Honours Course   BE Sem-VII   Subject: **410401: Internet of Things and Embedded Security**

Following are Internet of Things and Embedded Security NPTEL Courses available on NPTEL Repository
●

Online Book:
●

Unit I Introduction: Securing the Internet of Things, Vulnerabilities, attacks and countermeasures Defining the IoT, IoT uses today, The IoT in the enterprise, The IoT of the future and the need to secure, Primer on threats - The classic pillars of information assurance, Threats, Vulnerability, Risks, vulnerability, and risks; Primer on attacks and countermeasures- Common IoT attack types, Attack trees, Fault (failure) trees and CPS; Today's IoT attacks – attacks; Threat modeling an IoT system	
Unit II Security Engineering for IoT Development Building security in to design and development, Secure design - Security in agile developments, Focusing on the IoT device in operation, Safety and security design - Threat modeling, Privacy impact assessment, Safety impact assessment, Compliance, Security system integration, Processes and agreements, Technology selection – security products and services- IoT device hardware, Selecting an MCU, Selecting a real-time operating system (RTOS) , IoT relationship platforms, Cryptographic security APIs , Authentication/authorization	
Unit III The IoT Security Lifecycle The secure IoT system implementation lifecycle, Implementation and integration - IoT security CONOPS document, Network and security integration, System security verification and validation (V&V), Security training, Secure configurations, Operations and maintenance - Managing identities, roles, and attributes, Security monitoring, Penetration testing, Compliance monitoring, Asset and configuration management, Incident management, Forensics, Dispose - Secure device disposal and	

zeroization, Data purging, Inventory control, Data archiving and records management	
Unit IV Cryptographic Fundamentals for IoT Security Engineering Cryptography and its role in securing the IoT, Types and uses of cryptographic primitives in the IoT, Encryption and decryption- Symmetric encryption , Asymmetric encryption, Hashes, Digital signatures- Symmetric (MACs), Random number generation, Ciphersuites, Cryptographic module principles, Cryptographic key management fundamentals - Key generation- Key establishment, Key derivation, Key storage, Key escrow, Key lifetime, Key zeroization, Accounting and management, Examining cryptographic controls for IoT protocols- Cryptographic controls built into IoT communication protocols(ZigBee, Bluetooth, Near field communication (NFC)), Cryptographic controls built into IoT messaging protocols – MQTT,CoAP,DDS, REST, Future directions of the IoT and cryptography	
Unit V Identity and Access Management Solutions for the IoT (08 Hours) An introduction to identity and access management for the IoT- The identity lifecycle, Establish naming conventions and uniqueness requirements, Secure bootstrap, Credential and attribute provisioning, Account monitoring and control, Account updates, Account suspension, Account/credential deactivation/deletion, Authentication credentials- Passwords, Symmetric keys, Certificates X.509, IEEE 1609.2, Biometrics, New work in authorization for the IoT, IoT IAM infrastructure - 802.1x, PKI for the IoT, Authorization and access control	
Unit VI Identity management models (08 Hours) Introduction – Identity management, identity Portrayal, Different Identity management models – local identity, network identity, federated identity, global web identity, Identity management in internet of things – user-centric identity management, hybrid identity management	●