Shri Vile Parle Kelavani Mandal's

Dwarkadas J. Sanghvi College of Engineering

(Autonomous College Affiliated to the University of Mumbai)

Proposed Scheme and detailed syllabus

Final Year B.Tech

in

Computer Science and Engineering

(IoT and Cyber Security with Blockchain Technology)

(Semester VII)

Prepared by:- Board of Studies in Computer Science & Engineering

(IoT and Cyber Security with Blockchain Technology)

With effect from the Academic Year: 2026-2027

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)

Course Structure for Final Year Undergraduate Program in Computer Science and Engineering (IoT and Cyber Security with Block Chain Technology): Semester VII (Autonomous)

(Academic Year 2026-2027)

Sr. No.	Course Code	Course	Teaching Scheme				Semester End Examination (SEE) - A						Continuous Assessment (CA) - B						Aggregate (A+B)
			Theory (Hrs.)	Practical (Hrs.)	Tutorial (Hrs.)	Credits	Duration (Hrs)	Theory	Oral	Pract	Oral & Pract	SEE Total (A)	Term Test 1 (TT1)	Term Test 2 (TT2)	Term Test 3 (TT3)	Term Test Total (TT1 + TT2 + TT3)	Term work	CA Total (B)	
1	DJS23BCPC701	Blockchain for Enterprise	3	–	–	3	2	60	--	–	–	60	15	15	10	40	--	40	100
	DJS23BLPC701	Blockchain for Enterprise Laboratory	–	2	–	1	2	–	25	--	–	25	–	--	–	–	25	25	50
2	DJS23BCPE711	Quantum Cryptography	3	--	–	3	2	60	–	–	–	60	15	15	10	40	--	40	100
	DJS23BLPE711	Quantum Cryptography Laboratory	--	2	--	1	2	–	25	–	–	25	–	–	–	–	25	25	50
	DJS23BCPE712	Artificial Intelligence for Cybersecurity	3	–	–	3	2	60	–	--	–	60	15	15	10	40	--	40	100
	DJS23BLPE712	Artificial Intelligence for Cybersecurity Laboratory	--	2	–	1	2	--	25	--	–	25	–	–	–	–	25	25	50
	DJS23BCPE713	Cyber Threat Intelligence and Security Analytics	3	--	--	3	2	60	–	–	–	60	15	15	10	40	--	40	100
	DJS23BLPE713	Cyber Threat Intelligence and Security Analytics Laboratory	--	2	--	1	2	--	25	--	–	25	–	–	–	–	25	25	50
3	DJS23BCPE714	Reinforcement Learning	3	--	--	3	2	60	–	–	–	60	15	15	10	40	--	40	100
	DJS23BLPE714	Reinforcement Learning Laboratory	--	2	–	1	2	–	25	--	–	25	--	–	–	–	25	25	50
	DJS23BCPE715	Agentic AI	3	--	–	3	2	60	–	--	–	60	15	15	10	40	--	40	100
	DJS23BLPE715	Agentic AI Laboratory	--	2	–	1	2	--	25	--	–	25	--	–	–	–	25	25	50
	DJS23BCPE716	Prompt Engineering	3	--	–	3	2	60	–	–	–	60	15	15	10	40	--	40	100
	DJS23BLPE716	Prompt Engineering Laboratory	--	2	--	1	2	--	25	–	–	25	--	–	–	–	25	25	50
4	DJS23BCMD701	Large Language Models	2	--	--	2	2	60	–	--	–	60	15	15	10	40	–	40	100
	DJS23BLMD701	Large Language Models Laboratory	--	2	--	1	2	–	25	--	–	25	--	–	–	–	25	25	50
5	DJS23ITELX12	Research Ecosystem	–	–	2	2	--	--	--	–	--	--	–	--	--	--	50	50	50
6	DJS23IPELX13	Major Project	–	8	–	4	2	–	–	–	50	50	–	--	--	--	50	50	100
7	DJS23BCSC701	Reliable Cloud and Machine Learning Infrastructure	1	--	--	1	–	--	–	--	–	–	15	15	10	40	–	40	40
8	DJS23ICHSX11	Disaster Management and Preparedness	2	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
		Total	**14**	**16**	**2**	**22**	**18**	**240**	**100**	**–**	**50**	**390**	**75**	**75**	**50**	**200**	**200**	**400**	**790**

Prepared by
Mr. Swapnil Gharat

Verified by
Dr. Vishkha Shelke

Dr. Narendra Shekokar
HoD &Vice Principal

Dr. Hari Vasudevan
Principal

Program: B.Tech in Computer Science and Engineering(IoT and Cybersecurity with Block chain Technology)	Final Year B.Tech	Semester : VII
Course : Blockchain for Enterprise	Course Code: DJS23BCPC701	
Course: Blockchain for Enterprise Laboratory	Course Code: DJS23BLPC701	

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	Term Test 3	Total	
				60			15	15	10	40	100
				Laboratory Examination			Term Work				
3	2	--	4	Oral	Practical	Oral & Practical	Laboratory Work	Mini project	Total Term work		50
				25	–	–	15	10	25		

Prerequisite:

1. Introduction to Blockchain Technology
2. Blockchain for Cybersecurity
3. Cloud Computing Laboratory

Course Objectives: The objective of the course is

1. To understand enterprise blockchain architecture and frameworks.
2. To explore blockchain applications in enterprise ecosystems such as supply chain, finance, and healthcare.
3. To study interoperability, scalability, and governance challenges in enterprise blockchain systems.
4. To design and deploy enterprise-grade blockchain solutions ensuring security, privacy, and performance.

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

1. Describe the role and need for blockchain in enterprise systems.
2. Analyze and differentiate blockchain architecture for enterprise-grade applications.
3. Design and Develop enterprise smart contracts using for business processes automation.
4. Evaluate scalability, privacy, and interoperability of enterprise blockchain networks.
5. Integrate blockchain with existing enterprise IT infrastructure.
6. Develop prototype of blockchain-based solutions for real-world industrial challenges.

Detailed Syllabus:		
Unit	**Description**	**Duration**
1	**Introduction to Enterprise Blockchain** Concept of Enterprise blockchain – definition, characteristics, and benefits, Business process, automation using blockchain, Role of blockchain in digital transformation, Enterprise Needs: Transparency, Traceability, Compliance, and Efficiency, Blockchain adoption in enterprises. Blockchain-as-a-Service (BaaS) Overview: AWS, Azure, IBM Blockchain	**08**
2	**Enterprise Blockchain Frameworks** Architecture and components of Hyperledger Besu, Ethereum for Enterprises: Private Ethereum, Quorum, and Corda Enterprise and its Contract States Model, Consensus Mechanisms for Enterprise (Raft, Proof of Authority), Comparative study of frameworks. **Identity management in enterprise blockchain**: Decentralized digital identity, Decentralized Identifiers (DIDs), DID Architecture and work flow, Blockchain based DID Registry, Verifiable Credentials (VC), VC Trust Model, Combining DIDs and VCs, Hyperledger Aries:Use of Blockchain for VCs	**08**
3	**Enterprise Integration and Smart Contract Automation** Integration with legacy systems (ERP, CRM, SCM); Blockchain–cloud integration, Interoperability standards: Polkadot, Cosmos, and Hyperledger Cactus, API gateways and oracles for enterprise data synchronization. Enterprise Smart Contracts: Design Patterns and Best Practices, Solidity for Business Logic Automation, Chaincode in Hyperledger Fabric (Go/Node.js).	**06**
4	**Blockchain Interoperability** Interoperability in Permissionless and Permissioned Blockchains, Cross Chain Asset Transfer, Trusted Third Party (TTP) based Asset Transfer, Cross Chain Asset Exchange, Atomic Cross-chain Swaps, Hashlock and Timelock, HTLC: Hashed Timelock Contract, Multi Party Atomic Cross chain Swap, Interoperation in Permissioned Blockchains-Use Case, Verifiable Data Transfer in Permissioned Blockchain, Hyperledger Indy: Indy Key Characteristics, Overview and Projects.	**08**
5	**Blockchain Integration with Enterprise IT Infrastructure** RESTful and gRPC APIs for Blockchain, Blockchain and IoT Integration Platforms: AWS and Azure services and case study Blockchain and AI/ML for Predictive Analytics and Fraud Detection using AWS Sagemaker and Azure ML studio.	**06**
6	**Blockchain Applications in Enterprise Domains** Regulatory Landscape: GDPR, DPDP Act, and Data Governance in Blockchain Enterprise NFTs and Digital Twin Use Cases, Enterprise application of Block chain: Cross border payments, Know Your Customer (KYC), Food Security, Block chain enabled Trade, Supply Chain Financing, Identity on Block chain, Blockchain in energy sector, Blockchain in governance	**06**
	Total	**42**

List of Laboratory Experiments:	
Sr. No.	**Suggested Experiments**
1	Case study: Analyse enterprise motivations (transparency, traceability, compliance) and compare BaaS offerings (AWS, Azure, IBM).
2	To design and implement a decentralized web application that allows a user to store and retrieve data on the Ethereum blockchain using Solidity and a basic web interface.
3	To develop a blockchain-based voting application that records votes securely and transparently using Solidity smart contracts and a web-based frontend
4	Deploy a sample permissioned network using a cloud BaaS and run basic transactions
5	Setup a Private Ethereum Network using Ganache and MetaMask
6	Build a simple CorDapp demonstrating the contract-states model.
7	Develop and Deploy a Smart Contract for Supply Chain Asset Tracking
8	Develop and deploy chaincode (Go/Node.js) to automate an enterprise process
9	Write secure Solidity contracts implementing standard enterprise patterns (Ownable, Pausable, Upgradeable proxy) for a business workflow.
10	Integrate off-chain enterprise data via an oracle into smart contracts
11	Develop an Enterprise NFT-based Digital Asset Registry
12	Implement DID creation, registration, and resolution using tools like Hyperledger Aries or Indy and demonstrate decentralized digital identity authentication.
13	Issue VCs using a blockchain-based registry; allow other nodes to verify and trust credentials based on the VC trust model
14	Implement a Hashed Timelock Contract for asset exchange between two simulated blockchains
15	Use Azure ML Studio to create predictive analytics workflow using blockchain transaction data
16	Build and deploy a Solidity smart contract for a business scenario (e.g., automated invoicing) on private Ethereum(or testnet)
17	Miniproject: (A group of 3 to 4 students is required to develop an Enterprise application using blockchain technology and submit report).

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

Books Recommended:

Text Books:

1. Narayan Prusty, Blockchain for Enterprise, 1st Edition, Packt Publishing, ISBN: 9781788477130, 2018
2. Nitin Gaur, Luc Desrosiers, Venkatraman Ramakrishna, Petr Novotny, Arthur G. Gauer, Blockchain for Business – A Practical Guide to the Next Digital Revolution, 1st Edition, O'Reilly Media, ISBN: 9781492042791, 2020.
3. Ambadas Choudhari, Arshad Sarfarz, Sham M R, Blockchain for Enterprise Application Developers, 1st Edition, Wiley Publishing, ISBN: 9788126599967, 2020.
4. Joseph Holbrook, Architecting Enterprise Blockchain Solutions, 1st Edition, Packet Publishing, ISBN: 9781839217715, 2020.
5. Imran Bashir , Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more, 3rd Edition, Packet Publishing, ISBN: 9781839213199, 2020

Reference Books:

1. Alessandro Parisi , Securing Blockchain Networks like Ethereum and Hyperledger Fabric, Packt Publishing, ISBN: 9781838646486, 2020.
2. Nitin Gaur, Hands-On Blockchain with Hyperledger: Building decentralized applications with Hyperledger Fabric and Composer, Packt Publishing, 2018.
3. Richard Ma, Jan Gorzny, Edward Zulkoski, Kacper Bak, Olga V. Mack, Fundamentals of Smart Contract Security, Momentum Press, 2019.
4. Kevin Werbach, the Blockchain and the New Architecture of Trust, the MIT Press, 2018.

Web resources:

1. Blockchain-as-a-Service (BaaS): https://crustlab.com/blog/blockchain-as-a-service/
2. AWS Managed Blockchain: https://aws.amazon.com/managed-blockchain/
3. Microsoft Azure Blockchain Documentation: https://learn.microsoft.com/en-us/azure/blockchain/
4. IBM Blockchain Platform: https://www.ibm.com/blockchain/platform
5. Enterprise Ethereum Alliance (EEA): https://entethalliance.org/
6. W3C Decentralized Identifiers (DID) and Verifiable Credentials (VCs): https://www.w3.org/TR/did-core/, https://www.w3.org/TR/vc-data-model/

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
4. Blockchain Council – Enterprise Blockchain Certification
   https://www.blockchain-council.org/

Semester End Examination (A):

Theory:

1. Question paper will be based on the entire syllabus summing up to 60 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.**ontinuous Assessment (B)**

Theory:

1. Term Test 1 (based on 40 % syllabus) of 15 marks for the duration of 45 min.
2. Term Test 2 (on next 40 % syllabus) of 15 marks for the duration of 45 min.
3. Term Test 3 conduction can be Assignment / course project / group discussion /presentation / quiz/ any other for 10 marks.

Laboratory: (Term work)

Term work shall consist of minimum 6 experiments.

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

i. Laboratory work (Performance of Experiments): 10 Marks
ii. Assignments (Quiz, Descriptive/Analytical Questions): 5 marks
iii. Miniproject (Implementation, Report): 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 Computer Science and Engineering(IoT and Cybersecurity with Block chain Technology)	Final Year B.Tech	Semester : VII
Course : Quantum Cryptography	Course Code: DJS23BCPE711	
Course : Quantum Cryptography Laboratory	Course Code: DJS23BLPE711	

<table>
<tr><td colspan="4" rowspan="2">Teaching Scheme (Hours / week)</td><td colspan="8">Evaluation Scheme</td></tr>
<tr><td colspan="4">Semester End Examination Marks (A)</td><td colspan="3">Continuous Assessment Marks (B)</td><td>Total marks (A+ B)</td></tr>
<tr><td rowspan="3">Lectures</td><td rowspan="3">Practical</td><td rowspan="3">Tutorial</td><td rowspan="3">Total Credits</td><td colspan="4">Theory</td><td>Term Test 1</td><td>Term Test 2</td><td>Term Test 3</td><td>Total</td><td></td></tr>
<tr><td colspan="4">60</td><td>15</td><td>15</td><td>10</td><td>40</td><td>100</td></tr>
<tr><td colspan="4">Laboratory Examination</td><td colspan="3">Term Work</td><td rowspan="3">50</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">1</td><td rowspan="2">--</td><td rowspan="2">4</td><td>Oral</td><td>Practical</td><td>Oral & Practical</td><td>Laboratory Work</td><td>Tutorial / Mini project / presentation / Journal/ Practical</td><td>Total Term work</td></tr>
<tr><td>--</td><td>25</td><td>--</td><td>15</td><td>10</td><td>25</td></tr>
</table>

Prerequisite:

1. Linear Algebra and Optimization
2. Probability and Statistical Inference
3. Applied Cryptography
4. Quantum Computing

Course Objectives: The objective of the course is

1. To provide foundational knowledge of classical and quantum cryptography, including their principles and security challenges
2. To develop understanding of quantum mechanics concepts relevant to cryptography.
3. To enable learners to explore quantum key distribution protocols and advanced quantum cryptographic techniques for secure communication.
4. To introduce post-quantum cryptography and real-world applications of quantum cryptographic systems in modern security frameworks

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

1. Analyze the principles of classical and quantum cryptography and the impact of quantum algorithms on security.
2. Describe fundamental concepts of quantum mechanics, including qubits, superposition, entanglement, and quantum gates
3. Illustrate quantum key generation protocols and evaluate their security in quantum communication

systems.

4. Analyze advanced quantum cryptographic protocols and their applications in secure communication.
5. Assess post-quantum cryptographic techniques for developing quantum-resistant security systems.
6. Apply quantum cryptography concepts to real-world secure communication and distributed computing scenarios.

Detailed Syllabus:

Unit	Description	Duration
1	**Quantum Cryptography** **Introduction to Quantum Computing**: Classical vs Quantum Computing **Quantum Algorithms:** Introduction to Quantum Algorithms, Shor's Algorithm for Integer Factorization, Grover's Search Algorithm, Quantum Speedup Concepts **Impact of Quantum Computing on Cybersecurity:** Impact of quantum computing (Shor's, Grover's algorithms) **Introduction to quantum cryptography:** Information-theoretic security, Quantum Security Principles, Quantum Randomness and Secure Key Generation	08
2	**Fundamentals of Quantum Mechanics** Basics of quantum mechanics: qubits, superposition, measurement, Dirac notation, quantum states, Bloch sphere, Quantum gates and circuits, Heisenberg uncertainty principle, Quantum entanglement and no-cloning theorem	07
3	**Quantum Key Generation** Basic ideas of two parties quantum key generation, Security issues of QKG protocols, Multiparty key generation, Entanglement-based QKG protocols, Unconditional security of QKG, Experimental quantum cryptography. **Quantum key exchange (QKE)** BB84 Protocol, B92 Protocol, SARG04, Six-State Protocol, E91	08
4	**Quantum Cryptographic Protocols** Device-independent QKD, measurement-device-independent (MDI-QKD), continuous-variable QKD, satellite QKD (e.g., Micius), loss-tolerant protocols Quantum Teleportation and Superdense Basic principles, Teleportation circuit, Quantum secret, Superdense coding	06
5	**Post-Quantum Cryptography** Need for post-quantum cryptography, Lattice-based cryptography, Code-based cryptography, Hash-based cryptography, Multivariate cryptography, Quantum-resistant algorithms	08
6	**Quantum Cryptography Applications** Quantum digital signatures, quantum coin flipping, blind quantum computing, quantum money, quantum-secure multiparty computation, hybrid classical-quantum protocols.	04
	Total	42

List of Laboratory Experiments:	
Sr. No.	**Suggested Experiments**
1	Case study of IEEE/ScienceDirect/Springer/Elseveir research paper on classical cryptographic techniques (symmetric & asymmetric) and their limitations.
2	Study quantum computing simulators (e.g., Qiskit) and perform representation of qubits, superposition, and measurement.
3	Implement Grover's search algorithm and analyze its speedup over classical search.
4	Simulate Shor's algorithm for integer factorization (small numbers).
5	Represent qubits using Bloch sphere visualization tools and perform operations using quantum gates and observe state changes. verify superposition and measurement outcomes.
6	Implement fundamental quantum gates (Hadamard, Pauli-X, Pauli-Z) and construct basic quantum circuits.
7	Simulate quantum entanglement using Bell states and demonstrate the no-cloning theorem in a quantum system
8	Implement the BB84 protocol for secure quantum key distribution
9	Simulate and compare different QKD protocols based on performance and security.
10	Simulate E91 protocol using entangled qubits. Analyze key generation process and security against eavesdropping and Compare with BB84 protocol performance.
11	Simulate of quantum teleportation and superdense coding circuits.
12	Implementation of a basic post-quantum cryptographic scheme (e.g., lattice-based or hash-based signatures).

Books Recommended:

Text Books:

1. Michele Mosca, Phillip Kaye, Raymond Laflamme, An Introduction to Quantum Computing, 1st Edition, Oxford University Press, ISBN: 9780198570493, 2007
2. Jozef Gruska, Quantum Computing, 1st Edition, McGraw-Hill / International Thomson Publishing, ISBN: 9780077095033, 1999
3. Chris Bernhardt, Quantum Computing for Everyone, 1st Edition, MIT Press paperback edition, 2020
4. Arthur Pittenger, An Introduction to Quantum Computing Algorithms, Progress in Computer Science and Applied Logic, Volume 19, Springer Science+ Business Media, LLC, 2001
5. Parag Lala, Quantum Computing- A beginner's Introduction, McGraw Hill Education, 2020

Reference Books:

1. Thomas G. Wong, Introduction to Classical and Quantum Computing, 1st Edition, Rooted Grove, ISBN: 9798985593105, 2022
2. Elias F. Combarro and Samuel Gonzáles-Castillo, A Practical Guide to Quantum Computing: Hands-on approach to quantum computing with Qiskit, 1st Edition, 2022
3. Robert S. Sutor, Dancing with Qubits, 2nd Edition, Packt, 2024
4. Jack D. Hidary, Quantum Computing: An Applied Approach, 2nd Edition, Springer, 2021
5. Leslie E. Ballentine, Quantum Mechanics: A Modern Development, 2nd Edition, World Scientific, 2020
6. Ciaran Hughes et al., Quantum Computing for the Quantum Curious, 1st Edition, Springer, 2021

Web resources:

1. IBM Quantum & Qiskit: https://qiskit.org/ and https://quantum.ibm.com
2. Qiskit Textbook: https://learning.quantum.ibm.com
3. Quantum Zeitgeist: https://quantumzeitgeist.com/
4. GitHub Quantum Resources: https://github.com/MonitSharma/Learn
5. QOSF Resources: https://qosf.org/learn_quantum/

Online Courses: NPTEL / Swayam

1. Introduction to Quantum Computing: Quantum Algorithms and Qiskit, By Prof. Prabha Mandayam, Prof. Anupama Ray, Prof. Sheshashayee Raghunathan, IIT Madras, IBM Research, IBM Systems
   https://onlinecourses.nptel.ac.in/noc26_cs89/preview
2. Quantum Computation and Quantum Information, By Prof. Chiranjib Mitra, IISER Kolkata
   https://onlinecourses.nptel.ac.in/noc26_ph02/preview

Evaluation Scheme:

Semester End Examination (A):

Theory:

1. Question paper will be based on the entire syllabus summing up to 60 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. Term Test 1 (based on 40 % syllabus) of 15 marks for the duration of 45 min.
2. Term Test 2 (on next 40 % syllabus) of 15 marks for the duration of 45 min.
3. Term Test 3 conduction can be Assignment /presentation /quiz/ any other for 10 marks.

Laboratory: (Term work)

Term work shall consist of minimum 8 experiments and Assignments

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

i. Laboratory work (Performance of Experiments, Write-up): 15 Marks
ii. Assignment (Quiz, Descriptive/Analytical Questions): 10 marks

Prepared by **Checked by** **Head of the Department** **Vice Principal** **Principal**

Program: B. Tech in Computer Science and Engineering (IoT and Cybersecurity with Block chain Technology)				Final Year B.Tech				Semester: VII
Course : Artificial Intelligence for Cybersecurity				Course Code: DJS23BCPE712				
Course Laboratory: Artificial Intelligence for Cybersecurity Laboratory.				Course Code: DJS23BLPE712				
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	Assignment	Total
				60	15	15	10	40	100
				Laboratory Examination			Term work	Total Term work	50
3	2	--	4	Oral	Practical	Oral & Practical	Laboratory Work	Tutorial / Mini project / presentation/ Assignment	
				25	--	--	15	10	25

Prerequisite:

1. Artificial Intelligence.
2. Machine Learning.

Course Objectives: The objective of the course is

1. Understand AI governance, security, and privacy through regulations, frameworks, lifecycle management, risk assessment, compliance, and secure deployment.
2. Analyse AI/ML security risks across training and inference phases, including vulnerabilities, data threats, adversarial attacks, robustness and ethics.
3. Examine adversarial ML and privacy-preserving methods such as attacks, defences, anonymization, differential privacy, federated learning, encryption and data protection laws.
4. Investigate AI and GenAI in cybersecurity for threat detection, autonomous defence, adversarial risks, alignment challenges and advanced security solutions.

Course outcomes: On completion of this course, learner will be able to:

1. Explain AI security and privacy measures during model development and deployment.
2. Analyze AI system vulnerabilities and classify different types of AI security threats..
3. Evaluate adversarial attack techniques including FGSM, PGD, and black-box methods on machine learning models.
4. Apply differential privacy, federated learning, and encryption to protect data in AI systems.
5. Develop AI-based solutions for threat detection, anomaly monitoring, phishing and spam mitigation, and autonomous cyber defense while addressing adversarial risks.
6. Assess risks and security implications of Generative AI in modern cybersecurity environments.

Detailed Syllabus:		
Unit	**Description**	**Duration**
1	**AI Security and Privacy Architecture** Unified AI governance architecture, AI regulations, frameworks, and principles: AI Regulations and Frameworks and Common AI Principles, **AI Governance:** Organization Structure and R&R, Policies and Procedures. **AI Management:** AI Model Development. **Data Management Security and Privacy Protection:** AI Security Assessment in SDLC,AI Model Explainability, Privacy Protection. **AI Model Acquisition**: Licensing Agreement Compliance, Due Diligence Assessment Integration Security Protection. **AI Model Deployment and Operations:** Algorithmic Impact Assessment (AIA),Secure the Infrastructure,Isolation,Detection,Human Involvement.	08
2	**The AI Security Threat Landscape.** Understanding the AI/ML Pipeline and Attack Surfaces , Attacks during Training Phase: Data Poisoning and Back-dooring, Attacks during Inference Phase: Evasion and Model Stealing, Data Security vs. Model Security, Membership Inference Attacks, Model Inversion Attacks. **AI Risks and Challenges:**Data and Model quality risks, Robustness, Reliability and Safety, bias and Discrimination, Data Accuracy and Integrity, security and privacy risks, AI ethics and social risks.	06
3	**Adversarial Attacks: The Offense.** About Adversarial Examples, Adversarial Attacks Working: Exploiting Gradients, White-Box Attacks: Full Knowledge, Fast Gradient Sign Method (FGSM) , Projected Gradient Descent (PGD), Black-Box Attacks: Limited Knowledge, Query-Based Attacks , Transferability of Attacks. Physical Adversarial Attacks: Stickers, Patches, and 3D Objects.	08
4	**Data Privacy in Artificial Intelligence:** The Importance of Data in AI and Associated Privacy Risks, Anonymization and Pseudonymization Techniques, Introduction to Differential Privacy, The Core Concepts: Epsilon and Delta, Mechanisms: Laplacian and Gaussian, Federated Learning: Training Models without Centralizing Data, Homomorphic Encryption: Computing on Encrypted Data, Overview of Global Data Protection Regulations (GDPR, CCPA, DPDP Act).	05
5	**AI for Cybersecurity: The Dual Role.** Using AI to Enhance Security, AI-Powered Threat Detection and Analysis, Anomaly Detection in Networks and User Behaviour, AI in Phishing and Spam Detection, **The Arms Race:** Adversarial Attacks Against AI-based Security Systems, Autonomous Cyber Défense Systems.**VR, AR, and XR:** Definition, Key Components and Core Functions, security and privacy implications. Security and privacy by design for XR. **Metaverse:** Definitions, Metaverse Characteristics and Forms, Metaverse challenges and risks, security and privacy by design for the Metaverse.	09
6	**GenAI Model Security.** **Navigating the GenAI Security Landscape**: The Rise of GenAI in Business, Emerging Security Challenges in GenAI, GenAI Impacts to Cybersecurity Professional. Fundamentals of Generative Model Threats, Ethical and Alignment Challenges, Advanced Security and Safety Solutions, Frontier Model Security.	06
	Total	42

List of Laboratory Experiments:	
Sr. No.	**Suggested Experiments**
1	Study and implement AI Model Risk Assessment using a sample AI application
2	Implement AI Model Vulnerability Assessment using Adversarial Attack Surface Analysis
3	Implement Data Poisoning Attack on a Machine Learning Model and analyze its impact
4	Implement FGSM Adversarial Attack on an Image Classification Model
5	Implement PGD Attack and compare its performance with FGSM
6	Implement Differential Privacy in Machine Learning using TensorFlow Privacy / Opacus
7	Implement Federated Learning using Flower or TensorFlow Federated
8	Implement Homomorphic Encryption for Secure AI Prediction
9	Implement AI-based Network Intrusion Detection System using Machine Learning
10	Implement Phishing Website Detection using Machine Learning
11	Implement User Behaviour Analytics for Insider Threat Detection
12	Study and Analyze Security Risks of Generative AI (Prompt Injection/Jailbreak Detection)

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

Books Recommended:

Text books:

1. Alang Tang Safeguarding-the-future-security-and-privacy-by-design-for-ai-metaverse-blockchain-and-beyond 1st edition CRC press 2024.
2. Ajit Singh, AI Security, Shroff Publishers 1st edition, 2025-26.

Reference Books:

1. Omar Santos , Petar Radanliev - Beyond The Algorithm Ai, Security, Privacy, And Ethics - Addison Wesley 2024.
2. Ken Huang,Yang Wang,Ben Goertzel,Yale Li,l, Sean Wright,Jyoti Ponnapalli - Generative AI Security Theories and Practices Springer 2024.

Web resoures:

1. https://www.coursera.org/specializations/ai-for-cybersecurity
2. https://www.eicta.iitk.ac.in/courses/gen-ai-in-cyber-security

Online Courses: Nptel /Swayam Courses:

1. Responsible & Safe AI Systems By Prof. Ponnurangam Kumaraguru, Prof. Balaraman Ravindran, Prof. Arun Rajkumar IIT Hyderabad.
   https://onlinecourses.nptel.ac.in/noc24_cs132/

Evaluation Scheme:
Semester End Examination (A):

Theory:

1. Question paper will be based on the entire syllabus summing up to 60 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. Term Test 1 (based on 40 % syllabus) of 15 marks for the duration of 45 min.
2. Term Test 2 (on next 40 % syllabus) of 15 marks for the duration of 45 min.
3. Assignment / Course project / group discussion /presentation / quiz/ any other for 10 marks.

Laboratory: (Term work)

1. Term Work shall consist of at least 8 practical's based on the above list.
2. The distribution of marks for term work shall be as follows:
   i. Laboratory work (Performance of Experiments, Write-up): 15Marks
   ii. Case study/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 Computer Science and Engineering (IoT and Cyber Security with Block Chain Technology)	Final Year	Semester: VII
Course: Cyber Threat Intelligence and Security Analytics	Course Code: DJS23BCPE713	
Course: Cyber Threat Intelligence and Security Analytics Lab	Course Code: DJS23BLPE713	

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	Term Test 3	Total	
				60			15	15	10	40	100
				Laboratory Examination			Term work			Total Term work	
3	1	-	4	Oral	Practical	Oral & Practical	Laboratory Work	Tutorial / Mini project/presentation/ Journal			50
				25	_	-	15	10		25	

Prerequisite:

1. Computer Network
2. Applied Cryptography
3. Network Security

Course Objectives: The objective of the course is

1. To introduce fundamental concepts of Cyber Threat Intelligence (CTI).
2. To understand the Cyber Threat Intelligence lifecycle and explore various data sources.
3. To develop skills in threat data collection and analysis, including the identification of indicators of compromise.
4. To provide knowledge of security analytics techniques.
5. To familiarize students with threat intelligence sharing standards and security operations.

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

1. Explain different types of cyber threat intelligence in real-world scenarios.
2. Apply the Cyber Threat Intelligence lifecycle to collect, process, and disseminate threat intelligence from multiple data sources.
3. Analyze cyber threat data using Indicators of Compromise and behavioral patterns.
4. Apply security analytics techniques and tools to analyze logs, correlate security events, and visualize security data for effective threat detection and monitoring.
5. Analyse threat intelligence sharing mechanisms using STIX, TAXII, and OpenIOC standards for effective cybersecurity collaboration
6. Design and apply security operations strategies using SIEM, SOAR, and threat hunting techniques.

Detailed Syllabus:

Unit	Description	Duration
1	**Introduction to Cyber Threat Intelligence (CTI)** Definition and Importance of Cyber Threat Intelligence, Types of Threat Intelligence- Strategic Intelligence, Tactical Intelligence, Operational Intelligence, Technical Intelligence, Threat Actors and Their Motivations- Cybercriminals, Hacktivists, Nation-state attackers, Insider threats, Cyber Attack Lifecycle Models- Cyber Kill Chain Model, MITRE ATT&CK framework overview.	08
2	**Threat Intelligence Lifecycle and Data Sources** Cyber Threat Intelligence Lifecycle- Planning and Direction, Data Collection, Processing and Analysis, Dissemination and Feedback, Threat Intelligence Data Sources- Open-Source Intelligence (OSINT), Dark Web Monitoring, Security Logs and Network Traffic, Threat Intelligence Platforms (TIP)- Functions and architecture, Integration with security tools.	09
3	**Cyber Threat Data Collection and Analysis** Indicators of Compromise (IoC), Threat Data Analysis Techniques-Malware indicators and Behavioral patterns, Network indicators and anomaly identification, Log Collection and Security Event Data-Sources of security logs, Data preprocessing techniques for security analytics, Threat pattern identification and correlation.	07
4	**Security Analytics Fundamentals** Introduction to Security Analytics, Role of Data Analytics in Cyber Security, Big Data Technologies for Security Analytics, Log Analysis Techniques, Event Correlation Method, Security Metrics and Key Performance Indicators (KPIs), Visualization of security intelligence and dashboards.	06
5	**Threat Intelligence Sharing and Standards** Threat Intelligence Sharing Models, Security Information Sharing Platforms Standards and Frameworks, STIX (Structured Threat Information Expression), TAXII (Trusted Automated Exchange of Indicator Information) OpenIOC, AI-driven Threat Detection Systems.	05
6	**Security Operations and Threat Mitigation** Threat Hunting Techniques, Cyber Threat Mitigation Strategies, Security Automation and Orchestration (SOAR), Security Information and Event Management (SIEM) Architecture, Incident Detection using SIEM, Event Correlation and Alert Management, Threat Intelligence in Enterprise Security, Security in Advanced Persistent Threats (APT).	07
	Total	42

List of Laboratory Experiments:	
Sr. No.	**Suggested Experiments**
1	To Study Strategic and Technical Threat Intelligence Investigation through an open-source intelligence (OSINT) Environment.
2	To implement map attack techniques for threat analysis and adversary behavior visualization.
3	To implement the Threat Data Extraction Technique for cyber threat intelligence investigations.
4	To study the Threat Intelligence Platform (TIP) Architecture for effective threat data management and intelligence sharing.
5	To Detect Malware Signatures for cybersecurity threat assessment by using the VirusTotal platform.
6	To study Log Aggregation and Preprocessing Techniques for security monitoring and event analysis by using Splunk software platform.
7	To study Data Visualization Techniques for Threat Intelligence using Kibana.
8	To implement security metrics for cybersecurity performance measurement and evaluation using Python.
9	To implement threat intelligence objects for structured threat information representation using STIX Data Modeling.
10	To Implement Automated Threat Intelligence Sharing for efficient cybersecurity collaboration using the TAXII Framework.
11	To implement Threat Hunting Techniques to Investigate Hidden Cybersecurity vulnerabilities using ELK Stack.
12	To implement the SIEM Architecture for Centralized Monitoring by using Splunk.
13	To study SOAR-Based Workflow Automation for Security Operations using Cortex XSOAR.
14	To study Advanced Persistent Threat (APT) Attacks for intrusion pattern investigation by using MITRE ATT&CK.
15	To demonstrate Dark Web Monitoring and Hidden Data Sources for cyber threat data acquisition using Tor Browser.

Books Recommended:

Text Books:

1. Valentin Pletzer, "Practical Threat Intelligence and Data-Driven Threat Hunting", Packt, 2025, ISBN-978-1-80323-375-8.
2. Ali Dehghantanha, Mauro Conti, Inez Miyamoto "Cyber Threat Intelligence", Springer 2018, ISBN-978-3-319-73950-2.

Reference Books:

1. Christopher Ahlberg, "The Threat Intelligence Handbook", CyberEdge Group, 2022, ISBN-13: 978-0-9990354-6-7.

2. Don Murdoch, "Blue Team Handbook: Incident Response Edition", Amazon KDP, 2019-2025,978-1091493896.
3. Chris Sanders, Jason Smith, "Applied Network Security Monitoring", Syngress (Elsevier), 2014, ISBN-978-0-12-417208-1.

Web resources:

1. Introduction to CTI: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/
2. Threat Intelligence Lifecycle & Data Sources:https://www.recordedfuture.com/threat-intelligence-lifecycle/
3. Threat Data Collection & Analysis: https://www.mandiant.com/resources/blog/indicators-of-compromise
4. Security Analytics Fundamentals: https://www.elastic.co/what-is/security-analytics
5. Threat Intelligence Sharing & Standards: https://oasis-open.github.io/cti-documentation/
6. Security Operations & Threat Mitigation: https://www.ibm.com/topics/siem

Online Courses: NPTEL / Swayam

1. Cyber Security and Privacy: Prof. D. Mukhopadhyay, IIT Kharagpur, https://nptel.ac.in/courses/106106129
2. Introduction to Cyber Security: Prof. Indranil Sengupta, IIT Kharagpur, https://nptel.ac.in/courses/106105217
3. Data Analytics with Python: Prof. Ragunathan Rengasamy, IIT Madras, https://nptel.ac.in/courses/106104189
4. Big Data Computing: Prof. S. Sadagopan, IIT Bangalore, https://nptel.ac.in/courses/106104189
5. Ethical Hacking: Prof. Indranil Sengupta, IIT Kharagpur, https://nptel.ac.in/courses/106105217

Semester End Examination (A):

Theory:

1. Question paper based on the entire syllabus total comprising of 60 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 performed during laboratory sessions.

Continuous Assessment (B):

Theory:

1. Term Test 1 (based on 40 % syllabus) of 15 marks for the duration of 45 min.
2. Term Test 2 (on next 40 % syllabus) of 15 marks for the duration of 45 min.
3. Term Test 3 conduction can be Assignment / course project / group discussion /presentation / quiz/ any other for 10 marks.

Laboratory: (Term work)

1. Term Work shall consist of at least 8 practicals based on the above list.
2. The distribution of marks for term work shall be as follows:
   i. Laboratory work (Performance of Experiments, Write-up): 15Marks
   ii. Assignment (HackerRank Task, quiz, Descriptive/Analytical Questions): 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 Computer Science and Engineering (IoT and Cybersecurity with Block chain Technology)	Final Year B.Tech	Semester: VII
Course: Reinforcement Learning	Course Code: DJS23BCPE714	
Course: Reinforcement Learning Laboratory	Course Code: DJS23BLPE714	

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	Term Test 3	Total	
				60			15	15	10	40	100
				Laboratory Examination			Term work			Total Term work	50
3	2	--	4	Oral	Practical	Oral & Practical	Laboratory Work		Tutorial / Mini project presentation Assignment		
				25	--	--	15		10	25	

Pre-requisite:

1. Machine Learning
2. Deep Learning

Course Objectives: The objective of the course is:

1. Introduce the fundamental concepts, principles, and approaches of Reinforcement Learning and its difference from supervised learning.
2. To develop understanding of various Reinforcement Learning techniques such as Dynamic Programming, Monte Carlo methods, Temporal Difference learning, and Policy Gradient approaches.
3. To enable students to analyze and implement Reinforcement Learning algorithms including SARSA, Q-Learning, Deep Q-Networks, and Actor-Critic methods.
4. To familiarize students with advanced concepts of Deep Reinforcement Learning and their real-world applications such as AlphaGo and intelligent decision-making systems.

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

1. Explain the fundamentals and key elements of Reinforcement Learning (RL).
2. Apply value-action based methods such as sample average, greedy, and ε-greedy approaches for action selection problems.
3. Describe the roles of agents, environments, goals, rewards, returns, and policies in Reinforcement Learning systems.

4. Apply policy evaluation, policy improvement, policy iteration, and value iteration methods to solve decision-making problems.
5. Analyze eligibility trace concepts, including N-step TD methods, online and offline updation, and TD(λ) approaches.
6. Describe the concepts and workflow of Deep Reinforcement Learning, including Deep Q-Networks (DQN) and methods for improving DQN performance.

Detailed Syllabus:

Unit	Description	Duration
1	**Introduction:** Reinforcement Learning (RL), Elements of Reinforcement Learning, Reinforcement Learning vs Supervised Learning, Approaches of solving Reinforcement Learning: Value based, policy based, model based, Exploration - Exploitation dilemma, Evolutionary methods, Immediate Reinforcement Learning, Deep Q-Network (DQN).	06
2	**Immediate Reinforcement Learning:** Bandit Problems: Bandit problems, Value-action based methods (sample average), Greedy method, ϵ-greedy method, Incremental Implementation, Nonstationary problem, Optimistic Initial values, UCB algorithm, Thompson Sampling. **Policy Gradient Approaches:** Linear reward Penalty Algorithm, Parameterised policy representation(Θ), Evaluation of policy($\eta(\Theta)$), REINFORCE algorithm.	07
3	**Full Reinforcement Learning** Difference between Immediate and Full Reinforcement Learning, Agents and Environment, Goals, Rewards, Returns, Policy in Full Reinforcement Learning, Episodic and Continuing Tasks. **Markov Decision Process (MDP)** Markov Property, Finite Markov Decision Process, Value functions, Bellman's equations, optimal value functions, Definition of MDP in Reinforcement Learning, Solution of the Recycling Robot problem	07
4	**Dynamic Programing** Policy evaluation, policy improvement, policy iteration, value iteration, Asynchronous Dynamic Programing, Generalized Policy Iteration (GPI), bootstrap, full back up. **Monte Carlo Method** Advantages of Monte Carlo over Dynamic Programing, Monte Carlo Control, on-policy, off-policy, Incremental Monte Carlo, Issues/Assumptions in Monte Carlo Methods, Solution of BlackJack using Monte Carlo Method	10
5	**Temporal Difference Learning** Defination, Advantages of Temporal Difference methods over Monte Carlo and Dynamic Programming methods, TD(0), Onpolicy vs off-policy, SARSA, Qlearning. **Eligibility traces** N-step Temporal Difference methods, On-line vs Off-line updation, TD(λ) : forward view, backward view, Traces: Accumulating trace, Dutch trace, Replacing trace, Equivalence of forward and backward view, SARSA(λ)	06

6	**Function Approximation** Drawbacks of tabular implementation, Function Approximation, Gradient Descent Methods, Linear parameterization, Policy gradient with function approximation **Deep Reinforcement Learning** Intro of Deep Learning in Reinforcement Learning, Deep learning training workflow, Categories of Deep learning, Deep Q-Network, Ways of improving Deep Q-Network, REINFORCE in Full Reinforcement Learning, Actor-Critic Algorithm, Algorithm Summary, DDPG, Case study on AlphaGo by Google DeepMind	06
Total		**42**

List of Laboratory Experiments:	
Sr.No.	**Suggested Experiments**
1.	Implementation of Greedy and Epsilon greedy methods.
2.	Implementation of Reinforcement algorithm on Cartpole/Lunar Lander.
3.	Implementation of gridworld using Dynamic Programming.
4.	Implementation of Dynamic Programming and monte Carlo Methods
5.	Implementation of Frozen lake using SARSA
6.	Implementation of Grid world using Q learning.
7.	Implementation of Temporal Difference.
8.	Implementation of Deep Q Network Algorithm.
9.	Implementation of Actor Citric.
10.	Case Study on recent topic in Reinforcement learning

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

Books Recommended:

Text Books

1.Richard S. Sutton and Andrew G. Barto, "Reinforcement Learning: An Introduction", MIT Press, 2nd Edition, 2018. 2.Laura Graesser Wah Loon Keng, "Foundations of Deep Reinforcement Learning," Pearson Education, 1st Edition, 2020.

Reference Books

1. Phil Winder, "Reinforcement Learning Industrial Applications of Intelligent Agents", O'Reilly, 1st Edition, 2020.

2. Csaba Szepesvari, "Algorithms for Reinforcement Learning," Morgan & Claypool Publishers, 1st Edition, 2019.

3. Enes Bilgin, "Mastering Reinforcement Learning with Python", Packt publication, 1st Edition, 2020.

4. Brandon Brown, Alexander Zai, "Deep Reinforcement Learning in Action", Manning Publications, 1st Edition, 2020.
5. Micheal Lanham, "Hands-On Reinforcement Learning for Games," Packt Publishing, 1st Edition, 2020.
6. Abhishek Nandy, Manisha Biswas, "Reinforcement Learning: With Open AI, TensorFlow and Keras using Python," Apress, 1st Edition, 2018.

Web Resources:

1. AI Games with Deep Reinforcement Learning: https://towardsdatascience.com/how-to-teach-an-ai- toplay-games-deep-reinforcement-learning-28f9b920440a
2. Deep Reinforcement Learning: https://www.v7labs.com/blog/deep-reinforcement-learning-guide

Online References

1. Reinforcement Learning by Prof. Balaraman Ravindran, IIT Madras, https://onlinecourses.nptel.ac.in/noc22_cs75/preview
2. Reinforcement Learning Course (Stanford University) by Emma Brunskill :https://web.stanford.edu/class/cs234/

Evaluation Scheme:

Semester End Examination (A):

Theory:

1. Question paper will be based on the entire syllabus summing up to 60 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. Term Test 1 (based on 40 % syllabus) of 15 marks for the duration of 45 min.
2. Term Test 2 (on next 40 % syllabus) of 15 marks for the duration of 45 min.
3. Term test 3 Assignment / course project / group discussion /presentation / quiz/ any other for 10 marks.

Laboratory: (Term work)

1. Term Work shall consist of at least 8 practical's based on the above list.
2. The distribution of marks for term work shall be as follows:
   i. Laboratory work (Performance of Experiments, Write-up): 15Marks
   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** **Head of the Department** **Vice Principal** **Principal**

Program: B. Tech in Computer Science and Engineering (IoT and Cybersecurity with Block chain Technology)	Final Year B.Tech	Semester: VII
Course: Agentic AI	Course Code: DJS23BCPE715	
Course: Agentic AI Laboratory	Course Code: DJS23BLPE715	

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	Term Test3	Total	
				60			15	15	10	40	100
				Laboratory Examination			Term work			Total Term work	50
3	2	--	4	Oral	Practical	Oral & Practical	Laboratory Work		Tutorial / Mini project / presentation/ Assignment		
				25	--	--	15		10	25	

Pre-requisite:

1. Artificial Intelligence
2. Machine Learning

Course Objectives: The objective of the course is:

1. To understand fundamentals of Agentic AI.
2. To Analyze and compare different agent architectures (deliberative, reactive, and hybrid) for various problem domains.
3. Apply modern frameworks like LangGraph and AutoGen to design and develop AI agents and multi-agent workflows.
4. To Understand and implement Agentic RAG systems, including adaptive retrieval and integration.

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

1. Analyze the structure and architecture of single-agent and multi-agent systems
2. Understand and differentiate between self-governance, agency, and autonomy with suitable examples.
3. Explain the fundamentals of LangGraph and its role in building AI agent workflows.
4. Analyze the architecture and key components of Agentic RAG systems.
5. Develop and implement AutoGen-powered agents for solving structured tasks.
6. Explain the concepts of AI agent observability and AgentOps, including their importance in real-world deployments.

Detailed Syllabus:		
Unit	**Description**	**Duration**
1	**Introduction**: Introduction to agentic AI, Agent structure and Architecture of multi agent system, Autonomous Agents, Human in the loops Systems, Multi Agent AI Systems, Agent AI Framework, Design Considerations and Best Practices, Autoregressive models and Transformer architecture LLM-powered AI agents ,Applications of generative AI Challenges and limitations of generative AI.	06
2	**Principles of Agentic Systems:** Technical requirements, Understanding self-governance, agency, and autonomy ,Self-governance Agency Autonomy Example of agency and autonomy in agents ,Reviewing intelligent agents and their characteristics, Exploring the architecture of agentic systems, Deliberative architectures, Reactive architectures, Hybrid architectures	08
3	**Building AI Agents with LangGraph:** Introduction to LangGraph , State Management , Trim and Filter Messages , Memory and External Memory , Short-Term and Long-Term Memory , Memory Schema , Deployment	06
4	**Agentic RAG:** Comparing Agentic RAG with Traditional RAG , Agentic RAG Architecture and Components, Adaptive RAG, Variants of Agentic RAG ,Applications of Agentic RAG , Agentic RAG with Llama Index	10
5	**Agent Development with AutoGen:** Autogen Introduction , Roles and Conversations , Conversation Patterns , Developing Autogen-powered Agents , Deployment and Monitoring , Multi-Agent Systems with LangGraph: Multi-Agent Systems ,Workflows ,Collaboration ,Multi-Agent Designs ,Workflow with LangGraph	06
6	**Deploying AI Agent:** AI Agent Observability and AgentOPs, AI Observability with Langsmith, Monitoring, AI Agent Performance, Managing AI Workflows, Implementing AI Experimentation and Observability	06
	Total	42

List of Laboratory Experiments:	
Sr.No.	**Suggested Experiments**
1.	Exploring different Agentic AI frameworks
2.	Implementing different Agentic AI design patterns
3.	Building a chatbot agent with LangGraph for an appropriate industry domain.
4.	Build an agent to perform appropriate market research implementing agentic RAG techniques
5.	Implement an AI Research Agent with Autogen
6.	Implement AI Observability with Langsmith
7.	Implementation of AgentOps for AI Workflow Monitoring
8.	Implementation of Multi-Agent Communication System
9.	Implement conversational agents with specialized roles
10.	Implement deployment of LangGraph-Based AI Agents

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

Books Recommended:

Text Books

1. Mastering AI Agents: From Design to Deployment of Autonomous Systems by Elbert Gale January 18, 2025 ISBN-13: 979-8307403822

2. Building AI Agent: Learn Building AI Agents, A Practical Guide for Building Intelligent Agents by Natenapis Faraksa March 2, 2024.

3. Build Your Own AI Agent: A Hands-On Guide for Beginners by Sujai G Pillai January 13, 2025, ISBN-13: 979-8306885971.

Reference Books

1. Agentic AI with Langchain & Langgraph, by Elliot R. Stroud,Amazon Digital Services LLC - Kdp, 2025

2. Building Agentic AI with Python and LangGraph", by Yuan Zhu, Amazon Digital Services LLC - Kdp, 2025.

Web Resources:

1. https://www.uipath.com/ai/agentic-ai
2. https://www.ibm.com/think/topics/agentic-ai

Online References

1. Applications of GenAI and Agentic AI in Business, By Dr. Anik Mukherjee, IIM Calcutta
https://elearn.nptel.ac.in/product-page/applications-of-genai-and-agentic-ai-in-business

Evaluation Scheme:

Semester End Examination (A):

Theory:

1. Question paper will be based on the entire syllabus summing up to 60 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. Term Test 1 (based on 40 % syllabus) of 15 marks for the duration of 45 min.
2. Term Test 2 (on next 40 % syllabus) of 15 marks for the duration of 45 min.
3. Term Test 3 Assignment / course project / group discussion /presentation / quiz/ any other for 10 marks.

Laboratory: (Term work)

1. Term Work shall consist of at least 8 practical's based on the above list.
2. The distribution of marks for term work shall be as follows:
   i. Laboratory work (Performance of Experiments, Write-up): 15Marks
   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	Head of the Department	Vice Principal	Principal

Program: B. Tech in Computer Science and Engineering (IoT and Cybersecurity with Block chain Technology)	Final Year B.Tech	Semester: VII
Course: Prompt Engineering	Course Code: DJS23BCPE716	
Course: Prompt Engineering Laboratory	Course Code: DJS23BLPE716	

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	Term Test 3	Total	
				60			15	15	10	40	100
				Laboratory Examination			Term work			Total Term work	50
3	2	--	4	Oral	Practical	Oral & Practical	Laboratory Work		Tutorial / Mini project presentation Assignment		
				25	--	--	15		10	25	

Pre-requisite:

1. Machine Learning.
2. Large Language Models.

Course Objectives: The objective of the course is:

1. To understand the importance of prompt engineering.
2. To design effective prompts for different tasks.
3. To build real world AI Workflows(chatbot).
4. To evaluate and improve AI outputs

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

1. Explain the fundamentals of prompt engineering, importance and evolution in modern AI systems.
2. Design prompts using suitable formats to achieve desired outputs from AI systems.
3. Implement structured reasoning approaches including chain-of-thought and step-by-step prompting to improve response accuracy.
4. Handle errors and ambiguity in prompts to improve clarity and response accuracy.
5. Implement techniques to control hallucinations and improve the reliability of generated content.
6. Deploy and run applications effectively on the Hugging Face platform.

Detailed Syllabus:		
Unit	**Description**	**Duration**
1	**Introduction:** Prompt Engineering, Clarity, Specificity, Context, Instructional Prompts, Eliminating Bias, Creativity and Constraint, Interactive Refinement, Sequential Prompts, Importance of Prompt Engineering, Evolution of Prompt Engineering, Overview of tools (ChatGPT, Claude, Gemini)	06
2	**The Five Principles of Prompting:** Overview of the Five Principles of Prompting, Give Direction, Specify Format, Provide Examples, Evaluate Quality, Divide Labor, Structure of good prompt, Prompt formats	06
3	**Prompt Techniques**: Anatomy of prompt, Writing Effective Prompt, Types of Prompt, Prompt Techniques: General Knowledge prompting, Automatic Prompt Engineering. Role prompting, Chain-of-thought prompting ,Step-by-step reasoning, Output formatting (tables, JSON)	06
4	**Building Custom Prompt:** A model Custom prompt, Sample custom prompts, Strategies for Prompt Engineering : Temperature Control, Length Control, Explicit Instruction, Informativeness, Constraint Handling, Error Handling, Handling Ambiguity, Ethical Prompt Engineering.	10
5	**Advanced Prompt design Techniques:** Multi turn Conversation Prompts, Contextual Prompt, Exploratory Prompts, Question Answering, Multi Model Prompting, Incorporating External Knowledge, Mitigating Bias and Fairness Issues. Controlling hallucinations, Prompt chaining	06
6	**Deployment with HuggingFace:** Create new Space, Deployment of Files, Building the Application, Running the Application, Deployment of applications. **Sample Use Cases:** Question Answering, Sentimental Analysis, Chatbots and assistants ,Content generation (blogs, emails) , Code generation , Data analysis prompts	08
	Total	42

List of Laboratory Experiments:	
Sr.No.	**Suggested Experiments**
1.	Program to analyzing Prompt Output Quality Based on Key Evaluation Metrics
2.	Program to perform Chain-of-Thought Prompting
3.	Program to perform Constraint-based Prompting
4.	Program to generate outputs with different temperature values.and Analyze creativity vs accuracy.
5.	Program to compare outputs from different LLMs.
6.	Program to perform open-ended prompts for brainstorming ideas.
7.	Program to maintain context across prompts and observe coherence.

8.	Program to build prompt-based sentiment analyzer
9.	Program to implement upload PDF/text and ask questions and perform Document-based Question Answering.
10.	Program to implement load a pre-trained model and test prompts using Hugging Face Transformers.

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

Books Recommended:

Text Books

1. Subramanian Venkataraman, "Crafting Effective Prompts A Practice to Prompt Engineering Kindle edition", 1 st edition, 2024.

2. James Phoenix and Mike Taylor, "Prompt Engineering for Generative AI", 1 st Edition, O'Reilly, 2024.

3. Yaswanth Sai Palaghat,,"Prompt Engineering: The Art of Asking", Notion Press, 2022

Reference Books

1. John Berryman, Albert Ziegler, Prompt Engineering for LLMs, O'Reilly Media, 2024.

2. Rakesh Vanzara , Paresh Solanki , Devang Pandya," Prompt Engineering: Master the Art of Asking AI", Notion Press Media Pvt. Limited,2025.

3. Ian Khan, "The Quick Guide to Prompt Engineering", Wiley, 1st edition,2024.

Web Resources:

1. Learn Prompt Engineering: https://learnpromptengineering.dev/?utm_source=chatgpt.com
2. Prompt Engineering: https://www.ibm.com/think/topics/prompt-engineering
3. Prompt Engineering Guide: https://learnprompting.org/docs/introduction?srsltid=AfmBOoq_tegurcUarQ9P3rABoYX9X2xyx_s5cocmVn2a4WSk54UoD06r

Online References

1. Course era Course on Prompt Engineering Specialization by Dr. Jules White: https://www.coursera.org/specializations/prompt-engineering/?utm_source=chatgpt.com

Evaluation Scheme:

Semester End Examination (A):

Theory:

1. Question paper will be based on the entire syllabus summing up to 60 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. Term Test 1 (based on 40 % syllabus) of 15 marks for the duration of 45 min.
2. Term Test 2 (on next 40 % syllabus) of 15 marks for the duration of 45 min.
3. Term Test 3 Assignment / course project / group discussion /presentation / quiz/ any other for 10 marks.

Laboratory: (Term work)

1. Term Work shall consist of at least 8 practical's based on the above list.
2. The distribution of marks for term work shall be as follows:
   i. Laboratory work (Performance of Experiments, Write-up): 15Marks
   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	Head of the Department	Vice Principal	Principal

Program: B. Tech in Computer Science and Engineering (IoT and Cybersecurity with Block chain Technology)	Final Year B.Tech	Semester : VII
Course : Large Language Models	Course Code: DJS23BCMD701	
Course: Large Language Models Laboratory	Course Code: DJS23BLMD701	

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	Term Test 3	Total	
				60			15	15	10	40	100
				Laboratory Examination			Term work			Total Term work	50
2	2	--	3	Oral	Practical	Oral & Practical	Laboratory Work		Tutorial / Mini project presentation Assignment		
				25	--	--	15		10	25	

Pre-requisite:

1. Machine Learning
2. Deep Learning

Course Objectives: The objective of the course is to:

1. Introduce the fundamental concepts and applications of Generative AI.
2. Provide in-depth understanding of Transformer architecture, the core building block of most Large Language Models (LLMs).
3. Explore various LLM architectures and techniques like BERT, prompt engineering, and fine-tuning.
4. Identify Multimodal LLMs that can process and understand different data modalities.

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

1. Introduce the fundamental concepts and applications of Generative AI.
2. Explore various LLM architectures and techniques like BERT, GPT-3, T5.
3. Describe the role of Large Reasoning model in solving complex task reasoning and memory retention.
4. Apply prompt engineering techniques for effective LLM interaction.
5. Analyze the concept of Retrieval Augmented Generation (RAG) and its role in LLMs.
6. Explore the different data modalities using Multimodal Architectures.

Detailed Syllabus:

Unit	Description	Duration
1	**Introduction to Generative AI &Transformer Architecture:** Domains of Generative AI, Small language model. Limitations of RNN & LSTM, Tokenization, LLM Parameters(temp, Top k etc), Transformer Architecture: encoders, decoders, attention mechanisms - types, Self-attention vs Flash Attention, feed-forward layer, Reinforcement Learning with AI Feedback (RLAIF), Reinforcement Learning from Human Feedback (RLHF)	06
2	**Language Models - Unveiling the Power of Words:** BERT (Bidirectional Encoder Representations from Transformers) and its applications, exploring other notable LLM architectures (e.g.GPT-3, T5), Mixture of Experts (MoE), Various benchmarks to evaluate LLMs – perplexity, BLEU score, Needle in a Haystack	04
3	**Large Reasoning Models:** Deep seek- v2: Multi head Latent Attention, Deep seek MoE, Mistral 7-B Architecture: sliding Window attention, Grouped Query Attention, Knowledge Distillation.	04
4	**Prompt Engineering &Agentic AI** Introduction to prompt, examples of prompt, prompt engineering, prompt techniques, zero shot, one shot, few-shot learning, Agentic AI- a chain of thought , ReAct , self-consistency, Tree of thought, Multimodal CoT, Graph prompting. Large Action Models(LAMs), LLM based Agents, Auto Gen, Context compression for deep agents.	04
5	**Retrieval Augmentation & Generation (RAG) and Fine-tuning for LLMs :** Understanding Retrieval and vector, vector storage: vector indexing and retrieval Algorithms: Annoy, HSNV, Inverted File System, LSH, vector quantization techniques: Scalar, Product, Binary, vector libraries, vector databases, Loading and retrieving in Lang Chain, Document loaders, Retrievers in Lang Chain. Fine-tuning: Quantization, PEFT. Full-Finetuning vs LoRA vs QLoRA, Fine-Tuning LLMs for different downstream tasks.	06
6	**Multimodal Architectures - Beyond Text** Introduction to Multimodal LLMs, Exploring architectures for Multimodal LLMs: Vision Transformer, Next GPT, Applications of Multimodal LLMs (e.g., image captioning, video summarization).	04
	Total	**28**

List of Laboratory Experiments:

Sr.No.	Suggested Experiments
1	Case study on Applications of Generative AI
2	Case study on role of Artificial Intelligence in achieving the Sustainable Development Goals
3	Fine Tuning Pre-trained Model On Custom Dataset (synthetic data) Using Transformer
4	Build your own LLM from scratch.
5	Query PDF using Lang Chain and Pine cone
6	Fine Tune Mistral7-B With Custom Dataset Using LoRA And QLoRA Techniques
7	Using in-built tools and creating custom tools for ReAct agent in Langchain.
8	Question Answering Application using LLM based agents.
9	Understanding various retrievers in Langchain.
10	Case study on comparison of Large Reasoning Models
11	Understanding multimodal models like Gemini vision

12	Build a simple multimodal generative model that combines text and image inputs to generate captions
13	Mini project (A group of 3 to 4 students is required to develop an application using LLM models and submit report)

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

Books Recommended:

Text Books

1. Ben Auffarth, "Generative AI with LangChain: Build large language model (LLM) apps with Python, ChatGPT, and other LLMs" by Packt Publishing, 2023.

2. Valentina Alto, "Modern Generative AI with ChatGPT and OpenAI Models", by Packt Publishing, 2023.

3. Jay Alammar, Maarten Grootendorst, "Hands-On Large Language Models", by O'Reilly, 2023

4. Thushan Ganegedara, "Natural Language Processing with TensorFlow", by Packt Publishing, Second Edition, 2022.

Reference Books

1. David Foster, "Generative Deep Learning", O'Reilly, 2020.

2. Lewis Tunstall, Leandro von Werra & Thomas Wolf," Natural Language Processing with Transformers", 2022.

3. Sebastian Raschka, "Build a Large Language Model (From Scratch)", ISBN 9781633437166

Web resources:

1. Mixture of Experts: Mixture of Experts Explained (huggingface.co)
2. PEFT:Efficient Model Fine-Tuning for LLMs: Understanding PEFT by Implementation | by Shivansh Kaushik | Medium
3. Various benchmarks to evaluate LLMs: LLM Benchmarks: Understanding Language Model Performance (humanloop.com)
4. Various benchmarks to evaluate LLMs: LLM Benchmarks: Understanding Language Model Performance (humanloop.com)
5. Types of attention mechanism: Understanding and Coding the Self-Attention Mechanism of Large Language Models From Scratch (sebastianraschka.com)
6. Agents| RAG: Intro to LLM Agents with Langchain: When RAG is Not Enough | by Alex Honchar | Mar, 2024 | Towards Data Science
7. React| Agent: Teaching LLMs to Think and Act: ReAct Prompt Engineering | by Bryan McKenney | Medium
8. LLM based Agents : Superpower LLMs with Conversational Agents | Pinecone
9. RAGAS: Evaluating RAG pipelines with Ragas + LangSmith (langchain.dev)

10. Model distillation: LLM distillation demystified: a complete guide | Snorkel AI
11. Sentence classifier |BERT: Classify text with BERT | Text | TensorFlow

Online Courses: NPTEL / Swayam

1. Course on- Introduction to Large Language Models (LLMs)- By Prof. Tanmoy Chakraborty, Prof. Soumen Chakraborti , IIT Delhi, IIT Bombay,

https://onlinecourses.nptel.ac.in/noc25_cs45/preview

Evaluation Scheme:

Semester End Examination (A):

Theory:

1. Question paper will be based on the entire syllabus summing up to 60 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. Term Test 1 (based on 40 % syllabus) of 15 marks for the duration of 45 min.
2. Term Test 2 (on next 40 % syllabus) of 15 marks for the duration of 45 min.
3. Term test 3 Assignment / course project / group discussion /presentation / quiz/ any other for 10 marks.

Laboratory: (Term work)

Term work shall consist of minimum 10 experiments.

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

i. Laboratory work (Performance of Experiments): 10 Marks

ii. Assignments: 5 Marks

ii. Mini project (Implementation, Report): 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: All programs	Final Year B. Tech.	Semester: VII/VIII
Course: Research Ecosystem (DJS23ITELX12)		

Pre-requisites:

1. Basic understanding of Engineering concepts and problem-solving techniques.
2. Fundamental knowledge of project-based learning, data analysis, and domain-specific tools.
3. Basic exposure to project development, technical report writing, and emerging technologies.

Objectives:

1. To understand and identify complex engineering, societal, and industrial problems suitable for research through structured analysis of literature, patents, and real-world needs.
2. To learn and apply advanced research methodologies—including experimental, simulation-based, and data-driven approaches—for designing and validating engineering solutions.
3. To gain proficiency in selecting and using appropriate tools, software, and platforms (AI/ML, simulation, CAD, IoT, etc.) for experiment design, data acquisition, and performance evaluation.
4. To transform research insights into innovative prototypes, products, or startup concepts by engaging with innovation ecosystems, TRLs, and funding mechanisms.
5. To analyze socio-technical systems, ethics, and sustainability implications of engineering solutions, ensuring responsible and impactful outcomes.
6. To integrate systems thinking, multidisciplinary perspectives, policy awareness, future technology trends, and technical documentation skills to develop comprehensive research proposals and outputs (papers, patents, reports).

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

1. Analyze complex engineering and societal problems to evaluate literature and patents and formulate clear research gaps.
2. Design and apply advanced research methods and tools to acquire data and evaluate solution performance.
3. Transform research insights into prototypes or startup concepts using innovation frameworks and Technology Readiness Levels.
4. Evaluate ethical, socio-technical, and sustainability issues and create responsible engineering solutions.
5. Synthesize multidisciplinary knowledge to create research proposals and scalable, future-ready solutions.

Research Ecosystem (DJS23ITELX12)		
Unit	**Description**	**Duration**

1	**Research Gap Identification & Advanced Problem Formulation**
	• Identifying high-impact problems from:
	  ▪ Industry and Society
	  ▪ Emerging technologies (AI, IoT, Blockchain, EV, etc.)
	• Research gap identification techniques:
	  ▪ Systematic Literature Review (SLR)
	  ▪ Patent analysis
	• Defining objectives, scope, constraints, and feasibility of the identified problem
	• Writing problem statement for:
	  ▪ Research paper
	  ▪ Product/Startup idea
	Activities:
	• Convert Industry/ Societal problem into research problem.
	• Analyze research articles and extract research gaps.
		05

2	**Experimental Design, Tools & Validation Techniques**
	• Advanced research methodologies:
	  ▪ Experimental, simulation, data-driven, design thinking
	• Tool selection:
	  ▪ Computational tools and software, simulation and analysis platforms, system prototyping and testing platforms
	• Data acquisition:
	  ▪ Data collection interfaces, Principles of data cleaning and organization (primary / secondary data)
	• Validation techniques:
	  ▪ Accuracy and performance metrics
	  ▪ Benchmarking with existing solutions
	• Result interpretation & visualization
	Activities:
	• Selection of Research Design for final year project.
	• Apply evaluation metrics (e.g., ML model accuracy, system efficiency).
		06

3	**Research to Innovation, Product & Startup Ecosystem** • Research → Prototype → Product → Startup lifecycle • Intellectual Property Rights (IPR), patents, copyrights • Technology readiness levels (TRL) • Case studies: ▪ AI startups, EV ecosystem, Smart Cities • Industry-academia collaboration models • Funding opportunities (grants, incubation, government schemes - Anusandhan National Research Foundation (ANRF)) **Activities:** • Convert project into startup idea or product pitch. • Analyze failure of a technology/product.	05

4	**Socio-Technical Systems, Ethics & Sustainability**
	• Socio-technical systems: Interaction of people, technology and environment
	• Ethical issues:
	  ▪ Plagiarism, AI bias, data privacy
	• Sustainability in Engineering:
	  ▪ Green practices, resource optimization and lifecycle considerations
	• Impact assessment:
	  ▪ Social, economic, environmental
		06

	• Policies and governance (data protection laws, standards and compliance requirements) **Activities:** • Case study: Facial recognition ethics / smart surveillance. • Impact analysis of student's own project.	
5	**Integrated Research, Policy and Future Engineering Challenges** • Systems thinking and holistic analysis • Multidisciplinary problem solving: ▪ Healthcare tech, climate tech, smart mobility • Writing research proposals: ▪ Problem → Methodology → Expected outcomes • Future trends: ▪ AI ethics, Quantum computing, Industry 5.0 / 6.0 • Scaling solutions from lab to society **Activities:** • *Capstone Task:* ▪ Identify real-world problem. ▪ Apply research methodology. ▪ Propose: o Technical solution o Societal impact o Possible commercialization	**06**
	Total	**28**

Term Work Guidelines:

The Term Work (TW) shall consist of continuous assessment based on tutorials activities and a final group presentation.

a) **Part A (25 Marks):**
Each student shall complete a minimum of five tutorials based on the syllabus topics during the semester. The tutorials may include activities such as research gap identification, literature survey, case study analysis, tool-based experimentation, impact analysis, technical report writing, and innovation-oriented problem solving.

b) **Part B (25 Marks):**
Students shall work in groups and select a project/research topic based on emerging engineering, industrial, or societal challenges. The group presentation shall include:

i. Identification of a real-world problem
ii. Application of appropriate research methodology
iii. Proposed technical solution
iv. Analysis of societal impact
v. Possible commercialization/startup opportunities

Books Recommended:

Reference Books:

- Kothari, C. R., Research Methodology: Methods and Techniques, New Age International Publishers, New Delhi, 2023.
- Booth, W. C., Colomb, G. G., Williams, J. M., Bizup, J., & FitzGerald, W. T., The Craft of Research, University of Chicago Press, Chicago, 2024.
- Montgomery, D. C., Design and Analysis of Experiments, Wiley, New York, 2020.
- Singh, Pooja, Katiyar, Aman, Rawat, Shalini, Dhuri, Archana, Research Methodology and IPR, RK Publications, India, 2025.

- Blok, Vincent (Ed.), Putting Responsible Research and Innovation into Practice: A Multi-Stakeholder Approach, Springer Cham, Switzerland, 2022.

Web References:

- Research Methodology: Quantitative Methods and Computer Application (https://onlinecourses.swayam2.ac.in/e-learning/preview/ini26_ma02)
- Research Methodology and IPR (https://onlinecourses.swayam2.ac.in/e-learning/preview/ntr26_ed28)
- Research and Publication Ethics (https://onlinecourses.swayam2.ac.in/e-learning/preview/nou26_ge46)
- Research Ethics and Plagiarism (https://onlinecourses.swayam2.ac.in/e-learning/preview/nou26_ge26)
- Quantitative and Mixed Methods Research for Management (https://onlinecourses.swayam2.ac.in/e-learning/preview/imb26_mg21)
- Doing Qualitative Research (https://onlinecourses.swayam2.ac.in/e-learning/preview/nou26_ge61)

Prepared by **Checked by** **Head of the Department** **Vice-Principal** **Principal**

Program: B. Tech. (Common to all Programmes)	B. Tech.	Semester: VII/VIII
Course: Major Project	Course Code: DJS23IPELX13	

Objectives

The primary purpose of the Major Project is to enable students to apply the knowledge and skills acquired across the programme to conceive, design, implement, and evaluate a comprehensive solution to a real-world problem. The project strengthens technical competence, communication, and teamwork by integrating design, development, technical writing, presentation, and collaborative work. It emphasises professional engineering practice and addresses a range of non-technical considerations such as economic factors, safety, reliability, ethics, sustainability, and environmental and societal impact.

Course Outcomes (CO)

On successful completion of the Major Project, the student will be able to:

CO1: Apply technical knowledge gained from previous courses to identify real-life, industry, or societal problems and design appropriate solutions.

CO2: Demonstrate the technical skills required to design, develop, build, and test engineering systems, products, software, or hardware using modern engineering and IT tools.

CO3: Apply project-management skills — scheduling work, procuring resources/components, budgeting, documenting technical and non-technical details, and working within defined deadlines as an effective team.

CO4: Develop and demonstrate the ability to test, validate, debug, and troubleshoot engineering systems (including software, hardware, and process components) and analyse the results.

CO5: Create technical reports and research papers in the prescribed format and effectively communicate and present the work to evaluators.

Scope and Nature of the Project Work

Final-year students have already undertaken project assignments in their pre-final year through Innovative Product Design / Mini Project work. In the final year, a group of a maximum of four students completes a comprehensive project based on the courses studied. The project work may be internally assigned or externally assigned by research institutes, industry, or similar organisations. Each group is assigned one faculty member as supervisor. The final-year project may be an extension of the Mini Project carried out in the pre-final year.

The main intention of the project work is to enable students to apply the knowledge and skills learnt across the programme to solve or implement a well-defined practical problem. The work may go beyond the scope of the curriculum or build upon courses studied, but the thrust should be on:

- Learning additional skills relevant to the chosen domain;
- Developing the ability to define, design, analyse, and implement a problem and carry it through to completion with proper planning;
- Learning behavioural science and professional ethics by working effectively in a group;
- Selecting a project area aligned with the student's intended higher education, employment, or self-employment goals;
- Choosing a topic that differs from, or meaningfully advances, the Mini Project topic;

- Using the opportunity to learn modern computational techniques, tools, and model development through an appropriate choice of project.

Continuous Assessment and Term Work

The department maintains a proper record of the progress of each project throughout the semester. At the end of the semester, the work is assessed for the award of Term Work (TW) marks by an approved internal faculty member appointed by the Head of the Institute, on the basis of:

- Scope and objectives of the project work;
- Extent and quality of the literature survey;
- Progress of the work (continuous assessment across reviews);
- Design, implementation, and analysis of the project work;
- Results, conclusions, and future scope;
- Report prepared in the prescribed University / institutional format.

Oral / Practical Examination: An approved external examiner together with an internal examiner appointed by the Head of the Institute assesses the project during the oral examination. The oral examination consists of a presentation by the group along with a demonstration of the work done. Each student is assessed individually for their contribution, understanding, and the knowledge gained.

Project Guide / Topic Allocation Policy

The project guide and topic-allocation policy is explained to students during the Orientation held in Semester VI. Each faculty member is allocated a minimum of one and a maximum of four project groups. As per the timeline in the academic calendar, the list of project topics and areas offered by each faculty member — three topics per faculty member — is displayed on the notice board. Allocation is carried out over successive rounds, and in each round students submit their preferences against the available topics and guides.

If a topic is preferred by only one group, that group is allocated to the corresponding guide and topic. If a topic is preferred by more than one group, the concerned faculty member reviews the applications and selects one group; the remaining groups carry forward to the next round. After each round, the list of groups and guides allotted so far is displayed, along with the topics and guides that remain available. Unallotted groups then submit fresh preferences from the available list. This process continues over successive rounds until every group has been allotted a guide, ensuring a uniform distribution of project groups among the faculty members.

Assessment Scheme

The Major Project carries a total of 100 marks — **Term Work (50)** assessed internally through continuous evaluation, and **Oral / Practical Examination (50)** assessed jointly by internal and external examiners. Each criterion is scored against three performance levels — Excellent, Satisfactory, and Below Expectation — as detailed below.

Rubric for Term Work (50 Marks)

Assessment Criteria (mapped CO)	Max	Excellent	Satisfactory	Below Exp.
Problem Definition, Objectives & Literature Survey (CO1)	**10**	8–10	5–7	0–4
Design, Methodology & Implementation Progress – Continuous Assessment (CO2)	**10**	8–10	5–7	0–4
Project Management & Teamwork (CO3)	**10**	8–10	5–7	0–4
Report / Thesis Writing – Written Communication (CO5)	**10**	8–10	5–7	0–4
Research Paper Writing / IPR – Patent or Copyright (CO5)	**10**	8–10	5–7	0–4
TOTAL	**50**			

Rubric for Oral / Practical / Presentation / Demonstration (50 Marks)

Assessment Criteria (mapped CO)	Max	Excellent	Satisfactory	Below Exp.
Concept & Problem Definition (CO1)	**5**	4–5	3	0–2
Design, Methodology & Implementation (CO2)	**15**	12–15	7–11	0–6
Project Management Skills (CO3)	**5**	4–5	3	0–2
Demonstration, Testing & Result Analysis (CO4)	**15**	12–15	7–11	0–6
Presentation & Oral Communication (CO5)	**10**	8–10	5–7	0–4
TOTAL	**50**			

Descriptive Assessment Rubric (Performance-Level Descriptors)

The following descriptors define each performance level and are applied consistently across all programmes. Examiners map a student's performance to the most appropriate level for each criterion before awarding the corresponding marks from the tables above.

Criteria	Excellent	Satisfactory	Below Expectation
Concept & Problem Definition	All major and minor objectives are identified and correctly prioritised. The problem statement is precise, relevant and well-scoped. All relevant information is gathered from valid sources and the proposed solution is well justified.	Major objectives identified but one or two minor ones missing or priorities not fully set. Problem statement mostly clear. Sufficient information from largely valid sources; solution mostly justified.	Several major objectives not identified. Problem statement vague or too broad. Insufficient information and/or invalid sources; proposed solution not justified.
Literature Survey	Comprehensive, current and well-organised survey of journals, standards, patents and existing products/systems. Research gap / novelty clearly identified and the chosen approach is well justified.	Adequate survey covering most key sources. Gap / novelty identified but only partially justified.	Sparse or outdated survey. Little or no identification of the gap; chosen approach not justified.
Design, Methodology & Implementation	Design is based on stated criteria, sound analysis and realistic constraints. Methodology is appropriate and well justified. Implementation is complete and robust and makes effective use of modern engineering / software tools.	Design is reasonable and methodology mostly appropriate. Implementation is largely complete; deeper analysis of alternatives or constraints could improve the outcome.	Only one solution considered or alternatives ignored. Weak methodology and incomplete implementation. Many constraints and criteria ignored.
Project Management & Teamwork	Responsibilities delegated fairly and every member contributes valuably. All members attend meetings and meet deliverable deadlines. Schedule, resources and budget are well managed.	Minor inequities in delegation; some members contribute more than others but all meet their responsibilities. Meetings mostly attended and deadlines mostly met.	Major inequities in delegation, with free-riders or dominating members. Meetings and deadlines frequently missed; poor planning of schedule and resources.
Demonstration, Testing & Result Analysis	Develops and follows logical testing / validation / experimental procedures. Selects appropriate tools, equipment, platforms or datasets and operates them confidently. Aware	Procedures mostly followed with occasional oversight. Needs some guidance in selecting tools / equipment and is tentative in operating them. Aware of errors but	Does not follow a proper procedure. Cannot select appropriate tools / equipment or operates them incorrectly, needing frequent supervision. Makes no attempt to

Criteria	Excellent	Satisfactory	Below Expectation
	of errors / limitations, accounts for them, and interprets and relates the results to the objectives and underlying theory.	accounts for them only minimally.	relate results to objectives.
Report / Thesis Writing (Written Communication)	Report is well organised and clearly written; the logic is easy to follow. Wording is precise; figures, tables and analyses enhance understanding. Grammatically correct, free of spelling errors, properly cited and free of plagiarism.	Report is mostly organised and clear; a few sections are harder to follow. Wording is good with minor exceptions; figures are consistent. Few grammatical / spelling errors that do not hinder the reader; some sources not fully cited.	Report lacks organisation and the logic is hard to follow. Figures absent or inconsistent. Grammatical and spelling errors hinder reading. Evidence of plagiarism or inadequate citation.
Research Paper Writing / IPR (Patent or Copyright)	A research / technical paper is drafted to publication standard in the required format, or a patent / copyright application is prepared and filed. Novelty and contribution are clearly articulated, claims and results are well supported, and the work is original with proper citations and no plagiarism.	A paper draft or IPR document is prepared and largely follows the required format. Novelty and contribution are stated but only partially developed, with minor gaps in supporting evidence or formatting.	No paper / IPR document, or a weak draft that does not follow the required format. Novelty or contribution is unclear or unsupported, with evidence of plagiarism or inadequate citation.
Presentation & Oral Communication	Slides are error-free and logically present the work and findings; they are readable and the graphics support the main ideas. Speakers are audible and fluent, do not rely on notes and answer questions accurately. Confident body language and eye contact convey strong engagement.	Slides are error-free and logical and mostly readable. Speakers are mostly fluent with minimal reliance on notes and answer most questions well. Slight discomfort or occasional distracting gestures.	Slides contain errors and lack logical flow; key aspects are absent and graphics confuse the audience. Speakers are inaudible or hesitant and rely heavily on notes, with difficulty answering questions. Body language conveys discomfort.

Prepared by **Checked by** **Head of the Department** **Vice Principal** **Principal**

Program: B.Tech Computer Science and Engineering(IoT and Cybersecurity with Block chain Technology)	Semester: VII
Course: Reliability, Cloud Computing and Machine Learning	Course Code: DJS23BCSC701

Teaching Scheme (Hours / week)				Evaluation Scheme							
				Semester End Examination Marks (A)			Continuous AssessmentMarks (B)				Total marks (A+ B)
Lectures	Practical	Tutorial	Total Credits	Theory			Term Test 1	TermTest 2	Term Test 3	Total	
				--			15	15	10	40	40
				Laboratory Examination			Term work				
1	--	--	1	Oral	Practical	Oral & Practical	Laboratory Work	Tutorial / Mini project / presentation/ Journal			--
				--	--	--	--	--	--	--	

Coursera Course: Reliability, Cloud Computing and Machine Learning

Link: https://www.coursera.org/learn/reliability-cloud-computing-and-machine-learning

Number of hours: 20 Hrs, Beginner level

About the Course:

The course explores advanced distributed database concepts, focusing on transaction management, reliability protocols, and data warehousing, while also diving deeper into cloud computing and machine learning. This will develop a solid understanding of transaction principles, concurrency control methods, and how to ensure database consistency during failures using ACID properties and protocols like ARIES. The course uniquely integrates Hadoop, MapReduce, and Accumulo, offering hands-on experience with large-scale data processing and machine learning applications such as collaborative filtering, clustering, and classification.

By mastering these advanced topics, student gain the skills necessary to work with cutting-edge technologies used in cloud-based data processing and scalable machine learning analysis. With practical applications in both reliability management and machine learning, this course prepares you to tackle complex data management challenges, making you well-equipped for careers in cloud computing, distributed systems, and data science.

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

1. Learn transaction management principles, including ACID properties, concurrency control, and deadlock management techniques for distributed systems.
2. Understand cloud computing with Hadoop, utilizing MapReduce for large-scale data processing, and apply machine learning techniques like clustering.
3. Understand cloud computing with Hadoop, utilizing MapReduce for large-scale data processing, and apply machine learning techniques like clustering.
4.

Detailed Syllabus:		
Unit	**Description**	**Duration**
1	**Introduction** Introduction to Reliability Engineering, Basics of Cloud Computing, Overview of Machine Learning, Relationship between Reliability, Cloud Platforms, and AI Systems, Real-world applications and case studies.	**01**
2	**Transaction Management & Concurrency Control** Java Example . Formal Transaction Definition ,ACID Properties ,Distributed Transaction Management Architecture ,Two Phase Locking ,Distributed Two Phase Locking . Timestamp Ordering Algorithm . Multi-version Timestamp Ordering . Optimistic Concurrency Control,Wait-For Graphs ,Deadlock Avoidance .	**06**
3	**Reliability Protocols, Data Warehousing, and Accumulo Architecture** Approaches to Cache Management, Example Transaction, Analysis and Redo Phases, Undo Phase, Termination Protocols, 3PC Timeout and Termination Protocols. Accumulo Architecture and Programming, Reliability Protocols, Self-Reflective Reading: ARIES Algorithm Crash During Recovery, Self-Reflective Reading: Implementing and Optimizing Visibility Criteria Removal in Accumulo.	**08**
4	**Cloud Computing, Hadoop Ecosystem, and Machine Learning Applications** Motivating Problems for MapReduce, Exploring MapReduce, Relational vs. Accumulo Approach, Enhancing Collaborative Filtering Techniques. Understanding Machine Learning Approaches.	**05**
	Total	**20**

Continuous Assessment (B)

Evaluation Scheme:

1. The identified courses shall focus on developing AI-related competencies and skills among students. Each selected course shall carry one (1) credit.
2. Faculty members shall act as mentors for the Coursera courses identified for various semesters of the program.
3. One faculty mentor shall be assigned to each division of the program for effective coordination and monitoring of this activity.
4. The assigned faculty mentor shall complete and review the course content before assigning the course to students.
5. The term work for these one-credit courses shall form a part of the Internal Continuous Assessment (ICA)component.
6. The Term work (ICA) component shall carry **40 marks**

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

- **15 Marks**: Coursera Course Completion and Certification
- **15 Marks**: Faculty-curated quiz conducted through the Coursera/Any other platform
- **10 Marks**: Internal faculty evaluation through quizzes, assignments, presentations, or Project

Prepared by **Checked by** **Head of the Department** **Vice Principal** **Principal**

Program: Final Year									Semester: VII/VIII
Course: Disaster Management and Preparedness									Course Code: DJS23ICHSX11
Teaching Scheme (Hours / week)				Evaluation Scheme					
				Semester End Examination Marks (A)			Continuous Assessment Marks (B)		
Lectures	Practical	Tutorial	Total Credits	Theory			Term Test 1	Term Test II / presentation / assignment / course project / group discussion / any other.	AVG	Total Marks = (A+ B)
				-			-	-	-	-
				Laboratory Examination			Term work		Total Term work	
2	-	-	-	Oral	Practical	Oral & Practical	Laboratory Work	Tutorial / Mini project / presentation/ Journal		-
				-	-	-	-	-	-	

Objectives:

1. To provide basic understanding of hazards, disasters and various types and categories of disaster occurring around the world.
2. To identify extent and damaging capacity of a disaster.
3. To study and understand the means of losses and methods to overcome /minimize it.
4. To understand roles and responsibilities of individual and various organizations during and after disaster.
5. To appreciate the significance of GIS, GPS in the field of disaster management.
6. To understand the emergency government response structures before, during and after disaster.

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

1. Apply disaster management principles & guidelines.
2. Conduct risk assessments.
3. Develop community awareness & participation.
4. Utilize Science & Technology tools (GIS, GPS).
5. Prepare disaster management plans.

Detailed Syllabus: (unit-wise)		
Unit	**Description**	**Duration**
1	**Understanding Disasters & Hazards:** • **Definition and types of disasters**: Natural, Man-made and hybrid disasters, **Study of Natural disasters**: Flood, drought, cloud burst, Earthquake, Landslides, Avalanches, Volcanic eruptions, Mudflow, Cyclone, Storm, Storm Surge, climate change, global warming, sea level rise, ozone depletion etc. **Study of Human/Technology Induced Disasters**: Chemical, Industrial and Nuclear disasters, internally displaced persons, road and train accidents Fire Hazards, terrorism, militancy, • Hazard & Vulnerability profiles of India (seismic zones, flood-prone areas). • India's vulnerability to disasters, and the impact of disasters on National development.	06
2	**Disaster Risk Reduction (DRR) & Mitigation:** • **Disaster Management Cycle**: Prevention, Mitigation, Preparedness, Response, Recovery. Need for disaster prevention and mitigation, mitigation guiding principles, challenging areas, structural and non-structural measures for disaster risk reduction. • Risk Assessment & Vulnerability Analysis. • **Science & Technology**: Use of information management, Geo informatics like RS, GIS, GPS and remote sensing mitigation measure.	06
3	**Disaster Preparedness & Response:** • Preparedness Planning, Early Warning Systems (EWS), & Communication. • Emergency Response: Search & Rescue, Logistics, Medical Aid. • Psychological Response & Management (Trauma, Stress). • Role of IT, Media, Govt., NGOs, & Community.	04
4	**Recovery, Rehabilitation & Reconstruction:** • Post-disaster damage assessment. • Rehabilitation, Reconstruction, & Livelihood Restoration. • Sanitation, Hygiene, & Waste Management.	04
5	**Policy, Governance & Capacity Building:** • National Disaster Management Authority (NDMA) & Legislation. • Institutional Mechanisms & Community Mobilization. Non-Structural Mitigation: Community based disaster preparedness, capacity development and training, awareness and education, contingency plans. **Case studies on disaster (National /International):** • Case study discussion of National Disasters: Tsunami (2004), Bhopal gas tragedy, Kerala and Uttarakhand flood disaster, 26th July 2005 Mumbai flood Case study discussion of International Disasters: Hiroshima – Nagasaki (Japan), Cyclone Phailin (2013), Fukushima, Daiichi nuclear disaster (2011), Chernobyl meltdown	08
	Total Number of Hours	**28**

Books Recommended:

Reference Books and Reports:

1. Disaster Management, by Harsh K. Gupta, Universities Press Publications (2003).
2. Disaster Management: An Appraisal of Institutional Mechanisms in India, by O. S. Dagur, published by Centre for land warfare studies, New Delhi, 2011.
3. Introduction to International Disaster Management, by Damon Copolla, Butterworth Heinemann Elsevier Publications (2015).
4. Disaster Management Handbook, by Jack Pinkowski, CRC Press, Taylor and Francis group (2008).
5. Disaster management & rehabilitation, by Rajdeep Dasgupta, Mittal Publications, New Delhi (2007).
6. Natural Hazards and Disaster Management, Vulnerability and Mitigation, by R B Singh, Rawat Publications (2006).
7. Concepts and Techniques of GIS, by C. P. Lo Albert, K.W. Yonng, Prentice Hall (India) Publications (2006).
8. Risk management of natural disasters, by Claudia G. Flores Gonzales, KIT Scientific Publishing (2010).
9. Disaster Management – a disaster manger's handbook, by W. Nick Carter, Asian Development Bank (2008).
10. Disaster Management in India, by R. K. Srivastava, Ministry of Home Affairs, GoI, New Delhi (2011)
11. The Chernobyl Disaster: Legacy and Impact on the Future of Nuclear Energy, by Wil Mara, Marshall Cavendish Corporation, New York, 2011.
12. The Fukushima 2011 Disaster, by Ronald Eisler, Taylor & Francis, Florida, 2013.

(Learners are expected to refer reports published at national and international level and updated information available on authentic web sites.)

Prepared by **Checked by** **Head of the Department** **Vice Principal** **Principal**