# INSTITUTE OF AERONAUTICAL ENGINEERING
## (Autonomous)
### Dundigal - 500 043, Hyderabad, Telangana

## COURSE CONTENT

### IOT ARCHITECTURES AND APPLICATIONS

**I Semester: ES**

| Course Code | Category | Hours / Week | | | Credits | Maximum Marks | | |
|---|---|---|---|---|---|---|---|---|
| | | L | T | P | C | CIA | SEE | Total |
| **BESE33** | **Elective** | 3 | - | - | 3 | 40 | 60 | 100 |
| **Contact Classes: 45** | **Tutorial Classes: Nil** | **Practical Classes: Nil** | | | **Total Classes: 45** | | | |
| **Prerequisite: Digital Electronics & Logic Design.** | | | | | | | | |

### I.COURSE OVERVIEW:

The course **"IoT Architectures and Applications"** introduces students to the Internet of Things (IoT) ecosystem, covering its architecture, communication protocols, practical constraints, and applications across multiple domains. Students will gain hands-on experience with IoT devices, understand cloud integration, and explore the design, deployment, and security aspects of IoT systems. The course also emphasizes real-world case studies such as smart cities, smart healthcare, and precision agriculture, preparing students to develop and secure IoT solutions in industry and research environments.

### II. COURSES OBJECTIVES:
**The students will try to learn**
  I.   The architectural overview of IoT and its enabling technologies.
 II.   The real-world design constraints and challenges in IoT systems.
III.   Select and implement suitable communication and messaging protocols for IoT applications.
 IV.   IoT applications across diverse domains and understand their impact.

### III.   COURSE OUTCOMES:
**At the end of the course students should be able to:**

CO1     Understand the architectural components, physical and logical design, and enabling technologies of IoT.

CO2     Enumerate and address the real-world design constraints, including connectivity, data representation, and visualization.

CO3     Select and implement appropriate IoT communication and messaging protocols (e.g., MQTT, CoAP, BLE, Wi-Fi).

CO4     Explore and evaluate IoT applications in domains such as smart cities, healthcare, transportation, and agriculture.

CO5     Analyze and implement security requirements and safeguards in IoT architectures and applications. CO6 Identify  Enumerate the need and the challenges in Real World Design Constraints.

### IV. COURSE CONTENT:

**MODULE - I:  IoT (9)**
Definition and Technologies that led to evolution of IOT, Characteristics of IoT, Physical Design of IoT, Logical Design of IoT, IoT Enabling Technologies, IoT Levels & Deployment. M2M and IoT Technology Fundamentals-Devices and gateways, Introduction to

cloud IOT platforms like MS Azure, AWS IOT, Google Cloud IOT, Thingworx, Business processes in IoT.

### MODULE –II: IOT REFERENCE ARCHITECTURE (9)
Introduction, Functional View, Information View, Deployment and Operational View, Other Relevant architectural views. IoT edge system architecture. Real-World Design Constraints: Technical Design constraints, Connectivity constraints, Data representation and visualization, Big Data Management.

### MODULE –III: IOT COMMUNICATIONS (9)
Data link and physical layer Protocols: PHY/MAC Layer (IEEE 802.11, IEEE 802.15), Bluetooth Low Energy, Thread, introduction to Wi-SUN. Network Layer Protocols: IPv6, 6LoWPAN; Transport layer protocols: TCP, UDP;
Messaging protocols: Quality of services in MQTT, standards and security in MQTT, CoAP, AMQP.

### MODULE –IV: CASE STUDIES (9)
Smart Cities, Smart Homes, Smart Transportation, Smart Healthcare, Precision Agriculture, Connected Vehicles. IOT in Indian Scenario: i) IOT and Aadhaar ii) IOT for health services. iii) IOT for financial inclusion. iv) IOT for rural empowerment v) India Urban Data Exchange (IUDX). Industry 4.0: Industrial Internet of Things (IIoT), Reference Architecture, Characteristics of Industry 4.0.

### MODULE –V: SECURING THE INTERNET OF THINGS (9)
Security Requirements in IoT Architecture - Security in Enabling Technologies, Security Concerns in IoT Applications. Security Architecture in the Internet of Things - Security Requirements in IoT, Insufficient Authentication/Authorization, Insecure Access Control, Threats to Access Control, Privacy, and Availability, Attacks Specific to IoT. Security and Vulnerabilities – Secrecy & Secret Key Capacity, Authentication/Authorization for Smart Devices, Transport Encryption, Secure Cloud/Web Interface, Secure Software/Firmware, Physical Layer Security.

### V. TEXT BOOKS:
1. Pethuru Raj and Anupama C. Raman, ―The Internet of Things: Enabling Technologies, Platforms, and
   Use Cases", 1st Edition, 2017, CRC Press.
2. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton, Jerome Henny "IoT Fundamentals: Networking technologies Protocols, and Use Cases for the internet of things", June, 2017, Cisco press.

### VI. REFERENCE BOOKS:
1. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton, Jerome Henny "IoT Fundamentals: Networking technologies Protocols, and Use Cases for the internet of things", June, 2017, Cisco press.
2. Practical Internet of Things Security (Kindle Edition) by Brian Russell, Drew Van Duren, Packt Publishing, 2016
3. Jan Holler, VlasiosTsiatsis, Catherine Mulligan, Stefan Avesand, Stamatis Karnouskos, David Boyle, ―From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence‖, 1st Edition, 2014, Academic Press.

### VII. MATERIALS ONLINE
1. Course template
2. Tutorial question bank
3. Assignments
4. Model question paper - I
5. Model question paper - II
6. Lecture notes
7. Power point presentations
8. Early Lecture Readiness Videos