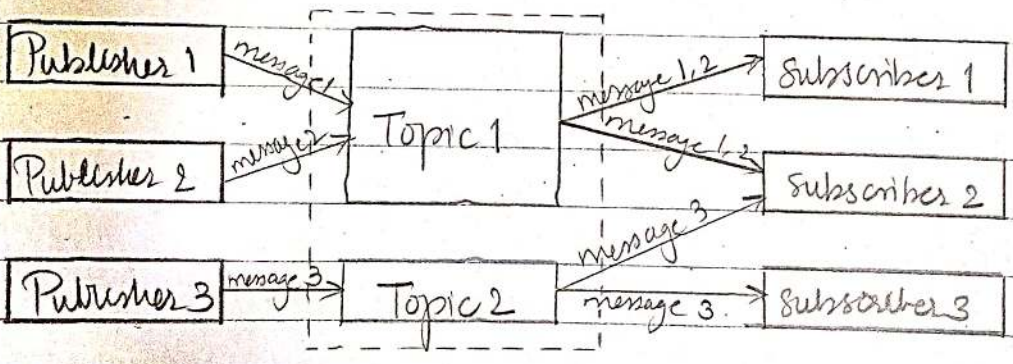
Q1. a. Demonstrate the working of publish - subscribe Communication model using diagram with suitable application.

ans : 1. Publisher - subscribe messaging is a form of asynchron-ous service to service communication used in modern computing environments.

2. In pub-sub communication model, any message published to a topic is immediately received by all of the subscribers of topic.

3. Pub-sub communication model can be used to enable event driven architectures or to decouple architectures in order to increase performance, reliability & scalability.



Publisher: entity that generates the messages (or data) and pushes them to a topic. A publisher need not be aware of all the subscribers for its messages that are pushed to topics.

Topic: entity that holds the messages sent by the publishers. A topic could receive messages from multiple publishers.

Subscribers: consumers that are interested to get messages (or data) on a particular topic w/o directly communicating with the publisher. A subscriber can subscribe to various topics.

Brokers: There could be an optional third party between publisher & subscriber called broker. A broker may hold the topics to which publisher can publish & subscribers can subscribe to.

Application:
Youtube channel subscription model.

1. Channel owner is the publisher that releases various videos.
2. Channel name is the topic under which the publisher publishes the new videos.
3. Youtube is a broker that holds these published videos and is aware of subscribers.
4. You are subscriber that has let known youtube to notify you when the publisher has published a new video on the channel. You could have subscribed to one or many youtube channels.

Representations:

1. A representation is information that is intended a reflect a past, current or desired state of a given resource.
2. It is in format that can be readily communicated via a payload. Example: it could be a HTML doc or a JPEG image
3. REST components perform actions on a resource by using a representation to capture the current or intended state of that resource by using a representation to capture the current or intended state of that resource & transferring that representation between components.
4. A representation is a sequence of bytes, plus representation metadata to describe those bytes

Connectors:

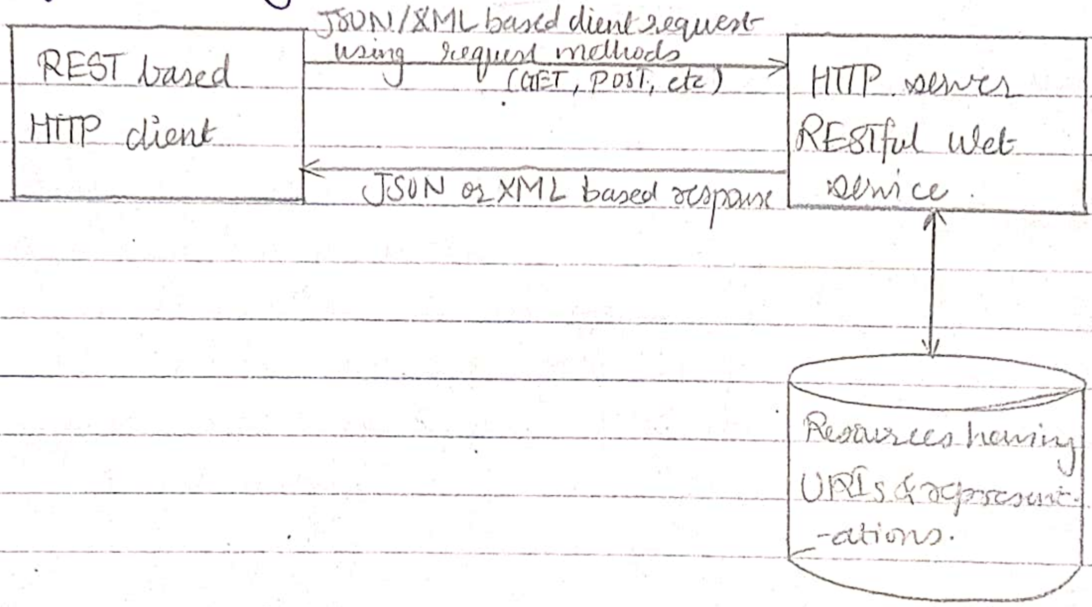
1. REST uses various connectors types to encapsulate the activities of accessing resources and transferring resource representations.
2. The connectors present at an abstract interface for component communication.
3. A connector manages network communication for a component and hence any info can be shared across multiple interactions in order to improve efficiency and responsiveness.

Request methods

1. Request method indicates the purpose for which the client has made the request and what is expected by the client as a successful result

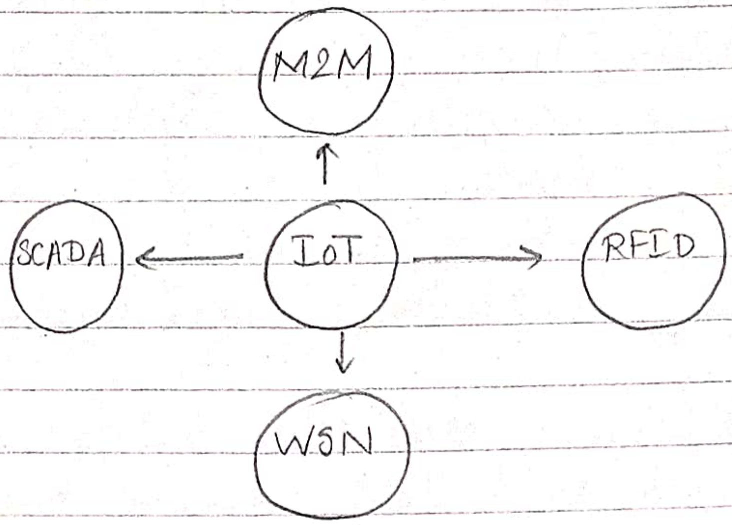
RESTful Web service (or APIs)

1. REST ful APIs work with HTTP according to REST architectural constraints (principles) using the various request methods such as GET and POST.
2. There could be several REST components such as client & server in the communication path.
3. Each resource has a specific identifier defined by its URI & has a representation associated with it.
4. RESTful APIs can use various media types for submitting requests or providing responses.
5. JSON & XML are most commonly used media types for working with RESTful APIs or web services.


REST based HTTP client
JSON/XML based client request using request methods (GET, POST, etc)
HTTP server RESTful Web service
JSON or XML based response
Resources having URIs & representations.

Q1. c. Classify the four pillars of IoT.

ans:



1. Machine to Machine (M2M)

- makes machine to machine communication & interaction successful. It encompasses all ~~tt~~ technolog
- It encompasses all technologies & mechanisms that enable IoT systems to communicate and interact with one another.
- Examples: wifi, cellular network, bluetooth.

2. Radio Frequency Identification (RFID):

- mechanism for uniquely identifying objects using radic frequencies.
- They can be used to uniquely identify IoT devices and system as well.
- It is important to uniquely identify the devices and systems so that you can provide appropriate inputs and receive and process output in the right way.

3. Wireless Sensor Networks (WSN):

- It is a large collection of sensor devices that can monitor several physical conditions
- Each sensor device is called sensor node
- Sensor nodes can monitor a several physical conditions such as temperature, air pressure, illumination, motion, windspeed, humidity etc.

4. Supervisory Control and Data Acquisition (SCADA)

- gathers and analyses real time data.
- They are used to monitor and control a plant or equipment in industries such as telecommunications, water & waste control, energy and oil gas refining.
- It gathers information such as where a leak on a pipeline has occurred etc.

Q2. a. Illustrate steps of IoT design methodology for smart irrigation system.

ans: 1. Define System requirements: Identify irrigation needs and determine the sensors and actuators.

2. Device selection: choose hardware like microcontrollers, sensors, and communication modules.

3. Connectivity & communication: Establish how devices will communicate. Ensure real time data transfer from sensors to the controller & actuators commands from the cloud

4. Data acquisition: Integerate sensors to collect environmental data. Use protocols like MQTT/HTTP to send data to the cloud or a centralised hub.

5. Data processing and analysis: Use cloud services or edge computing to process sensor data. Set thresholds to determine when irrigation is needed.

6. Automation and control: Implement algorithms to control water distribution. Use data to automate irrigation schedules, reducing water wastage.

7. User interface: Design a mobile/web app for monitoring real time data and controlling the sys manually when needed.

8. Testing & iteration: Test the system for real world performance. Optimize for energy consumption, connectivity & response times.

Q.2.b. Demonstrate use of SCADA with the help of suitable IoT applications.

ans: SCADA is widely used for monitoring & controlling industrial processes. When integerated with IoT, SCADA ~~enth~~ enhances remote monitoring and control through real time data from connected sensors & actuators

Smart Water Management:
Monitoring and controlling water distribution in municipal systems.

Role of SCADA:

1. collects real time data from IOT enabled water flow sensors ands pumps.
2. It controls the opening & closing of valves based on demand and water levels.
3. The system alerts operators when there's a leak or abnormal water usage
4. IOT integeration allows remote monitoring and control via a cloud interface.

Q.2c. Show the use of LORA protocol in any suitable IoT application development.

ans: LoRa is a low power wide area network (LPWAN) protocol designed for IoT apps requiring long range communication and low energy consumption.

Smart Agriculture IoT application using LoRa
Problem statement:
Farmers need to monitor vast agricultural fields for factors like soil, moisture, temperature & humidity to optimize irrigation and crop yield.

Solution: LoRa based smart agriculture system.
Architecture:

1. IoT devices: soil moisture sensors, temperature & humidity sensors and weather stations are spread across the fileds to gather data.

LoRa modules: Each sensor node is equipped with a LoRa module to transmit data over long distances to a central gateway.

LoRa Gateway: A central LoRa gateway collects data from all the sensor nodes and forwards it to a cloud server or central system via ethernet, wifi or cellular connection.

Cloud Platform: The collected data is processed & analysed in the cloud for real time monitoring and decision making.

User & Interface: Farmers can access data and control irrigation systems using a web or mobile app.

Q.3.a Classify between RFID & SCADA Protocol.

Ans:

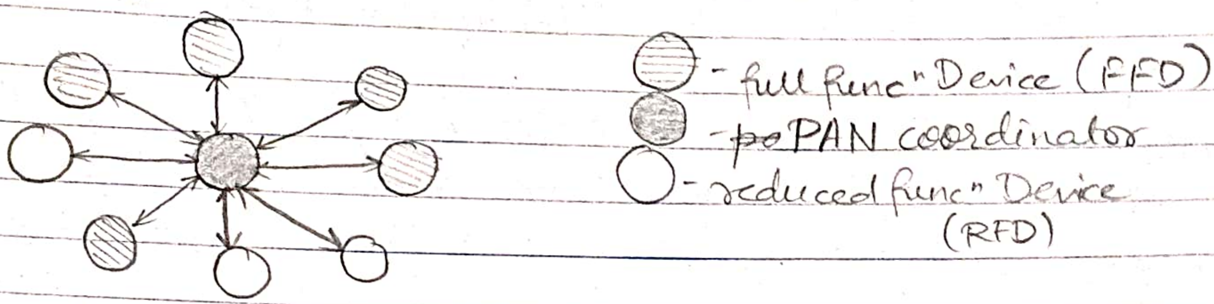
	Category	RFID	SCADA.
1.	Purpose	Identification and tracking of objects/assets	Monitoring & controlling industrial processes.
2.	Functionality	Reads/writes data from tags using radio waves	Supervises, collects data & controls equipments:
3.	Components:	RFID tags, readers, antennas	Sensors, controllers, HMI, communica^n networks
4.	Data flow	One way (from tag to reader)	Two way (data collection and control signals)
5.	Communica^n range	Short range (up to a few meters)	Long range depending ~~of~~ on communication network used.

Date: / /
Page No.:-

Q.3.b. Classify the different Topology of IEEE 802.15.4 and explain with suitable diagram.

ans: 1. Star Topology:

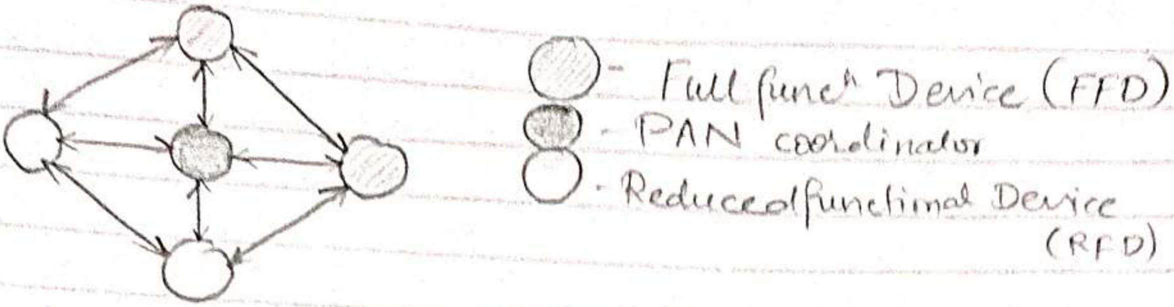
- communication is established between devices and single central controller called the PAN coordinat
- A device typically has some associated application and is either the initiation point, or the termination point for network communications.



- The PAN coordinator is the primary controller of the PAN.
- All devices operating on a network have unique addresses referred to as extended addresses.
- Star topology is usually used over small areas.

2 Peer-to-Peer Topology.

- any device can communicate ~~the~~ with any other device in the PAN (as long as they are in range of one another) w/o going through the PAN coordinator.
- The PAN coordinator, but it carries out its regular functions in coordinating & managing the network.



- All devices operating on a network have unique addresse referred to as extended addresses.

Q.3.c. Show the use of LoRa protocol in any suitable IOT application development.

ans: LoRa (Long Range) is widely used in IOT application due to its long range communication capability & low power consumption.

Smart Waste management Protocol System using LORA.
Traditional waste collection methods are inefficient because trucks follow fixed routes & schedules, even when some bins may not be full. This leads to unnecessary fuel consumption, higher costs & environmental impact.
Solution: LoRa based smart waste management system.
System Overview:
Sensors: waste bins across the city areequipped with IoT enabled ultrasonic sensors that measure the fill level of the bins.
LoRa Modules: Each sensor is connected to a LoRa module for long range data transmission to a centralized server.

Date:- / /

Page No.:-

LoRa Gateway: deployed in various parts of the city to receive data from multiple bins and forward it to the cloud through a backhaul network.

Cloud Platform : the collected data is processed and analysed on a cloud platform to monitor the fill levels and optimize the waste collection routes.

User Interface: City waste management authorities can monitor bin status in real time through a dashboard or mobile app. notifications are sent when bins need to be emptied.

Q.4. a Classify below Illustrate diff. issues with standardized IoT protocol.

ans: Issues with standardization of IoT protocols:

1. Interoperatibility: Devices from different vendors use diverse protocols making it hard for seamless communication.
2. Security & Privacy: Resource constrained IoT devices struggle to implement robust security, making standardization crucial for encryption & authentication
3. Scalability: Existing protocols may not efficiently handle the massive growth of IoT devices, especially in large scale application like smart grids.
4. Fragmentation: various industry bodies offer different protocols leading to a divided IoT ecosystems.

5. Power efficiency : many IoT devices need low power protocols for battery longetivity especially in remote deployments.

6. Latency & Real time : Applications like industrial automation need low latency protocols, challenging standardization

Q4. b. Illustrate the various IoT appⁿ. developed using IP based protocols.

ans : IoT applications using IP based protocols include:

1. Smart homes : devices like lights, thermostats and appliances communicate via protocols like MQTT and CoAP to provide automation & control.
2. Smart Cities : sensors for traffic, air quality and waste management use IP protocols for real time monitoring and data collection
3. Healthcare : Wearable devices & remote monitoring systems use IP protocols to transmit patient data.
4. Industrial IoT : machines & sensors in factories use IP based communication for automation and predictive maintenance

Q.4. C. Show with suitable reasons why zigbee is popular than wifi and bluetooth in IoT.

ans: Zigbee is more populer than Wifi & bluetooth in IOT due too:

1. Low power consumption: Zigbee is highly energy efficient ideal for battery powered IoT devices.

2 Mesh networking: It suppOrts large, scalable networks with multiple nodes unlike Wifi & standard Bluetooth

3. Range: Zigbee covers larger distances in mesh networks, while bluetooth has limited range and wifi consumes more power to cover similar distance

4. Low date rate: Zigbee is optimized for low data rate applications unlike wi-fi, which is better for high speed data transfers.

Q.5. a. Demonstate python web application framework-Django withe the suitable example.

ans: Django web application Example:

1. Install Django
2. Create project and app
3. Define a model:

```
class Book (models. Model) :
    title = models. CharField (max_length = 100)
    author = models. CharField (max_length = 100)
    published_date = models. DataField ()
```

4. Create a view

```
from django.shortcuts import render
from .models import Book
def book_list(request):
    books = book.objects.all()
    return render(request, 'book/book_list.html',
        {'books': books})
```

5. URL configuration:

```
from django.urls import path
from . import views
url patterns = [
    path('', views.book_list, name='book_list'),
]
```

6. Set up template:

```
<h1> Library books </h1>
<ul>
    {% for book in books %}
        <li> {{book.title}} by {{book.author}}
     ({{ book.published_date }}) </li>
        {% end for %}
</ul>
```

7. Run the server

Q5. b. Use the knowledge of Cloud Computing to demonstrate
i. Amazon Auto Scaling
ii. Xively Cloud for IoT.

ans: i. Amazon Autoscaling:

1. AWS auto scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost.

2. Characteristics & features of AWS auto scaling:

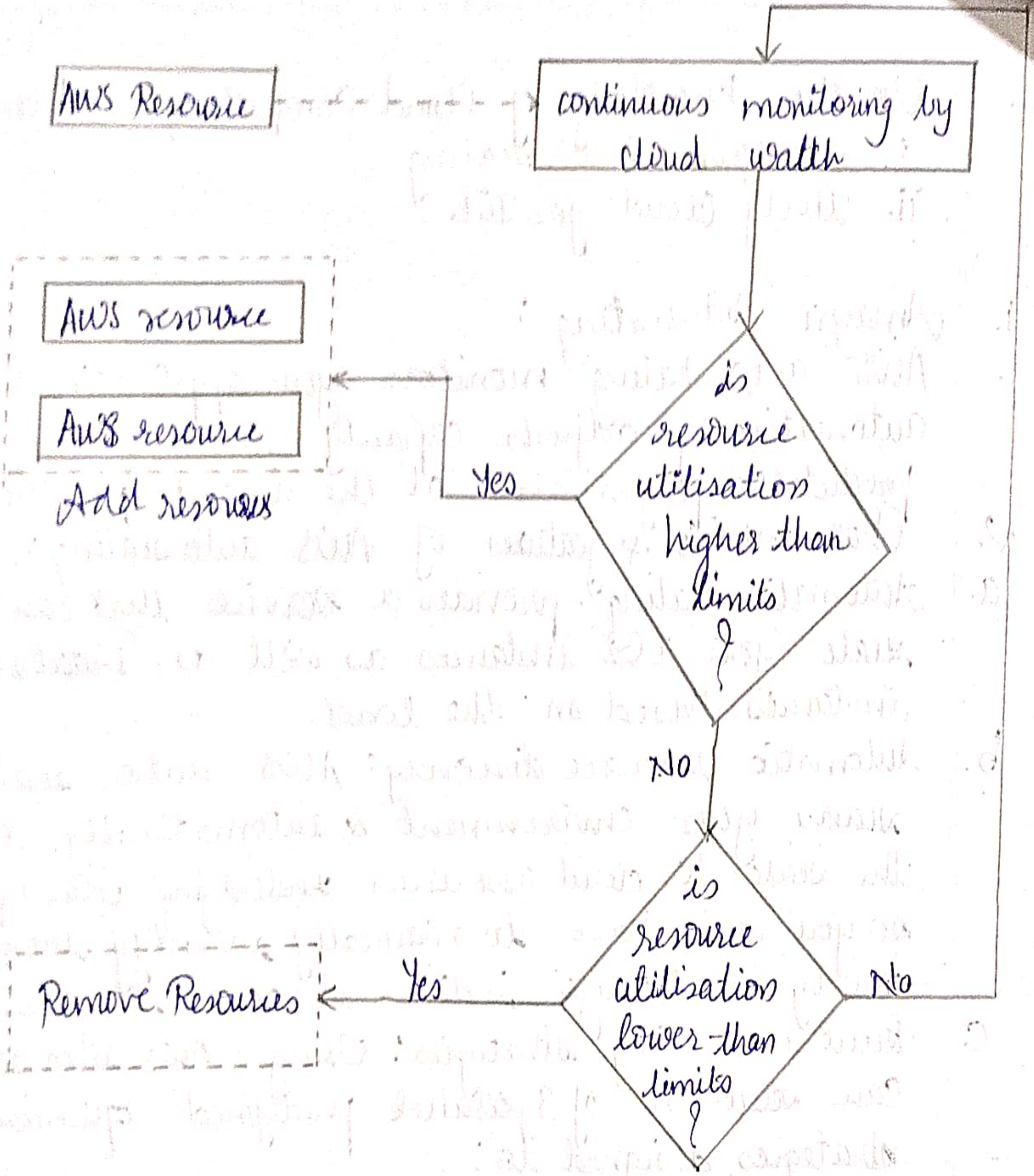
a. Automatic scaling. provides a service that can automatically scale your EC2 instances as well as Database instances based on the load.

b. Automatic resource discovery: AWS auto scaling scans your environment & automatically discovers the scalable cloud resources underlying your application so you don't have to manually indentify these resources one by one through individual service interfaces.

c. Built in scaling strategies: Using AWS auto scaling you can select one of 3 parallel predefined optimisation strategies designed to:

- optimise performance
- optimise costs or
- balance the two

d. Predictive scaling: predicts future traffic, including regularly occurring spikes, and provisions the right no. of EC2 instances in advance of predicted changes.


AWS Resource
continuous monitoring by cloud watch
AWS resource
AWS resource
Add resources
is resource utilisation higher than limits ?
Yes
No
is resource ulilisation lower than limits ?
Yes
No
Remove Resources

ii. Xively Cloud for IoT

ans: 1. Xively is an enterprise platform for building, managing and deriving business value from connected products.

2 It helps companies at any stage of the IoT journey provide additional value and bring connected products to market, quickly reliably and securely.

3. Xively services:

1. Run time messaging
2 Business logic
3. Security
4. Integeration.

4. Architecture:

a. Basic Infrastructure:

Messaging: provides a message broker for secure scalables guaranteed message delivery between devices users and application out of the box.

storage: you can store and query against historical changes to a device state or commands sent over the wire from the time series database.

B2. Devices:

device directory: you can define templates for your devices then store and query against the master record of their state or commands sent over the wire from time series database.

Embedded clients: use firmwares libraries that work with any hardware you choose.

3. Users

User directory: Create, store & manage user's & store their data in Xively's user management system.

Template mobile apps: You can use Xively's end user apps for iOS, android, and web.

4. Operational tools:

5. Management tools.

Q6. a. Show that WAMP and its key concepts are useful in Cloud based IOT applications development

ans: Wamp Concepts:

A Pubsub

1. Subsribers: They could subscribe to one of more topics that could be published by the Publishers via Brokers.

2. Publishers: push events and information to various topics by sending messages to a Broker

3. Broker: acts as a mediator between publishers & subscribers so as to decouple the communication between them.

B. Routed RPC:

1. Callers: makes procedure calls to the dealer through the URI of the procedure to be called & any callargs.

2. Callees: registers a procedure at a dealer using an URI that identifies the procedure.

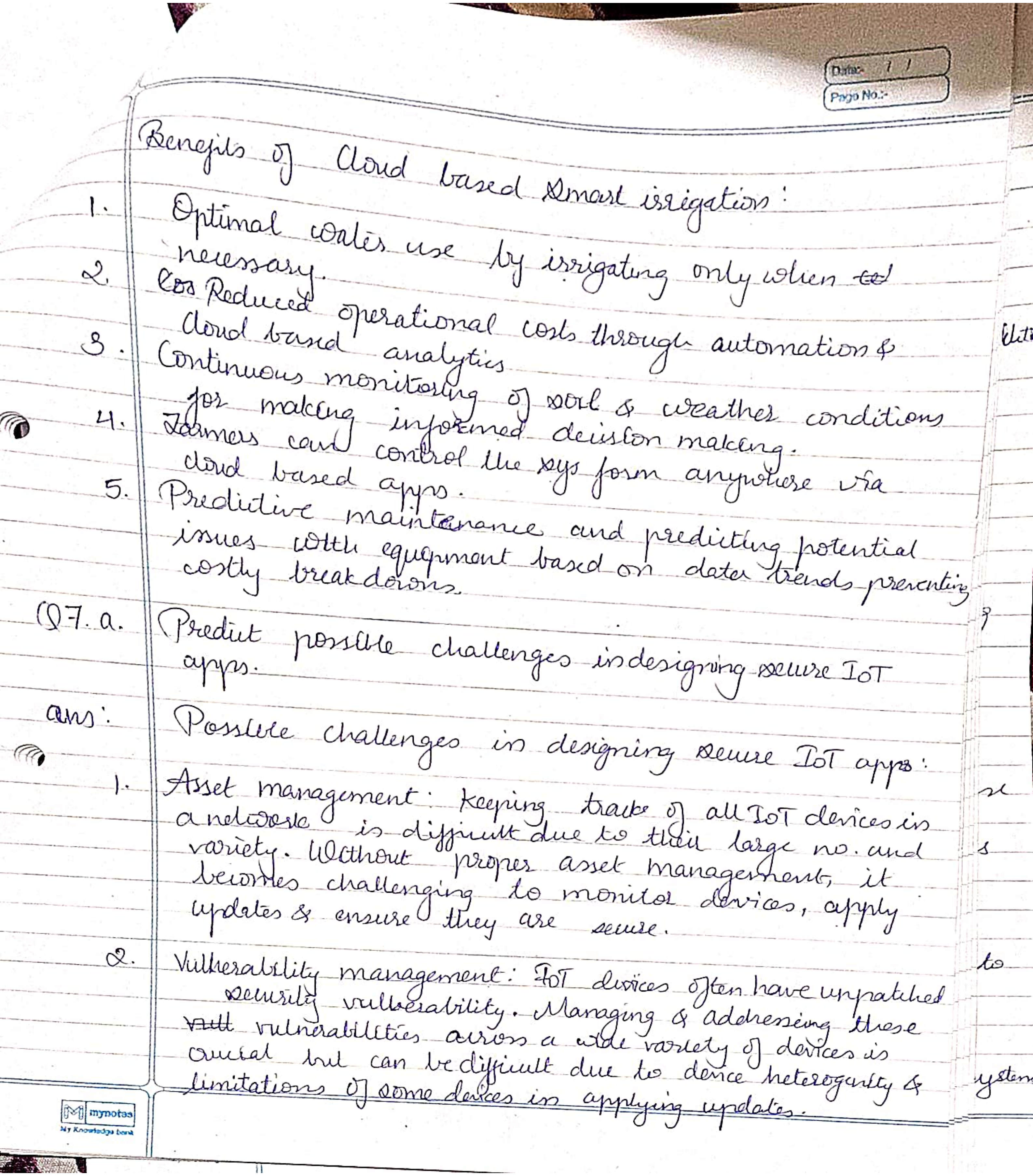
3. Dealer: is responsible for routing call originating from the caller to the callee and route back results.

These Web Application Messaging Protocol (WAMP) TA is highly useful in cloud based IoT application development due to its core features of realtime communication, scalability and event driven architecture

Q.6b. Apply the concept of cloud computing to design the smart irrigation system with proper explanation.

ans: A cloud based smart irrigation system integrates cloud computing, IoT devices and sensors to efficiently manage water usage in agricultural fields.

1. Data collection via IoT sensors:
   These sensors collect real time data and send it to central gateway - cloud server.
2. Data analytics & processing: Cloud provides scalable storage, analytics using AI/ML and integrate weather APIs to predict rain & adjust irrigation schedules accordingly
3. Decision making: Based on processed data, cloud system can automatically send commands to irrigation actuators



Benefits of Cloud based Smart irrigation:

1. Optimal water use by irrigating only when ~~to~~ necessary.
2. ~~Cos~~ Reduced operational costs through automation & cloud based analytics
3. Continuous monitoring of soil & weather conditions for making informed decision making.
4. Farmers can control the sys form anywhere via cloud based apps.
5. Predictive maintenance and predicting potential issues with equipment based on data trends preventing costly breakdowns.

Q7. a. Predict possible challenges in designing secure IoT apps.

ans: Possible challenges in designing secure IoT apps:

1. Asset management: Keeping track of all IoT devices in a network is difficult due to their large no. and variety. Without proper asset management, it becomes challenging to monitor devices, apply updates & ensure they are secure.

2. Vulnerability management: IoT devices often have unpatched security vulnerability. Managing & addressing these ~~vull~~ vulnerabilities across a wide variety of devices is crucial but can be difficult due to device heterogenity & limitations of some devices in applying updates.

3. Access management: Ensuring that only authorized users and devices have access to ~~B~~ sensitive IoT system is critical. Weak passwords, lack of proper authentication mechanisms or ~~p~~ improper access control configurations can lead to security breaches.

4. Incident detection: Identifying and responding to security incidents in real time is challenging in IoT networks due to the sheer volume of data generated and the variety of potential attack vectors such as malware or physical tampering.

5. Data Protection: IoT devices often handle sensitive data so protecting that data (both at rest & in transit) from ~~a~~ unauthorized access or tampering is essential. Many IoT devices lack the computational power to implement robust encryption & security protocols.

6. Information Flow Management: Ensuring that data flows securely between IoT devices, gateways, and cloud services is critical. A lack of proper controls can result in unauthorized data encryption or tampering as information flows through network.

7. PII Processing Permissions Management: The IoT device may collect PII indiscriminately to analyse, share or act upon the PII based on automated processes. IoT devices may be complex with sensing functionality that can collect PII being frequently added & removed.

8. Informed Decision Making: The IOT devices may lack interfaces that enable individuals to interact with it. Decentralised data processing functions & hetteregenous ownerships of IOT devices challenge traditional accountability processes.

Q.7.b. Illustrate the classic pillars of information assurance while securing the IoT application.

ans: To secure IoT applications the classic pillars of informations assurances are essential. They are:

1. Confidentiality: ensures that sensitivity data within IoT system is only accessible to authorized users and devices. For IOT this can be achieved through:

- Encryption

&

- accesscontrol.

2. Integrity: ensures that data collected, transmitted or processed by IOT devices remains accurate and unaltered. It's particularly important for IOT devices that rely on real time data for decision making.

Key mechanisms:

Hash functions:

and

Digital Signatures:

Date: / /
Page No.:-

Availability: ensures that IoT devices data & services are accessible when needed. IoT systems need to be always -on or available often in critical environmentas like healthcare or industrial control.
Measures to enhance availability include :
- Redundancy
  and
- DDoS protection

4. Authentication : verifies the identities of users & devices before granting them acess to the IoT system.
This is crucial in IoT environments to prevent unauthorized entities from accessing or controlling devices.
Methods include :
- Multi factor authentication
- Device authentication

5. Non - repudiation : ensures that the origin or recipient of a transaction or data exchange exchange cannot deny their involvement. It can be achieved through :
- Digital signatures
- and
- Audit logs.

5. a. Illustrate the threat model in securing IoT appns.

ans: 1. Like any other system, IoT system could be threat modelled as well.

2. A threat model depends on functionality that the system provides as well as the skills that the attacker might have to exploit the vulnerabilities contained in the sys.

3. So a threat model for an IoT sys helps you to identify threats and helps you to build a secure IoT system

4 Some common misuses or threats in IoT system are:

- stealing / manipulating credentials
- Unauthorised data access.
- Denial of service (DoS)
- Man-in-the-middle attack
- Tampering identifiers

5. Example: Smart speaker. It has:

- firmware.
- certificates & device unique keys
- log in credentials user or admin
- system configuration
- Event logs.
- Voice recordings
- Device resources.

Date:- / /
Page No.:-

Q.8.b. Use security concepts to identify different threats (at least 03) in each in the following IoT apps:

i. Smart home automation:

ans: 1. Unauthorized access: hacker can gain access to smart home devices through weak passwords or vulnerabilit in the system, potentially allowing unauthorized surveillance or entry into home.

2. Man-in-the-middle: attackers may intercept & alter the commands sent between devices by compromising network traffic.

3. Denial of service attacks: overwhelming smart home devices with traffic making critical devices like lights alarms / smart locks unresponsive impacting home security.

Q.ii. Smart parking system

ans: 1. location spoofing: fake vehicle locations mislead parking availability.

2. Data Tampering: Attackers alter parking data to cause incorrect fees or availability.

3. Device hijacking: hacker take over parking sensors sending fake data to system.

iii. Smart irrigation system:

ans: 1. data leakage: sensitive crop & water data exposed to unauthorized parties

2. Command injection: Hackers send false irrigation commands harming crop management.

3. System disruption: DOS attacks disable irrigation system halting proper watering.