MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY, WB

Syllabus for B.Sc.in Cyber Security Programme

(Effective for Students Admitted in Academic Session 2019-2020)

Semester 6:

Artificial Intelligence In Cyber security & Industry use cases

Unit-1: Introduction: Looking at the Various Aspects of Cyber security, Social engineering and phishing, Introducing ransomware, Malware intrusion, Non-malware intrusion, Detect, Respond, and Mitigate, Responding to and Recovering from Cyber attacks and Security Events, Challenges of Cybersecurity –[6L]

Unit-2: Fathoming Artificial Intelligence: Teaching Machines to be Smarter, Learning Algorithms, Supervised learning, Unsupervised learning, Being Smarter, Interacting with Humans, Natural Language Processing –[5L]

Unit-3: Applying Machine Learning and Deep Learning to Cybersecurity: Deep Learning and Deeply Layered Neural Networks, Deep Blue plays chess, introducing cognitive computing, Structured and Unstructured Data, Predictive Analytics, Introducing cognitive computing, Investigate Security Incidents taking Intelligent Action, Understand, Reason, and Learn, Winning with Threat Intelligence—[10L]

Unit-4: Trends in Cybersecurity: Responding to Ransomware, Combining Application development and Cybersecurity, Using Deep Learning to Detect DGA-Generated Domains Detecting Non-Malware Threats. Adaptive Honeypots and Honeytokens, Gaining a Better Understanding of How Neural Networks Work, Employing, Capsule Networks, Deep Reinforcement Learning. Protecting the IoT, Predicting the Future—[12L]

Unit-5: Industry Use Cases: Cognitive security with Watson, Tenable's ICS security capabilities, Cybersecurity Solutions - Real-time Insights **—[7L]**

Books:

1. Leslie F. Sikos, "AI in Cybersecurity", Springer, 2018
2. Ted Coombs, "Artificial Intelligence & Cybersecurity", IBM Limited Edition
3. Alessandro Parisi, "Hands-On Artificial Intelligence for Cybersecurity"

Block Chain & Cryptocurrency: (Elective-3)

Unit 1: Introduction: Introduction: Overview of Block chain, Public Ledgers, Bitcoin, Smart Contracts, Block in a Block chain, Transactions, Distributed Consensus, Public vs Private Block chain, Understanding Cryptocurrency to Block chain, Permissioned Model of Block chain, Overview of Security aspects of Block chain Basic Crypto Primitives: Cryptographic Hash Function, Properties of a hash function, Hash pointer and Merkle tree, Digital Signature, Public Key Cryptography --12L

Unit 2: Understanding Block chain for Enterprises: Permissioned Block chain: Permissioned model and use cases, Design issues for Permissioned block chains, Execute contracts, State machine replication, Overview of Consensus models for permissioned block chain- Distributed consensus in closed environment, Paxos, RAFT Consensus, Byzantine general problem, Byzantine fault tolerant system, Lamport-Shostak-Pease BFT Algorithm, BFT over Asynchronous systems. Enterprise application of Block chain: Cross border payments, Know Your Customer (KYC), Food Security, Mortgage over Block chain, Block chain enabled Trade, We Trade – Trade Finance Network, Supply Chain Financing, Identity on Block chain—12L

Unit 3: Block chain application development: Hyperledger Fabric- Architecture, Identities and Policies, Membership and Access Control, Channels, Transaction Validation, Writing smart contract using Hyperledger Fabric, Writing smart contract using Ethereum, Overview of Ripple and Corda ---8L

Unit 4: Crypto currency: A basic cryptocurrency. Bitcoin and Block chain: Creation of coins, Payments and double spending, Bitcoin Scripts, Bitcoin P2P Network, Transaction in Bitcoin Network, Block Mining, Block propagation and block relay. Working with Consensus in Bitcoin**:** Distributed consensus in open environments, Consensus in a Bitcoin network, Proof of Work (PoW) – basic introduction, Hashcash PoW, Bitcoin PoW, Attacks on PoW and the monopoly problem, Proof of Stake, Proof of Burn and Proof of Elapsed Time, The life of a Bitcoin Miner, Mining Difficulty, Mining Pool. --- 8L

BOOKS:

1. Melanie Swan, "Block Chain: Blueprint for a New Economy", O'Reilly, 2015
2. Josh Thompsons, "Block Chain: The Block Chain for Beginners- Guide to Block chain Technology and Leveraging Block Chain Programming"
3. Daniel Drescher, "Block Chain Basics", Apress; 1stedition, 2017
4. Anshul Kaushik, "Block Chain and Crypto Currencies", Khanna Publishing House, Delhi.
5. Imran Bashir, "Mastering Block Chain: Distributed Ledger Technology, Decentralization and Smart Contracts Explained", Packt Publishing
6. Ritesh Modi, "Solidity Programming Essentials: A Beginner's Guide to Build Smart Contracts for Ethereum and Block Chain", Packt Publishing
7. Salman Baset, Luc Desrosiers, Nitin Gaur, Petr Novotny, Anthony O'Dowd, Venkatraman Ramakrishna, "Hands-On Block Chain with Hyperledger: Building Decentralized Applications with Hyperledger Fabric and Composer", Import, 2018

Artificial Intelligence in Cyber security & Industry use cases:

Module 1: OWL Ontologies in Cybersecurity: Modeling of Cyber-Knowledge. [2]

Module 2: Knowledge Representation of Network Semantics for Reasoning-Powered Cyber-Situational Awareness. [4]

Module 3: The Security of Machine Learning Systems, Threat Model, Data Poisoning, Attacks at Test Time. [4]

Module 4: Patch Before Exploited: Approach to Identify Targeted Software Vulnerabilities, Supervised Learning Approaches, and Challenges of Exploit Prediction, Exploit Prediction Model, and Vulnerability and Exploit Analysis, [6]

Module 5: Applying Artificial Intelligence Methods to Network Attack Detection, Binary Classifiers, Training the Binary Classifier for Detecting Network Attacks, Schemes for Combining the Binary Classifiers, [8]

Module 6: Application of AI in Cyber Security and Use cases: Detect email threats such as spamming and phishing using AI, Polymorphic malware samples, Overcome antivirus limits in threat detection, Predict network intrusions and detect anomalies with machine learning, Verify the strength of biometric authentication procedures with deep learning. [10]

Text Books:

1. Hands-On Artificial Intelligence for Cybersecurity, Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies by Alessandro Parisi.
2. AI in Cybersecurity by Leslie F. Sikos, Springer, Cham.

Extra 16 credit for online courses: Total 136 credit.
Distribution semester wise

Semester	Credit	Online courses
SEM-1		
SEM-2		
SEM-3	4	• Windows Server Management and Security - Coursera • Linux Server Management and Security - Coursera • Network Security & Database Vulnerabilities - Coursera • Exploiting and Securing Vulnerabilities in Java Applications - Coursera • Cybersecurity Roles, Processes & Operating System Security - Coursera
SEM-4	4	• Introduction to Cloud Computing - Coursera • Enterprise System Management and Security - Coursera • Basic Cryptography and Programming with Crypto API - Coursera • Hacking and Patching - Coursera • Introduction to Cybersecurity Tools & Cyber Attacks - Coursera
SEM-5	4	• Introduction to Cybersecurity Tools & Cyber Attacks—Coursera • Cybersecurity for Business—Coursera • Applied Cryptography—Coursera • Cybersecurity and Privacy in the IoT—edX • Building a Cybersecurity Toolkit—edX • :Privacy and Security in Online Social Networks--NPTEL
SEM-6	4	• IBM Cybersecurity Analyst-Coursera • Secure Coding Practices—Coursera • Cybersecurity Capstone---edX • Cybersecurity for Critical Urban Infrastructure—edX • Cybersecurity: The CISO's View—edX • FinTech Ethics and Risks---edX