Shri Vile Parle Kelavani Mandal's
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING
(Autonomous College Affiliated to the University of Mumbai)
NAAC Accredited with "A" Grade (CGPA : 3.18)

Shri Vile Parle Kelavani Mandal’s

Dwarkadas J. Sanghvi College of Engineering

(Autonomous College Affiliated to the University of Mumbai)

Scheme and detailed syllabus

Third Year B.Tech

in

Computer Science and Engineering (IoT and Cyber Security with Blockchain Technology)

(Semester V)

Prepared by:- Board of Studies in Computer Science & Engineering (IoT and Cyber Security with Blockchain Technology)

With effect from the Academic Year: 2023-2024

Proposed Teaching Scheme for

Third Year B. Tech. in IoT and Cyber Security with Blockchain Technology Semester V (Autonomous) (Academic Year 2023-2024)

Sr No	Course Code	Course	Theory (hrs.)	Practical (hrs.)	Tutorial (hrs.)	Credits	Credits earned
1	DJ19ICC501	Microcontroller and Embedded Systems	**3**	**--**	**--**	**3**	**4**
	DJ19ICL501	Microcontroller and Embedded Systems Laboratory	**--**	**2**	**--**	**1**	
2	DJ19ICC502	Applied Cryptography	**3**	**--**	**--**	**3**	**4**
	DJ19ICL502	Applied Cryptography Laboratory	**--**	**2**	**--**	**1**	
3	DJ19ICC503	Introduction to Blockchain Technology	**3**	**--**	**--**	**3**	**4**
	DJ19ICL503	Introduction to Blockchain Technology Laboratory	**--**	**2**	**--**	**1**	
4	DJ19ICC504	Artificial Intelligence	**3**	**--**	**--**	**3**	**4**
	DJ19ICL504	Artificial Intelligence Laboratory	**--**	**2**	**--**	**1**	
5 @ Any 1 Core Elective	DJ19ICEC5011	Digital forensics	**3**	**--**	**--**	**3**	**4**
	DJ19ICEL5011	Digital forensics Laboratory	**--**	**2**	**--**	**1**	
	DJ19ICEC5012	Network Security	**3**	**--**	**--**	**3**	
	DJ19ICEL5012	Network Security Laboratory	**--**	**2**	**--**	**1**	
	DJ19ICEC5013	Vulnerability Assessment & Penetration Testing	**3**	**--**	**--**	**3**	
	DJ19ICEL5013	Vulnerability Assessment & Penetration Testing Laboratory	**--**	**2**	**--**	**1**	
6	DJ19ICL506	Web Application Development	**--**	**4**	**--**	**2**	**2**
7	DJ19ILL1	Innovative Product Development III	**--**	**2**	**--**	**1**	**1**
		Total	**15**	**16**	**--**	**23**	**23**

Proposed Scheme for
Third Year B. Tech. in IoT and Cyber Security with Blockchain Technology Semester V
(Autonomous) (Academic Year 2023-2024)

Sr No	Course Code	Course	Teaching Scheme(hr)			Continuous Assessment (A)			Semester End Assessment (B)					Aggregate (A+B)
			Theory	Practical	Credits	Th.	T/W	Total CA (A)	Theory	Oral	Pract	Oral & Pract	Total SEA(B)	
1	DJ19ICC501	Microcontroller and Embedded Systems	3	--	3	25	--	25	75	--	--	--	75	100
	DJ19ICL501	Microcontroller and Embedded Systems Laboratory	--	2	1	--	25	25	--	25	--	--	25	50
2	DJ19ICC502	Applied Cryptography	3	--	3	25	--	25	75	--	--	--	75	100
	DJ19ICL502	Applied Cryptography Laboratory	--	2	1	--	25	25	--	--	--	25	25	50
3	DJ19ICC503	Introduction to Block chain Technology	3	--	3	25	--	25	75	--	--	--	75	100
	DJ19ICL503	Introduction to Block chain Technology Laboratory	--	2	1	--	25	25	--	25	--	--	25	50
4	DJ19ICC504	Artificial Intelligence	3	--	3	25	--	25	75	--	--	--	75	100
	DJ19ICL504	Artificial Intelligence Laboratory	--	2	1	--	25	25	--	--	--	25	25	50
5 @ Any 1 Core Elective	DJ19ICEC5011	Digital forensics	3	--	3	25	--	25	75	--	--	--	75	100
	DJ19ICEL5011	Digital forensics Laboratory	--	2	1	--	25	25	--	25	--	--	25	50
	DJ19ICEC5012	Network Security	3	--	3	25	--	25	75	--	--	--	75	100
	DJ19ICEL5012	Network Security Laboratory	--	2	1	--	25	25	--	25	--	--	25	50
	DJ19ICEC5013	Vulnerability Assessment & Penetration Testing	3	--	3	25	--	25	75	--	--	--	75	100
	DJ19ICEL5013	Vulnerability Assessment & Penetration Testing Laboratory	--	2	1	--	25	25	--	25	--	--	25	50
6	DJ19ICL506	Web Application Development	--	4	2	--	25	25	--	--	--	25	25	50
7	DJ19ILL1	Innovative Product Development III (A)	--	2	1	--	25	25	--	25	--	--	25	50
		Total	**15**	**16**	**23**	**125**	**175**	**300**	**375**	**100**	**0**	**75**	**550**	**850**

Program: B.Tech. CSE in IoT and Cyber Security with Blockchain Technology

T.Y. B.Tech.

Semester: V

Course: Microcontroller and Embedded Systems (DJ19ICC501)

Course: Microcontroller and Embedded Systems Laboratory (DJ19ICL501)

Prerequisite:

1. Digital Logic Design and Applications
2. Introduction to Internet of Things.

Objectives:

1. To study concepts involved in embedded hardware and software for system realization.
2. To familiarize with the architecture and functionalities of microcontrollers.
3. To create an efficient code for embedded systems using programming languages.
4. To understand the concepts of real-time systems.

Outcomes: On completion of the course, learner will be able to:

1. Identify and describe various characteristic features and applications of embedded systems.
2. Understand AVR microcontroller architecture.
3. Compose AVR microcontroller assembly language Programming and understand its Interface.
4. Analyze and explain the design of Real Time Operating System (RTOS).

Detailed Syllabus: (unit wise)		
Unit	Description	Duration
1	**Introduction to Embedded systems** Characteristics and Design metrics of Embedded system, Challenges in Embedded system Design: Power, Speed and Code density, Power supply considerations in Embedded systems: Low power features-Idle & Power down mode, Sleep mode, and Brown-out detection, Applications of embedded system.	5
2	**AVR Microcontroller Architecture:** Introduction to microcontroller, Overview of AVR family, AVR architectural features and Memory organization.	7
3	**AVR Microcontroller assembly language programming:**	5

	Addressing modes of AVR microcontroller. Instruction Set: Data transfer, Arithmetic, Logical, Branching. Assembly Language Programming.	
4	**AVR Microcontroller Internal Hardware & Programming:** I/O port structure and programming, Interrupts and programming, Timer/ Counter and programming, Serial port and programming.	6
5	**AVR Microcontroller Interfacing & Applications:** Display interfacing: 7-segment LED display, 16x2 generic alphanumeric LCD display. Keyboard interfacing: 4x4 matrix keyboard. Analog devices interfacing: 8-bit ADC/DAC, temperature sensor (LM35). Motor interfacing: Relay, dc motor, stepper motor and servo motor	5
6	**Real Time Operating System:** Basics of RTOS, Real-time concepts, Hard Real Time System, Soft Real Time System, Firm Real Time System, Differences between general purpose OS & RTOS, Basic Architecture of RTOS, Features of RTOS, Scheduling algorithms in RTOS, Priority Inversion Problem, Solutions to Priority Inversion – Non-Blocking Critical Section, Priority Ceiling, Priority Inheritance, Interrupt management and Memory Management in RTOS environment.	11
	Total	39

List of Laboratory Experiments:

Sr. No	**Experiment**
1	Study of ATmega32 and AVR studio in detail
2	To add, subtract two hexadecimal numbers and show the result
3	To multiply two hexadecimal numbers using MUL and without MUL instruction.
4	To find the sum of first 10 integers.
5	To make an LED blinking, change brightness and ON/OFF.
6	To make LED ON/OFF by considering switch as input.
7	To interface analog input device considering potentiometer as input device.
8	To perform decade counter from 0 to 9 using one seven segment display.
9	To display the following waveforms with ATmega32:

	a) Square wave of frequency 3 kHz and 50% duty cycle b) Step wave of frequency 3 kHz (3 steps) c) Sawtooth wave d) Triangular wave
10	Introduction to FreeRTOS and FreeRTOS Task Creation – Understanding the System Core Clock
11	FreeRTOS Hello World App, Semi hosting & UART Setup

Books Recommended:

Text books:

1. M. A. Mazidi, Sarmad Naimi and Sepehr Naimi, "The AVR Microcontroller and Embedded Systems” Pearson Education, 2017.

2. Dr. K. V. K. K. Prasad, “Embedded Real Time System: Concepts, Design and Programming”, Dreamtech, New Delhi, New edition,2003

3. Sriram Iyer, Pankaj Gupta, “Embedded Real Time Systems Programming”, Tata McGraw Hill Publishing Company ltd.,2017.

Reference Books:

1. David Simon, “An Embedded Software Primer”, Pearson, first edition, 2002.

2. Jonathan W. Valvano, “Embedded Microcomputer Systems–Real Time Interfacing”, PublisherCengage Learning, 3rd Edition, 2012.

3. Frank Vahid, Tony Givargis, “Embedded System Design–A Unified Hardware/Software Introduction”, John Wiley & Sons Inc., 3rd edition, 2009.

4. Shibu K. V., “Introduction to Embedded Systems”, Tata McGraw Hill Education Private Limited, New Delhi, 2009.

Web resources:

1. Embedded Systems Academy- https://www.embedded-sys.com/plus/
2. Embedded Systems Basics by Tutorialspoint- https://www.tutorialspoint.com/embedded_systems/index.htm
3. Embedded Systems Programming Course by Udemy- https://www.udemy.com/course/introduction-to-embedded-systems/
4. Course on- Introduction to Embedded Systems Software and Development Environments- https://www.coursera.org/learn/introduction-embedded-systems

Online Courses: NPTEL/SWAYAM

1. Embedded Systems Design by By Prof. Anupam Basu IIT Kharagpur
   https://onlinecourses.nptel.ac.in/noc23_cs54/preview
2. Introduction to Embedded System Design By Prof. Dhananjay V. Gadre, Prof. Badri Subudhi , Netaji Subhas University of Technology, IIT Jammu-
   https://onlinecourses.nptel.ac.in/noc23_cs06/preview

Evaluation Scheme:

Semester End Examination (A):

Theory:

1. Question paper will be based on the entire syllabus summing up to 75 marks.

2. Total duration allotted for writing the paper is 3 hrs.

Continuous Assessment (B):

Theory:

1. Two term tests of 25 marks each will be conducted during the semester out of which; one will be a compulsory term test (on minimum 02 Modules) and the other can either be a term test or an assignment on live problems or a course project.

2. Total duration allotted for writing each of the paper is 1 hr.

3. Average of the marks scored in both the tests will be considered for final grading.

Laboratory

Oral examinations will be based on the entire syllabus including the practical's performed during laboratory sessions.

Laboratory: (Term work)

Term work shall consist of minimum 8 experiments.

The distribution of marks for term work shall be as follows:

i. Laboratory work (Performance of Experiments): 15 Marks

ii. Journal documentation (Write-up and/or Assignments): 5 marks

iii. Attendance (Theory + Practical):5 Marks

The final certification and acceptance of term work will be subject to satisfactory performance of laboratory work, and upon fulfilling minimum passing criteria in the term work.

Program: B.Tech. CSE in IoT and Cyber Security with Blockchain Technology

T.Y. B.Tech. **Semester: V**

Course: Applied Cryptography (DJ19ICC502)

Course: Applied Cryptography Laboratory (DJ19ICL502)

Prerequisite: Computer Networks

Objectives:

1. To introduce classical encryption techniques and concepts of modular arithmetic and number theory.
2. To learn the fundamental concepts of cryptography.
3. To explore the working principles and utilities of various cryptographic algorithms including secret key cryptography, hashes and message digests, and public key algorithms.
4. To develop the ability to use existing cryptographic utilities to build programs for secure communication.

Outcomes: On completion of the course, learner will be able to:

1. Understand the system security goals and concepts, acquire the fundamental knowledge of modular arithmetic and number theory.
2. Acquire the knowledge of various cryptographic techniques.
3. Apply different encryption and decryption techniques to solve problems related to confidentiality.
4. Understand and apply various hashing techniques, message authentication techniques and Digital Signature techniques to design secure application.

Detailed Syllabus: (unit wise)		
Unit	**Description**	**Duration**
1	**INTRODUCTION** An Overview of Information Security: Goals for Security, Security threat and vulnerability, Cyber security models (the CIA triad, the star model) , Cryptographic attack, service and mechanism **NUMBER THEORY** Modular Arithmetic, Euclidean Algorithm, Prime Numbers, Relatively Prime Numbers, Primitive Roots, Fermat’s Little Theorem, Euler Totient Function, Extended Euclidean Algorithm, Chinese Remainder Theorem, Discrete Logarithms, Index Calculus Algorithm.	**9**
2	**FUNDAMENTALS OF CRYPTOGRAPHY** Introduction, plain text and cipher text, Classical Encryption techniques, Symmetric cipher model, mono-alphabetic and polyalphabetic substitution techniques: Vigenere cipher,	**5**

	playfair cipher, Hill cipher, Affine Cipher, transposition techniques: keyed and keyless transposition ciphers.	
3	**SYMETRIC-KEY ENCRYPTION** Block Ciphers Stream Ciphers, Homomorphic encryption, Feistel Ciphers, Data Encryption Standard (DES), Cracking DES, Triple DES, Modes of Operation, Advanced Encryption Standard (AES), Modern Block Cipher, RC5, cryptanalysis, Weak Keys.	**8**
4	**PUBLIC-KEY CRYPTOGRAPHY** Public-Key Cryptography, Knapsack Cryptosystem, RSA Cryptosystem, Attack on RSA, ELGamal cryptosystem, Security of ElGamal, Diffie—Hellman Key Exchange, Elliptic Curve Cryptography [ECC],	**7**
5	**CRYPTOGRAPHIC HASH FUNCTIONS:** Cryptographic Hash Functions – MD5, attack on MD5, SHA-1, SHA-3, SHA-256,SHA-512 MAC, HMAC	**5**
6	**DIGITAL SIGNATURE SCHEMES and DIGITAL CERTIFICATES** Digital Signature – Process, Services, Attacks on Digital Signature, Digital Signature Schemes – RSA, El Gamal, Digital certificate, Chain of certificate, PKI, Quantum Crptography	**5**
	Total	**39**

List of Laboratory Experiments: (Minimum any eight experiments)

Sr. No.	Suggested Experiments
1	Implement the Euclidean Algorithm for integers and polynomials.
2	Design and Implementation of a product cipher using Substitution and Transposition ciphers.
3	Implementation of Simplified DES Encryption and decryption.
4	Implementation of AES encryption and decryption.
5	Implementation and analysis of RSA crypto system.
6	Implementation of Diffie Hellman Key exchange algorithm
7	Implementation of RC5 encryption and decryption.
8	Implementation of Message digest using MD5.
9	Implementation of Message digest using SHA-1.
10	Implementation of Digital Signatures in Cryptography.
11	Case Study /Seminar: Topic beyond syllabus related to topics covered.

Any other experiment based on syllabus may be included, which would help the learner to understand topic/concept.

Books Recommended:

Text Books:

1. William Stallings, Cryptography and Network Security, Principles and Practice, 6th Edition, Pearson Education, March 2013.
2. Behrouz A. Ferouzan, ―Cryptography & Network Security‖, Tata McGraw Hill.
3. Bernard Menezes, ―Cryptography & Network Security‖, Cengage Learning.
4. Network Security Bible, Eric Cole, Second Edition, Wiley.

Reference Books:

1. Applied Cryptography, Protocols Algorithms and Source Code in C, Bruce Schneier, Wiley.
2. Cryptography and Network Security, Atul Kahate, Tata Mc Graw Hill.

Web resources:

1. Data Encryption standard: https://www.geeksforgeeks.org/data-encryption-standard-des-set-1
2. Advance Encryption standard: https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
3. Digital Signature: http://www.javatpoint.com/java-digital-signature
4. Challenge Response Protocols: https://www.tutorialspoint.com/challenge-response-authentication-mechanism-cram

Online Courses: NPTEL / Swayam

1. https://nptel.ac.in/courses/106106221
2. https://www.coursera.org/learn/crypto
3. https://www.coursera.org/specializations/introduction-applied-cryptography

Evaluation Scheme:

Semester End Examination (A):

Theory:

1. Question paper will be based on the entire syllabus summing up to 75 marks.

2. Total duration allotted for writing the paper is 3 hrs.

Continuous Assessment (B):

Theory:

1. Two term tests of 25 marks each will be conducted during the semester out of which; one will be a compulsory term test (on minimum 02 Modules) and the other can either be a term test or

an assignment on live problems or a course project.

2. Total duration allotted for writing each of the paper is 1 hr.

3. Average of the marks scored in both the two tests will be considered for final grading.

Laboratory

Practical & Oral examinations will be based on the entire syllabus including the practical's performed during laboratory sessions.

Laboratory: (Term work)

1. Term work shall consist of minimum 8 experiments and Mini project.

The distribution of marks for term work shall be as follows:

i. Laboratory work (Performance of Experiments): 15 Marks

ii. Journal documentation (Write-up and/or Assignments): 5 marks

iii. Attendance (Theory + Practical):5 Marks

The final certification and acceptance of term work will be subject to satisfactory performance of laboratory work, and upon fulfilling minimum passing criteria in the term work.

Prepared by Checked by Head of the Department Principal

Program: B.Tech. CSE in IoT and Cyber Security with Blockchain Technology **T.Y. B.Tech.** **Semester: V**

Course: Introduction to Blockchain Technology (DJ19ICC503)

Course: Introduction to Blockchain Technology Laboratory (DJ19ICL503)

Prerequisite:

1. Networking Fundamentals
2. Distributed Operating Systems

Objectives:

1. To understand emerging Blockchain Technology and its relevance with cryptography.
2. To demonstrate the use of cryptography required for Blockchain.
3. To understand smart contracts, wallets, and consensus protocols.
4. To design and develop Blockchain applications.

Outcomes: On completion of the course, learner will be able to:

1. Acquire basic knowledge of Blockchain technology
2. Understand methods for securing blockchain networks, including cryptography and consensus protocols.
3. Use various tools for Blockchain implementation.
4. Analyze the real-world applications of Blockchain technology.

Detailed Syllabus: (unit wise)

Unit	Description	Duration
1	**Introduction to Blockchain Technology** The Model of Decentralization, Distributed Systems for Decentralization, Blockchain framework, Characteristics of Blockchain, Block structure, Block header, Types of Blockchain: Public, Private and Hybrid Blockchain.	**6**
2	**Basic Crypto primitives** Cryptographic Primitives, Cryptographic Hash, Hash Functions, SHA-256, Puzzle Friendly, Secure Hash Algorithm, Hash Pointers, Merkle Tree, Hash Chain, Construction of Chain of Blocks, Public Key Cryptography, Digital Signature.	**7**
3	**Bitcoin and Consensus** **The Evolution of Cryptocurrencies**: Design Goals for Cryptocurrency Development	**10**

	Introduction to Bitcoin: Bitcoin block, bitcoin P2P network, Transactions, Bitcoin mining, double spending attack, Forks, The Monopoly Problem-51% attack **Consensus:** Consensus Approach**,** Consensus Algorithms: Proof-of-Stake (PoS), Proof-of-Work (PoW), Proof-of-Burn (PoB), Proof-of-Elapsed Time (PoET), State Machine Replication as a Consensus, Crash Fault Tolerance, PAXOS, Byzantine Fault Tolerant (BFT), BFT Consensus, Practical BFT.	
4	**Ethereum** Ethereum and its Components, Ethereum Virtual Machine (EVM), Ethereum Ecosystem, Transaction, Comparison between Bitcoin and Ethereum, test-networks, Smart Contracts, Introduction to solidity programming, Ganache, MetaMask, Truffle	**6**
5	**Hyperledger** Introduction to Hyperledger Fabric, Key features of Hyperledger fabric, Hyperledger Fabric Architecture, Ethereum v/s Hyperledger framework, Fabric Test Network, Hyperledger Consensus, Fabric Transaction Flow, Hyperledger Tools and Libraries, Hyperledger Fabric Chaincode	**6**
6	**Blockchain Allied Technologies** Blockchain in DeFi: Case Study on any of the Blockchain Platforms, Blockchain in Healthcare, Blockchain and Artificial Intelligence, Blockchain and IoT, Blockchain and Machine Learning, Blockchain and Robotic Process Automation	**4**
	Total	**39**

List of Laboratory Experiments: (Minimum any six experiments)

Sr. No.	**Suggested Experiments**
1	To create basic Blockchain with sample transactions and print it.
2	To implement Merkle root from the transactions and verify the validity of transactions using it.
2	To implement Proof of Work (PoW) concept in Bitcoin Mining and demonstrating it.
3	To analyse and implement Unspent Transaction Outputs (UTXOs) in Bitcoin and demonstrate the transactions using UTXOs.
4	To create and deploy Smart Contract using Solidity and Remix IDE.
5	To perform Embedding wallet and transaction using Solidity and MetaMask.
6	To implement blockchain using Geth (Go-Ethereum).
7	To implement local Blockchain using tools viz. Ganache and Truffle.
8	To interacting with the Ethereum Blockchain Using Web3.js

9	To install Hyperledger Fabric and demonstrate its usability.
10	To query and invoke transactions on Fabric Test Network
11	Miniproject based on the real world application using blockchain (Group of 3-4 students will work together)

Any other experiment based on syllabus may be included, which would help the learner to understand topic/concept.

Books Recommended:

Text Books:

1. Imran Bashir , Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more, 3rd Edition, Packt Publishing, 2020, ISBN: 9781839213199,
2. Kumar Saurabh , Ashutosh Saxena, Blockchain Technology: Concepts and Applications , 1st Edition, Wiley Publication, 2020, ISBN:978-81-265-5766-0
3. S. Shukla, M. Dhawan, S. Sharma, S. Venkatesan, -Blockchain Technology: Cryptocurrency and Applications, Oxford University Press, 2019
4. Cryptography and Network Security – Principles and Practice by William Stallings, Pearson 2017

Reference Books:

1. Antony Lewis, Basics of Bitcoins and Blockchain, Mango Publishing, 2021
2. Blockchain for Beginners, Yathish R and Tejaswini N, SPD
3. Blockchain Basics, A non-Technical Introduction in 25 Steps, Daniel Drescher, Apress.
4. Blockchain with Hyperledger Fabric, Luc Desrosiers, Nitin Gaur, Salman A. Baset, Venkatraman Ramakrishna, Packt Publishing
5. Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions, Bikramaditya Singhal, Gautam Dhameja, Priyansu Sekhar Panda, Apress

Web resources:

1. Hyperledger Tutorials - https://www.hyperledger.org/use/tutorials
2. Ethereum Development Resources - https://ethereum.org/en/developers/
3. Solidity Tutorial- https://www.tutorialspoint.com/solidity/index.htm
4. Metamask- https://docs.metamask.io/guide/

Online Courses: NPTEL / Swayam

1. Blockchain and its Applications, By Prof. Sandip Chakraborty, Prof. Shamik Sural IIT Kharagpur
https://onlinecourses.nptel.ac.in/noc23_cs47/preview
2. Blockchain Architecture Design and Use Cases, By Prof. Sandip Chakraborty & Dr. Praveen Jayachandran | IIT Kharagpur and IBM,
https://onlinecourses.nptel.ac.in/noc19_cs63/preview
3. Blockchain, By Dr.Mayank Aggarwal ,Gurukul Kangri Vishwavidyalaya,Haridwar
https://onlinecourses.swayam2.ac.in/aic21_ge01/preview

Evaluation Scheme:

Semester End Examination (A):

Theory:

1. Question paper will be based on the entire syllabus summing up to 75 marks.
2. Total duration allotted for writing the paper is 3 hrs.

Continuous Assessment (B):

Theory:

1. Two term tests of 25 marks each will be conducted during the semester out of which; one will be a compulsory term test (on minimum 02 Modules) and the other can either be a term test or an assignment on live problems or a course project.
2. Total duration allotted for writing each of the paper is 1 hr.
3. Average of the marks scored in both the two tests will be considered for final grading.

Laboratory

Oral examinations will be based on the entire syllabus including the practical's performed during laboratory sessions.

Laboratory: (Term work)

Term work shall consist of minimum 6 experiments and a Mini project.

The distribution of marks for term work shall be as follows:

i. Laboratory work (Performance of Experiments, Assignments): 10 Marks
ii. Miniproject : 10 marks
iii. Attendance (Theory + Practical): 5 Marks

The final certification and acceptance of term work will be subject to satisfactory performance of laboratory work, and upon fulfilling minimum passing criteria in the term work.

Prepared by Checked by Head of the Department Principal

Program: B.Tech. CSE in IoT and Cyber Security with Blockchain Technology

T.Y. B.Tech.

Semester: V

Course: Artificial Intelligence (DJ19ICC504)

Course: Artificial Intelligence Laboratory (DJ19ICL504)

Pre-requisite:

1. Basic programming languages
2. Data Structures

Objectives:

1. To create a thorough understanding of AI basics and real-time applications in its sub-domains.
2. To explore AI techniques like informed, uninformed and adversarial searching to solve real-life problems in a state space tree representation.
3. To understand advanced topics of AI in IoT with real world examples.

Outcomes: On completion of the course, learners will be able to:

1. Develop a basic understanding of AI building blocks presented in intelligent agents.
2. Design an appropriate problem-solving method for an agent to find a sequence of actions to reach the goal state.
3. Analyse various AI approaches to knowledge– intensive problem solving, reasoning and planning.
4. Understand the applications of Artificial Intelligence in Semantic Web, Cyber Security and IoT.

Detailed Syllabus: (unit wise)		
Unit	Description	Duration
1	**Introduction to Artificial Intelligence:** Introduction, History of Artificial Intelligence, Intelligent Systems: Categorization of Intelligent System, Components of AI Program, Foundations of AI, Sub-areas of AI, Current trends in AI **Intelligent Agents:** Agents and Environments, The concept of rationality, The nature of environment, The structure of Agents, Types of Agents, Learning Agent.	06
2	**Problem solving:** Solving Problem by Searching: Problem Solving Agent, Formulating Problems, Example Problems. **Uninformed Search Methods:** Breadth First Search (BFS), Depth First Search (DFS), Depth Limited Search, Depth First Iterative Deepening (DFID) **Informed Search Methods:** Greedy Best first Search, A* Search	12

	Stochastic Local Search Algorithms: Hill climbing search, Simulated Annealing **Adversarial Search:** Game Theory, Algorithm Minimax, Alpha-Beta Pruning.	
3	**Knowledge and Reasoning:** Knowledge based Agents, The WUMPUS World, Inference in FOL, Forward chaining, Backward chaining, Knowledge Engineering in First-Order Logic, Unification, Resolution.	07
4	**Planning:** The planning problem, Planning with State Space Search, STRIPS, Goal Stack Planning, Planning graphs, Partial order planning, Hierarchical Planning.	06
5	**Semantic AI:** Introduction, Semantic AI in data integration, knowledge representation, search, and reasoning. **AI in Cyber Security:** Role of AI in Cyber Security, AI in Cyber Security: Need, Benefits, Adversarial Use of AI, Real life use cases of AI in cyber security.	04
6	**Artificial Intelligence in IoT** **Applications of Artificial Intelligence in Internet of Things,** Real world examples: Tesla Motors – Self Driving Cars, WildTrack – Endangered Species Preservation, Nest Labs – Smart thermostat, Automated vacuum cleaner – iRobot Roomba **IoT companies and vendors:** Commercially available IoT devices from vendors, Google Home Voice Controller, Amazon Echo Plus Voice Controller, August Doorbell Cam, August Smart Lock	04
	Total	**39**

List of Laboratory Experiments:

Sr. No.	Title of Experiments (Minimum any eight using Python /PROLOG)
1	Select a problem statement relevant to AI. i) Identify the problem ii) PEAS Description iii) Problem formulation
2	Identify and analyze uninformed search Algorithm to solve the problem. Implement BFS/DFS/DFID search algorithms to reach goal state.
3	Identify and analyze informed search Algorithm to solve the problem. Implement A* search algorithm to reach goal state.
4	Program to implement Local Search algorithm: World Block Problem using Hill climbing search
5	Experiment to illustrate Game playing.
6	Implementation on Wumpus world AI Problem.
7	Program to implement alpha beta pruning.
8	Implementation on Tic-tac-toe AI Problem.
9	Implementation on 8-Queens Problem AI Problem.

10	Case study on Planning Problem. Identify and analyze a planning problem
11	Case study of an AI Application

Any other experiment based on syllabus may be included, which would help the learner to understand topic/concept.

Books Recommended:

Text Books

1. Stuart J. Russell and Peter Norvig, "Artificial Intelligence A Modern Approach “Fourth Edition" Pearson Education,2022.
2. Saroj Kaushik “Artificial Intelligence”, Cengage Learning,1st Edition, 2011.
3. George F Luger “Artificial Intelligence” Pearson Education., 6th Edition,2021.
4. Deepak Khemani.” A First Course in Artificial Intelligence”, McGraw Hill Education (India), 6th Edition,2017.
5. "Semantic Web for the Working Ontologist: Effective Modeling in RDFS and OWL" Dean Allemang and James Hendler.

Reference Books

1. Ivan Bratko “PROLOG Programming for Artificial Intelligence”, Pearson Education, 4th edition, 2011
2. Elaine Rich and Kevin Knight “Artificial Intelligence” Third Edition,2017.
3. Patrick Henry Winston, “Artificial Intelligence”, Addison-Wesley, Third Edition.1992
4. Lavika Goel **, “Artificial Intelligence concept and applications”, WILEY Publishers, 2021**
5. N.P.Padhy , “Artificial Intelligence and Intelligent Systems”, Oxford University Press. 2005.
6. Dr. Nilakshi Jain.,” Artificial Intelligence”, WILEY Publishers, First Edition,2019.

Web resources:

1. Microsoft AI School- https://www.microsoft.com/en-us/ai
2. Google AI Education- https://ai.google/why-ai/
3. Practical tutorials and courses https://docs.fast.ai/

Online Courses: NPTEL / Swayam

1. Course on- Fundamentals Of Artificial Intelligence-

https://onlinecourses.nptel.ac.in/noc23_ge40/preview

2. **Course on-**Artificial Intelligence: Search Methods for Problem Solving-

https://onlinecourses.nptel.ac.in/noc23_cs92/preview

Evaluation Scheme:

Semester End Examination (A):

Theory:

1. Question paper based on the entire syllabus will comprise of 5 questions (All compulsory, but with

internal choice as appropriate), each carrying 15 marks, total summing up to 75 marks.
2. Total duration allotted for writing the paper is 3 hrs.

Laboratory:
1. Practical and Oral examinations will be based on the entire syllabus including the practical's performed during laboratory sessions.

Continuous Assessment (B):
Theory:
1. Two term tests of 25 marks each will be conducted during the semester out of which one will be a compulsory term test (on minimum 02 Modules) and the other can either be a term test or an assignment on live problems or a course project.
2. Total duration allotted for writing each of the paper is 1 hr.
3. Average of the marks scored in the both the tests will be considered for final grading.

Laboratory: (Term work)
Laboratory work will be based on DJ19ICL504 with a minimum of 08 experiments.

The distribution of marks for term work shall be as follows:
1. Laboratory work (Performance of Experiments): 15 Marks
2. Journal Documentation (Write-up and Assignments): 05 Marks
3. Attendance (Theory + Practical):5 Marks

The final certification and acceptance of term work will be subject to satisfactory performance of laboratory work and upon fulfilling minimum passing criteria in the term work.

Prepared by   Checked by   Head of the Department   Principal

Program: B.Tech. CSE in IoT and Cyber Security with Blockchain Technology **T.Y. B.Tech.** **Semester: V**

Course: Digital Forensics (DJ19ICEC5011)

Course: Digital Forensics Laboratory (DJ19ICL503)

Prerequisite: Cryptography, System Security, Computer Networks

Objectives:

1. To discuss the need and process of digital forensics and Incident Response Methodology.
2. To explore the procedures for identification, preservation, acquisition, and analysis of digital evidence.
3. To explore techniques and tools used in digital forensics for Operating system and malware investigation.
4. To explore techniques and tools used for Mobile forensics, browser, email forensics.

Outcomes: On completion of the course, learner will be able to:

1. Discuss the phases of Digital Forensics and methodology to handle the computer security incident.
2. Describe the process of identification, duplication, and collection of the digital evidence.
3. Describe the process of investigation and analysis of the acquired digital evidence.
4. Summarize the steps involved in Evidence Handling and produce an unambiguous investigation report.
5. Acquire adequate perspectives of digital forensic investigation in mobile devices.
6. Explore various tools to analyze malwares and perform browser and email content authentication.

Detailed Syllabus: (unit wise)

Unit	**Description**		**Duration**
1	**Introduction to Digital Forensics:**		**6**
	1.1	Introduction to Digital Forensics and Digital Evidence, The Need for Digital Forensics, Digital Forensics Categories - Computer Forensics, Mobile Forensics, Network Forensics, Database Forensics, Types of Digital Forensics, Digital Forensics Life Cycle.	
	1.2	Introduction to Computer Security Incident, Goals of Incident response, Incident Response Methodology, Initial Response, Formulating Response Strategy.	
2	**Digital Evidence, Forensic Duplication and Acquisition:**		**8**
	2.1	**Forensic Duplication:** Introduction to Forensic Duplication, Types of Forensic Duplicates, Introduction to Forensic Duplication Tools, Necessity of forensic duplication, Forensic image formats, Forensic duplication techniques.	

	2.2	**Forensic Acquisition:** Introduction to Static and Live/Volatile Data, Static Data Acquisition from Windows (FTK Imager), Static Data Acquisition from Linux (dd/dcfldd), Live Data Acquisition from Windows (FTK Imager). Network Forensics (wireshark)	
3	**Forensic Investigation and Analysis:**		**8**
	3.1	**Forensic Investigation:** Investigating Registry Files, Investigating Log Files, Data Carving (Bulk Extractor), USB Device Forensics, Identifying Unauthorized User Accounts or Groups, Identifying Rogue Processes, Checking for Unauthorized Access Points, Analyzing Trust Relationships	
	3.2	**Forensic Analysis:** Introduction to Forensic Analysis, Live Forensic Analysis in Windows, Live Forensic Analysis in Linux, Forensic Analysis of acquired data in Windows, Forensic Analysis of acquired data in Linux.	
4	**Evidence Handling and Forensic Reporting:**		**6**
	4.1	**Evidence Handling:** Digital evidence, Types of Digital Evidence, Characteristics of an Evidence, Challenges in acquiring Digital evidence, Admissibility of evidence, Faraday's Bag, , Types of Evidence, Evidence Handling Methodology, Chain of Custody.	
	4.2	**Forensic Reporting:** Goals of a Report, Layout of an Investigative Report, Guidelines for writing a report, Sample Forensic Report	
5	**Mobile Forensics:**		**6**
	5.1	**Android Forensics:** Mobile Device Forensic Investigation – Storage location, Acquisition methods, Data Analysis	
	5.2	**GPS forensics:** GPS Evidentiary data, GPS Exchange Format (GPX), GPX Files, Extraction of Waypoints and TrackPoints, Display the Tracks on a Map.	
	5.3	**SIM Cards Forensics:** The Subscriber Identification Module (SIM), SIM Architecture, Security, Evidence Extraction.	
6	**Browser, Email and Malware Forensics:**		**5**
	6.1	**Browser Forensics:** Web Browser Forensics, Google chrome, other web browser investigation	
	6.2	**Email Forensics:** Sender Policy Framework (SPF), Domain Key Identified Mail (DKIM), Domain based Message Authentication Reporting and Confirmation (DMARC)	
	6.3	**Malware Analysis:** Malware, Viruses, Worms, Essential skills and tools for Malware Analysis, List of Malware Analysis Tools and Techniques	
		Total	**39**

List of Laboratory Experiments: (Minimum any eight experiments)	
Sr. No.	**Suggested Experiments**
1	To perform static data acquisition from Windows OS

	• **Recommended Tool:** FTK Imager
2	To acquire live data from Windows OS • **Recommended Tool:** FTK Imager, TCP Dump
3	To perform static data acquisition from Linux OS • **Recommended Tool:** dd, dcfldd
4	To perform live data acquisition from Linux • **Recommended Tool:** Kali Linux, fdisk
5	To perform analysis of Forensic Duplicates • **Recommended Tool:** Autopsy, bulk Extractor
6	To recover Evidence from Forensic Images • **Recommended Tool:** Scalpel
7	To perform Data Carving from Forensic Images • **Recommended Tool:** Bulk Extractor
8	Performing RAM Forensic to analyze memory images to find traces of an attack. • **Recommended Tool:** Capturing RAM Using the DumpIt Tool, Volatility tool
9	Web Browser Forensics • **Recommended Tool:** DB Browser for SQLite
10	Case Study on Chain of Custody and Evidence Integrity Validation using Hash Values • **Recommended Tool:** Hashdeep, md5sum
11	Network forensics • **Recommended Tool:** Network Miner
12	Email Header Analysis
13	To perform penetration testing and vulnerability exploitation. • **Recommended Tool:** Metasploit (Kali Linux)

Any other experiment based on syllabus may be included, which would help the learner to understand topic/concept.

Books Recommended:

Text Books:

1 Digital Forensics by Nilakshi Jain & Kalbande, Wiley

2 Digital Forensics Basics A Practical Guide Using Windows OS — Nihad A. Hassan, APress Publication, 2019

3 Xiaodong Lin, ―Introductory Computer Forensics: A Hands-on Practical Approach, Springer Nature, 2018

Reference Books:

1 Kevin Mandia, Chris Prosise, ―Incident Response and computer forensics, Tata McGrawHill, 2006

2 Digital Forensics by Nilakshi Jain & Kalbande, Wiley

3 Build your own Security Lab, Michael Gregg, Wiley India

Web resources:

1. Ethical Hacking by Prof. Indranil Sengupta, IIT Kharagpur, https://freevideolectures.com/course/4070/nptel-ethical-hacking
2. Advanced System Security and Digital Forensics by Prof. Sridhar Iyer, University of Mumbai, https://www.youtube.com/playlist?list=PLx2aAxxVN1NVk9JwAQwCNA159FrSXQ5Hn
3. https://owasp.org/www-project-top-ten/
4. https://www.computersecuritystudent.com/
5. http://www.opentechinfo.com/learn-use-kali-linux/
6. Virtual Penetration Testing Labs- https://pentesterlab.com
7. Google Hacking Database - https://www.exploit-db.com/google-hacking-database

Online Courses: NPTEL / Swayam

1. Course on ―Ethical Hacking-https://nptel.ac.in/courses/106/105/106105217/
2. Course on ―Digital Forensics- https://onlinecourses.swayam2.ac.in/cec20_lb06/preview
3. Course on Cyber Incident Response https://www.coursera.org/learn/incident-response
4. Course on ―Penetration Testing, Incident Responses and Forensics- https://www.coursera.org/learn/ibm-penetration-testing-incident-response-forensics

Evaluation Scheme:

Semester End Examination (A):

Theory:

1. Question paper will be based on the entire syllabus summing up to 75 marks.
2. Total duration allotted for writing the paper is 3 hrs.

Laboratory:

1. Oral examinations will be based on the entire syllabus including the practical's performed during laboratory sessions.

Continuous Assessment (B):

Theory:

1. Two term tests of 25 marks each will be conducted during the semester out of which; one will be a compulsory term test (on minimum 02 Modules) and the other can either be a term test or an assignment on live problems or a course project.
2. Total duration allotted for writing each of the paper is 1 hr.
3. Average of the marks scored in the two tests will be considered for final grading.

Laboratory: (Term work)

Term work shall consist of minimum 8 experiments and Mini project.

The distribution of marks for term work shall be as follows:

i. Laboratory work (Performance of Experiments): 15 Marks
ii. Journal documentation (Write-up and/or Assignments): 5 marks
iii. Attendance(Theory + Practical):5 Marks

The final certification and acceptance of term work will be subject to satisfactory performance of laboratory work, and upon fulfilling minimum passing criteria in the term work.

Prepared by Checked by Head of the Department Principal

Program: B.Tech. CSE in IoT and Cyber Security with Blockchain Technology

T.Y. B.Tech.

Semester: V

Course: Network Security (DJ19ICEC5012)

Course: Network Security Laboratory (DJ19ICEL5012)

Prerequisite:

1. Computer Networks

Objectives:

1. To introduce Basics of Network security.
2. To perform various attacks on the network security.
3. To gain the knowledge of different networking protocols.
4. To understand the firewall and IDS for system security
5. To develop the ability to use Cloud security for data storage.

Outcomes: On completion of the course, learner will be able to:

1. Understand the basics of Internet and OS Security.
2. Study and describe different Network attacks in Internet Security.
3. Study and implement different security protocols.
4. Identify the function of an IDS and firewall for the system security
5. Study different mobile and cloud security mechanism.

Detailed Syllabus: (unit wise)		
Unit	Description	Duration
1.	**Basics of Network Security** **Security Concepts:** Introduction, The need for security, Goals of Security, Security Threat, Vulnerability, Introduction to Vulnerability Assessment, Types of Attacks, An model for Network Security.	4
2	**Network Attacks** Vulnerabilities and Exploits, TCP/IP Vulnerabilities, sync flooding attack, ICMP flooding attack, UDP flooding attack, ARP Soofing, Session Hijacking, DNS Spoofing, Cross Site Scripting, Cross Site Request Forgery Attacks, Phishing and Pharming Attacks, ID Theft Attack, Salami Attacks.	7
3	**Network Security protocols:** Virtual Private Networks, SSL/TLS, HTTPS, Secure Shell (SSH), POP3, IMAP, Password Salting, SET Protocol for secure online payments. **E-Mail Security:** PGP/GPG, S/MIME **IP Security:**	10

	IP Security overview, IP Security architecture, Authentication Header, Encapsulating security payload, Combining security associations, Internet Key Exchange	
4	**Introduction to Firewalls:** Basics of Firewalls, Types of Firewalls, Firewall Rules. **IDS and Honeypots:** Introduction to IDS/IPS , Need of IDS , Challenges of IDS and its Types, Honeypots, DMZ.	5
5	**Mobile Security:** Introduction to Mobile Security, Security of GSM Networks, Security of UMTS Networks, LTE Security, WEP, WPA, WPA2, WPA3, Attacks on Wireless Networks (Krack Attacks, Traffic Sniffing) Bluetooth Security, Mobile Malware and App Security, Android Security Model, Emerging Trends in Mobile Security.	7
6	**Cloud Security:** Introduction to Cloud Security, Infrastructure Security, Network level security, Host level security, Application-level security, Data security and Storage, Data privacy and security Issues, Jurisdictional issues raised by Data location, Identity & Access Management, Access Control, Trust, Reputation, Risk, Authentication in cloud computing, Client access in cloud, Cloud contracting Model, Commercial and business consideration	6
	Total	**39**

List of Laboratory Experiments:

Sr. No	Experiment
1	Study and Implement OS Security
2	Study and Implement Buffer Overflow
3	Study and Implement SQL Injection
4	Study and Implement Cross Site Scripting
5	Study and Implement DOS Attacks
6	Study and Implement Session Hijacking Attacks
7	Study and Implement VPN
8	Study and Implement PGP/GPG Encryption
9	Study and Implement Firewalls using iptables
10	Study and Implement IDS
11	Study and Implement Network traffic sniffing (Wireshark, Ettercap)
12	Case Study on Cloud Security

Books Recommended:

Textbooks:

1. William Stallings, Cryptography and Network Security, Pearson Publication, 7th Edition, 2017.
2. Charles P. Pfleeger “Security in computing”, Pearson Education, 5th Edition, 2018.
3. Behrouz A. Forouzan “Introduction to Cryptography and Network Security”, McGraw-Hill, 3rd

Edition, 2015.

Reference Books:

1. Practical Packet Analysis: Using Wireshark to Solve Real-Word Network problems by Chris Sanders. 3rd Editon, 2017.

2. Man Ho Au, Raymond Choo, Mobile Security and Privacy: Advances, Challenges and Future Research Directions, 1st Edition, 2016.

3. Roberta Bragg (Author), Mark Rhodes-Ousley (Author), Keith Strassberg (Author) Network Security: The Complete Reference, 1 July 2017

Web Resources:

1. Network World - https://www.networkworld.com/asia/
2. Course on - Palo Alto Networks Cybersecurity Professional Certificate- https://www.coursera.org/professional-certificates/palo-alto-networks-cybersecurity-fundamentals
3. SecurityTube - http://www.securitytube.net/
4. Reddit- https://www.reddit.com/r/netsec/
5. Network Security- https://www.mygreatlearning.com/academy/learn-for-free/courses/network-security

Online Courses: NPTEL/SWAYAM

1. Cryptography and Network Security By Prof. Sourav Mukhopadhyay,IIT Kharagpur- https://onlinecourses.nptel.ac.in/noc21_cs16/preview
2. Cyber Security By Dr.G.PADMAVATHI, Avinashilingam Institute for Home Science & Higher Education for Women,Coimbatore, https://onlinecourses.swayam2.ac.in/cec20_cs15/preview
3. Information Security: A Hands-On Approach: https://nptel.ac.in/courses/106/106/106106229/

Evaluation Scheme:

Semester End Examination (A):

Theory:
1. Question paper will be based on the entire syllabus summing up to 75 marks.
2. Total duration allotted for writing the paper is 3 hrs.

Laboratory:
Oral examinations will be based on the entire syllabus including the practical's performed during laboratory sessions.

Continuous Assessment (B):
Theory:
1. Two term tests of 25 marks each will be conducted during the semester out of which; one will be a compulsory term test (on minimum 02 Modules) and the other can either be a term test or an assignment on live problems or a course project.

2. Total duration allotted for writing each of the paper is 1 hr.
3. Average of the marks scored in both the tests will be considered for final grading.

Laboratory: (Term work)
Term work shall consist of a minimum of 8 experiments.
The distribution of marks for term work shall be as follows:
i. Laboratory work (Performance of Experiments): 15 Marks
ii. Journal documentation (Assignments): 5 marks
iii. Attendance (Theory + Practical):5 Marks

The final certification and acceptance of term work will be subject to satisfactory performance of laboratory work, and upon fulfilling minimum passing criteria in the term work.

Prepared by Checked by Head of the Department Principal

Program: B.Tech. CSE in IoT and Cyber Security with Blockchain Technology **T.Y. B.Tech.** **Semester: V**

Course: Vulnerability Assessment & Penetration Testing (DJ19ICEC5013)

Course: Vulnerability Assessment & Penetration Testing Laboratory (DJ19ICL503)

Prerequisite:

1. Computer Networks
2. Operating Systems
3. Programming skills

Objectives:

1. To find vulnerabilities in the system in a controlled manner by using various tools and techniques.
2. To learn about various methods, tools and techniques to perform ethical hacking.
3. To discover the system hacking methods and its advancement.
4. To assess the security of organization before exploited by hacker.
5. To prepare students to pursue a career in penetration testing domain.

Outcomes: On completion of the course, learner will be able to:

1. To understand the basic principles for Information Gathering and Detecting Vulnerabilities in the system
2. Understand the basic of vulnerability assessment & penetration testing.
3. Apply various tools and techniques to find vulnerabilities in the system.
4. Aware of the various ways through which hackers' attempts to compromise an Application.

Detailed Syllabus: (unit wise)		
Unit	**Description**	**Duration**
1	**Information Gathering and Evading techniques** Information Gathering Techniques - Active, Passive and Sources of Information Gathering - Approaches and Tools - Traceroutes, Neotrace, Whatweb, Netcraft, Xcode Exploit Scanner and NSlookup, Host discovery - Scanning for open ports and services - Types of Port, Vulnerability Scanner Function, pros and cons - Vulnerability Assessment with NMAP	**7**

2	**Introduction to penetration testing** Penetration testing concepts, Penetration testing methodology, Types of penetration testing, red/blue teaming, Tools and techniques used in penetration testing , testing methodologies (OSSTMM, PTES, and OWASP Testing Guide), and Rules of engagement, Vulnerability metrics (CVE, CWE, CVSS), Limitations of penetration testing tools	**8**
3	**Reconnaissance and scanning** Introduction, types of reconnaissance, various techniques of recon (social engineering, web based recon, DNS based recon, network based recon, Google hacking etc.), countermeasures, scanning, types of scanning (port scanning, network scanning, and vulnerability scanning), Sniffers	**6**
4	**Exploits** Architecture and Environment- Leveraging Metasploit on Penetration Tests, Understanding - Metasploit Channels, Metasploit Framework and Advanced Environment configurations - Understanding the Soft Architecture, Configuration and Locking, Advanced payloads and addon modules Global data store, module data store, saved environment Meterpreter.	**6**
5	**Web Application Security and vulnerabilities** Introduction to web applications security, threats and OWASP principles, OWASP top 10 web application vulnerabilities, introduction to secure design, web server: introduction a secure setup of apache, firewalling a server Browser: general concepts, functionalities, browsers war, configuration, and users tracking/profiling, browser security OWASP Privacy preserving: attacks to privacy, Tracking techniques, Advanced browser configuration, anonymity and onion routing (Tor). MIME & PGP, phishing, spamming & spoofing, DKIM, SPF, introduction to email forensics.	**8**
6	**Recent Trends in VAPT** Cloud-based VAPT, IoT Security Testing, Automated Vulnerability Scanning, Compliance-driven Assessments, Continuous VAPT	**4**
	Total	**39**

List of Laboratory Experiments: (Minimum any eight experiments)

Sr. No.	**Suggested Experiments**
1	To learn about hacking tools and skills
2	To study about foot printing and Reconnaissance
3	To study different types of vulnerability scanning and its types(network, port and vulnerability scanning)
4	Nmap and live scanning on ports and networks
5	Netcat usage on TCP/UDP ports
6	Wireshark basics and capturing data

7	NFS ,SMB ,SMTP enumeration
8	Nessus installation and configuration
9	Vulnerability scanning with Nessus
10	Web application assessment with nikto & burp suite
11	Vulnerability analysis with Metasploit framework
12	To learn & study about Sniffing & their tools

Any other experiment based on syllabus may be included, which would help the learner to understand topic/concept.

Books Recommended:

Text Books:

1. Pranav Joshi and Deepayan Chanda, Penetration Testing with Kali Linux: Learn Hands-on Penetration Testing Using a Process-Driven Framework, BPB Publication, 2021.
2. S. Oriyano and M. Solomon, Hacker Techniques, Tools, and Incident Handling, 3rd Edition, J B Learning, 2020.
3. M. Walker, CEH Certified Ethical Hacker All-in-One Exam Guide, Fourth Edition, 4th Edition, McGraw-Hill Education, 2019.
4. Chuck Easttom, Penetration Testing Fundamentals: A Hands-On Guide to Reliable Security Audits, Pearson Education, 2018

Reference Books:

1. Kali Linux Wireless Penetration Testing Beginner's Guide by Vivek Ramachandran, Cameron Buchanan, 2015 Packt Publishing
2. SQL Injection Attacks and Defense 1st Edition, by Justin Clarke-Salt, Syngress Publication
3. Mastering Modern Web Penetration Testing By Prakhar Prasad, October 2016 Packt Publishing
4. Kali Linux 2: Windows Penetration Testing, By Wolf Halton, Bo Weaver , June 2016, Packt Publishing
5. Practical Web Penetration Testing: Secure web applications using Burp Suite, Nmap, Metasploit, and more, Gus Khawaja,2018

Web resources:

1. OWASP (Open Web Application Security Project) - https://owasp.org/
2. NIST (National Institute of Standards and Technology) - https://www.nist.gov/
3. Penetration Testing Execution Standard (PTES) - http://www.pentest-standard.org/
4. SANS Institute - https://www.sans.org/
5. Metasploit Unleashed - https://www.metasploitunleashed.com/

6. CERT (Computer Emergency Response Team) - https://www.cert.org/

Online Courses: NPTEL / Swayam

1. Information Security: A Hands-On Approach: https://nptel.ac.in/courses/106/106/106106229/
2. Cyber Security : https://nptel.ac.in/courses/108/106/108106069/
3. Network Security and Cryptography: https://nptel.ac.in/courses/106/105/106105093/

Evaluation Scheme:

Semester End Examination (A):

Theory:

1. Question paper will be based on the entire syllabus summing up to 75 marks.
2. Total duration allotted for writing the paper is 3 hrs.

Laboratory:

1. Oral examinations will be based on the entire syllabus including the practical's performed during laboratory sessions.

Continuous Assessment (B):

Theory:

1. Two term tests of 25 marks each will be conducted during the semester out of which; one will be a compulsory term test (on minimum 02 Modules) and the other can either be a term test or an assignment on live problems or a course project.
2. Total duration allotted for writing each of the paper is 1 hr.
3. Average of the marks scored in both the two tests will be considered for final grading.

Laboratory: (Term work)

Term work shall consist of minimum 8 experiments and Mini project.

The distribution of marks for term work shall be as follows:

i. Laboratory work (Performance of Experiments): 15 Marks
ii. Journal documentation (Assignments): 5 marks
iii. Attendance(Theory + Practical):5 Marks

The final certification and acceptance of term work will be subject to satisfactory performance of laboratory work, and upon fulfilling minimum passing criteria in the term work.

Prepared by Checked by Head of the Department Principal

Program: B.Tech. CSE in IoT and Cyber Security with Blockchain Technology **T.Y. B.Tech.** **Semester: V**

Course: Web Application Development Laboratory (DJ19ICL506)

Prerequisite:

1. Basic Programming Skills
2. Knowledge of Internet and Networking

Objectives:

1. To orient students to Web Programming fundamental
2. To develop hands-on skills in building dynamic and interactive web applications using modern web development technologies and frameworks.
3. To enhance problem-solving abilities and encourage creativity and innovation in designing and implementing web applications
4. To Work collaboratively on web development projects to enhance teamwork, communication, and project management skills

Outcomes: On completion of the course, learner will be able to:

1. Design and develop responsive and user-friendly web applications.
2. Build dynamic and interactive web applications.
3. Design and Validate web applications for conformance to latest W3C markup and accessibility standards.
4. Explore new web development technologies and frameworks

Detailed Syllabus: (unit wise)		
Unit	**Description**	**Duration**
1	**Web Programming Fundamentals** Introduction to Web Programming, Installation of IDE, Introduction to basic structure of a website, Title, Script, Link & meta tags. Understanding of headings, paragraphs. Image and Anchor tags, Understanding Lists & Tables, Forms and Input tags, PHP connection code to db, Local server setup and uses, Inline and block elements, Ids and Classes concept, Working of web browser, XML introduction, HTTP protocol, Json introduction	**8**
2	**Static web page design –HTML, CSS and CSS3** HTML entities and semantic tags. HTML Media, Video, Audio, Plugins. HTML API's (Geolocation, Web Storage, SSE, etc)	**10**

	Concepts of CSS: Introduction to CSS, Inline, Internal and External CSS, Selectors, Developer tools in chrome, CSS Box model, margin, padding, fonts, colors, Borders, backgrounds, Float and clear, links, buttons Creating Navigation menu, display property, positions (absolute, relative, fixed & sticky), visibility, z-index, flexbox, web units, media queries, pseudo selectors, shadow properties, Introduction to animation and key frames, responsive properties, Introduction to bootstrap 4 & 5,	
3	**Client side scripting – JavaScript** Introduction to Javascript (Frontend & backend), writing in-browser javascript & developer console. Variables, Data types, Operators, String and String functions, scope, conditional statements, functions, loops, DOM library functions, Event Listeners, arrow functions.	
4	**NodeJs** NodeJs introduction and installation, First app, Asynchronous programming, Callback concept, Event loops, REPL, Event emitter, Networking module, Buffers, Streams, File system, Web module.serving HTML files using NodeJs, Node package manager, Basics of Express and Postman	**6**
5	**Introduction to Angular** Angular Development Environment, Basic Angular Component and Template, Data Binding and Event Handling, Fetching Data from APIs and Displaying using HTTP Client, Routing and Navigation, Forms, Form Validation, Authentication and Authorization, Testing Angular Components and Services, Implementing in Angular Applications	**6**
6	**Introduction to ReactJs and Advance React** Introduction and Installation, understanding JSX, Prop & Prop Types, Understanding State and Event Handling, TextUtils, Functional components-Refs, Use effects, Hooks, Flow architecture, Model-View Controller framework, Flux, Bundling the application. Webpack	**9**
	Total	**39**

List of Laboratory Experiments: (Minimum any ten experiments)

Sr. No.	Suggested Experiments
1	**XML:** a. Creating XML Documents and Validating XML Syntax b. Creating XML-based Web Services c. Converting XML to JSON and vice versa
2	**HTML, HTML5:** a. Creating a Basic Web Page Using HTML and HTML5 tags b. Incorporating Multimedia Elements with HTML5 (e.g., Audio, Video) c. Building a Navigation Menu using HTML5 Semantic Elements
3	**CSS:** a. Enhancing User Interfaces with CSS Transitions and Animations b. Creating Responsive Layouts with CSS Grid

4	**CSS3:** a. Design a responsive web page using media queries and CSS3 b. Implementing CSS3 Filters and Effects for Visual Enhancements
5	**Bootstrap:** a. Building a Responsive Layout with Bootstrap Grid System b. Styling Buttons and Forms using Bootstrap Components c. Implementing Bootstrap Dropdowns and Accordions for Content Organization
6	**JavaScript:** a. Creating Interactive Web Elements with JavaScript Event Handling b. Implementing Form Validation using JavaScript c. Building Dynamic Content with JavaScript DOM Manipulation
7	Program to design a calculator using JavaScript.
8	**NodeJs:** a. Setting up a Node.js Development Environment b. Creating and Running a Simple Node.js Server c. Building a RESTful API with Node.js and Express
9	Working with Databases in Node.js (e.g., MongoDB, MySQL)
10	**Postman:** a. Introduction to Postman and API Testing Basics b. Sending GET Requests and Handling Response Data in Postman c. Testing POST Requests and Data Validation with Postman d. Writing and Executing Test Scripts in Postman
11	**Angular:** a. Creating Dynamic and Responsive User Interfaces with Angular Directives b. Building Forms and Performing Form Validation in Angular c. Deploying an Angular Application to a Web Server
12	**ReactJs:** a. Setting up a React Development Environment b. Implementing Component State and Handling User Interactions in React c. Fetching Data from APIs and Displaying it in React d. Testing React Components and Hooks
13	**Advance React:** a. Building React Components with Flux Data Flow b. Implementing Model-View-Controller in React with State Management Libraries c. Implementing Controllers for Handling User Interactions in React MVC
14	**Webpack:** a. Setting up a Webpack Development Environment b. Configuring Webpack for Bundling JavaScript Modules c. Handling CSS and Style Assets with Webpack
15	Mini Project – Complete website development using client and server side technologies.

Any other experiment based on syllabus may be included, which would help the learner to understand topic/concept.

Books Recommended:

Text Books:

1. DT Editorial Services, “HTML5 Black Book”, 2nd Edition, Dreamtech Press, 2016.

2. Ben Frain, “Responsive Web Design with HTML5 and CSS3”, 2nd Edition, Packt Publishing, 2015.

3. Steve Suehring, “JavaScript Step by Step”, 3rd Edition, Pearson Education, 2013.

4. Stoyan Stefanov, “React Up Running Building Web Applications”, 1st Edition, O’Reilly Media Inc., 2016.

5. David Sklar, “Learning PHP 5”, 1st Edition, O’Reilly Media Inc., 2004.

Reference Books:

1. Benjamin LaGrone, “HTML5 and CSS3 Responsive Web Design Cookbook”, 1st Edition, Packt Publishing, 2013.

2. DT Editorial Services, “Web Technologies: Black Book”, 1st Edition, Dreamtech Press, 2018.

3. Christopher Schmitt, Kyle Simpson, “HTML5 Cookbook”, 1st Edition, O'Reilly Media Inc., 2011.

4. Uttam K. Roy, “Web Technologies”, 1st Edition, Oxford University Press, 2010.

5. Greg Sidelnikov, “React. Js Book: Learning React JavaScript Library from Scratch”, 1st Edition, Independently Published, 2017.

6. Luke Welling; Laura Thomson, “PHP and MySQL Web Development”, 5th Edition, Addison-Wesley Professional PTG, 2017.

Web resources:

1. https://www.coursera.org/learn/html-css-javascript-for-web-developers?action=enroll
2. https://reactjs.org/tutorial/tutorial.html
3. https://react-redux.js.org/introduction/quick-start
4. https://webpack.js.org/
5. https://developer.mozilla.org/en-US/
6. https://www.w3schools.com/
7. https://css-tricks.com/
8. https://www.smashingmagazine.com/

Online Courses:NPTEL/Swayam

1. Web Technologies - Prof. Soumya Kanti Ghosh , Course link: Web Technologies - NPTEL
2. Introduction to Modern Application Development - Prof. Soumya Kanti Ghosh, Course link: Introduction to Modern Application Development - NPTEL
3. Web Development with Django - Prof. Vimal Kumar, Course link: Web Development with Django - NPTEL
4. Web Development - Prof. Balaji Sampath, Course link: Web Development - NPTEL
5. Modern Web Applications with AngularJS - Prof. Sridhar Iyer, Course link: Modern Web Applications with AngularJS - NPTEL

Evaluation Scheme:

Practical and oral examination will be based on the entire syllabus including, the practical's performed during laboratory sessions and guided mini project covering the relevant concepts of web application development. This helps them to apply the knowledge gained during laboratory sessions to solve real time problems.

Laboratory: (Term work)

Term work shall consist of minimum 8 experiments and Mini project.

The distribution of marks for term work shall be as follows:

i. Laboratory work (Performance of Experiments): 10 Marks
ii. Mini project: 10 Marks
iii. Attendance : 5 marks

The final certification and acceptance of term work will be subject to satisfactory performance of laboratory work, and upon fulfilling minimum passing criteria in the term work.

Prepared by   Checked by   Head of the Department   Principal

Program: B.Tech. CSE in IoT and Cyber Security with Blockchain Technology **T.Y. B.Tech.** **Semester: V**

Course: Innovative Product Development III (DJ19ILL1)

Objectives:

1. To acquaint the students with the process of identifying the need (considering a societal requirement) and ensuring that a solution is found out to address the same by designing and developing an innovative product.
2. To familiarize the students with the process of designing and developing a product, while they work as part of a team.
3. To acquaint the students with the process of applying basic engineering fundamentals, so as to attempt at the design and development of a successful value added product.
4. To inculcate the basic concepts of entrepreneurship and the process of self-learning and research required to conceptualise and create a successful product.

Outcome:

Learner will be able to:

1. Identify the requirement for a product based on societal/research needs.
2. Apply knowledge and skills required to solve a societal need by conceptualising a product, especially while working in a team.
3. Use standard norms of engineering concepts/practices in the design and development of an innovative product.
4. Draw proper inferences through theoretical/ experimental/simulations and analyse the impact of the proposed method of design and development of the product.
5. Develop interpersonal skills, while working as a member of theteam or as theleader.
6. Demonstrate capabilities of self-learning as part of the team, leading to life-long learning, which could eventually prepare themselves to be successful entrepreneurs.
7. Demonstrate product/project management principles during the design and development work and also excel in written (Technical paper preparation) as well as oral communication.

Guidelines for the proposed product design and development:

- Students shall form a team of 3 to 4 students (max allowed: 5-6 in extraordinary cases, subject to the approval of the department review committee and the Head of the department).
- Students should carry out a survey and identify the need, which shall be converted into conceptualization of a product, in consultation with the faculty supervisor/head of department/internal committee of faculty members.
- Students in the team shall understand the effective need for product development and accordingly select the best possible design in consultation with the faculty supervisor.
- Students shall convert the best design solution into a working model, using various components drawn from their domain as well as related interdisciplinary areas.
- Faculty supervisor may provide inputs to students during the entire span of the activity, spread over 2 semesters, wherein the main focus shall be on self-learning.

- A record in the form of an activity log-book is to be prepared by each team, wherein the team can record weekly progress of work. The guide/supervisor should verify the recorded notes/comments and approve the same on a weekly basis.
- The design solution is to be validated with proper justification and the report is to be compiled in a standard format and submitted to the department. Efforts are to be made by the students to try and publish a technical paper, either in the institute journal, “Techno Focus: Journal for Budding Engineers” or at a suitable publication, approved by the department research committee/ Head of the department.
- The focus should be on self-learning, capability to design and innovate new products as well as on developing the ability to address societal problems. Advancement of entrepreneurial capabilities and quality development of the students through the year long course should ensure that the design and development of a product of appropriate level and quality is carried out, spread over two semesters, i.e. during the semesters V and VI.

Guidelines for Assessment of the work:

- The review/ progress monitoring committee shall be constituted by the Head of the Department. The progress of design and development of the product is to be evaluated on a continuous basis, holding a minimum of two reviews in each semester.
- In the continuous assessment, focus shall also be on each individual student’s contribution tothe team activity, their understanding and involvement as well as responses to the questions being raised at all points in time.
- Distribution of term work marks during the subsequent semester shall be as given below:
  - Marks awarded by the supervisor based on log-book 10
  - Marks awarded by review committee 10
  - Quality of the write-up 05

In the last review of the semester VI, the term work marks will be awarded as follows.

- Marks awarded by the supervisor (Considering technical paper writing) 15
- Marks awarded by the review committee 10

Review/progress monitoring committee may consider the following points during the assessment.

- In the semester V, the entire design proposal shall be ready, including components/system selection as well as the cost analysis. Two reviews will be conducted based on the presentation given by the student’s team.
- First shall be for finalisation of the product selected.

Second shall be on finalisation of the proposed design of the product.

- In the semester VI, the expected work shall be procurement of components/systems, building of the working prototype, testing and validation of the results based on work completed in semester III.
- First review is based on readiness of building the working prototype.
- Second review shall be based on a presentation as well as the demonstration of the working model, during the last month of semester IV. This review will also look at the readiness of the proposed technical paper presentation of the team.

The overall work done by the team shall be assessed based on the following criteria;

1. Quality of survey/ need identification of the product.
2. Clarity of Problem definition (design and development) based on need.
3. Innovativeness in the proposed design.
4. Feasibility of the proposed design and selection of the best solution.
5. Cost effectiveness of the product.

6. Societal impact of the product.
7. Functioning of the working model as per stated requirements.
8. Effective use of standard engineering norms.
9. Contribution of each individual as a member or the team leader.
10. Clarity on the write-up and the technical paper prepared.

- The semester reviews (V and VI) may be based on relevant points listed above, as applicable.

Guidelines for Assessment of Semester Reviews:

- The write-up should be prepared as per the guidelines given by the department.
- The design and the development of the product shall be assessed through a presentation and demonstration of the working model by the student team to a panel of Internal and External Examiners, preferably from industry or any research organisations having an experience of more than five years, approved by the Head of the Institution. The presence of the external examiner is desirable only for the 2nd presentation in semester IV.Students are compulsorily required to present the outline of the technical paper prepared by them during the final review in semester VI