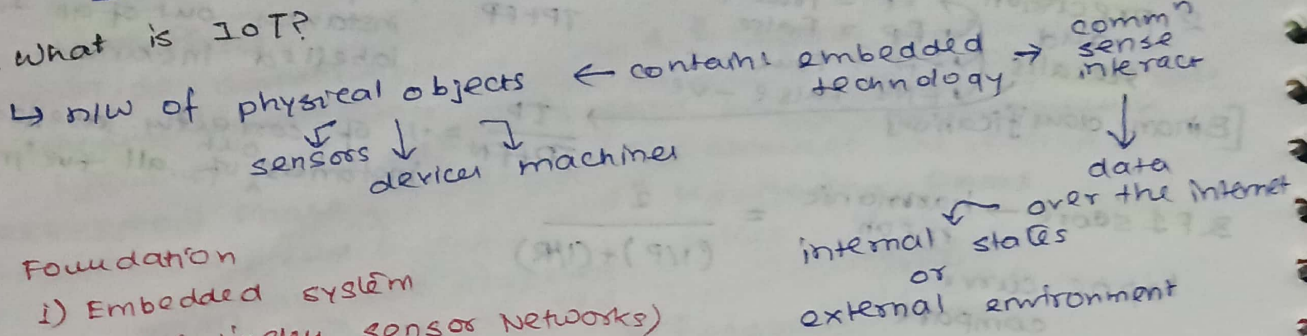


ToT Learning Plan

Day 1

1. IoT Foundations + Networking.

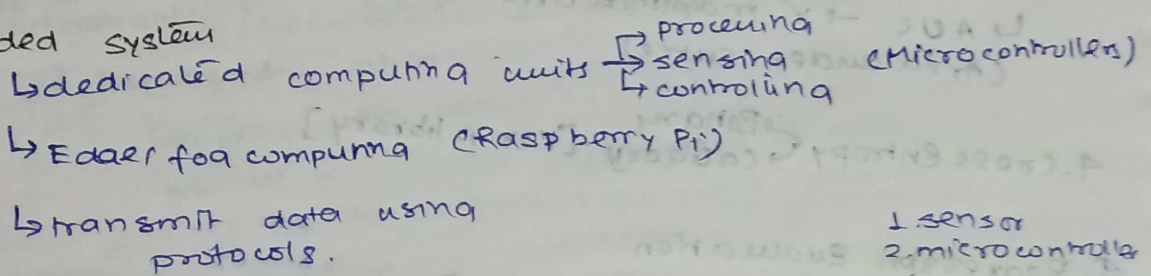
1. What is IoT?



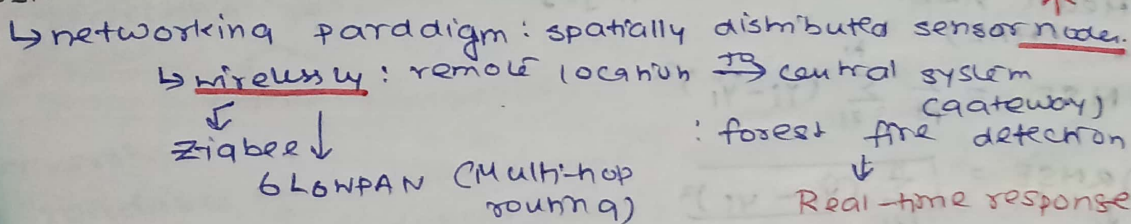
2. Foundation

- i) Embedded system
- ii) WSN (Wireless Sensor Networks)
- iii) Machine-to-Machine comm'n (M2M)

i) Embedded system



ii) WSN



- 1. sensor
- 2. microcontroller
- 3. radio module
- 4. power source

iii) M2M

- ↳ direct comm'n btw devices w/o human intervention
- ↳ Autonomous
- ↳ cellular n/w
- Protocols: MQTT, CoAP, HTTP etc.

eg: Smart home

[Ac automatically adjust based on

* IoT devices need to communicate over the n/w. [room sensor data]

OSI is a conceptual model used for understanding

↓
TCP/IP = real-world stack used in IoT

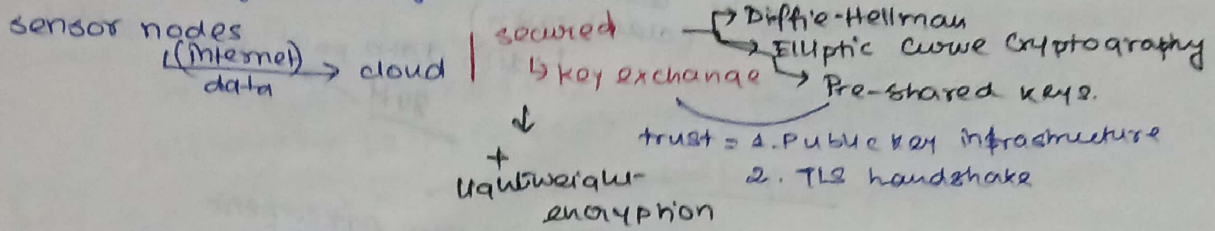
- 1. transport layer protocol: UDP (lightweight data)
- 2. app'l layer " : MQTT (minimal energy use)



IoT Learning Plan

Day 2

Sensor Node + cloud communication
for Key Exchange.



Cyber Physical Systems

↳ Internet based

↳ networked monitoring

+ controlling system

governed by

Eq: self driving cars.

↓
feedback-based control Algorithms.

Cloud computing

↳ pool of multiple resources.

Eq.: AWS IoT core

↓ servers ↓ storage ↓ hw → over internet.

↳ (Cisco)

Fog computing

↳ distr architecture

↳ a layer between edge and cloud → local processing

Eq.: Traffic camera triggers nearby signals w/o waiting for the cloud.

↓
to avoid service latency.

IoT Sensing + Actuation

↓ detect data

↓ perform actions

Sensor → process → Actuator
[sensor → collects → send data
Actuator ← Receiver ← Perform Action]

IoT Processing Topologies + Types

↳ deciding architecture of the deployment

1. Batch processing : Historical data in chunks
2. stream " : Real-time analysis
3. Event-driven : Motion (security) detection.

Data Protocols in IoT

↳ MQTT: reliable messaging via broker

↳ CoAP: direct device-to-device comm

1. Why lightweight cryptography?

- ↳ enough security
- ↳ optimized algorithms
- ↳ practical (fits the device constraints)

2. Post Quantum Security consideration?

- ↳ threaten traditional cryptography (Shor's algo)
- ↳ Lattice based cryptography
- ↳ runs on classical computers
- ↳ designed for realworld deployment

3. IoT Anomaly Detection with MLOps

sensors → MQTT → auto encoder → validation → containment

↓
auto training ← cloud backends
pipelines

4. Security challenges in IoT?

- ↳ network security (MITM)
- ↳ scalability issues

5. Authentication in IoT

Gateway ↔ cloud
↑
Mutual

Authentication ensures only legitimate ^{biometric} entities interact, while privacy safeguards sensitive data from misuse.

6. Rider location Updates with lightweight- protocols

↳ MQTT, CoAP, gRPC

↑
since mobile n/w → unstable
→ bandwidth limited

7. Food delivery optimization

with IoT + ML

↳ nearest available riders
↕ predicted preparation time.
traffic ← GPS

↓
Batch optimization (aggregating multiple orders along the same route)
↳ Liveness tracking [websockets]

8. post-quantum-resilient IoT in healthcare

hash-based firmware
AES-256-GCM [bulk data]
Terminate heavy crypto @ gateways
Update

PKI → hybrid X.509 with clear rotation policies

IoT Learning plan

Day 4

1. Current security check

TLS → Mosquitto / MQTT

↳ Kafka: token based authentication