CSET555 - Cyber Security with Blockchain

Course Type - Specialization Elective L-T-P Format 2-0-2 Credits - 3

COURSE SUMMARY

The course explains the cyberthreat landscape and Security Challenges. The students will build Blockchain-based apps for authentication and for storing DNS entries and implement various decentralized applications using blockchain to provide various security services.

COURSE-SPECIFIC LEARNING OUTCOMES (CO)

CO1: To articulate the cyberthreat landscape and Security Challenges.

CO2: To build Blockchain-based apps for authentication and for storing DNS entries.

CO3: To implement various decentralized applications using blockchain to provide various security services.

Detailed Syllabus

Module 1 (Contact hours: 8)

Cyber Security, Internet Governance – Challenges, Constraints, Threats, Cyber Warfare, Cyber Crime, Terrorism, Espionage, Need for a Cyber Security Policy, Nodal Authority requirement, Requirement of an International Convention on Cyberspace, CIA model, Cyber Security vulnerabilities, Cyber Security attacks.

Module 2 (Contact hours: 8)

Security services, Blockchain on the CIA Security Triad, Authentication mechanisms, Two-Factor Authentication with Blockchain, PKI Infrastructure, Deploying PKI-Based Identity with Blockchain, IPNS, Blockchain-Based DNS Security Platform, Deploying Blockchain-Based DDoS Protection, EIP Block for DDoS attacks, Security related issues in smart contracts development, Smart contract testing.

Module 3 (Contact hours: 6)

Exception handling, debugging of applications, Formal verification, smart contracts security Oyente, why3 for smart contracts, Solgraph based formal verification, implications of blockchain technology for digital privacy, implication for Security, Membership and Access control in Fabric, authentication in fabric network.

Module 4 (Contact hours: 6)

Privacy in Fabric, Channel encryption, Blockchain Security (Fabric SideDB), Security of a ledger, anonymity, pseudonymity, blockchain Implementation Challenges, privacy law applicability, startups in blockchain based cyber security applications.

STUDIO WORK / LABORATORY EXPERIMENTS:

Cyber-Security with Blockchain is to make companies, products, systems, and services as resilient as possible to cyber-attacks, by looking at security from the outset and throughout their entire life cycle. This lab enables students to get practical knowledge on cryptographic primitives, design, and analysis of authentication protocols. Further, this lab mainly focusses on Transaction and communication security, preventing DDOS attacks, preventing data manipulation, and protection from compromised nodes.

TEXTBOOKS/LEARNING RESOURCES:

a) R. Gupta, Hands-on cybersecurity with blockchain (1st ed.), Packt Publishing, 2018. ISBN 978-788990189.

REFERENCE BOOKS/LEARNING RESOURCES:

a) Yassine Maleh, Mamoun Alazab, Mohammad Shojafar, Imed Romdhani, Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications (1st ed.), CRC Press, 2020. ISBN 9781000060164.