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

Shri Vile Parle Kelavani Mandal's

Dwarkadas J. Sanghvi College of Engineering

(Autonomous College Affiliated to the University of Mumbai)

Scheme and detailed syllabus

Third Year B. Tech

in

Computer Science and Engineering (IoT and Cyber Security with Block Chain Technology)

(Semester VI)

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

With effect from the Academic Year: 2025-2026

Scheme for Third Year B. Tech. CSE (IoT and Cybersecurity with Blockchain Technology) Semester VI (Autonomous) (Academic Year 2025-2026)

Academic Year 2025-2026

Sr. No.	Course Code	Course	Teaching Scheme				Semester End Examination (SEE)- A						Continuous Assessment (CA)- B						Aggregate (A+B)	Credits Earned	
			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	DJS23BCPC601	Network Security	3	--	–	3	2	60	–	–	–	60	15	15	10	40	–	40	100	3	4
	DJS23BLPC601	Network Security Laboratory	–	2	--	1	2	--	25	–	–	25	--	–	--	--	25	25	50	1	
2	DJS23BCPC602	Blockchain for Cybersecurity	3	--	–	3	2	60	–	–	--	60	15	15	10	40	--	40	100	3	4
	DJS23BLPC602	Blockchain for Cybersecurity Laboratory	–	2	–	1	2	--	25	–	–	25	--	–	--	–	25	25	50	1	
3	DJS23BLPC603	DevSecOps Laboratory	--	2	–	1	2	–	–	--	25	25	--	--	–	–	25	25	50	1	1
4.a	DJS23BCPE611	IoT Data Analytics	3	--	–	3	2	60	–	–	–	60	15	15	10	40	--	40	100	3	4
	DJS23BLPE611	IoT Data Analytics Laboratory	–	2	–	1	2	--	25	–	–	25	--	–	--	–	25	25	50	1	
	DJS23BCPE612	IoT Protocol Architeture	3	--	–	3	2	60	–	–	–	60	15	15	10	40	--	40	100	3	4
	DJS23BLPE612	IoT Protocol Architeture Laboratory	–	2	–	1	2	–	25	–	--	25	--	--	–	–	25	25	50	1	
	DJS23BCPE613	Industrial Internet of Everything	3	–	–	3	2	60	--	--	–	60	15	15	10	40	–	40	100	3	4
	DJS23BLPE613	Industrial Internet of Everything Laboratory	–	2	–	1	2	–	25	–	--	25	–	--	--	–	25	25	50	1	
5.a	DJS23BCPE614	Software Engineering and Testing	3	--	–	3	2	60	–	–	–	60	15	15	10	40	--	40	100	3	4
	DJS23BLPE614	Software Engineering and Testing Laboratory	–	2	--	1	2	–	25	–	–	25	--	–	–	--	25	25	50	1	
	DJS23BCPE615	Malware Analysis	3	–	--	3	2	60	–	–	–	60	15	15	10	40	–	40	100	3	4
	DJS23BLPE615	Malware Analysis Laboratory	–	2	--	1	2	--	25	–	–	25	--	–	--	--	25	25	50	1	
	DJS23BCPE616	Digital Forensics	3	–	--	3	2	60	--	–	–	60	15	15	10	40	–	40	100	3	4
	DJS23BLPE616	Digital Forensics Laboratory	--	2	–	1	2	–	25	--	–	25	--	--	–	--	25	25	50	1	
6	DJS23BCMD601	Machine Learning	3	–	–	3	2	60	–	–	–	60	15	15	10	40	–	40	100	3	4
	DJS23BLMD601	Machine Learning Laboratory	–	2	–	1	2	--	–	–	25	25	--	–	--	–	25	25	50	1	
7	DJS23IPSCX04	Innovative Product Development IV	–	2	--	1	2	–	--	–	25	25	--	–	–	--	25	25	50	1	1
8	DJS23ICHSX09	Constitution of India	1	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	
		Total	**16**	**14**	–	**22**	**24**	**300**	**100**	–	**75**	**475**	**75**	**75**	**50**	**200**	**175**	**375**	**850**	**22**	**22**

Prepared By

Checked By

Head of Department

Vice Principal

Principal

Program: B.Tech. in Computer Science and Engineering (IoT and Cyber Security with Block Chain Technology)	T.Y.B.Tech	Semester: VI
Course: Network Security	Course Code: DJS23BCPC601	
Course: Network Security Laboratory	Course Code: DJS23BLPC601	

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

Prerequisite:

1. Fundamentals of Sensor and Secured Technologies
2. Applied Cryptography
3. Computer Network

Course Objectives: The objective of the course is

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

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

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

Detailed Syllabus:

Unit	Description	Duration
1	**Network and Transport Layer Security:** Attacks at network layer: IP Spoofing, ICMP Flood, Packet Sniffing, Routing Attacks, DNS Cache Poisoning, Fragmentation Attacks, Security architecture for IP, Security Associations (SA) and Security Policy Database (SPD), Authentication Header (AH), Encapsulating Security Payload (ESP), Transport Mode and Tunnel Mode comparison, IPv4 vs IPv6 security considerations.	07
2	**Key Management and Internet Key Exchange:** Attacks at network layer: Replay Attacks, Man-in-the-Middle (MITM), Cryptographic Downgrade Attacks, Key distribution and management fundamentals, Internet Key Exchange (IKE) – Phases 1 & 2, IKEv2 enhancements and operation, Internet Security Association and Key Management Protocol (ISAKMP), Cryptographic suite negotiation	07
3	**Wireless Network Security:** Data Link Layer attacks: MAC Spoofing, Evil Twin Attack, Rogue Access Points IEEE 802.11 wireless LAN Overview, IEEE 802 Protocol Architecture, IEEE 802.11i wireless LAN Security, Mobile Device Security: Wireless Application Protocol (WAP) Architecture, Wireless Application Environment (WAF), Wireless Transport Layer Security (WTLS), Wireless authentication and key management, Mobile Device Security and Policy Enforcement (MDM concepts), Common wireless security protocols and countermeasures, Mobile App Security Threats: insecure APIs, permission abuse	08
4	**Web Security:** Attacks in Web security: Cross-Site Scripting (XSS), SQL Injection, Session Hijacking Web security considerations, Secure Socket Layer (SSL) & Transport Layer Security (TLS), HTTPS: Operation, Certificates, and Handshake Process, Secure Shell (SSH) for secure remote access, API Security Basics (Rate Limiting, Token-Based Auth, API Abuse Prevention), Web Application Security Issues: OWASP Top 10 overview (SQL Injection, XSS, CSRF, etc.), Web authentication and session management	08
5	**E-mail Security:** Attacks in email security: Phishing, Spam, Email Spoofing, Malware Attachments. E-mail security requirements and threats, PGP (Pretty Good Privacy): Architecture, Key Rings, Certificates, PGP Trust Model, Key Recreation, PGP Pocket, S/MIME (Secure/Multipurpose Internet Mail Extension), MIME and Secure MIME functionalities	06
6	**Authentication, Network Access Control, and Network Defense:** Attacks related to authentication, network access: Unauthorized Access, Password Cracking, Brute Force, Insider Attacks, IDS Evasion, Entity Authentication mechanisms and protocols, IEEE 802.1x Port-based Access Control, Network Security Firewalls – packet filtering, proxy, stateful inspection, Intrusion Detection Systems (IDS): Signature-based and Anomaly-based detection	06
	Total	**42**

List of Laboratory Experiments:

Sr. No.	Suggested Experiments
1	Study and Implementation of Wireshark tools
2	Implementation of VLAN (Large 2-Security).
3	a. Implementation of IPsec protocol in Tunnel Mode. b. Implementation of IPsec protocol in Transport Mode.
4	Implementation of secure wireless LAN for homes and enterprises N/W.
5	Configuration of SSL/SSH in secure client/server model.
6	Implementation of Firewall –Iptable.
7	To implement Pretty Good Privacy (PGP) for email encryption and signing
8	Encryption & Decryption data using open SSL.
9	Nmap tool for live scanning on ports and networks
10	Nessus installation and configuration
11	To configure and analyze snort functionality
12	Simulation of SQL injection attack

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

Books Recommended:

Text Books:

1. Cryptography and Network Security by Behrouz A. Forouzan and Debdeep Mukhorpadhyay, Edition 3, Tata McGraw Hill, 2017
2. Network Security Essentials: Applications and Standards by William Stallings,6th Edition, Pearson, 2017
3. Cryptography and Network Security: Principal and Practice By William Stallings, 7th edition, Pearson, 2018

Reference Books:

1. Cryptography and Network Security by Atul Kahale 4th edition, Tata McGraw Hill,2013
2. Network Security: Private Communication in a Public World by Charlie Kaufman, Radia Perlman, Mike Speciner, Ray Perlner Pearson, 2022

Web resources:

1. Network Security https://www.youtube.com/watch?v=zIWGjkr0ENE by simplilearn
2. Network Security https://www.youtube.com/watch?v=VJelZrYc49c by Sundeep Saradhi Kanthety
3. Digital Forensics MIT(CS)-202.pdf

Online Courses: NPTEL / Swayam/CISCO

1. Network Security https://onlinecourses.nptel.ac.in/noc25_ee54/preview by Prof. Gaurav S. Kasbekar from IIT Bombay
2. Cryptography And Network Security https://onlinecourses.nptel.ac.in/noc22_cs90/preview by Prof. Sourav Mukhopadhyay IIT Kharagpur
3. Network Security https://www.netacad.com/courses/network-security?courseLang=en-US

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. 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. Mini Project/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

<table>
<tr><td colspan="8">Program: B.Tech in Computer Science and Engineering(IoT and Cybersecurity with Block chain Technology)</td><td colspan="2">T.Y.B.Tech</td><td colspan="2">Semester : VI</td></tr>
<tr><td colspan="8">Course : Blockchain for Cybersecurity</td><td colspan="4">Course Code: DJS23BCPC602</td></tr>
<tr><td colspan="8">Course: Blockchain for Cybersecurity Laboratory</td><td colspan="4">Course Code: DJS23BLPC602</td></tr>
<tr><td colspan="4" rowspan="2">Teaching Scheme
(Hours / week)</td><td colspan="8">Evaluation Scheme</td></tr>
<tr><td colspan="3">Semester End Examination Marks (A)</td><td colspan="4">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="3">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="3">60</td><td>15</td><td>15</td><td>10</td><td>40</td><td>100</td></tr>
<tr><td colspan="3">Laboratory Examination</td><td colspan="4">Term Work</td><td rowspan="3">50</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">2</td><td rowspan="2">--</td><td rowspan="2">4</td><td>Oral</td><td>Practical</td><td>Oral &amp; Practical</td><td>Laboratory Work</td><td colspan="2">Tutorial / Mini project /presentation / Journal/ Practical</td><td>Total Term work</td></tr>
<tr><td>25</td><td>--</td><td>--</td><td>15</td><td colspan="2">10</td><td>25</td></tr>
</table>

Prerequisite:

1. Computer Networks
2. Introduction to blockchain technology
3. Applied Cryptography

Course Objectives: The objective of the course is

1. To understand how blockchain can be utilized for cybersecurity and privacy.
2. To explore emerging trends and innovations in blockchain technology and their implications for cybersecurity practices
3. To analyze the potential utility of blockchain in digital forensic applications.
4. To design, develop, and implement secure blockchain solutions that address real-world cybersecurity challenges.

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

1. Describe the taxonomy of blockchain threats and vulnerabilities.
2. Gain the competence to secure diverse digital systems with blockchain from evolving cyber threats.
3. Review existing blockchain based data sharing frameworks and identify strengths and weaknesses.
4. Evaluate decentralized distributed data sharing platform architecture using blockchain.
5. Design applications of blockchain in digital forensics.

Yhelolar

6. Enable learners to detect, assess, and remediate smart contract vulnerabilities.

Detailed Syllabus:

Unit	Description	Duration
1	**Blockchain Threats and Vulnerabilities:** Cybersecurity threats and incidents on blockchain network, Classification of blockchain threats and vulnerabilities, **Clients vulnerabilities:** Digital signature, Hash function, Mining malware, software's Flaw, User's address vulnerabilities **Consensus mechanism vulnerabilities:**51% Vulnerability, Alternative History Attack, Finney Attack, Race Attack, Vector76 Attack **Mining pool vulnerabilities: Block Withholding Attack**, Bribery Attack, Pool Hopping Attack, Block Discarding Attack, Selfish Mining Attack, Fork-After-Withholding Attack **Network vulnerabilities**: Partition Attacks, Delay Attacks, Distributed Denial-of-Service Attack, Sybil Attack, Time-Jacking Attack, Transaction Malleability Attack Risks in Blockchain: Eclipse Attack and Front Running Attack	10
2	**Cybersecurity with Blockchain:** Blockchain in Cybersecurity: Advantages and disadvantages, blockchain on the CIA Security Triad, Public Key Infrastucture (PKI) Infrastructure, Deploying PKI Based Identity with blockchain, Domain Name System (DNS), blockchain-based DNS Security Platform, Deploying blockchain-based DDoS Protection	08
3	**Blockchain based Secure Data Sharing:** Issues with existing data sharing framework, Requirements for secure blockchain based data sharing framework, blockchain based data sharing platforms and protocols: Case studies on Inter Planetary File System (IPFS), Privacy- enhancing technologies (PETs): zero-knowledge proofs, Homomorphic encryption	06
4	**Ensuring Data integrity in Blockchain based Platform:** Architecture of decentralized platform: Data encryption and distribution, Data decryption and verification, Data provider, Data requester Privacy-preserving searching model, Ensuring digital-twin integrity, Data Integrity in Decentralized Systems	06
5	**Blockchain based Digital Forensics Framework:** Overview of Digital forensics process and Blockchain technology, Challenges in digital forensics and Feasible Solution Using Blockchain, Blockchain-based evidence management and access control, Benefits of blockchain based digital forensics framework	06
6	**Smart Contract Security Auditing:** Types of Smart Contract Audits: Manual Code Review vs. Automated Security Analysis Automated Security Analysis Tools: Mythril, Slither, Echidna, Manticore, Manual Code Review Techniques, Threat Modeling and Risk Assessment, Static and Dynamic Analysis of Smart Contracts, Audit Report Writing and Remediation Strategies	06
	Total	**42**

List of Laboratory Experiments:

Sr. No.	Suggested Experiments
1	Case study of on threats and vulnerabilities on blockchain network with the help of research paper in IEEE, Springer, Sciencedirect, Elsevier etc.
2	Conduct code reviews and static analysis to identify potential security flaws such as reentrancy bugs, integer overflows, or unchecked user inputs in smart contract
3	Deploy the public key infrastructure (PKI) with an Ethereum blockchain
4	Implement Ethereum based secure DNS infrastructue
5	Deploy the blockchain-based DDoS protection platform
6	Develop Blockchain-based PKI solutions and apps for storing DNS entries
7	Design smart contracts for tasks such as data validation or access control
8	Design smart contracts to handle data storage and transfer operations securely on the blockchain.
9	Install Mythril, Slither, Echidna, and Manticore in a Linux-based environment. Deploy vulnerable smart contract. Compare the effectiveness of different security analysis tools
10	Perform a threat modeling exercise on a deployed smart contract.
11	Conduct a complete smart contract audit and generate a professional audit report.
12	Design and implement a blockchain-based secure data sharing solution for a specific use case
13	Write Smart Contracts with Hyperledger Composer
14	Design transaction model and chaincode with Golang.
15	Deploy Composer REST Gateway
16	Access the Composer transactions Maintain, monitor, and govern blockchain solutions

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

Books Recommended:

Text Books:

1. Yassine Maleh, Mohammad Shojafar, Mamoun Alazab, Imed Romdhani, Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Application, 1st Edition, CRC Press, Taylor & Francis Group, ISBN: 9781000060164, 2020.
2. R. Gupta, Hands-on cybersecurity with blockchain, 1st Edition Packt Publishing, ISBN: 978788990189, 2018.
3. Rajneesh Gupta, Hands-on Cybersecurity with Blockchain. Implement DDoS Protection, PKI-based Identity, 2FA and DNS Security using Blockchain, Packt Publishing, 2018.
4. Richard Ma, Jan Gorzny, Edward Zulkoski, Kacper Bak, Olga Mack, Fundamentals of Smart Contract Security, 1st Edition, Momentum Press, ISBN:978-1949449372, 2019
5. Ghassan Karame, Elli Androulaki, Bitcoin and Blockchain Security, Artech Publisher, 2017.

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 and Cybersecurity: https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media- telecommunications/Blockchain-and-Cyber.pdf
2. Blockchain Security : https://www.edx.org/course/blockchain-andfintech-basics-applications-and- limitations
3. Best Practices for Smart Contracts Security: https://www.leewayhertz.com/smart-contracts-security/
4. Blockchain Security: https://www.ibm.com/topics/blockchain-security
5. Digital Twin Integirty:https://widgets.weforum.org/blockchain-toolkit/data-integrity/index.html#solutions-for-data-integrity-in-a-blockchain-context

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. Cyber Security and Privacy, By Prof. Saji K Mathew, IIT Madras
   https://onlinecourses.nptel.ac.in/noc23_cs127/preview
5. Cyber Security, By Dr.G.Padmavathi, Avinashilingam Institute for Home Science & Higher Education for Women,Coimbatore
   https://onlinecourses.swayam2.ac.in/cec20_cs15/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 / course project / group discussion /presentation / quiz/ any other for 10 marks.

Laboratory: (Term work)

Term work shall consist of minimum 8 experiments

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

i. Laboratory work (Performance of Experiments, Write-up): 15 Marks
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)	T.Y.B.Tech	Semester: VI
Course: DevSecOps Laboratory	Course Code: DJS23BLPC603	

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

Pre-requisite:

1. Structure Programming in C
2. Object Oriented Programming Java
3. Programming in Python

Course Objectives: The objective of the course is:

1. To understand the concept of distributed version control.
2. To demonstrate the use of Jenkins for continuous integration and testing of applications.
3. To familiarize with the concept of Software Configuration Management with Continuous Monitoring.
4. To learn the concept of Cloud and Infrastructure as a Code.

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

1. Understand the concepts of distributed version control using GIT and GITHUB
2. Apply Jenkins to Build, Deploy and Test the Software Applications
3. Analyze & illustrate the Containerization of OS images and deployment of applications over Docker
4. Deploy and Examine the Software Configuration management using Ansible and Continuous monitoring and alerting using Prometheus and Nagios
5. Use Automated Monitoring and Alerting Using Splunk and Nagios tools.

6. Implement Terraform scripts to manage VMs on a cloud.

Detailed Syllabus:

Unit	Description	Duration
1	**Introduction to DevSecOps and Version Control** Overview of DevSecOps principles and practices, Importance of version control in DevSecOps, Git fundamentals: repositories, commits, branches. Merges Using GitHub for remote repository management and collaboration.	04
2	**Continuous Integration and Continuous Deployment (CI/CD)** Introduction to CI/CD pipelines and tools, Setting up Jenkins for automated builds, Jenkins pipelines: scripted and declarative, Integrating automated testing in CI pipelines (JUnit, Selenium).	06
3	**Containerization with Docker** Basics of containerization and Docker architecture, Running applications and operating systems in Docker containers, Creating and managing Docker images and Dockerfiles, Publishing Docker images to Docker Hub.	04
4	**Infrastructure Automation and Configuration Management** Introduction to infrastructure as code (IaC), Configuration management with Ansible. Automating continuous deployment with Ansible playbooks.	04
5	**Monitoring and Alerting in DevSecOps** Importance of monitoring in DevSecOps pipelines, Using Prometheus for automated monitoring and alerting, Continuous monitoring tools: Splunk, Nagios.	04
6	**Security in DevSecOps** Principles of security testing in DevSecOps, Application and code security testing tools and techniques, Static Application Security Testing (SAST) with SonarQube, Using Snyk for vulnerability scanning, Threat modeling concepts and tools (Threat Dragon) **Cloud and Infrastructure as Code (IaC)** Basics of cloud computing platforms (AWS, Azure, GCP), Working with virtual machines on the cloud, Infrastructure deployment using Terraform scripts.	06
	Total	**28**

List of Laboratory Experiments:

Sr.No.	Suggested Experiments
1	To implement Version control for different files/directories using GIT
2	To implement version control using GITHUB to sync local GIT repositories and perform various related operations.
3	To deploy and test Java/web/Python application on jenkins server
4	To implement Jenkins pipeline using scripted/declarative pipeline
5	To use jenkins to deploy and run test cases for Java/Web application using Selenium/JUnit
6	To use docker to run containers of different applications and operating Systems
7	To create a custom docker image using Dockerfile and upload it to the docker hub
8	To implement continuous deployment using Ansible
9	To Implement automated monitoring and alerting using Prometheus
10	To implement continuous monitoring using Splunk/NagiOS
11	To implement Application and code security testing using snyk
12	To implement Static Application Security Testing using SonarQube
13	To implement threat models to identify threats in the system using Threat Dragon
14	To create and work with virtual machine on cloud (GCP / AWS / Azure)
15	To implement terraform script for deploying compute/Storage/network infrastructure on the public cloud platform (GCP / AWS / Azure)

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

Books Recommended:

Text Books:

1. Prem Kumar Ponuthorai, Jon Loeliger, Version Control with Git, 3rd Edition,O'Reilly Media,2024.
2. John Ferguson Smart,"Jenkins, The Definitive Guide", O'Reilly Publication,2011.
3. Karl Matthias & Sean P. Kane, Docker: Up and Running, O'Reilly Publication,2015.
4. Russ McKendrick, Learn Ansible, Pakt Publication,2024.
5. Yevgeniy Brikman, Terraform: Up and Running, 3rd Edition,O'Reilly Publication,2022.

Reference Books

1. Sanjeev Sharma and Bernie Coyne,"DevOps for Dummies", Wiley Publication, 2017
2. Httermann, Michael, "DevOps for Developers",Apress Publication,2012.
3. Joakim Verona, "Practical DevOps",Pack publication, 2016.

Web resources:

1 GIT Cheat sheet https://www.atlassian.com/git/tutorials/atlassian-git-cheatsheet

2 Jenkins 1) https://www.javacodegeeks.com/2021/04/how-to-create-run-ajob-in-jenkins-using-jenkins-freestyle-project.html

3 https://k21academy.com/devops-foundation/ci-cd-pipelineusing-jenkins/

4 Docker https://docs.docker.com/get-started/docker_cheatsheet.pdf

5 Ansible https://docs.ansible.com/ansible/latest/index.html

6 Prometheus https://prometheus.io/docs/introduction/overview/

7 Snyk https://snyk.io/learn/application-security/static-application-securitytesting/

8 Threatdragon https://www.threatdragon.com/#/

9 SonarQube https://docs.sonarqube.org/latest/

10 Terraform https://developer.hashicorp.com/terraform/intro

Online Courses: NPTEL / Swayam / Udemy

1. Course on- DevSecOps Fundamentals - Including Hands-On Demos By Northern APT, https://www.udemy.com/course/devsecops-fundamentals/

Evaluation Scheme:

Semester End Examination (A):
Laboratory:
Oral and Practical examination will be based on the entire syllabus including, the practical's performed during laboratory sessions.

Continuous Assessment (B)
Laboratory: (Term work)
Term work shall consist of minimum 8 experiments.
The distribution of marks for term work shall be as follows:
i. Laboratory work (Performance of Experiments): 15 Marks
ii. Journal documentation (Write-up and/or Assignments): 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)	**T.Y.B.Tech**	**Semester: VI**
Course : IoT Data Analytics	**Course Code: DJS23BCPE611**	
Course: IoT Data Analytics Laboratory	**Course Code: DJS23BLPE611**	

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

Prerequisite:

1. Database Management Systems
2. Python programming Laboratory
3. Embedded System and IoT

Course Objectives: The objective of the course is to

1. Understand the fundamentals of Big Data analytics, its characteristics, technologies, and infrastructure for handling large-scale data.
2. Study and apply ETL (Extract, Transform, Load) techniques in the context of IoT for real-time, heterogeneous, and large-volume data processing.
3. Explore the Hadoop framework, MapReduce programming model, and associated ecosystem tools for distributed data storage and computation.
4. Analyse and manage unstructured data using NoSQL databases and advanced data mining techniques such as frequent pattern mining and clustering.

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

1. Explain the concepts, characteristics, and challenges of Big Data and describe the technologies and infrastructures used for Big Data analytics.
2. Apply ETL processes to handle real-time, large-scale, and heterogeneous IoT data sources using suitable tools and architectures.

3. Implement distributed data processing using Hadoop Distributed File System (HDFS) and the MapReduce programming model for solving large-scale data problems.
4. Utilize components of the Hadoop ecosystem for data management and workflow automation in Big Data environments.
5. Design and analyse data models using NoSQL databases such as MongoDB and apply Spark for big data analysis.
6. Employ data mining algorithms such as frequent pattern mining and clustering to extract insights from large datasets.

Detailed Syllabus:

Unit	Description	Duration
1	**Introduction to Big Data Analytics:** Introduction to Big Data, Big Data characteristics, types of Big Data, Traditional vs. Big Data business approach. Technologies Available for Big Data, Infrastructure for Big Data, Big Data Challenges, Case Study of Big Data Solutions.	06
2	**IoT ETL (Extract, Transform, Load in Internet of Things):** Introduction, ETL techniques to handle real-time, large-scale, and diverse IoT data sources. Need for IoT ETL, IoT ETL Architecture, ETL Phases in IoT, Tools and Platforms.	06
3	**Hadoop and MapReduce:** Introduction to Hadoop, Core Hadoop Components, Hadoop Distributed File System (HDFS) & Architecture, MapReduce – Introduction, The Map Tasks, The Reduce Tasks, Combiners, Components of MapReduce, Details of MapReduce Execution, MapReduce Algorithms and applications – Matrix Multiplication by MapReduce.	08
4	**Hadoop Ecosystem:** Introduction to Hadoop Ecosystem components, Reading and Writing Large Datasets – Apache PIG, Apache HIVE, Apache Sqoop, Hadoop Management: YARN, Apache Oozie, Apache Zookeeper, Apache Ambari.	09
5	**NoSQL Database:** Introduction to NoSQL, NoSQL business drivers, CAP Theorem and BASE Properties, NoSQL case studies. NoSQL data architecture patterns: Key-value stores, Graph stores, Column family (Bigtable) stores, Document stores, Variations of NoSQL architectural patterns. Analyzing big data with a shared-nothing architecture; Choosing distribution models: master-slave versus peer-to-peer. Introduction to MongoDB, Introduction to Apache Spark.	08
6	Applications of IOT and Big Data: IOTPowered intelligent traffic management, Smart Healthcare, Big Data analytics For Personalized treatment and early Disease Detection, Smart Grid, Smart Inventory System, IOTDriven Infrastructure and Services in urban settings. Digital Twins: Virtual representations of physical systems for real-time analysis.	05
	Total	**42**

Thelokar.

List of Laboratory Experiments:

Sr. No.	Suggested Experiments
1	Install and configure a small Hadoop cluster using virtual machines or cloud services.
2	Implement the following file management tasks in Hadoop: a. Adding files and directories b. Retrieving files c. Deleting files
3	To implement Matrix Vector Multiplication with Hadoop Map Reduce.
4	To install and run Pig to write Pig Latin scripts to sort, group, join, project, and filter data.
5	To install and run Hive then use Hive to create, alter, and drop databases, tables, views, functions, and indexes.
6	Managing and monitoring a Hadoop Cluster using Apache Ambari
7	Exploring Distributed Coordination using Apache Zookeeper
8	Set up HBase and perform Create, Read, Update, and Delete operations on data stored in HBase tables.
9	Real-time IoT Data Cleaning and Transformation using ETL Pipeline
10	To perform NoSQL database using MongoDB to create, update and insert.
11	Analytics with MongoDB Aggregation Framework
12	To write Spark application to perform data Analysis using PySpark.
13	Explore technologies like Apache Kafka for real-time data streaming and processing.
14	To implement Bloom Filters for filter on Stream Data
15	Streaming Transformation & Aggregation with Apache NiFi / Spark Streaming
16	Mini Project (A group of 3 to 4 students is required to develop an application and submit reports).

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

Books Recommended:

Textbooks:

1. Mining of Massive Datasets by Jure Leskovec, Anand Rajaraman, Jeff Ullman, 3rd Edition, Cambridge University Press, 2020
2. Big Data Analytics: Introduction to Hadoop, Spark, and Machine-Learning, By Raj Kamal, Preeti Saxena, McGraw Hill Education (India), 1st Edition (2019)

3. SQL and NoSQL Databases: Modeling, Languages, Security, and Architectures for Big Data Management, CRC Press, 2019.
4. By Michael Kaufmann & Andreas Meier, 2nd Edition, Springer, 2023.

Reference Books:

1. Data Mining: Concepts and Techniques, By Jiawei Han, Jian Pei, Hanghang Tong, 4th Edition, Morgan Kaufmann, Elsevier, 2022.
2. Data Analytics in the Era of the Industrial Internet of Things, Springer, 1st ed. 2021.
3. Hadoop in Practice, By Alex Holmes, 2nd Edition, Manning Publications, 2014.
4. Data Analytics for Internet of Things Infrastructure" edited by Rohit Sharma, Gwanggil Jeon, and Yan Zhang, published by Springer, 1st edition (2023)..
5. Big Data Analytics, by Radha Shankarmani, M Vijayalakshmi, 2nd Edition, Wiley India, 2016
6. Internet of Things and Big Data Analytics-Based Manufacturing, by Arun Kumar Rana; Sudeshna Chakraborty; Pallavi Goel; Sumit Kumar Rana; Ahmed A. Elngar, CRC Press / Taylor & Francis (Taylor & Francis Group), 2024.

Web resources:

1. Big Data Analytics Overview
   https://www.ibm.com/analytics/big-data
   IoT ETL Concepts and Tools
   https://aws.amazon.com/iot/
   https://nifi.apache.org/
2. Hadoop and MapReduce
   https://hadoop.apache.org/
   https://data-flair.training/blogs/hadoop-mapreduce-tutorial/
   Hadoop Ecosystem Components
   https://pig.apache.org/
   https://hive.apache.org/
   https://sqoop.apache.org/
3. NoSQL Databases and Spark
   https://www.mongodb.com/
   https://spark.apache.org/
4. Frequent Pattern Mining and Clustering
   https://www.geeksforgeeks.org/data-mining/
   https://towardsdatascience.com/clustering-algorithms

Online Courses: NPTEL / Swayam:

1. Big Data Computing — NPTEL / SWAYAM (IIT Patna, Prof. Rajiv Misra)
   https://elearn.nptel.ac.in/shop/nptel/big-data-computing/?utm_source=chatgpt.com
2. NOC: Algorithms for Big Data — NPTEL (IIT Madras)
   https://nptel.ac.in/courses/106106142

3. NOC: Scalable Data Science, IIT Gadhinagar IIT Kharagpur
   Prof. Anirban Dasgupta, Prof. Sourangshu Bhattacharya
   https://nptel.ac.in/courses/106105186
4. Data Science and Big Data, Prof. Sandeep Singh Rawat, Indira Gandhi National Open University, New Delhi
   https://onlinecourses.swayam2.ac.in/nou25_cs29/preview?utm_source=chatgpt.com

Evaluation Scheme:

Continuous Assessment (A)

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)

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

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

i. Laboratory work (Performance of Experiments, Write-up): 15 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.

Semester End Examination (B):

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.

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)									T.Y.B.Tech		Semester: VI
Course: IoT Protocol and Architecture									Course Code: DJS23BCPE612		
Course: IoT Protocol and Architecture Laboratory									Course Code: DJS23BLPE612		
Teaching Scheme (Hours / week)				Evaluation Scheme							
				Semester End Examination Marks (A)			Continuous Assessment Marks (B)				Total marks (A+ B)
				Theory			Term Test 1	Term Test 2	Assignment	Total	
Lectures	Practical	Tutorial	Total Credits	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. Network Fundamentals
2. Operating Systems

Objectives: The objective of the course is:

1. Understand IoT Characteristics and Conceptual Framework.
2. Comprehend network architecture and design of IoT
3. Identify the role and characteristics of smart objects in the Internet of Things (IoT) ecosystem.
4. Correlate the connection of smart objects and IoT access technologies.

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

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

Detailed Syllabus: (unit wise)

Unit	Description	Duration
1	**Introduction to IoT** Introduction to IoT- Defining , Characteristics , Conceptual Framework of , Physical design, Logical design , Functional blocks, Communication models & APIs, Basics of networking Communication protocol, wireless sensor networks. Convergence of IT and OT (Operational Technology), IoT Challenges, IoT protocol vs Web Protocol stack	**06**
2	**IoT Network Architecture and Design** Drivers Behind New Network Architectures : Scale,Security,Constrained Devices and Networks ,Data,Legacy Device Support , Architecture : The IoT World Forum (IoTWF) Standardized Architecture :Layer 1-7, IT and OT Responsibilities in the IoT Reference Model, Additional IoT Reference Models, A Simplified IoT Architecture, The Core IoT Functional Stack ::Layer 1-3 , Smart Services and IoT Data Management.	**08**
3	**Smart Objects IoT:** Sensors, Actuators, and Smart Objects, Attributes of Sensors, Actuators, Micro-Electro-Mechanical Systems (MEMS) Smart Objects: A Definition, Trends in Smart Objects, Sensor Networks, Wireless Sensor Networks (WSNs), Communication Protocols for WSN, RFID and NFC.	**06**
4	**Connecting Smart Objects** Communications Criteria: Range, Frequency Bands, Power Consumption, Topology, Constrained Devices, Constrained-Node Networks, Data Rate and Throughput, Latency and Determinism, Overhead and Payload. IoT Access Technologies : Standardization and Alliances , Physical Layer , MAC Layer , Topology ,Security concepts of IEEE 802.15.4 , IEEE 802.15.4g and 802.15.4e ,IEEE 1901.2a ,IEEE 802.11ah , LoRaWAN, and NB-IoT and Other LTE Variations , LTE Cat 0 , LTE-M, NB-IoT.	**07**
5	**IoT Network Layer and Application protocols** RPL, Objective Function Rank, RPL Headers, Metrics , Authentication and Encryption on Constrained Nodes, ACE, DICE, Profiles and Compliances, Internet Protocol for Smart Objects Alliance, Wi-SUN Alliance, Thread, IPv6 Ready Logo. Transport Layer, IoT Application Transport Methods, Generic Web-Based Protocols.	**07**
6	**Securing IoT** A Brief History of OT, **Security Common Challenges in OT Security** : Erosion of Network Architecture, Pervasive Legacy Systems, Insecure Operational Protocols , Device Insecurity.**Security Knowledge:** IT and OT Security Practices and Systems Vary, The Purdue Model for Control Hierarchy, OT Network Characteristics Impacting Security. **Security Priorities:** CIA, Security Focus Formal Risk Analysis Structures: OCTAVE and FAIR, FAIR. The Phased Application of Security in an Operational Environment, Secured Network Infrastructure and Assets, Deploying Dedicated Security Appliances, Higher-Order Policy Convergence and Network Monitoring.	**08**
	Total	**42**

Ghelokar

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

Books Recommended:

Text Books:

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

Reference Books:

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

Web resources:

1. https://owasp.org/www-project-internet-of-things/
2. https://www.edx.org/learn/computer-architecture/waseda-university-iot-system-architecture-design-and-evaluation.
3. https://www.coursera.org/learn/iot-architecture.
4. https://www.classcentral.com/course/iot-software-architecture-6507.

Online Courses: NPTEL / Swayam :

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

Evaluation Scheme:

Semester End Examination (A):

Theory:

1. Question paper will be based on the entire syllabus summing up to 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. Mini Project/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 Cybersecurity with Block chain Technology)	**T.Y.B.Tech**	**Semester: VI**
Course: Industrial Internet of Everything	**Course Code: DJS23BCPE613**	
Course Laboratory: Industrial Internet of Everything Laboratory	**Course Code: DJS23BLPE613**	

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

Prerequisite:

1. Introduction to Internet of Things
2. Internet of Things with Real Time Applications

Objectives: The objectives of the course are:

1. To understand the key skills of Industrial IoT and Applications.
2. To analyse the suitable Industrial Internet Architecture Framework with modern communicational protocols.
3. To explore IP, Non-IP IOT protocols and Business models used in IIoT deployments.
4. To Implement IIoT Data Analytics and Applications of IIoT in robotics.

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

1. Present key skills used in the IIoT manufacturing and Embedded systems applications.
2. Design suitable network architecture with Industrial Ethernet and Gateways.
3. Introduce operating systems, Networking and wireless communication protocols used in IIoT deployments.
4. Comprehend different protocols and Business models for Industrial Internet of Everything.
5. Deployment of IIoT Data Analytics by using Machine Learning algorithms.
6. Implement cloud-enabled robotics Applications of IIoT in robotics.

Detailed Syllabus: (unit wise)

Unit	Description	Duration
1	**Introduction of IIoT:** Market Size and Potential Definition IoT v IIoT, Next Generation Sensors, Sensor's calibration and validate sensor measurements, placement of IoT devices, Industrial Internet, Impact of Industrial Internet, Industrial Sensing, low-cost communication system design, Top application areas include manufacturing, oil & gas, Embedded systems in the Automotive and Transportation market segment.	07
2	**Industrial Internet Architecture Framework** Functional Viewpoint, Operational Domain, Information Domain, Application Domain, Business Domain, Implementation View point, Architectural Topology, Three Tier Topology, Data Management, Field Bus Technologies, Modern Communication Protocols, Industrial Ethernet, Industrial Gateways.	07
3	**IIoT Methodology** Industrial Processes-Features of IIoT for Industrial processes, Top operating systems used in IIoT deployments, Networking and wireless communication protocols used in IIoT deployments. Smart Remote Monitoring Unit, components of monitoring system, control and management, Wireless Sensor Network (WSN). Device and Sensor Security for the detection of industrial sensors and controllers. Secure firmware integrity verification for IIoT devices.	07
4	**Protocols and Architecture of IIoT** WPAN, NFC, WebSockets, Wireless HART Protocol, IP and Non-IP Protocols, **Comparison of secure and insecure IIoT protocols**, Z- Wave, NB-IoT, Business Models of IIoT, Categorization of reference architecture in IIoT, introduction to Interoperable Industrial Internet of Things (IIRA), IIRA- Framework. Security layers within the Three-Tier IIoT Architecture (Edge-Gateway-Cloud). Identity and trust management across heterogeneous industrial systems.	08
5	**IIoT Data Analytics** Categorization of analytics- IIoT and Industry 4.0 context, Usefulness of IIoT analytics, implementation of industrial IoT Data flow, Deployment of analytics, big data and how to prepare data for machine learning algorithms, Applications of ML in Industries, Healthcare Applications in industries.	07
6	**Internet of Robotic Things (IoRT)** Introduction to stationary and mobile robots, Brief introduction to localization, mapping, planning, and control of robotic systems; Introduction to cloud-enabled robotics; Applications of IIoT in robotics; Architectures for IoRT, Examples and case studies: Open issues and challenges.	06
	Total	42

Cyshelokar.

List of Laboratory Experiments: (Minimum any eight experiments)

Sr. No.	Suggested Experiments
1	To implement an Autonomous Inventory Management System Using IIoT.
2	To Design a Smart Warehouse System using Industrial IoT and RFID.
3	To Perform Monitoring and Controlling Industrial Equipment using IIoT Sensors.
4	To design Smart Factory Automation with IIoT-Based Wireless Sensor Networks.
5	To analyse cybersecurity risk assessment for safeguarding industrial IoT (IIoT) environments.
6	To develop an Edge Computing Solution for Industrial IoT Applications.
7	To perform Predictive Analytics for Industrial Energy Management using IoT Data.
8	To perform IIoT-Based Environmental Monitoring in Manufacturing Plants.
9	To deploy sensors to monitor machine health parameters (vibration, temperature, pressure).
10	To analyse Industrial IoT Device Calibration and Data Transmission using MQTT.
11	To analyse Fault Detection in Industrial Systems Using IoT and AI Techniques.
12	To analyse Remote Condition Monitoring of Power Grids using IIoT Solutions.
13	To perform a system to monitor the location and condition of products in real-time application using Technologies like Wi-Fi (Indoors: 30–50 meters), Bluetooth (10 meters) and LoRaWAN (Urban areas: 3–5 kilometers).
14	To perform Industrial Robotics Control through IoT-Based Network using protocols like MQTT or HTTP.
15	Mini Project(Students with group of 3/4 will develop application based on Industrial Internet of Thing along with Report).

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

Books Recommended:

Text Books:

1. Michael Peppler and Peter Domsch "Hands-On Industrial Internet of Things: Create a powerful Industrial IoT infrastructure using Industry 4.0", Packt Press, ISBN: 1789537223, 2018.
2. K. V. S. Murthy and V. S. Kumar "Industrial Internet of Things: Design, Implementation, and Applications", 1st Edition, CRC Press, ISBN: ISBN 9780367608675, 2024.
3. Shrey Sharma, "Mastering IoT for Industrial Environments", 1st Edition Packt Publishing, ISBN: 9788197081972, 2024
4. Shriram K Vasudevan, Abhishek S. Natarajan, RMD Sundaram, "Internet of Things", Wiley Publishing, ISBN: 9789388991018, 2020.

Reference Books:

1. Alasdair Gilchrist "Industry 4.0: The Industrial Internet of Things", Apress, 2020, ISBN: 9781484220467.
2. Sudip Misra, Chandana Roy, Anadarup Mukherjee "Introduction to Industrial Internet of Things and Industry 4.0", CRC Press,2021, ISBN: 9780367897581.
3. Giacomo Veneri, Antonio Capasso "Hands on Industrial Internet of Things", Packt Press, 2021, ISBN NO: 978-1789537222.
4. Yashavant Kanetkar, Shrirang Korde, "IoT Experiments", BPB Publications, ISBN: 9789386551832, 2020.

Web resources:

1. Introduction of IIoT: https://www.trendmicro.com/vinfo/in/security/definition/industrial-internet-of-things-iiot
2. IIoT Architecture : https://www.spiceworks.com/tech/iot/articles/what-is-iiot/
3. https://www.coretigo.com/what-is-the-industrial-internet-of-things-iiot-and-what-are-its-benefits/
4. https://azure.microsoft.com/en-us/solutions/iot/iot-technology-protocols
5. https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT
6. https://thinkpalm.com/blogs/what-is-the-internet-of-robotic-things-does-this-concept-help-in-improving-the-connectivity-and-functioning-of-platforms/

Online Courses: NPTEL / Swayam

1. Introduction to Industry 4.0 and Industrial Internet of Things, By Prof. Sudip Misra, IIT Kharagpur.
   https://nptel.ac.in/courses/106105195

2. ACM India Summer School on IoT and Embedded Systems, By prof. Debabrata Das, IIT Madras.
   https://archive.nptel.ac.in/courses/128/106/128106020/

3. Fundamentals of sensors, including their classification, By Prof. Mitradip Bhattacharjee, IISER Bhopal.
   https://onlinecourses.nptel.ac.in/noc23_ee95/preview

4. Internet of Things (IoT) and Embedded Systems: By Prof. Sudip Misra, IIT Kharagpur.
   https://onlinecourses.nptel.ac.in/noc22_cs53/preview

5. Advanced Sensors and Transducers by Prof. Ankur Gupta, IIT Delhi.
   https://onlinecourses.nptel.ac.in/noc23_ee105/preview

6. Internet of Things (IoT) for Smart Cities, By Sudip Misra, IIT Kharagpur.
   https://onlinecourses.nptel.ac.in/noc23_cs82/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:

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)

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

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

i.Laboratory work (Performance of Experiments, Write-up): 15 Marks

ii.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

<table>
<tr><td colspan="9">Program: B. Tech in Computer Science and Engineering (IoT and Cybersecurity with Block chain Technology)</td><td colspan="2">T.Y.B.Tech</td><td>Semester: VI</td></tr>
<tr><td colspan="9">Course : Software Engineering and Testing</td><td colspan="3">Course Code: DJS23BCPE614</td></tr>
<tr><td colspan="9">Course: Software Engineering and Testing Laboratory</td><td colspan="3">Course Code: DJS23BLPE614</td></tr>
<tr><td colspan="4" rowspan="2">Teaching Scheme
(Hours / week)</td><td colspan="8">Evaluation Scheme</td></tr>
<tr><td colspan="3">Semester End Examination Marks (A)</td><td colspan="4">Continuous Assessment Marks (B)</td><td rowspan="2">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="3">Theory</td><td>Term Test 1</td><td>Term Test 2</td><td>Assignment</td><td>Total</td></tr>
<tr><td colspan="3">60</td><td>15</td><td>15</td><td>10</td><td>40</td><td>100</td></tr>
<tr><td colspan="3">Laboratory Examination</td><td colspan="3">Term work</td><td rowspan="2">Total Term work</td><td rowspan="3">50</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">2</td><td rowspan="2">--</td><td rowspan="2">4</td><td>Oral</td><td>Practical</td><td>Oral & Practical</td><td colspan="2">Laboratory Work</td><td>Tutorial / Mini project / presentation/ Assignment</td></tr>
<tr><td>25</td><td>--</td><td>--</td><td colspan="2">15</td><td>10</td><td>25</td></tr>
</table>

Pre-requisite:

1. Object-Oriented Programming using JAVA.

Course Objectives: The objective of the course is:

1. To provide knowledge of software engineering discipline.
2. To apply analysis, design and testing principles to software project development.
3. To demonstrate and evaluate real time projects with respect to software engineering principles.

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

1. Understand and demonstrate basic knowledge in software engineering.
2. Identify requirements, and develop UML modelling.
3. Explore various levels of Software Design.
4. Identify risks, manage the change to assure quality in software projects.
5. Apply testing principles on software project and understand the maintenance concepts.
6. Analyze Software Using Structural Testing Techniques.

Detailed Syllabus:

Unit	Description	Duration
1	**Introduction to Software Engineering and Process Models** Nature of Software, Software Engineering, Software Process, Capability Maturity Model (CMM) Generic Process Model, Prescriptive Process Models: The Waterfall Model, V-model, Incremental Process Models, Evolutionary Process Models, Concurrent Models, Agile process, Agility Principles, Extreme Programming (XP), Scrum, Kanban model	06
2	**Requirements Analysis, Modelling and Project Scheduling** Requirement Elicitation, Software requirement specification (SRS), Developing Use Cases (UML) Requirement Model – Scenario-based model, Class-based model, Behavioral model. Project scheduling: Defining a Task Set for the Software Project, Timeline charts, Tracking the Schedule Software Project Estimation: LOC, FP and COCOMO	12
3	**Secure Software Design** Design Principles & Concepts, Objectives, Levels of Software Design, Secure Software Design Principals, Effective Modular Design, Cohesion and Coupling, Architectural design.	06
4	**Software Risk and Configuration Management** Risk Identification, Risk Assessment, Risk Projection, RMMM Software Configuration management, SCM repositories, SCM process.	04
5	**Software Testing and Maintenance** Strategic Approach to Software Testing, Unit testing, Integration testing Verification, Validation Testing, System Testing, Software Testing Fundamentals, White-Box Testing, Basis Path Testing, Control Structure Testing, Black-Box Testing, Software maintenance and its types, Software Re-engineering, Reverse Engineering	06
6	**Testing Techniques and Quality Assurance** Functional Testing Techniques: Equivalence Class Partitioning, Boundary Value Analysis, Decision Tables. Structural Testing Technique: Control Flow Testing and Data Flow Testing. Software Quality, Five Views of Software Quality, McCall's Quality Factors and Criteria Guidelines for Automation, Characteristics of Automated Test Cases, Structure of an Automated Test Case, Test Automation Infrastructure	08
	Total	**42**

Gphulokar

List of Laboratory Experiments:

Sr.No.	Suggested Experiments
1	Prepare detailed statement of problem for the selected / allotted mini project and identify suitable process model for the same with justification.
2	Develop Software Requirement Specification (SRS) document in IEEE format for the project.
3	Use project management tool to prepare schedule for the project.
4	Prepare RMMM plan for the project.
5	Identify scenarios & develop UML Use case and Class Diagram for the project.
6	Draw DFD (2 levels) and prepare Data Dictionary for the project.
7	Develop Activity / State Transition diagram for the project.
8	Develop Sequence and Collaboration diagram for the project
9	Change specification and make different versions using any SCM Tool.
10	Develop test cases for the project using white box testing.
11	Integrate Jira tool with katalon studio for generating defect tracker.

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

Books Recommended:

Text Books

1. Roger Pressman, —Software Engineering: A Practitioner's Approach",McGraw-Hill Publications,2010
2. Ian Sommerville, —Software Engineeringǁ, Pearson Education (9th edition),2012
3. Asoke K. Talukder, Manish Chaitanya, Architecting Secure Software Systems, ISBN 9781420087840, 2008
4. Software Security Engineering A Guide for Project Managers by Julia H.Allen, ean J. Barnum, Robert J. Ellison and Gary McGraw, May 11, 2008.
5. Software Testing and Quality Assurance: Theory and Practice, Sagar Naik, University of Waterloo, Piyu Tripathy, Wiley, 2008.
6. Sagar Naik , Piyu Tripathy .Software Testing and Quality Assurance: Theory and Practice, , University of Waterloo, , Wiley, 2008.

Reference Books

1. Ugrasen Suman, —Software Engineering – Concepts and Practicesǁ, Cengage Learning, 2012.
2. Pankaj Jalote, "An integrated approach to Software Engineering", Springer/Narosa, 2005.
3. Jibitesh Mishra and Ashok Mohanty, —Software Engineeringǁ, Pearson, 2011.

4. Rajib Mall, "Fundamentals of Software Engineering", Prentice Hall India, 2012.

Web resources:

1. https://hyperproof.io/resource/secure-software-development-best-practices/
2. https://www.javatpoint.com/software-engineering

Online Courses: NPTEL / Swayam

1. Software Engineering, By Prof. Rajib Mall, IIT Kharagpur
https://onlinecourses.nptel.ac.in/noc21_cs65/preview

2. Secure Systems Engineering, By Prof. Chester Rebeiro, IT Madras
https://archive.nptel.ac.in/noc/courses/noc21/SEM1/noc21-cs30/

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): 15 Marks
   ii.Journal documentation (Write-up and/or Assignments): 10 marks

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

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

Program: B.Tech. in Computer Science and Engineering (IoT and Cyber Security with Block Chain Technology)	**T.Y.B.Tech**	**Semester: VI**
Course: Malware Analysis	**Course Code: DJS23BCPE615**	
Course: Malware Analysis Laboratory	**Course Code: DJS23BLPE615**	

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

Prerequisite:

1. Applied Cryptography
2. Network Security
3. Operating System

Course Objectives: The objective of the course is

1. To introduce the fundamentals of malware, types and its effects.
2. To learn basic and advanced malware analysis techniques.
3. To analyze malware samples using static, dynamic analysis, and reverse engineering techniques.
4. To detect and analyze obfuscation and anti-malware techniques.

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

1. Identify different types of malwares and describe their core characteristics and behaviors.
2. Explain how various malware families operate and the impact of their functionalities on systems.
3. Apply static analysis techniques to interpret malware structure, metadata, and indicators of compromise.
4. Apply dynamic analysis concepts to understand malware behavior during execution.
5. Use appropriate theoretical tools, frameworks, and methodologies for analyzing malicious code.
6. Explore and discuss advanced obfuscation and evasion methods used by modern malware.

Detailed Syllabus:

Unit	Description	Duration
1	**Introduction Malware Analysis:** Introduction to of Malware & Threat Landscape, Types of malware, General rules for Malware Analysis. Malware Attack Life Cycle - The Combat Teams - Anti-malware Products- Overview of Static and Dynamic Analysis, Reverse Engineering for Windows and Linux systems, Legal, Ethical, and Operational Considerations, The Structure of a Virtual Machine, Malware Analysis Environment Setup	07
2	**Static Malware Analysis:** PE File Format and Structure (Windows binaries), Linked Libraries and Functions, Hashing: MD5, SHA256 – for sample identification, String Analysis & Metadata Extraction, File Dependencies and Imports, Recognizing Packers and Obfuscators, Identifying Indicators of Compromise (IOCs), Antivirus Scanning, Static Tools Overview: PEview, PEStudio, DIE/Detect It Easy	06
3	**Obfuscation and Evasion Techniques:** File Obfuscation, Binary Obfuscation Techniques, Assembly of Data, Encrypted Data Identification, decrypting with x86dbg, Control Flow Flattening, Garbage Code Insertion, Dynamic Library Loading, String Obfuscation, Unpacking using automated tools	07
4	**Advanced Static Analysis Techniques:** Basics of x86 Assembly: Registers, Stack, Instruction Set, Control Flow: Jumps, Calls, Conditional Execution, Debugging vs Disassembling, Global and local variables, Arithmetic operations, Loops, Understanding Function Calls and Parameters, Code Injection & API Hooking Basics, C Main Method and Offsets. Function analysis, Graphing using IDA Pro, Anti-static analysis techniques: obfuscation, packing, metamorphism, polymorphism.	08
5	**Malware Functionality:** Downloaders and Launchers, Backdoors, Credential Stealers, Persistence Mechanisms, Handles, Mutexes, Privilege Escalation, Covert malware launching- Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection, Memory Dumping & Memory Forensics, Fileless Malware Basics	07
6	**Advanced Dynamic Analysis Techniques:** Behavioral Analysis vs Code Analysis, Sandboxing Malware Safely, Monitoring File System, Registry, system calls and Process Activity, common Windows APIs used in malware, Network Behavior Analysis, Anti-dynamic analysis techniques, VM detection techniques, Evasion techniques, Packet Sniffing with Wireshark, Kernel vs. User-Mode Debugging, OllyDbg, Breakpoints, Tracing, Exception Handling, Patching	07
	Total	**42**

List of Laboratory Experiments:

Sr. No.	Suggested Experiments
1	Setting up a malware analysis environment using VirtualBox, FLARE VM, and Remnux
2	Identify malware using file hashing techniques (MD5, SHA-256) to verify integrity and detect tampering.
3	Examine malware using Portable Executable (PE) analysis tools such as PEiD and Exeinfo PE to gather insights into executable file structures.
4	Execute malware safely in a sandboxed environment (Cuckoo Sandbox) to observe its runtime behavior and interactions.
5	Monitor malware activities using Process Monitor and Process Explorer to track system changes and detect malicious operations.
6	Reverse-engineer malware binaries using tools like Radare2 and Ghidra to analyze their internal structure and functionality.
7	Tracing execution flow and understanding API calls
8	Behavioral monitoring with ProcMon, Regshot, and Process Explorer
9	Capturing and analyzing malicious network traffic with Wireshark & FakeNet
10	Investigate malware persistence mechanisms using Autoruns to analyze auto-starting entries and registry modifications.
11	Analyze memory dumps using the Volatility framework to extract forensic artifacts and detect hidden malware.
12	De-obfuscate malware through XOR decryption to reveal hidden payloads and bypass encoding mechanisms.
13	Debug and analyze packed malware samples using OllyDbg to unpack and examine malicious binaries.
14	Study real-world ransomware samples in a secure environment to understand their encryption techniques and impact.
15	Implement malware workflow orchestration using Apache Airflow or Jenkins to automate the analysis pipeline.
16	Utilize VirusTotal API for online scanning and reputation analysis of suspicious files and URLs.
17	Develop and apply basic YARA rules for signature-based malware detection.
18	Conduct Android malware analysis using MobSF to examine malicious applications and identify security threats.

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

Books Recommended:

Text Books:

1. Abhijit Mohanta, Anoop Saldanha, Malware Analysis and Detection Engineering a Comprehensive Approach to Detect and Analyze Modern Malware, 1st edition, Apress ISBN 978-1-4842-6192-7, 2020.
2. S. Oriyano and M. Solomon, Hacker Techniques, Tools, and Incident Handling, 3rd Edition, J B Learning, 2020.

3. Michael Sikorski and Andrew Honig, Practical Malware Analysis No Starch Press, ISBN: 9781593272906 2012
4. Alexey Kleymenov, Amr Thabet Mastering Malware Analysis Packt Publishing 2019

Reference Books:

1. Jamie Butler and Greg Hoglund, "Rootkits: Subverting the Windows Kernel" by 2005, Addison-Wesley Professional.
2. Bruce Dang, Alexandre Gazet, Elias Bachaalany, SébastienJosse, "Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation", 2014.
3. Victor Marak, "Windows Malware Analysis Essentials" Packt Publishing, O'Reilly, 2015.
4. Ken Dunham, Shane Hartman, Manu Quintans, Jose Andre Morales, Tim Strazzere, "Android Malware and Analysis",CRC Press, Taylor & Francis Group, 2015.
5. Windows Malware Analysis Essentials by Victor Marak, Packt Publishing, 2015.

Web resources:

1. OWASP (Open Web Application Security Project) – https://owasp.org/ https://www.coursera.org/learn/malware-analysis-and-assembly
2. Penetration Testing Execution Standard (PTES) – http://www.pentest-standard.org/
3. SANS Institute - https://www.sans.org/
4. Metasploit Unleashed - https://www.metasploitunleashed.com/ 6. CERT (Computer Emergency Response Team) - https://www.cert.org/

Online Courses: NPTEL / Swayam

1. Ethical Hacking: NPTEL :: Computer Science and Engineering - NOC:Ethical Hacking
2. Cyber Security: https://nptel.ac.in/courses/108/106/108106069/
3. Malware Analysis and Introduction to Assembly Language by IBM Skills Network Team https://www.coursera.org/learn/malware-analysis-and-assembly#modules

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.

Thelhokar

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. Mini Project/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)	T.Y.B.Tech	Semester: VI
Course: Digital Forensics	Course Code: DJS23BCPE616	
Course: Digital Forensics Laboratory	Course Code: DJS23BLPE615	

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	1	-	4	Oral	Practical	Oral & Practical	Laboratory Work	Tutorial / Mini project / presentation/ Journal			
				25	_	-	15	10		25	

Prerequisite:

1. Applied Cryptography
2. Network Security
3. Operating System
4. Computer Network

Course Objectives: The objective of the course is

1. To understand digital forensics principles, crime types, and legal frameworks.
2. To acquire knowledge of storage media, file systems, and operating system artifacts.
3. To develop hands-on skills in forensic data acquisition, recovery, and analysis.
4. To prepare and present digital forensic reports as per legal standards.

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

1. Explain the digital forensic investigation process and apply it to cybercrime cases.
2. Perform forensic imaging, memory analysis, and recover hidden or deleted data.
3. Analyze digital evidence from OS, network, email, and mobile sources.
4. Create forensic reports and maintain legal integrity of the investigation.

Detailed Syllabus:

Unit	Description	Duration
1	**Introduction to Digital Forensics:** Digital Forensics Defination, Digital Forensics Goals, Digital Forensics Categories - Computer Forensics, Mobile Forensics, Network Forensics, Database Forensics Digital evidence: characteristics, types, and admissibility, Role and responsibilities of a first responder, Digital investigation process, Introduction to Incident - Computer Security Incident, Goals of Incident Response, CSIRT, Incident Response Methodology, Phase after detection of an incident Chain of custody and documentation standards	07
2	**Digital Evidence, Forensics Duplication and Digital Evidence Acquisition:** Digital evidence, Types of Digital Evidence, Challenges in acquiring Digital evidence, Admissibility of evidence, Challenges in evidence handling, Chain of Custody Digital Forensics Examination Process - Seizure, Acquisition, Analysis, Reporting. Necessity of forensic duplication, Forensic image formats, Forensic duplication technique Acquiring Digital Evidence - Forensic Image File Format, Acquiring Volatile Memory (Live Acquisition), Acquiring Nonvolatile Memory (Static Acquisition), Hard Drive Imaging Risks and Challenges, Network Acquisition	09
3	**Forensics Investigation:** Analyzing Hard Drive Forensic Images, Analyzing RAM Forensic Image, Investigating Routers Malware Analysis - Malware, Viruses, Worms, Essential skills and tools for Malware Analysis, List of Malware Analysis Tools and Techniques	04
4	**Windows and Unix Forensics Investigation:** Investigating Windows Systems - File Recovery, Windows Recycle Bin Forensics, Data Carving, Windows Registry Analysis, USB Device Forensics, File Format Identification, Windows Features Forensics Analysis, Windows 10 Forensics, Cortana Forensics Investigating Unix Systems - Reviewing Pertinent Logs, Performing Keyword Searches, Reviewing Relevant Files, Identifying Unauthorized User Accounts or Groups, Identifying Rogue Processes, Checking for Unauthorized Access Points, Analyzing Trust Relationships	07
5	**Mobile Forensics, Reporting and Emerging Challenges:** Android Forensics, Mobile Device Forensic Investigation - Storage location, Acquisition methods, Data Analysis, GPS forensics - GPS Evidentiary data, GPS Exchange Format (GPX), GPX Files, Extraction of Waypoints and TrackPoints, Display the Tracks on a Map. SIM Cards Forensics - The Subscriber Identification Module (SIM), SIM Architecture, Security, Evidence Extraction.	08
6	**Browser, Email Forensic & Forensic Investigation Reporting** Web Browser Forensics, Google chrome, web browser investigation Email forensics - Sender Policy Framework (SPF), Domain Key Identified Mail (DKIM), Domain based Message Authentication Reporting and Confirmation (DMARC) Investigative Report Template, Layout of an Investigative Report, Guidelines for Writing a Report	05
	Total	**42**

List of Laboratory Experiments:

Sr. No.	Suggested Experiments
1	Disk imaging and hash verification using FTK Imager
2	RAM acquisition and memory analysis with Volatility.
3	Recover deleted files/partitions using TestDisk
4	File system analysis with Autopsy or Sleuth Kit.
5	Data carving using Foremost or Bulk Extractor.
6	Windows registry and event log analysis.
7	Email header and attachment analysis
8	Web browser history and metadata extraction
9	Network packet capture and analysis using Wireshark
10	Password cracking using John the Ripper.
11	Mobile data extraction using Android tools/emulator.
12	Forensic report writing and expert witness simulation .

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

Books Recommended:

Text Books:

1. Nilakshi Jain, Dhananjay R. Kalbande Digital Forensic: The Fascinating World of Digital Evidences Wiley India Pvt. Ltd.ISBN-13: 978-8126565740

Reference Books:

1. Kevin Mandia, Chris Prosise, —Incident Response and computer forensicsl, Tata McGrawHill, 2006
2. Digital Forensics Basics A Practical Guide Using Windows OS — Nihad A. Hassan, APress Publication, 2019
3. Xiaodong Lin, —Introductory Computer Forensics: A Hands-on Practical Approachl, Springer Nature, 2018

Web resources:

1. Digital Forensic tools GitHub - mesquidar/ForensicsTools: A list of free and open forensics analysis tools and other resources
2. Digital Forensics MIT(CS)-202.pdf

Online Courses: NPTEL / Swayam

1. Course on Ethical HackingI https://nptel.ac.in/courses/106/105/106105217/
2. Course on Digital ForensicsI https://onlinecourses.swayam2.ac.in/cec20_lb06/preview
3. Course on Cyber Incident Response https://www.coursera.org/learn/incident-response

Ghellokar.

4. Course on Penetration Testing, Incident Responses and Forensicsl https://www.coursera.org/learn/ibm-penetration-testing-incident-response-forensics

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. 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. Mini Project/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 Cybersecurity with Block chain Technology)	T.Y.B.Tech	Semester: VI
Course: Machine Learning	Course Code: DJS23BCMD601	
Course: Machine Learning Laboratory	Course Code: DJS23BLMD601	

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

Pre-requisite:

1. Artificial Intelligence
2. Linear Algebra and Optimization Technique.
3. Probability and Statistical Inference

Course Objectives: The objective of the course is:

1. To understand basic concepts of Machine Learning.
2. To explore different machine learning methods.
3. To familiarize with regression, clustering, classification.
4. To evaluate SVM models effectively using accuracy, precision, recall, and F1-score metrics

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

1. Define various machine learning terminologies.
2. Apply major dimensionality reduction techniques.
3. Apply regression analysis to real-world problems and datasets.
4. Assess classification models using standard performance metrics.
5. Identify patterns in data and classify or cluster information into distinct categories.
6. Analyze different SVM techniques.

Detailed Syllabus:

Unit	Description	Duration
1	**Introduction to Machine Learning:** Terminologies in machine learning, History, Types of Machine Learning, Issues in Machine Learning, Application of Machine Learning, Steps involved in developing a Machine Learning Application, Hypothesis, and Inductive Bias, Training Error, Generalization error, Overfitting, Under fitting, Bias and Variance trade-off, Handling skewed data: Data Metrics for skewed classes.	06
2	**Dimensionality Reduction** Dimensionality Reduction Techniques, Principal Component Analysis, Eigen Values, Eigen Vectors, Orthogonality, Linear Discriminant Analysis, Independent component Analysis, Single Value decomposition.	06
3	**Regression:** Linear Regression, Least Square Regression, Gradient Descent Algorithm, Univariate and Multivariate Linear Regression, Regularization, Logistic regression. Lasso and Ridge regression.	07
4	**Classification:** Artificial Neural Network: Back Propagation Algorithm, Self Organizing maps. Attribute Selection Measures, learning with Trees: Decision Trees, Constructing Decision Trees using Gini Index (Regression), Classification and Regression Trees (CART) Ensemble Models: Introduction to Ensemble Methods, Bagging, Boosting, Random forests. K-fold cross validation, Stumping, XGBoost Model Evaluation and Selection, Performance Metrics: Confusion Matrix, [Kappa Statistics], Sensitivity, Specificity, Precision, Recall, F-measure, ROC curve. Naïve Bayes Classifier	10
5	**Clustering:** Introduction to clustering with overview of distance metrics and major clustering approaches. Graph Based Clustering: Clustering with minimal spanning tree Model based Clustering: Expectation Maximization Algorithm. Density Based Clustering: DBSCAN	07
6	**Support Vector Machine:** Constrained Optimization, Optimal decision boundary, Margins and support vectors, SVM as constrained optimization problem, Quadratic Programming, SVM for linear and nonlinear classification, Basics of Kernel trick. Support Vector Regression, Multiclass Classification	06
	Total	42

List of Laboratory Experiments:

Sr.No.	Suggested Experiments
1.	Perform Linear Regression.
2.	Perform Logistic Regression.
3.	Implementing CART decision tree algorithm.
4.	Perform Ensemble methods
5.	Perform Artificial Neural Network
6.	Perform K-means clustering.
7.	Perform DBSCAN clustering.
8.	Analyze performance measures.
9.	To implement a Support Vector Machine.
10.	Mini project based on any machine learning application.

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

Books Recommended:

Text Books

1. Tom M.Mitchell, "Machine Learning", 1 st edition, McGraw Hill Education, 2017.
2. Peter Harrington, "Machine Learning in Action", 1 st Edition, DreamTec Press, 2012.
3. Ethem Alpaydın, "Introduction to Machine Learning", 3rd Edition, MIT Press, 2014.
4. Kevin P Murphy, "Machine Learning a probabilistic perspective", Illustrated edition, The MIT Press, 2012.

Reference Books

1. Kevin P. Murphy, "Machine Learning: A Probabilistic Perspective", 2nd Edition, The MIT Press, 2012.
2. Andreas C. Müller and Sarah Guido, "Introduction to Machine Learning with Python: A Guide for Data Scientists", 1 st Edition, O'reilly, 2016.
3. Stephen Marsland, "Machine Learning: An Algorithmic Perspective", 2 nd Edition, CRC Press, 2014.
4. Jiawei Han, Micheline Kamber, "Data Mining Concepts and Techniques", 3 rd Edition Morgann Kaufmann Publishers, 2011.

Web Resources:

1.https://towardsdatascience.com/machine-learning/home?gi=e6b8558a75dd

2.https://archive.ics.uci.edu/

Online References

1. Introduction to Machine Learning by Prof. Balaraman Ravindran, IIT Madras, https://nptel.ac.in/courses/106106139
2. Introduction to Machine Learning By Prof. Sudeshna Sarkar, IIT kharagpur

Thellokar

https://onlinecourses.nptel.ac.in/noc22_cs97/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 and Practical 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. Mini Project/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 Blockchain Technology)	**T.Y.B.Tech**	**Semester : VI**
Course: Innovative Product Development IV	**Course Code: DJS23IPSCX04**	

<table>
<tr><th colspan="4" rowspan="2">Teaching Scheme
(Hours / week)</th><th colspan="7">Evaluation Scheme</th></tr>
<tr><th colspan="3">Semester End Examination Marks (A)</th><th colspan="3">Continuous Assessment Marks (B)</th><th rowspan="2">Total Marks(A+B)</th></tr>
<tr><th rowspan="3">Lectures</th><th rowspan="3">Practical</th><th rowspan="3">Tutorial</th><th rowspan="3">Total Credits</th><th colspan="3">Theory</th><th>Term Test 1</th><th>Term Test 2</th><th>Assignment</th></tr>
<tr><td colspan="3">--</td><td>--</td><td>--</td><td>--</td><td>--</td></tr>
<tr><th colspan="3">Laboratory Examination</th><th colspan="3">Term work</th><th rowspan="2">Total Term work</th></tr>
<tr><td rowspan="2">--</td><td rowspan="2">2</td><td rowspan="2">--</td><td rowspan="2">1</td><th>Oral</th><th>Practical</th><th>Oral &amp; Practical</th><th>Laboratory Work</th><th colspan="2">Tutorial / Mini project / presentation/ Assignment</th></tr>
<tr><td>--</td><td>--</td><td>25</td><td></td><td colspan="2">25</td><td>25</td></tr>
</table>

Course Objectives:

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

Outcomes:

Learner will be able to:

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

Guidelines for the proposed product design and development:

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

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

Guidelines for Assessment of the work:

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

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

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

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

- In the semester V, the entire design proposal shall be ready, including components/system selection as well as the cost analysis. Two reviews will be conducted based on the presentation given by the student's team.
    - First shall be for finalization of the product selected.
    - Second shall be on finalization of the proposed design of the product.
- In the semester VI, the expected work shall be procurement of components/systems, building of the working prototype, testing and validation of the results based on work completed in semester III.
    - First review is based on readiness of building the working prototype.
    - Second review shall be based on a presentation as well as the demonstration of the working model, during the last month of semester IV. This review will also look at the readiness of the proposed technical paper presentation of the team.

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

1. Quality of survey/ need identification of the product.
2. Clarity of Problem definition (design and development) based on need.
3. Innovativeness in the proposed design.
4. Feasibility of the proposed design and selection of the best solution.
5. Cost effectiveness of the product.
6. Societal impact of the product.
7. Functioning of the working model as per stated requirements.
8. Effective use of standard engineering norms.
9. Contribution of each individual as a member or the team leader.
10. Clarity on the write-up and the technical paper prepared.

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

Guidelines for Assessment of Semester Reviews:

- The write-up should be prepared as per the guidelines given by the department.
- The design and the development of the product shall be assessed through a presentation

and demonstration of the working model by the student team to a panel of Internal and External Examiners, preferably from industry or any research organisations having an experience of more than five years, approved by the Head of the Institution. The presence of the external examiner is desirable only for the 2nd presentation in semester IV. Students are compulsorily required to present the outline of the technical paper prepared by them during the final review in semester VI.

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) Common to all Programs	T.Y.B.Tech	Semester: VI
Course: Constitution of India	Course Code: DJS23ICHSX09	

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	Assign ment	Total	
				--			--	--	--	--	--
				Laboratory Examination			Term work			Total Term work	
				Oral	Practical	Oral & Practical	Laboratory Work	Tutorial / Mini project / presentation/ Assignment			
1	--	--	--	--	--	--	--	--		--	--

Course Objectives:

1. To provide basic information about Indian constitution.
2. To identify individual role and ethical responsibility towards society.
3. To understand human rights and its implications.

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

1. Have general knowledge and legal literacy and thereby to take up competitive examinations.
2. Understand state and central policies, fundamental duties.
3. Understand Electoral Process, special provisions.
4. Understand powers and functions of Municipalities, Panchayats and Co-operative Societies.
5. Understand Engineering ethics and responsibilities of Engineers.
6. Understand Engineering Integrity & Reliability.

Constitution of India (DJS23ICHSX09)		
Unit	**Syllabus Content**	**Duration**
1	**Introduction to the Constitution of India** The Making of the Constitution and Salient features of the Constitution. Preamble to the Indian Constitution. Fundamental Rights & its limitations.	02
2	**Directive Principles of State Policy:** Relevance of Directive Principles, State Policy, Fundamental Duties. Union Executives – President, Prime Minister, Parliament, Supreme Court of India.	02

3	**State Executives:** Governor, Chief Minister, State Legislature, High Court of State. Electoral Process in India, Amendment Procedures, 42nd, 44th, 74th, 76th, 86th & 91st Amendments.	03
4	**Special Provisions:** For SC & ST, Special Provision for Women, Children & Backward Classes, Emergency Provisions.	02
5	**Human Rights:** Meaning and Definitions, Legislation Specific Themes in Human Rights, Working of National Human Rights Commission in India, Powers and functions of Municipalities, Panchayats and Co-Operative Societies.	03
6	**Scope & Aims of Engineering Ethics:** Responsibility of Engineers and Impediments to Responsibility. Risks, Safety and liability of Engineers. Honesty, Integrity & Reliability in Engineering.	02
	Total hours	14

Books Recommended:

Text books:

1. Durga Das Basu, *"Introduction to the Constitution on India"*, (Students Edition) Prentice Hall EEE, 19th / 20th Edition, 2001.
2. Charles E. Haries, Michael S. Pritchard and Michael J. Robins, *"Engineering Ethics"*, Thompson Asia, 2003.

Reference Books:

1. M. V. Pylee, *"An Introduction to Constitution of India"*, Vikas Publishing, 3rd Edition, 2003.
2. M. Govindarajan, S. Natarajan, V. S. Senthilkumar, *"Engineering Ethics"*, Prentice Hall of India Pvt. Ltd. New Delhi, 2013.
3. Brij Kishore Sharma, *"Introduction to the Constitution of India"*, PHI Learning Pvt. Ltd., New Delhi, 7th Edition 2015.
4. Latest Publications of *Indian Institute of Human Rights*, New Delhi

Website Resources:

1. www.nptel.ac.in
2. www.hnlu.ac.in
3. www.nspe.org
4. www.preservearticles.com

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