

Branch Name:	CYBER SECURITY
Program Code:	ET207
Course Title:	IOT security and Forensics
Course Code:	2ET2070104T
Pre-requisite Course:	Introduction to IoT, Architecture, Characteristics, IoT protocols, Security requirements in IoT, IoT vulnerabilities and attacks, Threat modelling, Authentication, Authorization and access control in IoT systems.

Course Objectives: After successful completion of the course, student will be able to

1. To impart the knowledge architecture reference layer Security issues and challenges of Internet of Things technology.
2. To provide knowledge about Enables students to get acquainted with practical IoT based smart application development interfaced with other required disciplines such as hardware
3. Provides an in-depth study of the rapidly changing and fascinating field of digital forensics.
4. Combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)								Total (Marks)
					Theory (Marks)				Practical (Marks)				
	L	T	P	Total	SEE		CCA		SEE		CCA		
					Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.	
3	3	-	-	3	24	60	16	40	-	-	-	-	100

Course Contents:

Unit No	Topics	Total Hours	Weight age (%)
1	Review of computer communication concepts (OSI layers, components, packet communication, Networks, TCP-IP, subnetting, IPV4 addressing and challenges), IPV6 addressing. IoT architecture reference layer	08	20
2	IoT protocols-Link layer protocols, Network layer protocols IPV4, IPV6, 6LoWPAN, Transport layer protocols, Infrastructure-IPv6 -LowPAN, Identification-Electronic Product Code -uCode, Transport-Bluetooth - LPWAN, Data -MQTT – CoAP. Need for encryption, standard encryption protocol, light weight cryptography, Quadruple Trust Model for IoT-A – Threat Analysis and model for IoT-A, Cloud security	14	30
3	Introduction to Digital Forensics, branches of digital forensics, digital evidence, Types of Evidence, Chain of custody, types of Cyber Crime, types of cyber criminals, crime scene management, evidence collection techniques - Switched Off System, Live System, Live response and triage-based acquisition techniques, order of volatility	10	20
4	Analysis of evidence, concept of imaging and cloning, file formats of forensic images, concept of write blocker, Hardware and Software Write blocker, Hash Function, fuzzy hash and hash collision, data recovery, tools for image creation and analysis. MFT analysis, recycle bin forensics, i30 analysis, other NTFS artifacts - data, UsnJrnl, amcache, shimcache, shellbags, lnk files, jump lists, USB, and Bring Your Own Device (BYOD) Forensic Examinations, Incident response procedure, browser forensics, printer artifacts, yellow dot concept in printer forensics.	14	30

Text Books:

1. Digital Forensics: The Fascinating World of Digital Evidences, Neelakshi Jain, D.R Kalbande, Wiley Books G.B. Thomas and R.L. Finney, Calculus and Analytic geometry, 9th Edition, Pearson, Reprint, 2002
2. Digital Forensics and Incident Response: A practical guide to deploying digital forensic techniques in response to cyber security incidents : Gerard Jhansen, Packt Publishers

Reference Books:

1. Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence by William Oettinger , Pckt Publishers
2. John Sammons, the Basics of Digital Forensics, Elsevier, 2014.
3. John Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications, 2015.
4. Bayuk, J. (2010). Cyber Forensics: Understanding information security investigations. Springer Science & Business Media.

List of Open-Source Software/learning website:

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.iotforall.com/5-worst-iot-hacking-vulnerabilities>

Course Learning Outcomes (CLO):

Course Outcomes	Description	Bloom's Taxonomy Level
COL1	Explain the concepts computer communication concepts and IoT architecture reference layer	Understanding (2) Applying (3)
COL2	Find appropriate security/privacy and Build Trustable cloud based IoT systems	Applying (3)
COL3	Knowledge on digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation	Applying (3)
COL4	Knowledge on E-evidence collection and preservation, digital forensics Analyze the various mechanism of computer forensics.	Applying (3)

Mapping of CLO with PO and PSO

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes(PSOs)			
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CLO1	H	M	M		M											
CLO2	H	M			M							L				
CLO3	H	M	M		M											
CLO4	M	M	M		M							L				
CLO5	M	M										L				

H: High, M: Medium, L: Low