21IOT07	PRIVACY AND SECURITY IN IOT	L	T	P	C
		3	0	0	3

Course Objectives

- To know the state-of-the-art methodologies in Cyber Physical system.
- To impart knowledge on Model threats and countermeasures.
- To explore the Privacy Preservation and Trust Models in Internet of Things (IoT)
- To apply the concept of Internet of Things Security in the real-world scenarios

UNIT I	CYBER PHYSICAL SYSTEMS AND INTERCONNECTION OF THREATS	9 Hours

IoT and cyber-physical systems, IoT security (vulnerabilities, attacks, and countermeasures), security engineering for IoT development, IoT security lifecycle. Network Robustness of Internet of Things- Sybil Attack Detection in Vehicular Networks- Malware Propagation and Control in Internet of Things- Solution-Based Analysis of Attack Vectors on Smart HomeSystems.

UNIT II	CRYPTO FOUNDATIONS	9 Hours

Block ciphers, message integrity, authenticated encryption, hash functions, Merkle trees, elliptic curves, public-key crypto (PKI), signature algorithms

UNIT III	PRIVACY PRESERVATION FOR IOT	9 Hours

Privacy Preservation Data Dissemination- Privacy Preservation Data Dissemination- Social Features forLocation Privacy Enhancement in Internet of Vehicles- Lightweight and Robust Schemes for Privacy Protection in Key Personal IoT Applications: Mobile WBSN and Participatory Sensing

UNIT IV	TRUST MODELS FOR IOT	9 Hours

Authentication in IoT- Computational Security for the IoT- Privacy-Preserving Time Series Data Aggregation- Secure Path Generation Scheme for Real-Time Green Internet of Things- Security Protocols for IoT Access Networks- Framework for Privacy and Trust in IoT- Policy-Based Approach for InformedConsent in Internet of Things.

UNIT V	INTERNET OF THINGS SECURITY	9 Hours

Security and Impact of the Internet of Things (IoT) on Mobile Networks- Networking Function Security-IoT Networking Protocols, Secure IoT Lower Layers, Secure IoT Higher Layers, Secure Communication Links inIoTs, Back-end Security -Secure Resource Management, Secure IoT Databases, Security Products-Existing Test bed on Security and Privacy of IoTs, Commercialized Products.

Course Outcome:

1. 1Identify the areas of cyber security for the Internet of Things.
2. Assess different Internet of Things technologies and their applications.
3. Model IoT to business
4. Customize real time data for IoT applications.
5. Solve IoT security problems using light weight cryptography
6. Build security systems using elementary blocks

Text Books:

- Hu, Fei. Security and privacy in Internet of things (IoTs): Models, Algorithms, and Implementations, 1st edition,CRC Press, 2016.
- Russell, Brian, and Drew Van Duren. Practical Internet of Things Security, 1st edition, Packt PublishingLtd, 2016.

Reference Books:

- Whitehouse O. Security of things: An implementers' guide to cyber-security for internet of thingsdevices and beyond, 1st edition, NCC Group, 2014
- DaCosta, Francis, and Byron Henderson. Rethinking the Internet of Things: a scalable approach toconnecting everything, 1st edition, Springer Nature, 2013.