CYBER SECURITY AND PRIVACY IN IOT

ASET, AUMP

Course Credits	03	**Total Hours**	30
Course Code	CSI501	**Programme**	BTech

Course Outcomes:

- Ability to Understand the security requirements in IOT
- Understanding the cryptographic fundamentals of IOT
- Ability to Understand the authentication credentials and access control
- Understand various types of trust models and cloud security

Syllabus

MI: Securing the Internet of Things	● Security requirements in IoT architecture ● Security in enabling technologies ● Cipher suites ● Security architecture in the Internet of Things ● Security requirements in IoT ○ Insufficient authentication/authorization ○ Insecure access control ○ Threats to access control, privacy, and availability ● Attacks specific to IoT ● Vulnerabilities ● Secrecy and secret-key capacity ● Authentication/authorization for smart devices ● Transport encryption ● Attack trees and fault trees
MII: Cryptographic Fundamentals for IoT	● Cryptographic primitives and their role in IoT ● Encryption and decryption ● Hashes ● Digital signatures ● Random number generation ● Cipher suites ● Key management fundamentals ● Cryptographic controls in IoT messaging and communication protocols ● IoT node authentication
MIII: Identity and Access Management for IoT	● Identity lifecycle ● Authentication credentials ● IoT IAM infrastructure

	• Authorization with publish/subscribe schemes • Access control
MIV: Privacy Preservation and Trust Models for IoT	• Concerns in data dissemination • Lightweight and robust privacy protection schemes • Trust and trust models for IoT • Self-organizing things • Preventing unauthorized access
MV: Cloud Security for IoT Cloud Services and IoT	• IoT offerings from cloud service providers • Cloud IoT security controls • Enterprise IoT cloud security architecture • New directions in cloud-enabled IoT computing