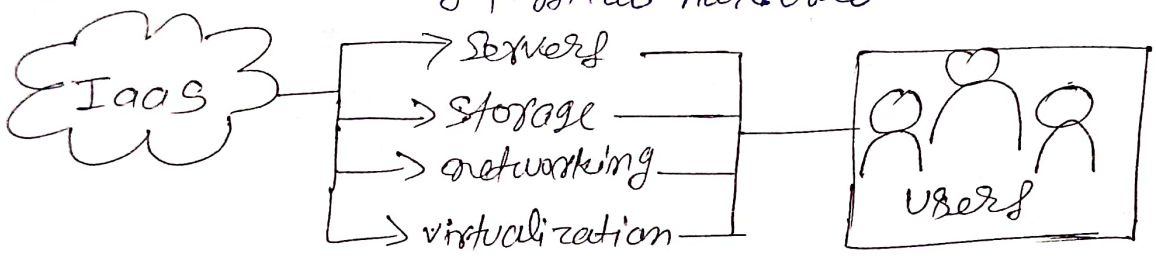
③ Scalability: Automatically scales applications based on demand making it easier to handle traffic spikes

Disadvantage:

(i) Limited control: Users may have less control over the underlying infrastructure and configuration settings.

(ii) Security concerns: Similar to SaaS, sensitive data may be stored off-site, raising security and privacy concerns.

③ Infrastructure as a Service (IaaS): IaaS provides virtualized computing resources over the internet, including servers, storage and networking. Users can rent these resources on a pay-as-you-go basis. Rather than purchasing and maintaining physical hardware.



Example: Amazon web service, IBM cloud, Microsoft Azure

Advantages:

(i) Cost-Effective: pay only for what you use, reducing costs and operational expenses.

(ii) website hosting: Running ~~web~~ websites using IaaS can be less expensive than traditional web hosting.

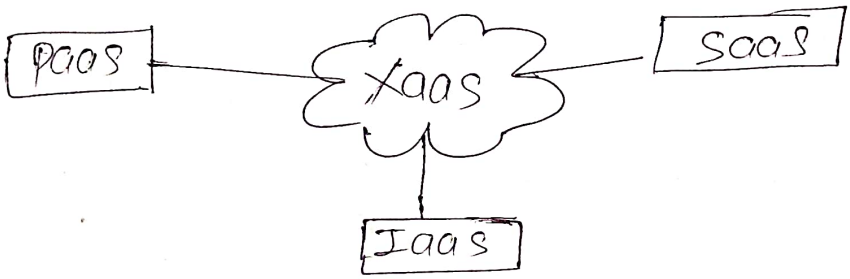
(iii) Control: Users have complete control over their infrastructure allowing for customization based on specific needs

(iv) Maintenance: There is no need to manage; This is already managed by Iaas cloud service provider

Disadvantage:

Security and Privacy Risks: Storing sensitive data on third party servers can cause concerns about data privacy and security because it can be hacked by hackers.

(4) Everything as a Service (Xaas): It is also known as Anything as a Service. Xaas is a broad term that comprises of various cloud services, including Saas, Paas, Iaas and more.



Example: Desktop as a service. Database as a Service
Storage as a Service

Advantages:

(i) cost-effectiveness: pay-as-you-go

(ii) Scalability: Easily scale resources up or down to meet changing demands

(iii) flexibility: It can be used to provide a wide range of services, such as storage, databases, networking., we can customize it to meet specific needs.

Advantages: Dependence on the provider: Users are dependent on the Xaas provider for the scalibility and reliability of the service

(5) Discuss cloud Deployment Models, monitor and evaluate the data collection, storage and computing with cloud computing.

→ cloud Deployment Models → Already done

Monitoring and Evaluating Data collection, storage, and Computing in cloud Computing

1. Data Collections: [redacted] cloud providers offer tools to monitor data collection processes, ensuring data is accurately captured from multiple sources. Example includes AWS cloudwatch, Azure monitor and Google cloud operations. Many cloud providers enable real-time data streaming and analytics to detect issues in data collection, ensuring data is collected consistently and accurately.

2. Data storage: cloud platforms allow continuous tracking of storage usage, helping to identify underutilized or over-utilized storage resources. Tools like AWS S3 storage, Lens and google cloud storage are commonly used. Cloud providers offer features such as encryption, access controls, and logging to monitor data security. Cloud providers regularly test backup and recovery procedures to ensure data integrity and availability.

(3) Computing Resources: cloud providers provide dashboards and tools to monitor CPU, memory, and network utilization, helping to evaluate if resources are meeting performance requirements. This ensures efficient resource allocation and workload balancing.

(PYQ) Explain the usage of cloud platforms for IoT applications and services with examples of xively (Pachube/COSM) and Nimbits.

ans ⇒ usage of cloud platforms for IoT applications

1. Data collection: IoT devices generate vast amounts of data that need to be collected in real-time. cloud platforms enables the seamless transmission of data from devices to the cloud for processing.

2. Data storage: The cloud provides storage solutions to handle the massive volumes of data generated by IoT devices. This storage can be structured (like database).

3. Data processing and Analysis: Cloud platforms offer tools for processing and analyzing data. This can include real-time analytics, machine learning algorithms, and data visualization tools to derive insights from the data collected.

4. Device management: cloud platforms typically include features for managing IoT devices, such as monitoring their status, updating firmware, and managing security protocols.

5. Integration with other services: cloud platforms can easily integrate with other services (like APIs, databases, and third party applications), enabling the creation of complex workflows and ecosystems.

6. Scalability: cloud platforms can automatically scale resources up or down based on demand, making it easier to manage varying loads typical in IoT applications.

Q8. Also, Describe the latest features of Xively (pachube/cosm), Nimbits cloud platforms.

Ans → Xively formerly known as pachube, cosm before that at

Xively Definition: Xively is a cloud-based platform designed to facilitate the creation, management and analysis of IoT applications. It serves as a middleware that connects devices and applications, enabling users to collect and share data effectively. The platform provides an application programming interface (API) for developers to integrate IoT data into their applications seamlessly.

Features:

(1) Data collection and storage: It supports real-time data collection and processing from multiple devices offers persistent storage for device data, allowing users to access historical data easily.

(2) RESTful API: It provides a simple RESTful API for easy integration with applications, enabling developers to send and receive data efficiently.

(3) Device management: It facilitates the registration and management of devices, ensuring secure communication and data integrity.

(4) Alerts and Notifications: Users can set up alerts based on specific data thresholds.

(5) Security: It ensures data security by data encryption protecting sensitive information from unauthorized access.

(6) Integration: It supports integration with various third party applications and services, extending functionality.

Advantages:

(i) Easy to use: Xively provides simple interface and comprehensive API documentation, making it easier for developers to create and manage IoT applications.

(ii) Real-time processing: Offers real-time data streaming and processing, enabling immediate responses and actions based on incoming data.

(iii) Scalability: The cloud-based nature allows for easy scaling, growing as no of devices increasing.

(iv) Secure data Handling: Robust security features ensures that is protected against unauthorized access.

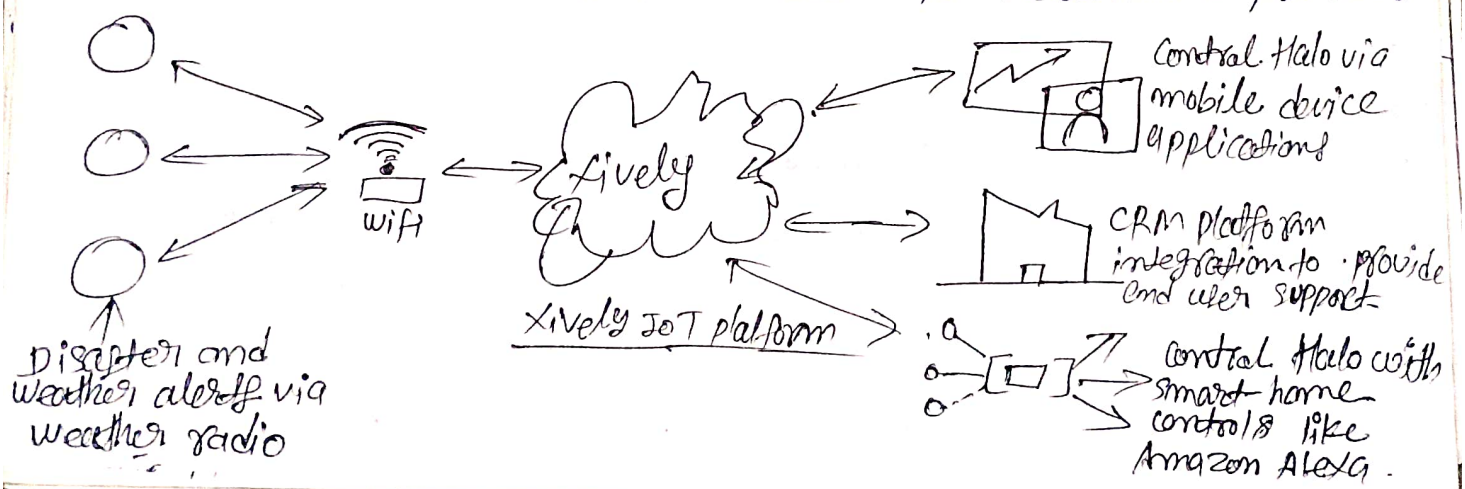
Disadvantages: (i) Cost: Xively can be more expensive

(ii) Complexity for Beginners: Users without tech-background can be challenging.

(iii) Limited customization: Xively may not offer the level of customization some businesses requires for their specific use cases.

Examples: Smart Agriculture: Can be used for monitor soil moisture levels, temperature.

Health and fitness: Xively can be used for Health and fitness devices can send real-time data to healthcare providers.



Nimbits Definition: Nimbits is an open-source platform designed for storing and analyzing time-series data. It is particularly useful for applications that require real-time data collection, storage, and visualization, such as IoT Applications, environmental monitoring, and industrial automation.

In other words

Nimbits can be defined as a cloud-based, open-source time series database and platform that enables users to collect, store, and analyze data over time. It provides a flexible and scalable way to manage data from various sensors and devices, allowing users to visualize trends and insights derived from that data. Nimbits built in Java and NoSQL databases, making it a versatile solution for developers.

features of Nimbits

(i) Time series data Management: Nimbits specializes in handling time-series data, allowing users to track changes over time effeciently

(ii) Data collections: Nimbits can collect data from a variety of sources, including sensors, microcontrollers and other devices it also supports RESTful APIs.

(iii) visualization: Nimbits provides built-in tools for visualizing data through graphs and charts, helping users to interpret trends and patterns.

(iv) User management: It includes features for user authentication and management, allowing multiple users to access.

(v) open source: Being open-source, Nimbits can be modified and distributed freely, promoting community collaboration.

(vi) Alerts and Notification: Users can set up alerts and notifications based on specific data conditions.

(vii) Integration with other services: Nimbits can integrate with other services, such as IFTTT and Zapier, to automate tasks and create custom workflows.

Advantages:

(i) Real-Time Data processing: Nimbits allows for real-time data collection and analysis, which is crucial for time-sensitive applications.

(ii) Community support: Open source means there is a community of developers who contribute to its improvement and provide support.

(iii) Easy to use: Nimbits is easy to set up and use, even for those with limited technical expertise.

(iv) Scalability: The platform can handle a large number of devices and data streams.

(v) flexibility: Nimbits can be used for a wide range of IoT applications, from home automation to industrial.

(vi) Cost-effective: Nimbits is a cost-effective solution for IoT projects, as it eliminates the need for expensive hardware and software.

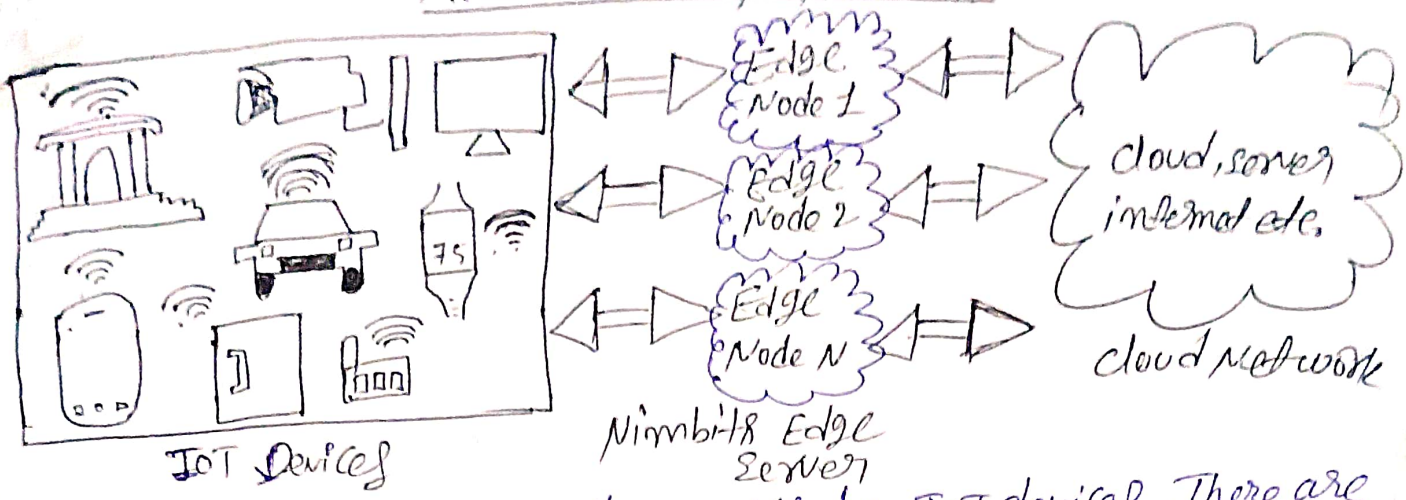
Disadvantage

(i) Limited Documentation: Although there is community support, some users may find the documentation lacking for advanced use cases.

(ii) Maintenance overhead: As an open-source platform, users are responsible for maintaining and updating the system, which can require additional resources.

Example: Nimbits can be used in environmental monitoring applications. For example, a city might use Nimbits to collect data from a network of sensors that measure air quality, temperature, and humidity.

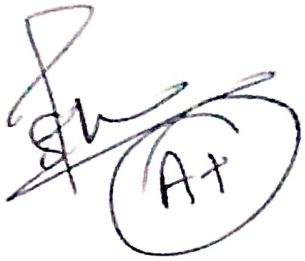
Architecture of Nimbits



In this Architecture first there will be IoT devices, There are variety of IoT devices based on embedded system one can have Arduino uno, Raspberrypi, these IoT devices communicating with variety of protocols, those protocols can be Zegbee, wifi, Ethernet. IoT devices are continuously sensing the data and IoT devices are connected with Nimbits Edge servers that filters the data from IoT devices and what ever is required information is Aquired that is being transfered to cloud and it will be stored here.

Assignment - 2

Sub → IOT
Name → Rawshan kumari
CAN : 2221139
URN : 2203751



Q1. Difference b/w IP and MAC address along with the Application layer protocol.

Sol ⇒

parameters	MAC address	IP Address
Full form	Media Access Control Address	Internet protocol Address
Definition	MAC Address is used to ensure the physical address of the computer. It uniquely identifies the device on a network.	IP addresses are used to uniquely identifies the connection of the network with the device takes part in a network.
Address formate	MAC Address is a six byte hexadecimal address.	IP Address is either 4-byte or a sixteen-byte (IPV6) address.
purpose	Identifies a device within a local network (LAN)	Identifies the network location of a device globally.
provided by	NIC (Network Interface card) Manufacturer.	Internet Service provider (ISP).
Address TYPE	MAC Address is used to ensure the physical address of a computer.	IP Address is the logical address of the computer.
Operating layer.	MAC Address operates in the data link layer.	IP Address operates in the network layer.
Persistence	fited and permanent	Can change with network or ISP.
Helps	MAC Address helps in simply identifying the device.	IP Address identifies the connection of the device on the network.

found	MAC Address can't be found easily by a third party.	IP Address can be found by a third party.
classes	No classes used for MAC	It uses A, B, C, D and E classes for IP addressing.
Used for	MAC addresses can be used for broadcasting.	The IP addressing can be used for broadcasting or multicasting.
oriented	MAC address is hardware oriented	IP address is software oriented.
Example	00:FF:FF:AB:BB:AA	IPv4: 192.168.1.1, IPv6: FFFF:f200:3209:0B00
Application layer protocol	The Application layer protocols uses MAC address to deliver accurate data over Local Area Network	The Application layer operate over IP address to communicate across networks.

(b) List the services offered at Amazon EC2 and TCUP.

Here is a services offered by Amazon EC2

(1) Compute instances: It runs virtual servers with options like on-demand, Reserved, Spot, and Dedicated Hosts to fit different needs and budgets.

(2) Auto Scaling: Adjusts the no of instances up or down automatically based on your app's demand.

(3) Elastic Load Balancing: Spreads the incoming traffic across multiple instances to keep your app available and responsive.

(4) Storage: Includes Amazon EBS for storing data permanently and Instance store for temporary storage needs.

(5) Networking: offers Elastic IPs, Virtual private cloud for secure networks, and security Groups for controlling access.

6. Amazon Machine Images: Ready-to-use templates to quickly launch instances with your chosen OS and software.
7. EC2 Image Builder: Creates and manages custom EC2 images, making it easier to set up new instance.

TCUP (TCS Connected Universe platform)

TCUP is designed as an IoT platform focusing on managing connected devices and data analytics. It provides services are especially useful for industries needing real time data and asset management.

(i) Device Management: Manages IoT devices using protocols like MQTT, HTTP and LWM2M.

(ii) Sensor Data management: Collects, stores and processes sensor data in real time, supporting use cases like remote monitoring and predictive analytics.

(iii) Event-driven Analytics: Provides tools for big data, real-time analytics, often used in manufacturing, healthcare and smart utilities for maintenance and optimization.

(iv) platform Agnosticism: TCUP can be deployed on various cloud platforms, including AWS and Azure and supports integration with third party systems for flexibility deployment.

Q2. Describe the virtualization concept in usage of the cloud services.

Virtualization: virtualization in cloud services is a foundational technology that enables the efficient use of computing resources by creating virtual versions of physical hardware resources, such as servers, storage, networks, and even entire operating systems. This allows cloud providers to maximize resource utilization, improve flexibility, and lower costs, as multiple users or applications can share the same physical infrastructure while running in isolated environments.

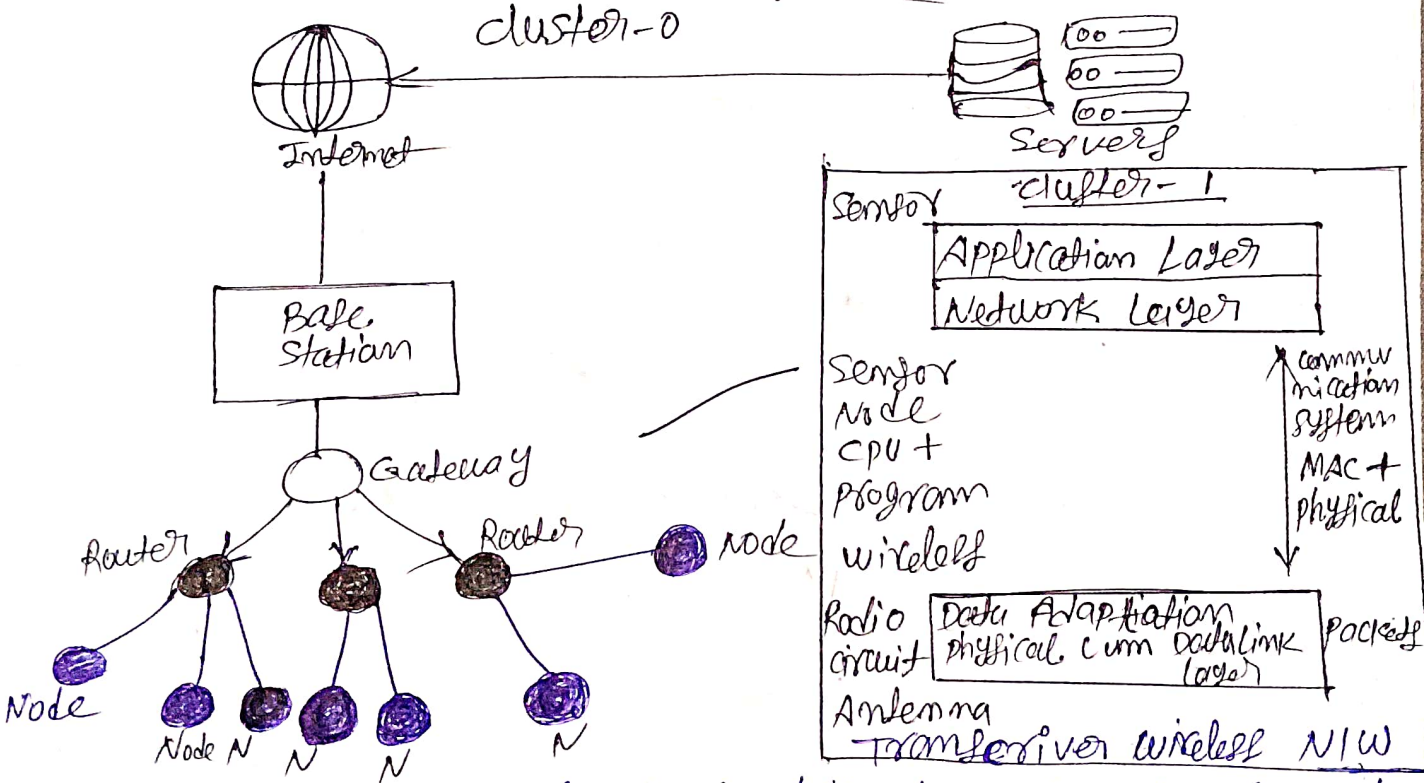
how virtualization enhances cloud services

1. Resource pooling and sharing: virtualization allows cloud providers to pool their physical resources, like CPU, memory, and storage and allocate them dynamically among users.
2. Scalability and flexibility: Through virtualization, cloud providers can quickly add or remove virtual resources based on demand. This makes it easy to scale applications up or down as needed, allowing users to pay only for what they use.
3. Improved Resource utilization: virtual machines and containers allow providers to run multiple applications on a single physical server, reducing capacity and maximizing the use of each servers computing power.
4. Disaster Recovery and High Availability: virtualization supports backup and recovery strategies and it can be easily replicated and moved across physical servers.
5. Cost effective: Virtualization allows cloud providers to reduce operational costs by running multiple isolated instances on shared physical infrastructure leading significant cost saving.

4. Explain WSN Architecture, protocols and Secure communication In WSN in details.

WSN: WSN Stands for wireless sensor Network is an infrastructure-less wireless network that is deployed in a large no of wireless sensors. that is used to monitor the system, physical or environmental conditions. sensors nodes are used in WSN with the onboard microcontroller that manages and monitors the environment in a particular area. They are connected to the Base station. The base station in a WSN system is connected through the Internet to share data.

Architectural diagram



Wireless Sensor Network Architecture is structured into three main layers

① Physical Layer ② Data Link layer ③ Application Layer

① Physical Layer: This Layer connects sensor nodes to the base station using technologies like radio waves, Bluetooth.

② Data Link layer: This layer is responsible for establishing a reliable connection between sensor node and the base station. It uses protocols such as IEEE 802.15.4 to manage data transmission and ensure efficient communication within the network.

③ Application layer: Enables sensor nodes to communicate specific data to the base station. It uses protocols like ZigBee

These layers work together to facilitate the seamless operation and data flow within a wireless sensor network.

Protocols in WSN

1. Medium Access control (MAC):

(i) IEEE 802.15.4: A popular standard for WSNs, providing low-power, low-data-rate communication.

(ii) S-MAC (Sensor MAC): It prioritizes energy efficiency by scheduling transmissions to minimize energy consumption.

(iii) LEACH (Low Energy Adaptive clustering Hierarchy): A clustering based protocol that rotates cluster heads to distribute energy consumption.

2. Routing protocols:

(i) LEACH: It also used for routing, where cluster heads forward data to the base station.

(ii) TEEN (Topology-based Energy Efficient Network): Conserves energy by optimizing routing paths based on node energy levels.

Secure Communication in WSN

Wireless Sensor Network face several security challenges because of their limited resources. These challenges include

(i) Energy constraint: The network's devices have limited battery life, so using energy intensive security algorithms is difficult.

(ii) Resource constraint: The devices have limited processing power and memory, which makes it hard to implement complex security measure.

(iii) Wireless Medium: The signals transmitted over the air are ~~vulnerable~~ unsafe and interference, making the network less secure.

To overcome these challenges

(i) Encryption: by Applying encryption algorithms like → AES-128

(ii) ~~Authentication~~ Authentication: by applying secure authentication protocols.

(iii) Secure Routing: protocols like SEAD prevents attackers from altering routes or dropping packets.

Q5 (a) Explain electronic product code Architecture global framework.

The Electronic product code (EPC) is a unique identifier used to track individual items in supply chains and inventory systems. The EPC is designed to identify each individual instance ~~box of a cereal~~ of a product uniquely. This is often implemented using RFID technology, where an EPC is encoded onto an RFID tag attached to a product.

EPCglobal Architecture framework provides a collection of interrelated standards for hardware, software, and data interfaces, along with core services that are operated by EPCglobal and its delegates.

Key components of the EPCglobal Architecture Framework

- EPCglobal Network: This is the backbone of the framework, enabling communication and data exchange b/w diff participants.
- EPC tag: A small, wireless device attached to a physical object that containing an EPC, which is a unique identifier for that object.
- EPC Reader: A device that reads the EPC from an EPC tag and transmits the information to the EPCglobal Network.
- EPCIS (EPC Information Services): A set of standards for capturing, storing and sharing EPC data.
- EPCIS Core Services: Core services provided by EPCglobal that enable the exchange of EPC data between different participants in the supply chain.
- EPCIS Application Services: Application-specific services built on top of the EPCIS core service to meet the specific needs for different industries and use cases

(CO1) (PSM) Elucidate sensor technology for sensing the real world using analog and digital sensors and examples for sensing devices for IoT and M2M.

Sensor: A sensor is a device that detects and responds to some type of input from the physical environment

such as light, temperature, motion, pressure, or other physical properties. Sensors convert these physical measurements into signals, typically electrical signals, that can be interpreted by other systems, such as computers or microcontrollers.

Types of sensors

(i) Analog sensors (ii) Digital sensors

(i) Analog sensors: Analog sensors produce continuous signals that vary in proportion to the quantity they measure. They generate a voltage or current output that represents the value of the sensed parameter. Ex → 0–5 V

Ex ⇒ Potentiometers.

Use of Analog sensors

(i) climate control systems (Temperature sensing)

(ii) Medical devices (measuring vital signs)

(iii) Industrial process monitoring (pressure or liquid monitoring).

(ii) Digital Sensor: Digital sensors produce discrete signals typically in binary form (0s and 1s). These sensors use analog-to-digital converters to convert the measured quantity into a digital signal.

Ex ⇒ Digital temperature sensors, accelerometers, PIR motion sensor.

Use of Digital Sensors.

(i) Home automation (eg motion sensors)

(ii) consumer electronics (eg. accelerometers in smartphone)

Example for sensing devices for IOT and M2M
Role of Sensors in IoT and M2M

IoT Application: Enable real time data collection and transmission to cloud platforms. Facilitate smart applications like home automation, ~~health~~ healthcare monitoring and environmental sensing.

M2M Applications: Support communication b/w devices without human ~~interact~~ intervention. Common in industrial automation and predictive maintenance systems.

Examples of Sensing Devices:

(i) IOT sensors: Environmental Sensors:
Temperature and Humidity Sensor (DHT11)
Use: Monitor indoor air quality in smart homes.

(ii) Motion Sensors:
Accelerometers and Gyroscopes.
Use: fitness trackers like ~~fitbit~~ fitbit.

(2) M2M Sensors:
Industrial Sensors:
Vibration Sensors for predictive maintenance of machinery
Use: Detecting wear and tear in industrial motors.

proximity Sensors:
Ultrasonic or Infrared Sensors.
Use: Automated conveyor belt system in manufacturing.
obstacle avoidance car, radar.

(c) RFID : RFID stands for Radio Frequency Identification. It is a technology that uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information that can be read from a distance without direct line-of-sight.

Types of RFID tags:

(i) Passive Tags: These don't have a power source and rely on the reader's emitted energy to power them.

(ii) Active Tags: Active tags have their own power source, like a battery, and can transmit data over longer distances.

(iii) Semi-passive Tags: These tags have a battery to run the the circuitry but still rely on the reader's energy to communicate.

Applications of RFID

(i) Access control : RFID cards for secure entry into buildings

(ii) Asset Tracking : Tracking valuable items

(iii) Animal Tracking : Tags for pets or livestock to monitor.

(iv) Supply chain management : Real time tracking of products.

(d) Security protocols, Tomography

Security protocol:

(i) Open Trust Protocol (OTrP): purpose: Manages Security configuration in a Trusted Execution Environment, it facilitates secure installation, updates, and deletion of application and services.

(ii) DTLS (Datagram Transport layer security): Ensures Privacy and Security for data transmission over datagrams., primarily used with protocols like CoAP and LWM2M.

(iii) X.509: Manages digital certificates for secure web communication. Issues certificates using a public key infrastructure managed by a Trusted Third party.

* Security Tomography: It refers to a method of assessing and ensuring Security within an IoT network by using multiple observation ~~points~~ or "views" to detect ~~multiple~~ vulnerabilities and threats across the system.

How does it work?

(i) Data collection: Security tomography collects data from various sources within IoT system, such as Network traffic, Device configuration.

(ii) Data Analysis: The collected data is analyzed to identify patterns and anomalies that may indicate potential security threats. This includes statistical analysis, Machine learning technology.

(3) Visualization: The results of the analysis are visualized in a way that is easy to understand, such as a 3D model of the IoT system. This visualization can help identify areas of weakness and priorities.

Types of security Tomography

(i) IoT Security Tomography
(ii) IoT Computational Tomography

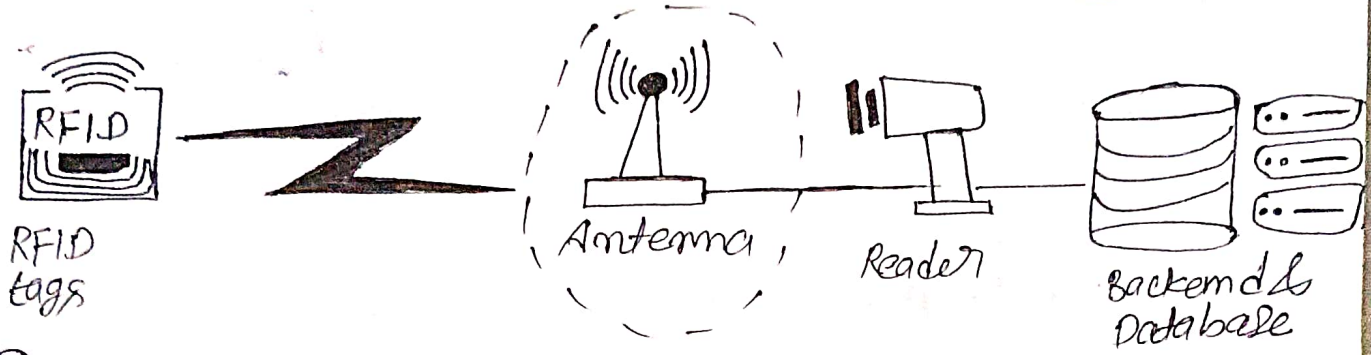
(i) IoT security Tomography: This type of tomography focuses on identifying and addressing security risks in the entire IoT system, including devices, networks.

(2) IoT Computational Tomography: This type of tomography provides visibility into the internal workings of IoT devices and networks, helping to identify and mitigate potential issues.

6. Case Study (a) & (b)

Describe / design develop the Architectural view of RFIDs IDs for a supply chain Application for container tracking system and Internet connected smart Home Services and Monitoring. (Introduction → Definition of RFID, types done before).

Architectural diagram of RFID



(i) RFID Tag: RFID tags are small devices that attach to or embed in objects. They contain data / information about the object, such as a unique identifier. Each tag includes (i) Antenna: Enables communication with the reader by transferring and receiving signals.

(ii) Microchip: Stores data, Process signals, and perform basic computation.

(iii) Power source: Either passive (no battery) or Active (with battery).

(2) RFID Reader: The RFID reader is a device that sends and receives signals to communicate with tags. Reader includes

(i) Antenna: Transmits and receives radio signals to and from RFID tags.

(ii) RFID Module: Handles signal modulation, processing, and data reading.

(iii) Controller: Processes the received data and interface with the system's backend.

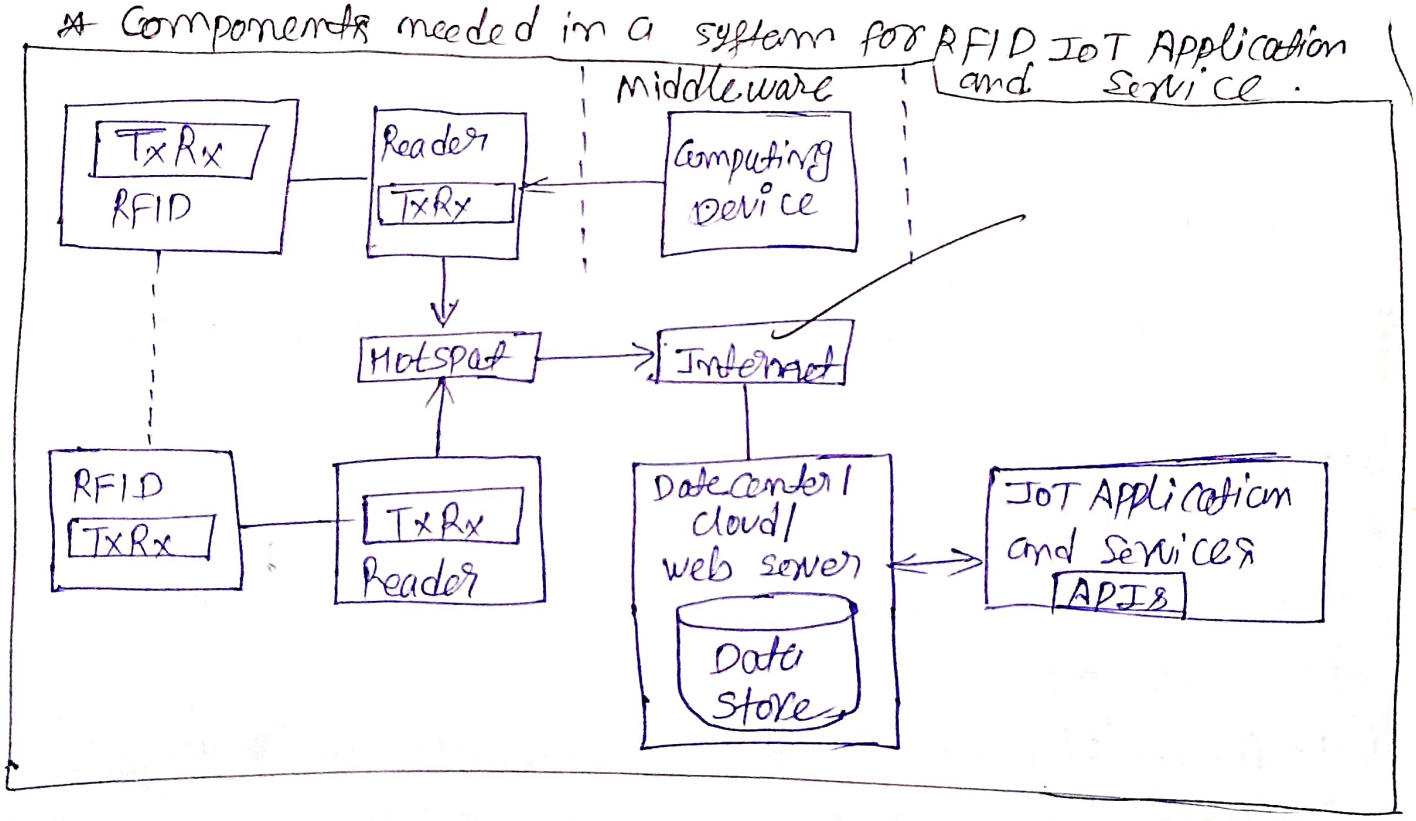
3. Middleware: Middleware acts as a bridge b/w RFID reader and the backend system. It includes Device management, Data filtering, Data processing, raw data collecting, Real-time event monitoring.

4. Backend and database: The backend system comprises applications and databases where RFID data is stored, processed, and used for decision-making.

Database: Stores data received from tags (such as item IDs, locations, timestamps etc.)

Appl
Examples of RFID: Inventory management
Supply chain tracking
Access control.
Asset management.

* Components needed in a system for RFID IoT Application and Service.



RFID data transfer for a supply chain Application for container tracking system. A case study

In the globalized supply chain, efficient and accurate tracking of shipping containers is crucial for businesses to maintain customer satisfaction. GLC (Global Logistics corporation) GLC faced several challenges in its container tracking operations including
- manual Data Entry Errors
- Lack of Real-time visibility
- Inefficient Inventory management

To address these challenges, GLC implemented an RFID based Container tracking system. This system comprises of

(i) RFID Tags : Attached to containers to store info such as container id, contents, and destination.

(ii) RFID Readers: Fixed and RFID readers were installed at various checkpoints throughout the supply chain, including ports, warehouses and distributed centers.

(iii) Centralized Data Management system: A centralized software system collected and analyzed data from RFID readers, providing real-time infos like location, movements and status.

Implementation procedure:

(1) Tagging: Each container was tagged with a unique RFID tag.

(2) Reader installation: RFID readers were strategically placed at key locations to capture data as containers passed through.

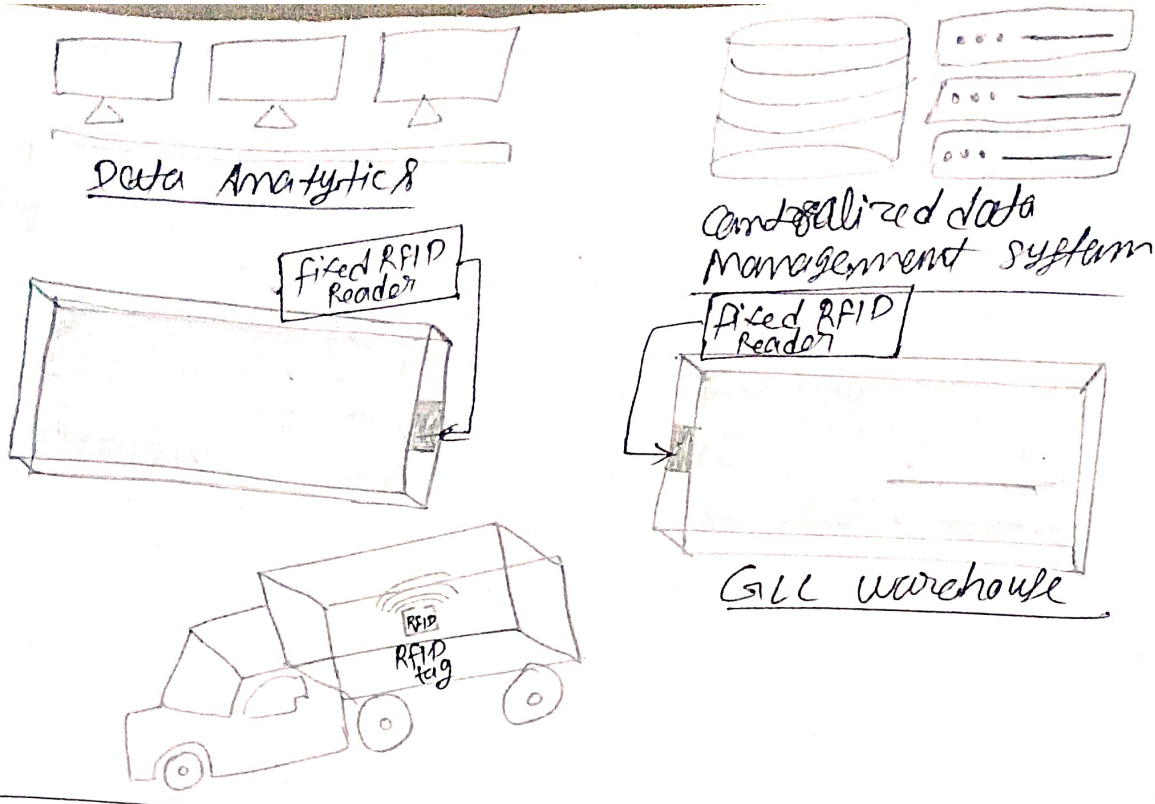
(3) Data integration: The RFID system was integrated with GLC's existing warehouse management system.

(4) Real-Time Tracking: The system enabled real-time tracking of containers, allowing GLC to monitor their location and status.

(5) Alert and Notification system: Automated alerts were generated for deviations from planned schedules, delays, issues.

(6) Data Analytics: Advance analytics tools were used to identify trends & optimize routes and improve overall efficiency.

Advantage → Faster inventory management, improved Accuracy



* RFIDs for Internet connected smart home services and monitoring.

The Integration of RFID into smart home systems has changed home automation and monitoring. By using RFID tags and readers smart homes can now track and manage various devices and objects.

(i) RFID Tags: These are attached to various objects within the home, such as appliances, furniture, refrigerators.

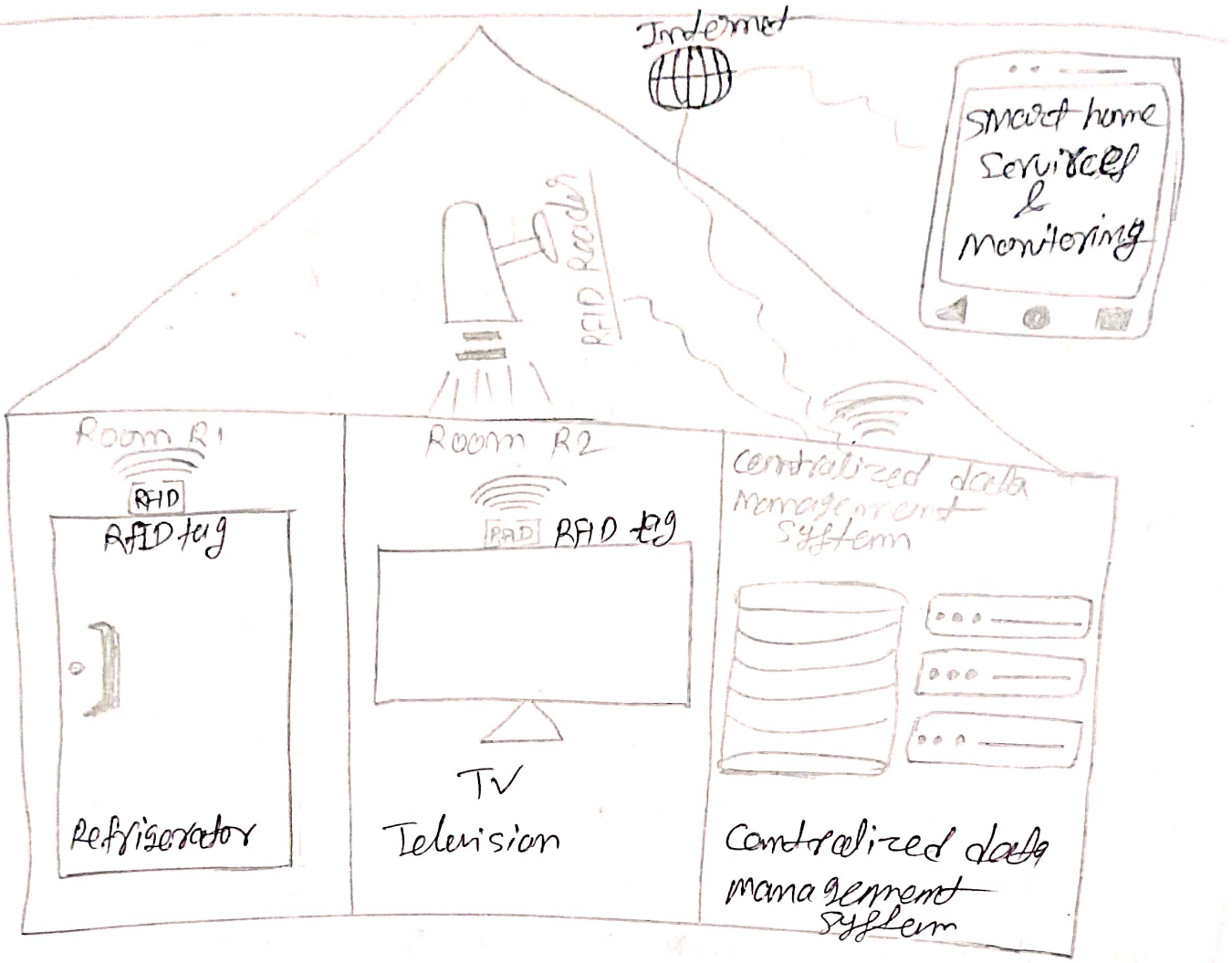
(ii) RFID Reader: Installed at strategic locations to read the tags and gather data. and communicates with other smart home devices.

(iii) Centralized data management system: A central processing unit that collects data from RFID readers and communicates with other smart home devices.

(iv) User Interface: A Mobile app or Web interface that allows users to monitor and control their smart home system.

Applications: Inventory management: RFID tags on household items help keep track of inventory, automatically updating stock levels and reordering supplies when needed.

Security monitoring : RFID tags on doors and windows can alert homeowners if they are opened or tampered with, providing real-time security updates.



Q Elucidate the Security Model and Access control for Industrial usage in IOT.

Soln: The Security Model and Access control for Industrial Internet of Things (IIOT) focuses on protecting sensitive data, ensuring the operational integrity of systems, and preventing unauthorized access.

Core components of the IIOT security Model

(i) Device Security: Ensure that only authorized software loads onto the device, Regularly update firmware, ensure encryption and authentication protocols to protect data transmission. Implement measures to safeguard devices from physical tampering.

(ii) Network Security: Use secure protocols like TLS/SSL for encrypted communication, Monitor network traffic for anomalies, filter incoming and outgoing traffic

(iii) Data security: Use Hashing mechanisms to hash the original data, protects sensitive data stored on IIOT devices and cloud services.

(iv) Authentication and Authorization: verifies user identity using authentication or second verification authentication, only allow data access to Authorized user.

Access Control: Access control mechanism define who can access what resources and under what conditions. In IIOT access control is critical to prevent unauthorized access to sensitive data.

Core components of the IIOT Access Control

(i) Role-Based Access control (RBAC): Assigning permissions based on roles Eg: administrator, operator, technician.

② Attribute - Based Access control: Assigning permissions based on attributes of users, devices, and resources.

③ Identity - Based Access control: Assigning permissions based on digital certificates for authentication and authorization.

④ Time - Based Access control: Temporary access rights for maintenance workers.

⑤ Describe participatory sensing used for city traffic, densities management using IOT.

participatory sensing: It is a technique where devices collaboratively collect and share data for a common goal. When applied to managing city traffic, density management, participatory sensing leverage / take benefit of IOT devices.

How it works

① Citizen participation: Each human collects traffic related data such as GPS location, speed, Traffic light status using installed dedicated apps or enable specific features on their device that collect and transmit relevant traffic data.

② Data Aggregation: The collected data from individual devices is aggregated and transmitted to a central server or cloud platform.

③ Real time Analysis: Advanced analytics techniques are applied to the aggregated data to derive meaningful insights.

④ Intelligent Traffic management: The insights gained from data analysis are used to optimize traffic flow. Such as Dynamic Traffic signal control, Quickly response to accidents, public Transportation optimization.

(PYQ) Examine functions for source identity-management, identity establishment, device message access-control, message-integrity, message non-repudiation and ~~availability~~ availability in IOT applications and services.

Ans ⇒

① Source identity Management:

purpose: To manage the identities of IOT devices, applications, and users efficiently.

functions:

(i) Unique identifier Assignment: Assigning unique IDs like MAC address, UUID to each IOT device.

(ii) Authentication protocols: Supporting multi-factor authentication or device fingerprinting.

(iii) Role-Based Access Management: Giving access of the resources to devices and users based on specific roles to control privileges.

(iv) Credential Management: storing updating, and revoking credentials like passwords, certificates.

② Identity-Establishment:

purpose: To authenticate and authorize devices and users to access resources and services.

functions:

(i) password-based Authentication: Authenticate users based on password.

(ii) Token-based Authentication: Authenticate users based on one time password (eg OTP) or time-based tokens.

(iii) Biometric authentication: Authenticate users based on fingerprints, facial recognition, or voice recognition.

(iv) Certificate-based authentication: ~~verifying digital Authentica~~ users based on digital certificates.

(3) Device message Access Control:

Purpose: To restrict access to messages or data based on permissions and policies.

Functions:

(i) Role-based access control: Assigning roles to users and devices to determine their access privileges.

(ii) Attribute-based access control: Access control based on attributes of the user, device or resources.

(iii) policy-based access control: Defining who can access which messages and under what conditions.

(4) Message integrity:

purpose: To ensure the content of messages is not altered during transmission.

functions:

(i) cryptographic Hashing: Generating a unique hash value for each message

(ii) Message Authentication codes: Using a secret key to generate a tag that verifies message integrity and ~~authenticity~~ authenticity.

(5) message Non-Repudiation:

purpose: To ensure that the ~~messages are deli~~ senders of a message cannot deny having send it.

functions: (i) Digital signatures: Using public-key cryptography to sign messages and prove their origin.

(iv) Timestamping services: Recording the time of message creation or transmission.

(6) Message Availability:

Purpose: To ensure that messages are delivered reliably and timely.

functions:

(i) Redundancy: Implementing duplicate hardware or network paths to ensure continuity.

(ii) Load Balancing: Distributing network traffic to multiple servers to improve performance.

(iii) Secure communication protocols (TLS/SSL): Encrypting data to protect it from unauthorized access.

PYQ (a) State the function of Data Acquistion. Explain the function of Data validation. Define spatial Data.

(b) Demonstrate Event-driven industrial IOT system? List out the steps used in internet gateway device. formulate the significant use of Raspberry pi in smart cities and industrial appliances.

(c) Data Acquisition (DAQ): Data Acquisition is the process of collecting data from various sources for analysis, processing and storage. This can involve gathering data from sensors, surveys, satelite imagery, GPS devices or other digital systems. The primary function of data acquistion is to ensure that accurate, relevent and timely data is collected.

functions:

(i) Data sensing: DAQ system utilize sensors to convert physical quantities into measurable electrical signals.

(2) Signal conditioning: The captured signals may need amplification, filtering.

(3) Analog-to-Digital Conversion: Analog signals from sensors are converted into digital form for processing.

(4) Data Transfer: The data is transferred to a data storage device.

(5) Data Storage: The collected data is stored for later analysis and retrival.

Data validation: Data validation is the process of ensuring the accuracy, completeness and consistency of data. It involves checking data against predefined rules and standards to identify and correct errors.

functions:

(i) Data completeness: verifying that all required data fields are filled.

(ii) Data Accuracy: checking data for correctness and consistency with known values.

(iii) Data consistency: Ensuring that data is collected to a specific formats, rules, and relationships.

(iv) Data uniqueness: Identifying and removing duplicate records

Spatial Data

Spatial data refers to information about the location, shape and relationships of physical objects on Earth's surface. It is also known as geospatial data. This data is represented in terms of coordinates, latitude, longitude.

Event-Driven Industrial IoT Systems

Event-driven Industrial IoT systems focus on responding to specific events in real-time, such as sensor data changes, alarms, or user inputs. These systems ensure timely communication, decision making and action.

Steps in Internet Gateway Device:

(i) Sensor Data Acquisition: Collects data from various sensors

(ii) Data processing: Applies algorithms to extract meaningful insights from the raw data.

(iii) Data transmission: Transmits the data to the cloud using wifi, cellular.

(iv) Security: Implements robust security and authentication mechanisms to protect sensitive data.

Use of Raspberry pi in Smart cities and Industrial Appliances. In smart cities:

(i) Environmental Monitoring: Tracks air quality, temperature and humidity.

(ii) Traffic Management: processes real-time traffic data to optimize signals.

(iii) Waste Management: Monitors waste bin levels and optimizes collection routes.

In industrial Appliances

(i) Remote monitoring: Tracks the performance of industrial equipment remotely.

(ii) Quality control: Monitors product quality parameters

(iii) Energy Efficiency: Optimizes energy consumption

(iv) Automation: Automates repetitive tasks, improving productivity and reducing human error.

(Q8) related to RFID
Explore the concept of the web of Things (WoT) applied to RFID technology. How does WoT enhance the accessibility and interaction of RFID-enabled devices on the web?

ans ⇒ The web of Things (WoT) and RFID is a powerful combination. The web of things is an extension of the internet of things that leverages web technologies to enhance the interoperability and accessibility of devices. When combined with Radio frequency identification. WoT opens up a word of possibilities for seamless interaction b/w physical objects and the digital world.

How WoT enhances RFID accessibility and interaction.

WoT provides a standardized way to access and control RFID enabled devices through web-based interfaces. This eliminates the need for ~~proprietary~~ software or hardware making it accessible to the users. It ensures that RFID devices can be accessed and controlled from any devices with a web browser. WoT enables real-time data exchanges between RFID devices and web application for immediate updates. WoT enables users to monitor and control RFID devices remotely from anywhere in the world using internet.

Ex ⇒ supply chain, Manufacturing, Healthcare.

Compare and contrast IPV4 and IPV6 protocols. Also the limitations of IPV4 and how IPV6 addresses. Define Media Access Control and explain its function in network communication. Provide an example of a scenario where MAC address are crucial for device communication.

Features	IPV4	IPV6
Definition	IPV4 is a protocol used to identify devices on internet. offering 4.3 billion unique addres	IPV6 is a protocol used to identify devices on internet providing almost unlimited unique addresses
Address Length	32 bit	128 bit
Address space	Approximately 4.3 billion Addresses	Approximately 3.4×10^{38} addresses
Address representation	Dotted decimal format.	Hexadecimal format with colons (:)
Header complexity	Simple header	Complex header
Broadcasting	supports broadcasting	No broadcasting uses multicasting
Security	Less than IPV6	more than IPV4
Uses	universal and widely used	Designed for future needs
support	It is supported by all the devices	It is supported by limited devices.

Limitations of IPV4 and How IPV6 addresses them

(i) Limited address space: IPV4 is 32 bit address space supports about 4.3 billion unique addresses which is insufficient for growing no of devices.

IPV6 Solution: IPV6 is 128 bit address space provides an almost unlimited no of address.

(ii) Address Configuration: IPV4 often required manual configuration.
IPV6 Solution: IPV6 supports stateless address auto-configuration.

(iii) Security: IPV4 lacks built-in security features.
IPV6 Solution: IPV6 mandates IPSec for encryption and secure communication.

- Media Access Control: Media access control is a unique identifier assigned to a network interface card of a device. It operates at the data link layer (layer 2) of the OSI model and facilitates communication within a local network.

functions in network communication

(i) Identification: MAC Addresses uniquely identify devices on a local network.

(ii) Data Delivery: Ensures data packets reach the correct device.

(iii) Collaboration with IP: Works with IP addresses for end-to-end communication, where the MAC address operates locally and IP facilitates broader.

Example Scenario: In a wi-fi network, a router uses MAC addresses to ensure data packets reach the correct device. Multiple devices are connected to a home wifi network. The router uses the MAC addresses of these devices to differentiate them and deliver the correct packets.

(EMPSC) Differentiate between ETSI, ITU-T and Two domain Models with reference to the functions and capabilities of each layer along with real time example demonstration.

Ans ⇒ Introduction

1. ETSI: ETSI Stands for European Telecommunication Standards Institute. ETSI focus on creating standards for ICT systems. particularly in network functions virtualization. virtualized network. It provides a framework for telecom service providers to implement virtualized network services.

ITU-T: ITU-T stands for International Telecommunication union - Telecommunication Standardization Sector. ITU-T is responsible for international standardization of telecommunication networks and services, such as optical Transport Networks and OSI reference model.

Two-Domain Models: This model divides system architecture into two domains: physical (hardware, infrastructure) and logical (software, virtualization). It is commonly used in Software defined Networking (SDN) and NFV for clear separation of concern. (Network function virtualization - NFV)

functions and capabilities of each layers

features	ETSI	ITU-T	Two Domain Model
purpose	standardizes NFV for flexible telecom networks	standardize global telecommunication services.	Separates physical and logical components
layers scope	primarily Europe	Global scope	used in modern network design like SDN
Real time example	European 5G network	International roaming services	SDN in cloud data centers.

Feature	ETSI	ITU-T	Two Domain
Layer	Two Domains D1 → Device and Gateway Domain D2 → Application and Network Domain	four layers L1 → Device layer L2 → Transport and Network layer L3 → Service and Application-support layer L4 → Application layer	Two Domains D1 → Application and Network domain D2 → Device and Gateway Domain
function	Simplifies network service deployment	Define protocols and inter-layer standards	Enable SDN and NFV framework
Capabilities	Focuses on European regulations.	focus on Global regulation	Efficient and scalable network management
Stands for	European Telecommunication standards institute	International Telecommunication union - Telecommunication standardization - sector	———
flexibility	High	Moderate	High

Real-Time example Demonstration

1. ETSI Example: A telecom provider like Vodafone uses ETSI NFV standards to deploy a virtualized 5G network

2. ITUT-Example: International telecommunication like submarine cables use ITU-T standards for optical Transport Networks to enable smooth data flow across continents.

3. Two Domain models Example: SDN in a data center
   - Physical Domain: NW devices like switches routers
   - Logical Domain: SDN controller manages traffic flows