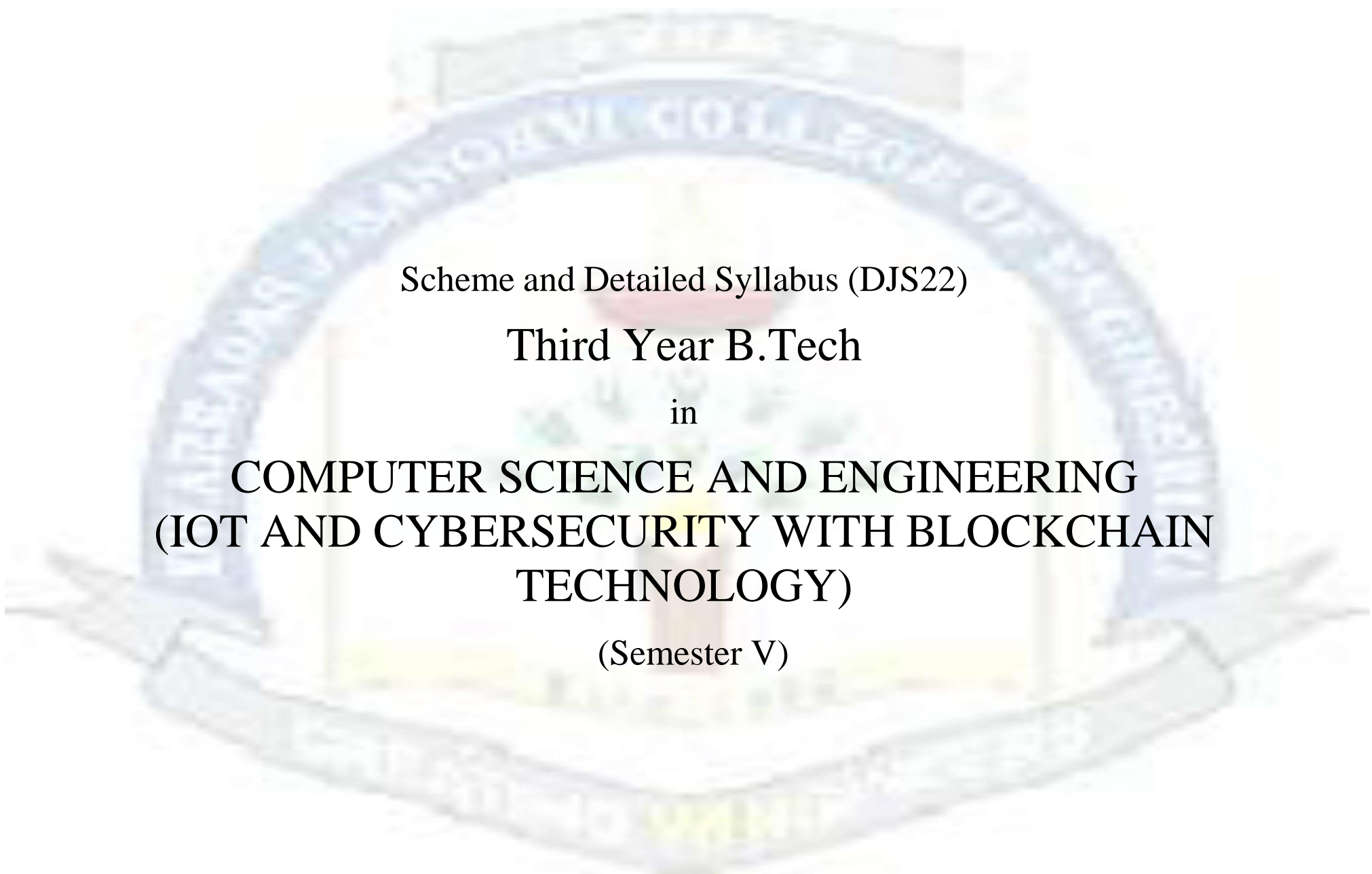


Scheme for Third Year Undergraduate Program in CSE(ICB) (Autonomous) (DJS22Scheme)
SEMESTER V



Scheme and Detailed Syllabus (DJS22)
Third Year B.Tech
in
**COMPUTER SCIENCE AND ENGINEERING
(IOT AND CYBERSECURITY WITH BLOCKCHAIN
TECHNOLOGY)**
(Semester V)

**Scheme for Third Year Undergraduate Program in CSE(ICB) (Autonomous) (DJS22Scheme)
SEMESTER V**

Sr	Course Code	Course	Teaching Scheme (hrs.)			Continuous Assessment (A)			Semester End Assessment (B)					Aggregate (A+B)
			Th	P/T/L	Credits	Th	T/W	Total CA (A)	Th	O	P	O & P	Total SEA(B)	
1	DJS22ICC501	Network Security	3	-	3	35	--	35	65	--	--	--	65	100
	DJS22ICL501	Network Security Laboratory	--	2	1	--	25	25	--	25	--	--	25	50
2	DJS22ICC502	Introduction to Block chain Technology	3	--	3	35	--	35	65	--	--	--	65	100
	DJS22ICL502	Introduction to Block chain Technology Laboratory	--	2	1	--	25	25	--	25	--	-	25	50
3	DJS22ICC503	Artificial Intelligence	3	--	3	35	--	35	65	--	--	--	65	100
	DJS22ICL503	Artificial Intelligence Laboratory	--	2	1	--	25	25	--	--	--	25	25	50
4 @ Any 1 Core Elective	DJS22ICC5011	Digital forensics	3	--	3	35	--	35	65	--	--	--	65	100
	DJS22ICL5011	Digital forensics Laboratory	--	2	1	--	25	25	--	25	--	--	25	50
	DJS22ICC5012	Vulnerability Assessment & Penetration Testing	3	--	3	35	--	35	65	--	--	--	65	100
	DJS22ICL5012	Vulnerability Assessment & Penetration Testing Laboratory	--	2	1	--	25	25	--	25	--	-	25	50
	DJS22ICC5013	IoT Architecture and Protocols	3	--	3	35	--	35	65	--	--	--	65	100
	DJS22ICL5013	IoT Architecture and Protocols Lab	--	2	1	--	25	25	--	25	--	--	25	50
5	DJS22ICL504	UI/UX Laboratory	--	4	2	--	25	25	--	--	--	25	25	50
6	DJS22A3	Environmental Studies	1	--	--	--	--	--	--	--	--	--	--	--
7	DJS22ILLL1	Innovative Product Development III	--	2	1	--	25	25	--	25	--	--	25	50
		Total	13	14	19	140	150	290	260	100	--	50	410	700

Prepared by

Checked by

Head of the Department

Vice Principal

Principal



Program: Third Year B.Tech. in in IoT and Cyber Security with Blockchain Technology							Semester : V			
Course : Network Security							Course Code: DJS22ICC501			
Course: Network Security Laboratory							Course Code: DJS22ICL501			
Teaching Scheme (Hours / week)				Evaluation Scheme						
				Semester End Examination Marks (A)			Continuous Assessment Marks (B)			Total marks (A+ B)
Lectures	Practical	Tutorial	Total Credits	Theory			Term Test1	Term Test2	Total Term Test	
				65			20	15	35	100
				Laboratory Examination			Term work		Total Term work	50
3	2	--	4	Oral	Practical	Oral & Practical	Laboratory Work	Tutorial / Mini project / presentation/ Journal		
				25	--	--	15	10	25	

Pre-requisite: Knowledge of Computer Network, Applied Cryptography.

Course Objectives: The objective of the course is.

1. To acquaint students with network threats, attacks, and mitigation techniques.
2. To make students learn about the security of Network layer, Transport layer and Application layer.
3. To provide knowledge about the wireless network security, entity authentication as well as network access control.

Course Outcomes: On successful completion of this course, student should be able to:

1. Discuss the various network attacks and suggest their counter measures.
2. Get the knowledge of IPsec Security, working of Internet key exchange protocol along with its uses in IPsec.
3. Understand the working and security of wireless networks.
4. Gain the knowledge of Transport layer security.
5. Understand the working of E-mail security protocol.
6. Identify the security significance of entity Authentication as well as Network access control.



Network Security (DJS22ICC501)		
Unit	Description	Duration
1	Introduction to network Security Need of network Security, Threats to network security, Networks attacks, Mitigation to network attacks.	04
2	Network Layer Security IP Security, Transport Mode, Tunnel Mode, Comparison, Authentication Header (AH), Encapsulating Security Payload (ESP), IPV4 and IPV6, Security Association, Security Policy, Internet Key Exchange(IKE), IKE Phases, Internet Security Association and Key Management Protocol (ISAKMP) .	08
3	Wireless Network Security Wireless Security, Mobile Device Security, IEE 802.11 wireless LAN Overview, IEE 802.11i wireless LAN Security.	04
4	Transport level Security Web Security consideration, Secured Socket Layer, Transport level Security, HTTPS, Secured Shell [SSH].	08
5	Application Layer Security E-mail Architecture, E-mail Security, PGP, Key Rings, PGP Algorithms, PGP Certificate, Trust Model in PGP, Key Recreation, PGP Pocket, PGP merge, Multipurpose Internet Mail Extension (MIME), S/MIME .	08
6	Entity Architecture and Network Access Controls Entity Authentication, Network Access Control, Extensible Authentication Protocol, IEE 802.1x port base network access control, Network Security Firewall, IDS.	07
	Total	39



List of Laboratory Experiments: (Minimum any eight experiments)	
Exp.	Suggested experiments
1	Study and Implementation of Wireshark tools.
2	Implementation of VLAN (Large 2-Security)
3	a. Implementation of IPsec protocol in Tunnel Mode. b. Implementation of IPsec protocol in Transport Mode.
4	Implementation of secure wireless LAN for homes and enterprises N/W.
5	Configuration of SSL/SSH in secure client/server model.
6	Implementation of Firewall -Iptable.
7	Implementation of IPS-Snort.
8	Implementation of PGP Tool.
9	Encryption & Decryption data using open SSL.
10	Implementation of NMAP-port scanning tool.

Any other experiment based on syllabus may be included, which would help the learner to understand topic/concept .A minimum of 8 experiments from the above suggested list or any other experiment based on syllabus will be included, which would help the learner to apply the concept learnt.

Books Recommended:

Textbooks:

1. Cryptography and Network Security by Behrouz A. Forouzan and Debdeep Mukhopadhyay, Edition 3, Tata McGraw Hill, 2017
2. Cryptography and Network Security: Principal and Practice By William Stallings, 7th edition, Pearson, 2018

Reference Books:

1. Cryptography and Network Security by Atul Kahale 4th edition, Tata McGraw Hill,2013
2. Network Security Essentials: Applications and Standards by William Stallings,6th Edition, Pearson, 2017



Evaluation Scheme:

Semester End Examination (A):

Theory:

1. Question paper will be based on the entire syllabus summing up to 65 marks.
2. Total duration allotted for writing the paper is 2 hrs.

Laboratory:

1. Oral & Practical examination will be based on the entire syllabus including the practical performed during laboratory sessions.

Continuous Assessment (B):

Theory:

1. One term test of 20 marks and one term test/presentation/assignment/course project / group discussion/ any other of 15 marks will be conducted during the semester.
2. Total duration allotted for writing each of the paper is 1 hr.

Laboratory: (Term work)

Term work shall consist of a minimum of 10 experiments and a minimum of 2 assignments.

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

- i. Laboratory work (Performance of Experiments):15 Marks
- ii. Journal documentation and Assignment: 10 marks

The allocation of marks for laboratory work and tutorials shall adhere to the pre-established rubric parameters.

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 Vice Principal Principal



Program: Third Year B.Tech. in in IoT and Cyber Security with Blockchain Technology					Semester : V				
Course : Introduction to Blockchain Technology					Course Code: (DJS22ICC502)				
Course Laboratory: Introduction to Blockchain Technology Laboratory					Course Code: (DJS22ICL502)				
Teaching Scheme (Hours / week)				Evaluation Scheme					
				Semester End Examination Marks (A)			Continuous Assessment Marks (B)		
Lectures	Practical	Tutorial	Total Credits	Theory			Term Test1	Term Test2	Total Term Test
				65			20	15	35
				Laboratory Examination			Term work		Total Term work
3	2	--	4	Oral	Practical	Oral & Practical	Laboratory Work	Tutorial / Mini project / presentation/ Journal	
				25	--	--	15	10	

Prerequisite:

1. Networking Fundamentals
2. Applied Cryptography

Objectives: The objective of the course is.

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. Implement cryptographic primitives useful for Blockchain
3. Understand bitcoin cryptocurrency networks and consensus mechanisms.
4. Design smart contracts for various blockchain applications
5. Use various tools for Blockchain implementation.
6. Analyze the recent trends 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 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.	10
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 eight 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	To perform file storage using Inter-Planetary File System (IPFS).
12	Mini Project (Students with group of 3/4 will develop application based on Blockchain Technology along with report).

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 65 marks.
2. Total duration allotted for writing the paper is 2 hrs.

Laboratory:

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



Continuous Assessment (B):

Theory:

1. One term test of 20 marks and one term test of 15 marks will be conducted during the semester.
2. Total duration allotted for writing the paper is 1 hr.

Laboratory: (Term work)

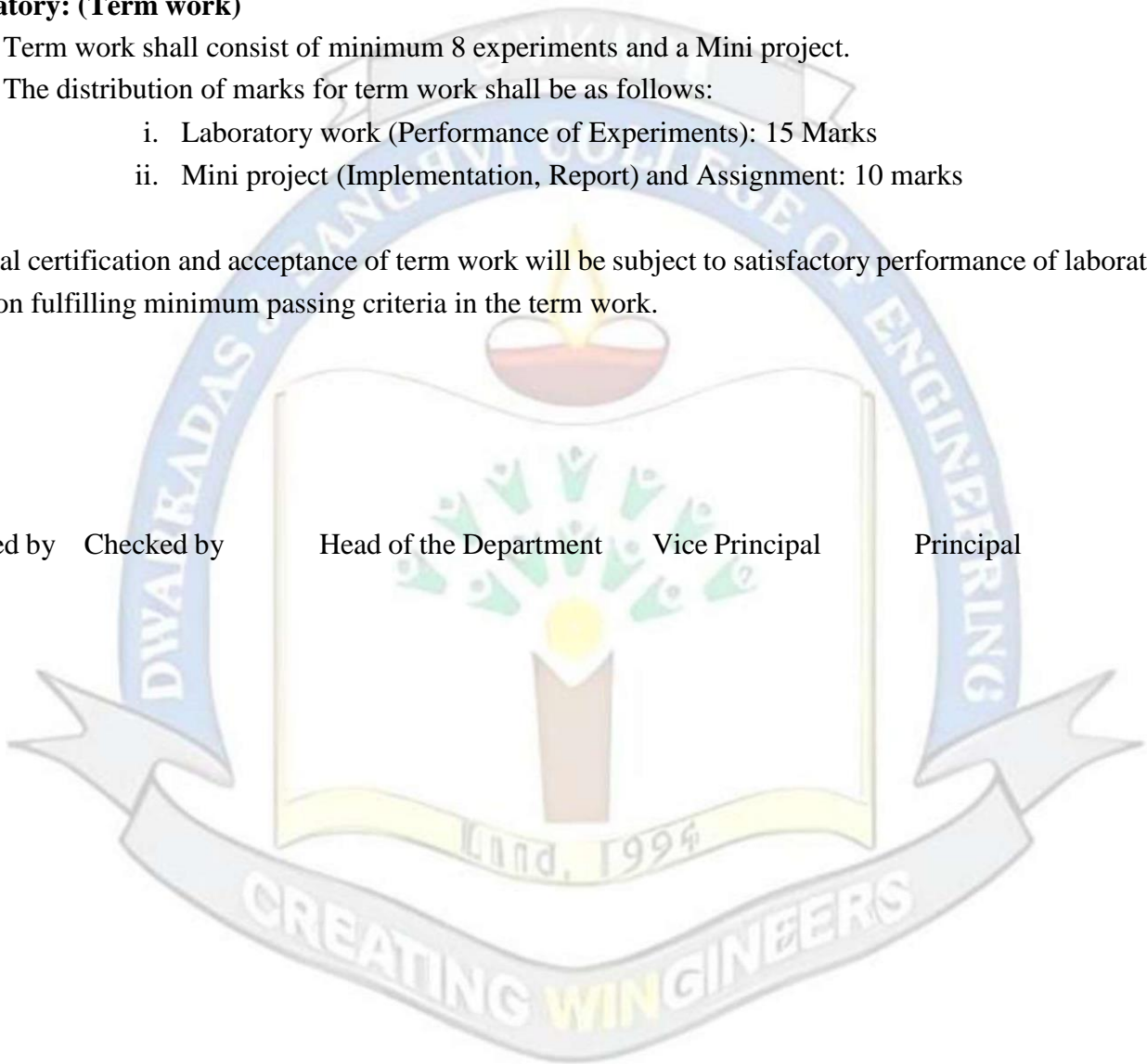
Term work shall consist of minimum 8 experiments and a Mini project.

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

- i. Laboratory work (Performance of Experiments): 15 Marks
- ii. Mini project (Implementation, Report) and Assignment: 10 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 _____ Vice Principal _____ Principal _____





Program: B.Tech. in IoT and Cyber Security with Blockchain Technology					Semester : V					
Course : Artificial Intelligence					Course Code: (DJ19ICC503)					
Course Laboratory: Artificial Intelligence Laboratory					Course Code: (DJ19ICL503)					
Teaching Scheme (Hours / week)				Evaluation Scheme						
				Semester End Examination Marks (A)			Continuous Assessment Marks (B)			Total marks (A+ B)
Lectures	Practical	Tutorial	Total Credits	Theory			Term Test1	Term Test2	Total Term Test	100
				65			20	15	35	
				Laboratory Examination			Term work		Total Term work	50
				Oral	Practical	Oral & Practical	Laboratory Work	Tutorial / Mini project / presentation/ Journal		
3	2	--	4	--	--	25	15	10	25	

Pre-requisite:

1. Basic programming languages
2. Data Structures

Objectives: The objective of the course is.

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 the scope of Generative Networks in AI.

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. Analyze various AI approaches to knowledge-intensive problem solving, reasoning and planning.
4. Understand planning and various types of planning.
5. Acquire basic knowledge of Probabilistic Models.
6. Analyze the working and architecture for Generative Networks.



Detailed Syllabus: (unit wise)		
Unit	Description	Duration
1	<p>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</p> <p>Intelligent Agents: Agents and Environments, The concept of rationality, The nature of environment, The structure of Agents, Types of Agents, Learning Agent.</p>	06
2	<p>Problem solving: Solving Problem by Searching: Problem Solving Agent, Formulating Problems, Example Problems.</p> <p>Uninformed Search Methods: Breadth First Search (BFS), Depth First Search (DFS), Depth Limited Search, Depth First Iterative Deepening (DFID)</p> <p>Informed Search Methods: Greedy Best first Search, A* Search</p> <p>Stochastic Local Search Algorithms and Optimization Problems: Hill climbing search, Simulated Annealing, Genetic algorithms, Ant Colony Optimization.</p> <p>Adversarial Search: Game Theory, Algorithm Minimax, Alpha-Beta Pruning.</p>	12
3	<p>Knowledge and Reasoning: Knowledge based Agents, The WUMPUS World, Inference in FOL, Forward chaining, Backward chaining, Knowledge Engineering in First-Order Logic, Unification, Resolution.</p>	07
4	<p>Planning: The planning problem, Planning with State Space Search, STRIPS, Goal Stack Planning, Planning graphs, Partial order planning, Hierarchical Planning.</p>	06
5	<p>Expert System: Introduction, Phases in building Expert Systems, ES Architecture, Case Study on MYCIN Rule based system.</p>	04
6	<p>Generative AI Introduction, Overview of generative models and their importance in AI, Fundamentals of Probability theory and generative modeling, Introduction to GANs, VAEs and other generative models. Significance of generative models, Challenges with generative models.</p>	04
Total		39

List of Laboratory Experiments:

Sr. No.	Title of Experiments (Minimum any eight using Python)
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	Design and implement a Hidden Markov Models for outcome prediction.
12	Implementation of GAN algorithm.
13	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. Foster, D., 2022. Generative deep learning. " O'Reilly Media, Inc."
5. Koller, D. and Friedman, N., 2009. Probabilistic graphical models: principles and techniques. MIT press

Reference Books

1. Elaine Rich and Kevin Knight "Artificial Intelligence" Third Edition,2017.
2. Patrick Henry Winston, "Artificial Intelligence", Addison-Wesley, Third Edition.1992
3. [Lavika Goel](#) , "Artificial Intelligence concept and applications", WILEY Publishers, 2021
4. N.P.Padhy , "Artificial Intelligence and Intelligent Systems", Oxford University Press. 2005.
5. 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/>



Shri Vile Parle Kelyani Mandal's

DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING

(Autonomous College Affiliated to the University of Mumbai)

NAAC Accredited with "A" Grade (CGPA : 3.18)



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 will be based on the entire syllabus summing up to 65 marks.
2. Total duration allotted for writing the paper is 2 hrs.

Laboratory:

1. Oral examination will be based on the entire syllabus.

Continuous Assessment (B):

Theory:

1. One term test of 20 marks and one term test/presentation/assignment/course project / Group discussion/ any other of 15 marks will be conducted during the semester.
2. Total duration allotted for writing each of the paper is 1 hr.

Laboratory: (Term work)

Term work shall consist of at least 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): 10 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

Vice Principal & Head of the Department

Principal



Program: B.Tech. in in IoT and Cyber Security with Blockchain Technology				Semester : V					
Course : Digital forensics				Course Code: (DJS22ICC5011)					
Course: Digital forensics Laboratory				Course Code: (DJS22ICL5011)					
Teaching Scheme (Hours / week)				Evaluation Scheme				Total marks (A+ B)	
				Semester End Examination Marks (A)			Continuous Assessment Marks (B)		
Lectures	Practical	Tutorial	Total Credits	Theory			Term Test1	Term Test2	Total Term Test
				65			20	15	35
				Laboratory Examination			Term work		Total Term work
3	2	--	4	Oral	Practical	Oral & Practical	Laboratory Work	Tutorial / Mini project / presentation/ Journal	
				--	--	25	15	10	25

Prerequisite: Cryptography and Security, Computer Networks

Course Objectives: The objective of the course is.

1. To understand underlying principles and many of the techniques associated with the digital forensic practices and cyber crime
2. To explore practical knowledge about ethical hacking Methodology.
3. To learn the importance of evidence handling and storage for various devices
4. To develop an excellent understanding of current cyber security issues (Computer Security Incident) and analyzed the ways that exploits in securities.
5. To explore intrusion detection systems (IDS), technical exploits, router vulnerabilities,
6. To apply digital forensic knowledge to use computer forensic tools and investigation report writing.

Course Outcomes: Student will able to:

1. Define the concept of ethical hacking and its associated applications in Information Communication Technology (ICT) world.
2. Underline the need of digital forensic and role of digital evidences.
3. Explain the methodology of incident response and various security issues in ICT world, and identify digital forensic tools for data collection.
4. Recognize the importance of digital forensic duplication and various tools for analysis to achieve adequate perspectives of digital forensic investigation in various applications or devices like Windows/Unix system.
5. Apply forensic tools and techniques for data acquisition, imaging, and analysis to ensure integrity and authenticity of evidence.
6. Communicate forensic findings effectively through detailed network forensic reports, including analysis methodology, findings, and recommendations.



Detailed Syllabus: (unit wise)		
Unit	Description	Duration
1	Introduction to Ethical Hacking: Introduction to Ethical Hacking. Hacker Classifications: The Hats. Phases of Hacking. Introduction to footprinting, footprinting tools. Scanning methodology and tools. Enumeration techniques and enumeration tools.	4
2	Digital Forensics and Incident Response: Introduction to Digital Forensics and Digital Evidence, The Need for Digital Forensics, Types of Digital Forensics, Digital Forensics Life Cycle. Incident and Initial Response: Introduction to Computer Security Incident, Goals of Incident response, Incident Response Methodology, Initial Response, Formulating Response Strategy. Self-learning Topics: New Challenges of Digital Forensic Investigations	7
3	Forensic Duplication and Acquisition: Forensic Duplication: Introduction to Forensic Duplication, Types of Forensic Duplicates, Introduction to Forensic Duplication Tools. Data 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).	7
4	Forensic Investigation and Analysis: Investigating Registry Files, Investigating Log Files, Data Carving (Bulk Extractor), Introduction to Forensic Analysis, Live Forensic Analysis, Forensic Analysis of acquired data in Linux, Forensic Analysis of acquired data in Windows.	7
5	Evidence Handling and Forensic Reporting: Evidence Handling: Faraday's Bag, Characteristics of an Evidence, Types of Evidence, Evidence Handling Methodology, Chain of Custody. Forensic Reporting: Goals of a Report, Layout of an Investigative Report, Guidelines for writing a report, Sample Forensic Report.	7
6	Network Forensics: Introduction to Intrusion Detection systems, Types of IDS Understanding Network intrusion and attacks , Analyzing Network Traffic, Collecting Network based evidence, Evidence Handling. Investigating Routers, Handling Router Table Manipulation Incidents, Using Routers as Response Tools	7
	Total	39



List of experiments

Sr. No	Experiment
1	Analysis of forensic images using open source tools. • FTK Imager • Autopsy
2	Explore forensics tools in kali linux for acquiring, analyzing and duplicating data.
3	Performing RAM Forensic to analyze memory images to find traces of an attack. • Capturing RAM Using the DumpIt Tool • Volatility tool
4	Network forensics using Network Miner.
5	Windows Recycle Bin Forensics.
6	Data Carving using open source tools • Foremost • Scalpel • Jpegcarver .
7	USB Device Forensics using • USBDeview • USB Detective
8	Web Browser Forensics using DB Browser for SQLite
9	Generate a Timeline Report Using Autopsy
10	Email Analysis.
11	Performing penetration testing using Metasploit - kali Linux.
12	Case Study

Text Books:

1. EC- Council “Ethical Hacking and Countermeasures Attack Phases”, Cengage Learning, 2016
2. Computer Security Principles and Practice, William Stallings, Sixth Edition, Pearson Education 2018
3. Build your own Security Lab, Michael Gregg, Wiley India 2017

References:

1. Kevin Smith, “Hacking How to Hack - The ultimate Hacking Guide”, Hacking Intelligence 2018
2. Kevin Beaver, “Hacking for dummies” Wiley publication 2022
3. Incident Response & Computer Forensics by Kevin Mandia, Chris Prosise, Wiley 5th edition 2021
4. Digital Forensics by Nilakshi Jain & Kalbande, Wiley 2022.

Online References:

1. <https://freevidelectures.com/course/4070/nptel-ethical-hacking>
2. <https://owasp.org/www-project-top-ten/>
3. <https://www.computersecuritystudent.com/>
4. <http://www.opentechinfo.com/learn-use-kali-linux/>
5. <https://pentesterlab.com>
6. <https://www.exploit-db.com/google-hacking-database> Evaluation Scheme



Semester End Examination (A):

Theory:

3. Question paper will be based on the entire syllabus summing up to 65 marks.
4. Total duration allotted for writing the paper is 2 hrs.

Laboratory:

- 1.Oral & Practical examination will be based on the entire syllabus including the practical performed during laboratory sessions.

Continuous Assessment (B):

Theory:

- 1.One term test of 20 marks and one term test/presentation/assignment/course project /group discussion/ any other of 15 marks will be conducted during the semester.
2. Total duration allotted for writing each of the paper is 1 hr.

Laboratory: (Term work)

Term work shall consist of a minimum of 10 experiments and a minimum of 2 assignments.
The distribution of marks for term work shall be as follows:

- i. Laboratory work (Performance of Experiments):15 Marks
- ii. Journal documentation and Assignment: 10 marks

The allocation of marks for laboratory work and tutorials shall adhere to the pre-established rubric parameters.

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 Vice Principal Principal



Program: Second Year B.Tech. in in IoT and Cyber Security with Blockchain Technology					Semester : V					
Course : Vulnerability Assessment & Penetration Testing					Course Code: (DJS22ICC5013)					
Course Laboratory: Vulnerability Assessment & Penetration Testing Laboratory					Course Code: (DJS22ICL5013)					
Teaching Scheme (Hours / week)					Evaluation Scheme					
					Semester End Examination Marks (A)			Continuous Assessment Marks (B)		Total marks (A+ B)
Lectures	Practical	Tutorial	Total Credits	Theory			Term Test1	Term Test2	Total Term Test	
				65			20	15	35	100
					Laboratory Examination			Term work		Total
				Oral	Practical	Oral & Practical	Laboratory Work	Tutorial / Mini project / presentation/ Journal	Term work	50
3	2	--	4	25	--	--	15	10	25	

Prerequisite:

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

Objectives: The objective of the course is.

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.

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. Utilize exploit development frameworks and tools.
5. Analyze the impact of web application vulnerabilities.
6. Aware of the various ways through which hacker's 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, 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), 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 experiments

Sr. No	Experiment
1	To learn about different hacking tools and skills.
2	To study about foot printing tools and Reconnaissance.
3	To study different types of vulnerability scanning and its types(network, port and vulnerability scanning).
4	Nmap tool for 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 using Nessus.
10	Web application assessment with nikto & burp suite.
11	Vulnerability analysis with Metasploit framework.
12	To learn & study about Sniffing & their tools.

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:

Theory:

1. Question paper will be based on the entire syllabus summing up to 65 marks.
2. Total duration allotted for writing the paper is 2 hrs.

Laboratory:

1. Practical examination will be based on the entire syllabus including the practical performed during laboratory sessions.

Continuous Assessment (B):

Theory:

1. One term test of 20 marks and one term test/presentation/assignment/course project / group discussion/ any other of 15 marks will be conducted during the semester.
2. Total duration allotted for writing each of the paper is 1 hr.

Laboratory: (Term work)

Term work shall consist of a minimum of 8 experiments and a minimum of 2 assignments.

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

- i. Laboratory work (Performance of Experiments): 15 Marks
- ii. Journal documentation and Assignment: 10 marks

The allocation of marks for laboratory work and tutorials shall adhere to the pre-established rubric parameters.

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: Third Year B.Tech. in in IoT and Cyber Security with Blockchain Technology					Semester : V					
Course : IoT Architecture and Protocols					Course Code:(DJS22ICC5013)					
Course Laboratory: IoT Architecture and Protocols Laboratory					Course Code: (DJS22ICCL5013)					
Teaching Scheme (Hours / week)				Evaluation Scheme						Total marks (A+ B)
				Semester End Examination Marks (A)			Continuous Assessment Marks (B)			
Lectures	Practical	Tutorial	Total Credits	Theory		Term Test1	Term Test2	Total Term Test	100	
				65	20	15	35			
3	2	--	4	Laboratory Examination		Term work		Total Term work	50	
				Oral	Practical	Oral & Practical	Laboratory Work	Tutorial / Mini project / presentation/ Journal		25
				--	--	25	15	10	25	

Prerequisite:

1. Network Fundamentals
2. Operating Systems

Objectives: The objective of the course is.

1. To understand IoT Characteristics and Conceptual Framework.
2. To comprehend network architecture and design of IoT
3. To understand smart objects in IoT.
4. To correlate the connection of smart objects and IoT access technologies.
5. To explore network layer and application layer protocols for IoT.
6. To explore IoT security aspect

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

1. Describe the IoT Characteristics and Conceptual Framework.
2. Differentiate between the levels of the IoT architectures.
3. Interpret sensor network and its components.
4. Analyze the IoT access technologies.
5. Illustrate various protocols at network layer and application layer for IoT.
6. Analyze and evaluate security issues in IoT and risk analysis structure.



Detailed Syllabus: (unit wise)		
Unit	Description	Duration
1	Introduction to IoT Introduction to IoT- Defining IoT, Characteristics of IoT, Conceptual Framework of IoT, Physical design of IoT, Logical design of IoT, Functional blocks of IoT, Communication models & APIs, Basics of networking Communication protocol, wireless sensor networks. Convergence of IT and OT , IoT Challenges, IoT protocol vs Web Protocol stack.	6
2	IoT Network Architecture and Design Drivers Behind New Network Architectures : Scale,Security,Constrained Devices and Networks ,Data,Legacy Device Support , Architecture : The IoT World Forum (IoTWF) Standardized Architecture :Layer 1-7, IT and OT Responsibilities in the IoT Reference Model, Additional IoT Reference Models, A Simplified IoT Architecture, The Core IoT Functional Stack ::Layer 1-3 , Smart Services and IoT Data Management.	8
3	Smart Objects IoT: Sensors, Actuators, and Smart Objects, Attributes of Sensors, Actuators, Micro-Electro-Mechanical Systems (MEMS) Smart Objects: A Definition, Trends in Smart Objects, Sensor Networks, Wireless Sensor Networks (WSNs), Communication Protocols for WSN, RFID, NFC.	5
4	Connecting Smart Objects Communications Criteria: Range, Frequency Bands, Power Consumption, Topology, Constrained Devices, Constrained-Node Networks, Data Rate and Throughput, Latency and Determinism, Overhead and Payload. IoT Access Technologies : Standardization and Alliances , Physical Layer , MAC Layer , Topology ,Security and Conclusion of IEEE 802.15.4 , IEEE 802.15.4g and 802.15.4e ,IEEE 1901.2a ,IEEE 802.11ah , LoRaWAN, and NB-IoT and Other LTE Variations , LTE Cat 0 , LTE-M, NB-IoT.	6
5	IoT Network Layer and Application protocols The Business Case for IP , The Key Advantages of Internet Protocol ,Adoption or Adaptation of the Internet Protocol ,The Need for Optimization ,Constrained Nodes , Constrained Networks IP Versions , Optimizing IP for IoT .RPL , Objective Function Rank, RPL Headers ,Metrics , Authentication and Encryption on Constrained Nodes , ACE , DICE, Profiles and Compliances, Internet Protocol for Smart Objects Alliance, The Transport Layer, IoT Application Transport Methods, Generic Web-Based Protocols.	7



6	<p>Securing IoT</p> <p>A Brief History of OT Security Common Challenges in OT Security : Erosion of Network Architecture, Pervasive Legacy Systems, Insecure Operational Protocols , Device Insecurity</p> <p>Security Knowledge: IT and OT Security Practices and Systems Vary, The Purdue Model for Control Hierarchy, OT Network Characteristics Impacting Security.</p> <p>Security Priorities: CIA, Security Focus Formal Risk Analysis Structures: OCTAVE and FAIR, FAIR. The Phased Application of Security in an Operational Environment , Secured Network Infrastructure and Assets, Deploying Dedicated Security Appliances, Higher-Order Policy Convergence and Network Monitoring.</p>	7
	Total	39

List of experiments

Sr. No	Experiment
1	To study and implement interfacing of different IoT sensors with Raspberry Pi pico/Arduino/ModeMCU.
2	To study and implement interfacing of actuators based on the data collected using IoT sensors. (like led switch ON/OFF, stepper motor)
3	To study and demonstrate Contiki OS for RPL (like Create 2 border router and 10 REST clients, Access border router from other network (Simulator))
4	To study and demonstrate working of 6LoWPAN in Contiki OS (simulator)
5	Write a program on Raspberry Pi to push and retrieve the data from cloud like thingspeak/thingsboard/AWS/ Azure etc
6	To study and implement IoT Data processing using Pandas.
7	Write a program on Arduino / Raspberry Pi subscribe to MQTT broker for temperature data and print it.
8	Write a program to create TCP Server on Arduino/Raspberry Pi and respond with humidity data to TCP client when Requested.
9	Write a program for ESP8266 DHT11/DHT22 Temperature and Humidity Web Server with Arduino IDE.
10	Write a program to Control ESP8266 From Anywhere in the World.
11	Write a program for Arduino / Raspberry Pi Publishing MQTT Messages to ESP8266.
12	Write a program to collect data from sensor encrypt data send it to receiver (server) and decrypt is at receiving end Arduino/Raspberry Pi/ Contiki OS (simulator)



Books Recommended:

Text Books:

1. Arsheep Bahga (Author), Vijay Madiseti, Internet Of Things: A Hands-On Approach Paperback, Universities Press, Reprint 2020
2. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry, IoT Fundamentals Networking Technologies, Protocols, and Use Cases for the Internet of Things CISCO. 2020

Reference Books:

1. Pethuru Raj, Anupama C. Raman, The Internet of Things: Enabling Technologies, Platforms, and Use Cases by , CRC Press. 2017
2. Raj Kamal, Internet of Things, Architecture and Design Principles, McGraw Hill Education, Reprint 2018.
3. Perry Lea, Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security, Packt Publications, Reprint 2018.
4. Amita Kapoor, Sheng-Lung Peng, "Hands on Artificial intelligence for IoT", 1st Edition, Packt Publishing, 2019.

Web resources:

1. <https://owasp.org/www-project-internet-of-things/>

Online Courses: NPTEL / Swayam

1. NPTEL: Sudip Misra, IIT Khargpur, Introduction to IoT: Part-1, <https://nptel.ac.in/courses/106/105/106105166/>
2. NPTEL: Prof. Prabhakar, IISc Bangalore, Design for Internet of Things, https://onlinecourses.nptel.ac.in/noc21_ee85/preview



Evaluation Scheme:

Semester End Examination (A):

Theory:

1. Question paper will be based on the entire syllabus summing up to 65 marks.
2. Total duration allotted for writing the paper is 2 hrs.

Laboratory:

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

Continuous Assessment (B):

Theory:

1. One term test of 20 marks and one term test/presentation/assignment/course project / group discussion/ any other of 15 marks will be conducted during the semester.
2. Total duration allotted for writing each of the paper is 1 hr.

Laboratory: (Term work)

Term work shall consist of a minimum of 10 experiments and a minimum of 2 assignments.

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

- i. Laboratory work (Performance of Experiments):15 Marks
- ii. Journal documentation and Assignment: 10 marks

The allocation of marks for laboratory work and tutorials shall adhere to the pre-established rubric parameters.

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 _____ Vice Principal _____ Principal _____

CREATING WINGINEERS



Program: B.Tech. in CSE(IoT and Cyber Security with Blockchain Technology)				Semester : V						
Course : UI/UX Laboratory				Course Code: DJS22ICL504						
Teaching Scheme (Hours / week)				Evaluation Scheme						
				Semester End Examination Marks (A)		Continuous Assessment Marks (B)		Total marks (A+B)		
Lectures	Practical	Tutorial	Total Credits	Theory			Term Test1	Term Test2	Avg.	
				Laboratory Examination			Term work		Total Term work	50
				Oral	Practical	Oral & Practical	Laboratory Work	Tutorial /Mini project /presentation / Journal / Assignment		
--	4	--	2		--	25	10	15	25	

Prerequisite: Knowledge of Web Programming.

Objectives: The objective of the course is.

1. Explore various user research methods and information architecture and to use them in interaction design, visual design and functional Layout Design.
2. Introduces students to usability testing which is performed on various design.

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

1. Identify user requirements.
2. Build UI for user Applications.
3. Create Wireframe and Prototype.
4. Generate test report using usability testing.
5. Work effectively as a member of the team.



Detailed Syllabus: (unit wise)		
Unit	Description	Duration
1	Introduction : Introduction to interface design, Understanding and conceptualizing Interface, Understanding user's conceptual cognition., The 5 Main Ingredients of UX: Psychology, Usability, Design, Copywriting & Analysis. Seven factors that influence user experience-useful, usable, findable, credible, desirable, accessible, valuable.	8
2	User Research: UX research, Difference between good and bad UX research, Five steps of UX research, Role of research in the UX design process, Value of UX research, Seven Great, Tried and Tested UX Research Techniques: Card sorting, Expert review, Eye movement tracking, Field studies, Usability testing, Remote Usability Testing, User Personas. Defining the UX, Design Process and Methodology, understanding user requirements and goals, Understanding the Business Requirements/Goals, User research, mental models, wireframes, prototyping, usability testing. Other Research Methods: User Interviews, Observation, Focus group discussion, Survey Competitor analysis, Empathy mapping.	8
3	Interaction Design: Ideation Methods _ Interaction, Wireframing and Prototyping, Paper Prototyping, Build your own Prototyping, Prototyping Tools For UI/UX Designers, Heuristic (Expert) Evaluation, Designing a Web / Mobile.	10
4	Visual Design: Web App UI Elements, Mobile App UI Elements, Grid Systems, Colors Theory and Palette, Understanding Typography _ Material UI. Usability Testing: Testing Methods - User Testing - A/B Testing - Conducting a Usability Test -Test Results Report.	8
5	Functional Layout Design: Z-Pattern, F-Pattern, and Visual Hierarchy, Browsing vs. Searching vs. Discovery, Page Framework, The Fold, Images, & Headlines, The Axis of Interaction Forms, Calls-to-Action, Instructions & Labels, Primary & Secondary Buttons.	10
6	Research, designing, ideating, & information architecture Identifying and Writing Problem Statements - Identifying Appropriate Research Methods - Creating Personas - Solution Ideation - Creating User Stories - Creating Scenarios - Flow Diagrams - Flow Mapping - Information Architecture.	8
	Total	52



List of Laboratory Experiments:	
Sr. No.	Suggested Experiments
1	Exploring various UI Interaction Patterns
2	Developing an interface with proper UI Style Guides
3	Understand the Grid System and implement the Web App / Mobile App
4	Implement colors Theory and Typography in your own Web App/ Mobile App Through Material UI and other UI Kit.
5	Create the own idea with Empathy Mapping
6	Developing Wireflow diagram for application using open source software
7	Hands on Design Thinking Process for a new product
8	Brainstorming feature for proposed product.
9	Defining the Look and Feel of the new Project
10	Identify a customer problem to solve
11	Conduct end-to-end user research - User research, creating personas, Ideation process (User stories, Scenarios), Flow diagrams, Flow Mapping
12	Sketch, design with popular tool and build a prototype and perform usability testing and identify improvements
13	Presentation on selected mini project topic

Books Recommended: Text books:

1. Joel Marsh, "UX for Beginners", O'Reilly , 2022
2. Jon Yablonski, "Laws of UX using Psychology to Design Better Product Services" O'Reilly 2021
3. Jenifer Tidwell, Charles Brewer, Aynne Valencia, "Designing Interface" 3 rd Edition , O'Reilly 2020
4. Donald Norman, "The Design of Everyday Things: Revised and Expanded Edition", Basic Books, 2013.
5. Rogers Sharp Peerce, " Interaction Design: Beyond Human Computer Interaction", 5th Edition, Wiley, 2019

Reference Books:

1. Jeff Johnson, "Designing with the mind in mind", 2nd Edition, Morgan Kaufmann Publication, 2014.
2. Alan Dix, Janet Finlay, Gregory Abowd, Russel Beale, "Human-Computer Interaction", Pearson, 2009.
3. Brian Fling, "Mobile Design and Development", First Edition , O'Reilly Media Inc., 2009.
4. Wilbert O. Galitz, "The Essential Guide to User Interface Design", Wiley publication, 2002.



Web Recourses:

1. <https://www.interaction-design.org/literature>.
2. <https://www.nngroup.com/articles/>
3. <https://thehipperelement.com/post/75476711614/ux-crash-course-31-fundamentals>
4. <https://uiuxtrend.com/user-experience-ux-process/>
5. Introduction:
 - a. <https://uxplanet.org/what-is-ui-vs-ux-design-and-the-difference-d9113f6612de>
 - b. <https://uxplanet.org/a-complete-list-of-ux-deliverables-d62ccf1de434>
 - c. <https://www.toptal.com/designers/ux/10-common-ux-deliverables>
 - d. <https://www.interaction-design.org/literature/article/what-is-design-thinking-and-why-is-it-so-popular>
 - e. <https://thehipperelement.com/post/72080847673/daily-ux-crash-course-3-of-31>
6. User research:
 - a. <https://careerfoundry.com/en/blog/ux-design/how-to-conduct-user-experience-research-like-a-professional/>
 - b. <https://www.interaction-design.org/literature/article/7-great-tried-and-tested-ux-research-techniques>
7. Visual Design
 - a. <https://www.awwwards.com/understanding-web-ui-elements-principles.html>
 - b. <https://blog.tubikstudio.com/mobile-ui-design-15-basic-types-of-screens/>
 - c. <https://appsamurai.com/6-necessary-elements-for-designing-a-perfect-mobile-app-user-interface/>
 - d. <https://www.smashingmagazine.com/2018/02/comprehensive-guide-to-mobile-app-design/>
 - e. <https://www.mockplus.com/blog/post/ui-grid-layout-https://careerfoundry.com/en/blog/ui-design/introduction-to-color-theory-and-color-palettes/>
8. Interaction Design:
 - a. <https://www.smashingmagazine.com/2018/03/guide-wireframing-prototyping/>
 - b. <https://medium.theuxblog.com/11-best-prototyping-tools-for-ui-ux-designers-how-to-choose-the-right-one-c5dc69720c47>
 - c. <https://careerfoundry.com/en/blog/ux-design/what-is-a-heuristic-evaluation-in-ux/#:~:text=A%20heuristic%20evaluation%20is%20a,is%20evaluated%20by%20usability%20experts.>
 - d. <https://designforfounders.com/web-app-ux/>
 - e. <https://uxplanet.org/best-practices-in-mobile-app-design-in-2020-7f5026818ade>
 - f. <https://www.toptal.com/designers/ux/mobile-ux-design-best-practices>
9. Usability Testing:
 - a. <https://www.nngroup.com/articles/usability-testing-101/>

Online Courses: NPTEL / Swayam:

1. UI By Prof. Saptarshi Kolay | IIT Roorkee <https://archive.nptel.ac.in/courses/124/107/124107008/>
2. Virtual Lab:
Creative Design, Prototyping & Experiential Lab : <https://cpe-iitg.vlabs.ac.in/>



Evaluation Scheme:

Semester End Examination (A):

Laboratory: Oral and practical examinations will be based on the entire syllabus including the Miniproject completed during laboratory sessions

Laboratory: (Term work)

Laboratory work will be based on experiments suggested in experiment list of **DJS22ICL504** along with Mini project.

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

1. Laboratory work (Performance of Task): 10 Marks
2. Assignments : 5 Marks
3. Mini project (Write-up, Power Point Presentation): 10 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.

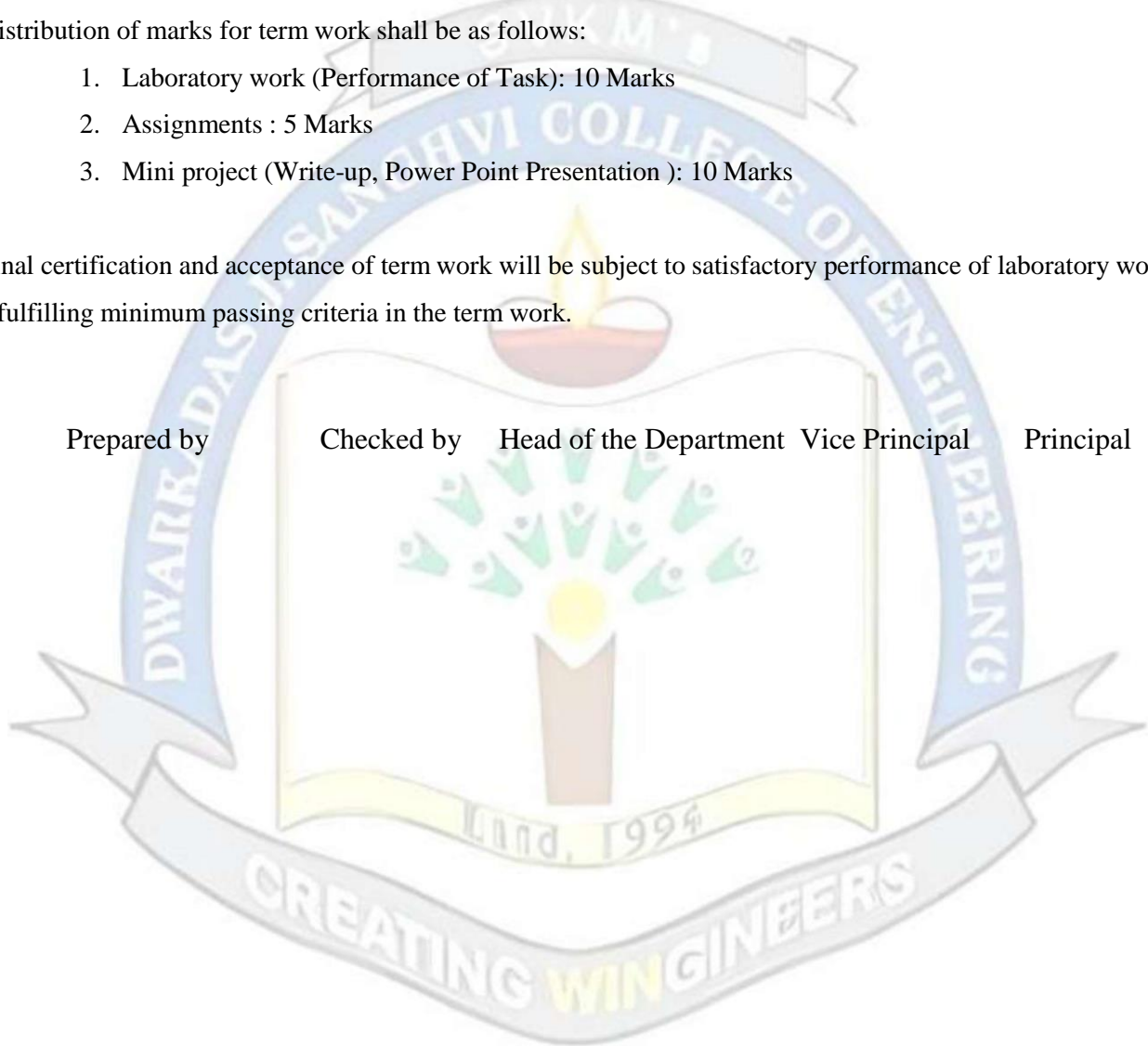
Prepared by

Checked by

Head of the Department

Vice Principal

Principal





Program: B.Tech. in IoT and Cyber Security with Blockchain Technology							Semester : V		
Course : Environmental Studies							Course Code:(DJS22A3)		
Teaching Scheme (Hours /week)				Evaluation Scheme					
				Semester End Examination Marks (A)			Continuous Assessment Marks (B)		Total marks (A+B)
Lectures	Practical	Tutorial	Total Credits	Theory			Theory	Term Test +Assignment	
				--	--	--	--	--	--
				Laboratory Examination			Term work		Total Term work
1	--	--	--	Oral	Practical	Oral & Practical	Laboratory Work	Tutorial / Mini project / presentation/ Journal	
				--	--	-	--	--	--

Pre-requisite:

1. Interest in Environment and its impact on Human

Objectives: The objective of the course is.

1. Understand environmental issues such as depleting resources, pollution, ecological problems and the renewable energy scenario.
2. Familiarize environment related legislation

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

1. Understand how human activities affect environment.
2. Understand the various technology options that can make a difference.

Detailed Syllabus: (unit wise)		
Unit	Description	Duration
1	Social Issues and Environment: Ecological footprint and Carrying Capacity, Depleting nature of Environmental resources such as soil, water minerals and forests, Carbon emissions and Global Warming.	04
2	Technological Growth for Sustainable Development: Social, Economical and Environmental aspects of Sustainable Development, Renewable Energy Harvesting, Concept of Carbon credit, Green Building, Power and functions of Central Pollution Control Board and State Pollution	04



	Control Board.	
3	Green Technology: History, Agenda, and Challenges Ahead. Sustainable Cloud Computing, and Risk Management, Sustainable Software Design, Data Center Energy Efficiency, Thin-Client and Energy Efficiency.	05
	Total	13

Books Recommended:

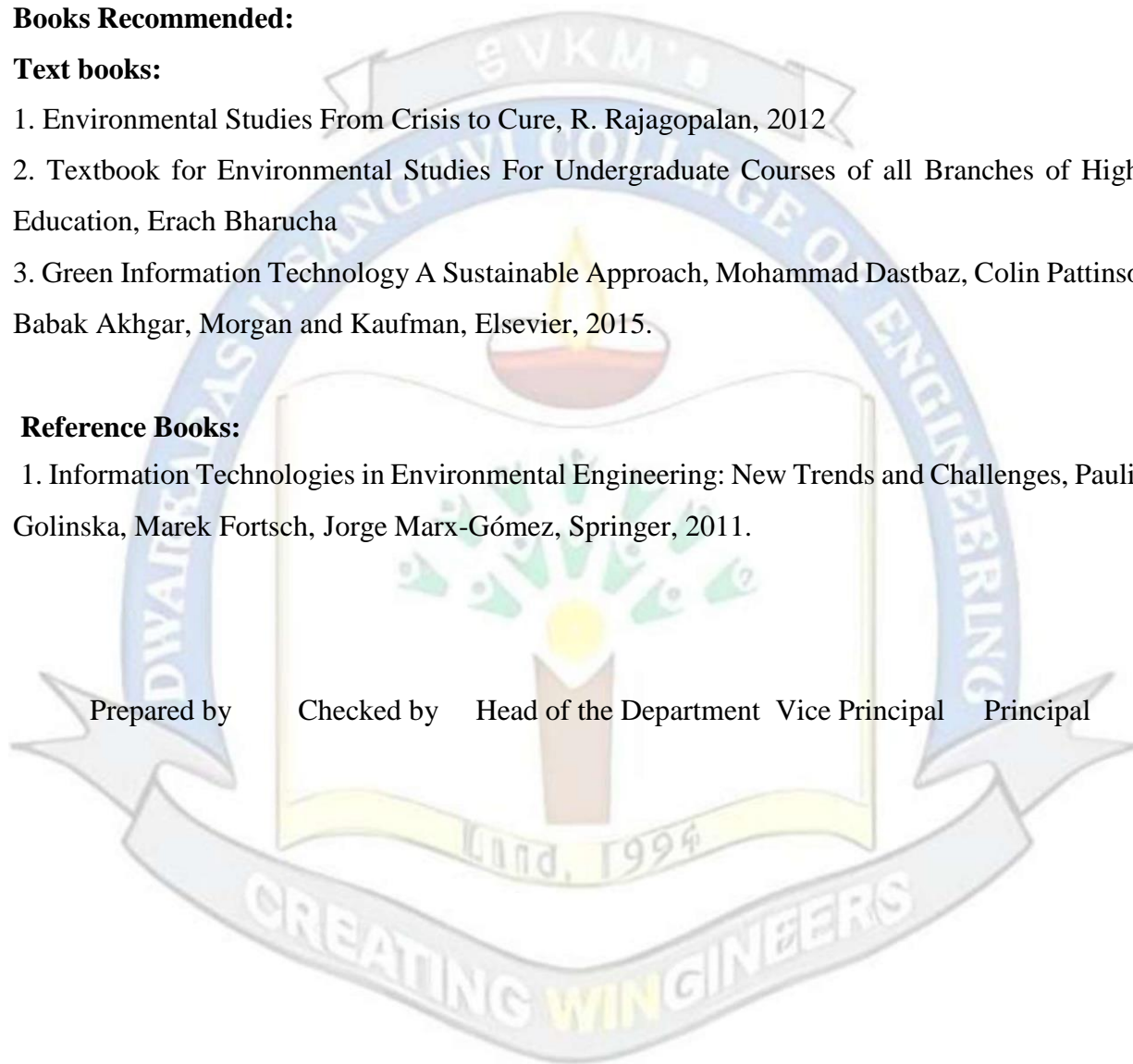
Text books:

1. Environmental Studies From Crisis to Cure, R. Rajagopalan, 2012
2. Textbook for Environmental Studies For Undergraduate Courses of all Branches of Higher Education, Erach Bharucha
3. Green Information Technology A Sustainable Approach, Mohammad Dastbaz, Colin Pattinson, Babak Akhgar, Morgan and Kaufman, Elsevier, 2015.

Reference Books:

1. Information Technologies in Environmental Engineering: New Trends and Challenges, Paulina Golinska, Marek Fortsch, Jorge Marx-Gómez, Springer, 2011.

Prepared by Checked by Head of the Department Vice Principal Principal





Program: B.Tech. in CSE(IoT and Cyber Security with Blockchain Technology)				Semester: V					
Course: Innovative Product Development II				Course Code: DJS22ILLL1					
Teaching Scheme (Hours / week)				Evaluation Scheme					
				Semester End Examination Marks (A)		Continuous Assessment Marks (B)			Total marks (A+ B)
Lectures	Practical	Tutorial	Total Credits	Theory		Term Test 1	Term Test 2	Avg.	
				--		--	--	--	--
				Laboratory Examination		Term work			
				Oral	Practical	Oral & Practical	Laboratory Work	Tutorial / Mini project / presentation/ Journal	Total Term work
--	2	--	1			25		25	50

Objectives: The objective of the course is.

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 conceptualize 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 conceptualizing 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 the team or as the leader.
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

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 be on individual contribution to the 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 semester V the subsequent semester shall be as given below:
 - Marks awarded by the supervisor based on performance 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 finalization of the product selected.
Second shall be on finalization 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 VI. 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 organizations 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 VI. Students are compulsorily required to present the outline of the technical paper prepared by them during the final review in semester VI

Prepared by

Checked by

Head of the Department

Vice Principal

Principal

