CTMTAIDS SII P5 EL1: Blockchain Security and Investigation

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To understand concept of Blockchain.
2. To learn various use-cases of Blockchain.
3. To understand fundamental of Blockchain security.
4. To learn various Blockchain security techniques.

UNIT–I

Introduction, Cryptography, Hash Function, Hash Pointers and One-Way Functions, Digital Signatures – ECDSA, Memory Hard Algorithm, Zero Knowledge Proof, Distributed Database, Two General Problem, Byzantine General Problem and Fault Tolerance, Introduction to Quantum Computing and How it will break existing methods

UNIT-II

Introduction, Advantages over Conventional distributed database, Blockchain Network, Mining Mechanism, Distributed Consensus, Merkle Patricia Tree, Transactions and Fee, Anonymity, Reward, Chain Policy, Life of Blockchain Application, Soft and Hard Fork, Private and Public Blockchain

UNIT–III

Nakamoto Consensus, Proof of Work, Proof of Stake, Proof of Burn, Difficulty Level, Sybil Attack, Energy Utilization, Alternate Smart Contract Construction

UNIT–IV

History, Distributed Ledger, Bitcoin Protocols – Mining Strategy and Rewards, Ethereum Construction, Gas Limit, DAO, Smart Contract, GHOST,

Vulnerabilities, Attacks, Sidechain, Name coin, Case Study related to – Naïve Blockchain Construction, Play with Go-Ethereum, Application using Blockchain

UNIT-V

Stakeholders, Roots of Bitcoin, Legal Aspects-Cryptocurrency Exchange, Black Market and Global Economy, Applications: Internet of Things, Medical Record Management System, Domain Name Service and Future of Blockchain, Case study related to Mining Puzzles

Reference Books: -

1. Bitcoin and Cryptocurrency Technologies: A comprehensive Introduction, Princeton University Press, 2016 by Arvind Marayan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder.
2. Bitcoin and Blockchain Security by Elli Androulaki and Ghassan Karame
3. Blockchain Cybersecurity, Trust and Privacy by Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo
4. Blockchain for Cyber Security and Privacy: Architectures, Challenges and Applications by Mamoun Alazab, Yassine Maleh, Mohammad Shojafar, Imed Romdhani
5. The Truth Machine: The Blockchain and the Future of Everything by Michael Casey and Paul Vigna
6. Blockchain for Distributed Systems Security by Laurent L. Njilla, Charles Kamhoua and Sachin Shetty
7. Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto
8. The Age of Cryptocurrency by Paul Vigna and Michael Casey
9. The Basics of Bitcoins and Blockchains by Antony Lewis
10. Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher