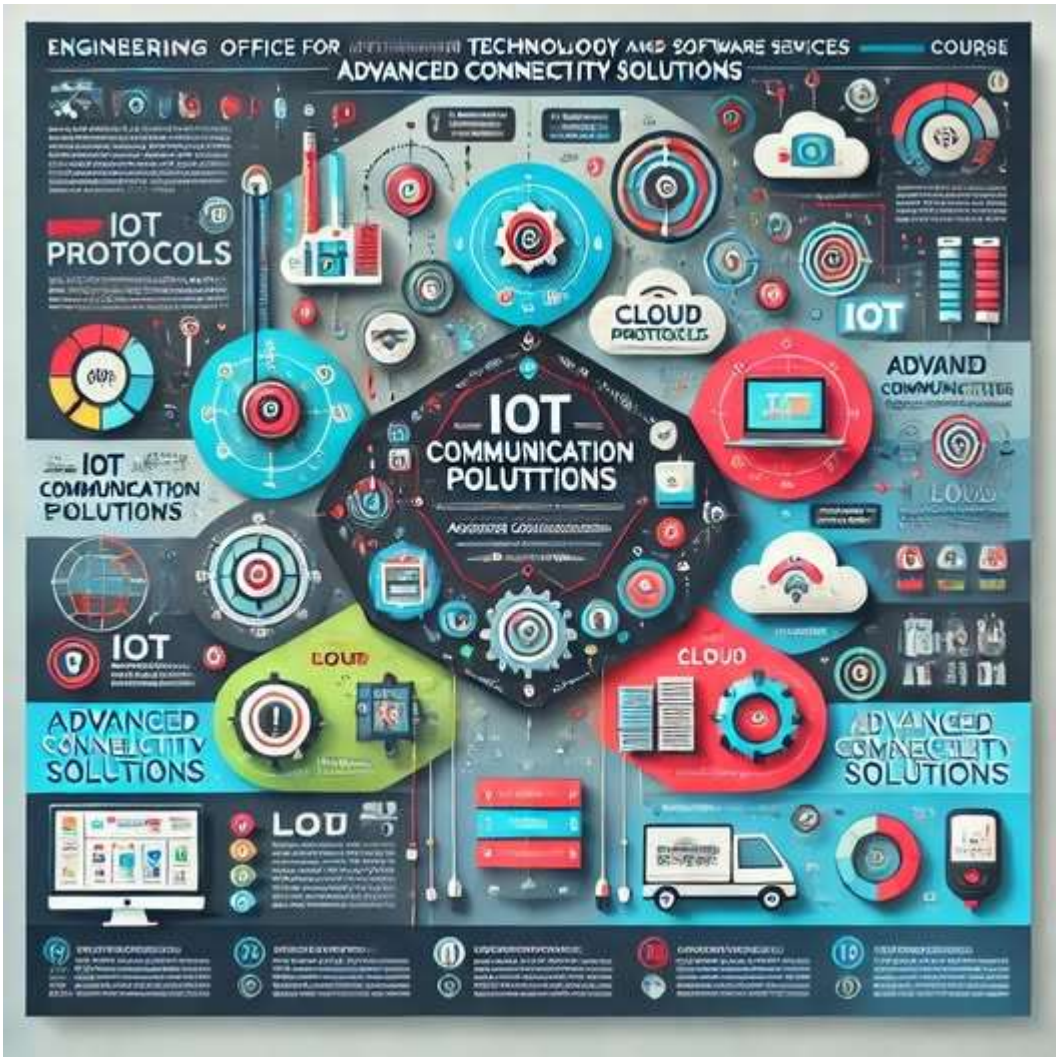
Course Title: IoT Communication Protocols: Advanced Connectivity Solutions



Course Code: 7009-EL

Main Branch: United building – E Shams –Front NBE , El Siouf _Alexandria
Tel: **01102060500-01144470856**

الفرع الرئيسي :عمارات المتحدة – عمارة عين شمس – امام البنك الاهلي – السيوف- الاسكندرية
تليفون: 01102060500 - 01144470856

E-mail. adelramadan@eotss-academy.com
info@eotss-academy.com

🧭 Introduction:

The Internet of Things (IoT) is transforming industries and daily life by enabling billions of devices to connect, interact, and exchange data. At the heart of this transformation are communication protocols that ensure reliable, secure, and efficient data transmission across diverse IoT environments.

📘 Description:

This course dives deep into the essential communication protocols used in IoT ecosystems, including **MQTT**, **CoAP**, and **HTTP**. It explores how these protocols facilitate interoperability, scalability, and security for a variety of IoT applications. Through hands-on labs and real-world case studies, participants will gain practical experience in building secure, cloud-connected IoT systems.

🎯 Objectives:

- Understand the architecture and importance of IoT communication protocols.
- Compare major IoT protocols and select the best fit for specific applications.
- Learn security considerations and implementation strategies.
- Explore integration with cloud platforms and remote management systems.

🧭 Module 1: Introduction to IoT and Communication Protocols

- 🌐 What is IoT? Applications and Real-World Impact
- 🧠 Key Components of IoT Systems (sensors, actuators, connectivity, cloud)
- 🔗 Role of Communication Protocols in IoT
- 📡 Overview of Protocol Categories (Application Layer, Transport Layer, etc.)

🧩 Module 2: Core IoT Communication Protocols

🔹 MQTT (Message Queuing Telemetry Transport)

- Architecture: Broker, Publisher, Subscriber
- Topics and QoS (Quality of Service) Levels
- Use cases in constrained environments
- Lab: Building a basic MQTT client with Mosquitto Broker

🔹 CoAP (Constrained Application Protocol)

- RESTful design and UDP transport
- Resource discovery and CoAP messaging models
- CoAP vs. HTTP vs. MQTT
- Lab: Simulating CoAP using Python and test servers

🔹 HTTP/HTTPS in IoT

- When and where HTTP is still relevant
- Limitations in resource-constrained devices
- Integration with web and REST APIs
- Lab: Sending sensor data via HTTP POST to a RESTful server

🔒 Module 3: Security and Privacy in IoT Protocols

- Common IoT vulnerabilities (man-in-the-middle, spoofing, DoS)
- 🔐 Encryption (TLS/SSL, DTLS) and secure transport
- Authentication and identity management in IoT

- Lab: Securing MQTT with TLS and Username/Password

☁️ Module 4: Cloud Integration and Device Management

- Overview of cloud platforms (AWS IoT Core, Azure IoT Hub, Google Cloud IoT)
- IoT Gateways and Edge Computing Basics
- Protocol bridges (e.g., MQTT to HTTPS)
- Remote device monitoring and firmware updates (OTA)
- Lab: Integrating IoT device with AWS IoT Core using MQTT

💉 Module 5: Practical Applications and Real-world Projects

- Smart Home Example: Sensor data collection and cloud visualization
- Industrial Monitoring: Real-time fault detection using MQTT
- Lab: Building a mini IoT system with Raspberry Pi/ESP32 and MQTT
- Group Activity: Design, implement, and present a complete IoT system

---

🎯 Module 6: Challenges, Optimization, and Future Trends

- Handling unreliable networks and packet loss
- Data compression and protocol optimization
- Scalability and multi-device management
- Future protocol trends (LwM2M, 6LoWPAN, Thread, Matter)

✅ Final Project

- **Objective:** Build and present a secure, connected IoT solution
- Must include:
  - Device communication via MQTT or CoAP
  - Cloud dashboard integration
  - Basic authentication and secure data transfer
- Evaluation: Functionality, security, scalability, and clarity of design

What You Will Learn:

- Key IoT protocols: **MQTT**, **CoAP**, and **HTTP** – structure, strengths, and use cases
- Security fundamentals: encryption, authentication, and device identity
- Protocol stack layering and how devices interact over different networks
- Integrating IoT systems with cloud platforms for data analysis and control
- Developing end-to-end IoT systems using common connectivity frameworks

Target Audience:

- IoT and embedded systems developers
- Network and communication engineers
- Cybersecurity specialists interested in IoT
- Students and researchers in electronics, computer science, and IT
- Professionals aiming to build or manage IoT-based solutions

Materials Provided:

- Lecture slides and protocol documentation

- Hands-on lab instructions and code samples
- Cloud integration guidelines (AWS IoT, Azure IoT, etc.)
- Real-world case studies and project templates

Instruction Methods:

- Instructor-led theory sessions
- Hands-on lab work with IoT kits and virtual simulators
- Real-life project-based learning
- Group discussions, troubleshooting, and evaluations

Time Frame:

Total Duration: 40 hours

- 20 hours theoretical sessions
- 20 hours practical labs and project implementation

Course Format:

- Available in on-site or online formats
- English instruction
- Includes quizzes, lab assessments, and a final project

Learning Outcomes:

By the end of the course, participants will:

✓ Understand the strengths and limitations of key IoT communication protocols

- ✓ Be capable of securing IoT systems through proper encryption and identity handling
- ✓ Integrate IoT devices with cloud services for remote control and data management
- ✓ Design and build reliable, scalable, and secure IoT networks from scratch
- ✓ Be prepared to apply these skills in industrial, home automation, or research-based IoT projects