Day 1

IoT Learning Plan.

1. IoT Foundations + Networking.

1. What is IoT?

↳ n/w of physical objects ← contains embedded technology → comm

↓ sensors ↓ devices ↓ machines

comm^{n} sense interact ↓ data over the internet ↙ internal states or external environment

2. Foundation

i) Embedded system

ii) WSN (Wireless Sensor Networks)

iii) Machine-to-Machine comm^{n} (M2M)

i) Embedded system

↳ dedicated computing units → processing → sensing → controlling (Microcontrollers)

↳ Edge/fog computing (Raspberry Pi)

↳ transmit data using protocols.

ii) WSN

↳ networking parddigm: spatially distributed sensor nodes.

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

↳ wirelessly: remote location → to central system (gateway)

↓ Zigbee ↓ 6LoWPAN (Multi-hop routing)

: forest fire detection ↓ Real-time response

iii) M2M

↳ direct comm^{n} btw devices w/o human intervention

Autonomous

↳ cellular n/w

Protocols: MQTT, CoAP, HTTP etc.

Eg: Smart homes [AC automatically adjusts based on ↑ room sensor data]

* IoT devices need to communicate over the n/w.

OSI is a conceptual model used for understanding

↓

TCP/IP = real-world stack used in IoT

↓

1. transport layer protocol: UDP (lightweight data)
2. appl^{n} layer " : MQTT (minimal energy use)

IoT Learning Plan

Day 2

Sensor Nodes + cloud communication for Key Exchange.

sensor nodes →(internet) data → cloud | secured ↳ key exchange → Diffie-Hellman
→ Elliptic curve Cryptography
→ Pre-shared keys.

↓ + lightweight encryption

trust = 1. Public key infrastructure
2. TLS handshake

Cyber Physical Systems
↳ Internet based
↳ networked ~~mto~~ monitoring + controlling system } governed by ↓ feedback-based control Algorithms.

Eg: self driving cars.

Cloud computing
↳ pool of multiple resources.
↓ servers ↓ storage ↓ n/w → over internet.

Eg. : AWS IOT core

(CISCO)
Fog computing
↳ distr architecture
↳ a layer between edge and cloud → local processing ↓ to avoid service latency.

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

IOT Sensing + Actuation
↓ detect data ↓ perform actions

sensor → process → Actuate
[sensor → collects → sends data
Actuator ← Receives ← Perform Action]

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

↳ deciding architecture of the deployment

Data Protocols in IoT
↳ MQTT : reliable messaging via broker
↳ CoAP : direct device-to-device commn

Day 3

IoT Learning Plan

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
   sensor → MQTT → autoencoder → validation → containerization
   ↓
   auto retraining pipelines ← cloud backends

4. Security challenges in IoT?
   ↳ network security (MITM)
   ↳ scalability issues

5. Authentication in IoT
   Gateway ⟷ cloud
   ↑
   Mutual
   Biometric

Authentication ensures only legitimate entities interact, while privacy safeguards sensitive data from misuse.

5. Rider location Updates with Lightweight protocols
   ↳ MQTT, COAP, gRPC
   since mobile n/w → unstable
   → bandwidth limited

. Food delivery optimization
   with IoT + ML
   ↳ nearest available rider
   → predicted preparation time.
   traffic ← GPS
   ↓
   Batch optimization (assigning multiple orders along the same route)
   Live tracking [websockets] ←

7. post-quantum-resilient IoT in healthcare
   hash-based firmware
   AES-256-GCM [bulk data]
   Terminate heavy crypto @ gateways
   ~~Update~~ 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