Course Code	Course Title	L	T	P	C
1156EC424	IoTSECURITY	0	0	0	2

a) Course Category

Independent Learning Course – Massive Open Online Course

b) Preamble

This course gives an overview of IoT system in security aspects.The course mainly focusses on current security risks IoT domain faces and countermeasure available for the known issues

c) Prerequisite

Nil

d) Related Courses

Internet of Things, IOT Wireless & cloud Emerging Technologies

e) Course Outcomes

On successful completion of this course the student will be able to

CO Nos.	Course Outcomes	Knowledge Level (Based on Revised Bloom's Taxonomy)
CO1	Understand IoT general models and security challenges.	K2
CO2	Recognize IoT security and vulnerability threats.	K1
CO3	Understand different IoT protocols and their security measures.	K2
CO4	Interpret how to secure an IoT environment	K2
CO5	Interpret differentIoT types of attacks.	K2

f) Course Content

UNIT I IOT-SECURITY OVERVIEW

IoTReference Model- Introduction -Functional View,**IoT Security Challenges**-Hardware Security Risks -Hardcoded/Default Passwords -Resource Constrained Computations -Legacy Assets Connections -Devices Physical Security, Software Security Risks -Software Vulnerabilities -Data Interception -Identification of Endpoints -Tamper Detection, **Lack of Industrial Standards**

UNIT II IOT- SECURITY &VULNERABILITY ISSUES

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

UNIT III SECURED PROTOCOLS FOR IOT

Infrastructure-IPv6 -LowPAN , **Identification**-Electronic Product Code -uCode, **Transport**-Bluetooth -**LPWAN**, **Data** -MQTT -CoAP, **Multi-layer Frameworks**-Alljoyn,-IoTivity

UNIT IV SECURING INTERNET OF THINGS ENVIRONMENT

IoT Hardware -Test Device Range-Latency and Capacity -Manufacturability Test -Secure from Physical Attacks, **IoT Software -**Trusted IoT Application Platforms, -Secure Firmware Updating -Network Enforced Policy -Secure AnalyticsVisibility and Control

UNIT V IOT ATTCAKS -CASE STUDY

MIRAI Botnet Attack -Iran's Nuclear FacilityStuxnet Attack -TeslaCryptojacking Attack -The TRENDnet Webcam Attack -The Jeep SUV Attack -The Owlet Wi-Fi Baby Heart Monitor Vulnerabilities -St. Jude_Hackable Cardiac Devices

g) Learning Resources

Online Resources

1. https://www.postscapes.com/internet-of-things-protocols/
2. https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot/index.html
3. https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html
4. https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/