Course Code	Type	Subject	L	T	P	Credits	TCA	TMS	TES	PCA	PES	Pre-requisites
		Internet of Things	3	1	0	4	25	25	50	0	0	C

COURSE OUTCOMES

1. To understand the concepts of IoT and related protocol.
2. To learn to develop the sensor networks for collecting the data.
3. To create IoT solutions using sensors, actuators, and Devices.
4. To understand the upcoming advancement in the domain of IoT.
5. To deploy an IoT solution for the nearby society for improving their experiences.

COURSE CONTENT

UNIT-I

Internet of Things, Sensors, sensor classes, types of sensors, Actuator, Actuation, types of actuators, IoT Networking, IoT component, Functional components of IoT, IoT dependencies, IoT service-oriented architecture, IoT categories, IoT gateways, IoT and associated technologies, technical derivation from regular web.

UNIT-II

IoT protocols, MQTT, SMQTT, CoAP, XMPP, IEEE802.15.4, AMQP, 6LoWPAN, Zigbee, 3GPP, NB-IoT, Wireless HART, RFID, ISA100, Z-Wave. LoRAWAN and Reference model, Integration of devices using LoRAWAN, Security in LoRAWAN

UNIT-III

Machine to Machine communication, Architecture, and components for M2M, Standardization Effort for M2M. Interoperability in IoT, IoT Architecture for Interoperability, Open Industry Standards, SDN Origins and Evolution, Centralized and Distributed Control and Data Planes, API in SDN, Control mechanism, Switch Deployment, Controller configuration software, SDN for WSNs, Software-Defined WSN Prototype, Performance Analysis of Software Defined Networks. WSNs, Cluster formation of sensors in WSNs, Routing algorithms in WSNs, UAV Network, 5G based communication among IoT devices.

UNIT-IV

Sensor cloud, Architecture, Service life cycle model, Layered structure, Management issues in Sensor-Cloud, Smart Grid, Distribution Intelligence in Smart Grid, Smart Grid communication and security, Web server for IoT, Cloud for IoT, RESTful web API, Body Area Sensor Network, Invasive and non-invasive sensors, Communication Architecture, Energy Efficient Routing Protocols, Security Threads.
IoT Case study: Healthcare, Different sensors used in healthcare domain, Establishment of connection to get the data, Uploading of data from different sensors over cloud.
Fog and Edge Computing Completing the Cloud, Advantages of FEC: SCALE, How FEC Achieves, These Advantages: SCANC, Hierarchy of Fog and Edge, Computing, Addressing the Challenges in Federating Edge Resources.

UNIV-V

IoT Security Challenges- Hardware Security Risks, Hardcoded/Default, Resource Constrained Computations, Devices Physical Security, Software Security Risks.
IoT Security Requirements, Data Confidentiality, Data Encryption, Data, Authentication, Secured Access Control, IoT Vulnerabilities, Secret key, Authentication/Authorization for Smart Devices,

Constrained System Resources, Device Heterogeneity, Fixed Firmware IoT, Attacks: Side-channel Attacks, Reconnaissance, Spoofing, Sniffing, Neighbour Discovery Rogue Devices, Man-in-Middle,
Building a machine learning based IoT application, provisioning machine learning to interact with sensors and actuators, Configuring ML device, Amazon Alexa.
Blockchain in IoT: System architecture, System Interface, System Interaction, Policy definition, Performance evaluation metrics

REFERENCES AND TEXTBOOKS:

1. Jan Holler, Vlasios Tsiatsis, 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, Academic Press, 2014.
2. Vijay Madisetti and Arshdeep Bahga, "Internet of Things (A Hands-onApproach)", 1st Edition, VPT, 2014
3. Francis daCosta, "Rethinking the Internet of Things: A Scalable Approach to Connecting Everything", 1st Edition, Apress Publications, 2013
4. Cuno Pfister, Getting Started with the Internet of Things, O"Reilly Media, 2011, ISBN: 978-1-4493- 9357-1