Subject Code	Subject Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSL701	DevSecOps Lab	--	2	--	--	1	--	1

Subject Code	Subject Name	Examination Scheme						
		Theory Marks				Term Work	Oral	Total
		Internal assessment			End Sem. Exam			
		Test1	Test 2	Avg. of 2 Tests				
CSL701	DevSecOps Lab	--	--	--	--	25	25	50

Lab Objectives:

Sr. No.	Lab Objectives
1	To understand the concept of distributed version control.
2	To familiarize myself with Jenkins, build & test software Applications & Continuous integration.
3	To understand Docker to build, ship and run containerized images.
4	To familiarize with the concept of Software Configuration Management with Continuous Monitoring.
5	To understand the basics of Application/code security testing and threat modeling.
6	To familiarize with the concept of Cloud and Infrastructure as a Code.

Lab Outcomes:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
On successful completion of the course students will be able to,		
1	Understand the concepts of distributed version control using GIT and GITHUB	L1
2	Apply Jenkins to Build, Deploy and Test the Software Applications	L3
3	Analyze & Illustrate the Containerization of OS images and deployment of applications over Docker	L3, L4
4	Deploy and Examine the Software Configuration management using Ansible and Continuous monitoring and alerting using Prometheus and Nagios	L4
5	Use Sonarqube and snyk to perform code quality checks and Threat Dragon to create threat models to identify threats in the system.	L3
6	Implement Terraform scripts to manage VMs on a cloud.	L3

Prerequisite: DevOps

Sr. No.	Module	Detailed Content	Hours	LO
0	Prerequisite	Concept of DevOps with related technologies which are used to Code, Build, Test, Configure & Monitor the Software Applications.	**02**	**-**
I	Version Control using GIT	To Perform Version Control on documents/files websites/ Software's using GIT & GITHUB that covers all GIT commands given in GIT cheat sheet. • To implement Version control for different files/directories using GIT • To implement version control using GITHUB to sync local GIT repositories and perform various related operations.	**04**	**LO 1**
II	Working with Jenkins	• To deploy and test Java/web/Python application on jenkins server. • To implement Jenkins pipeline using scripted/declarative pipeline • To use jenkins to deploy and run test cases for Java/Web application using Selenium/JUnit	**04**	**LO 2**
III	Containerization	• To use docker to run containers of different applications and operating Systems. • To create a custom docker image using Dockerfile and upload it to the docker hub.	**04**	**LO 3**
IV	Software Configuration Management and Continuous Monitoring	• To implement continuous deployment using Ansible • To Implement automated monitoring and alerting using Prometheus • To implement continuous monitoring using Splunk/NagiOS	**04**	**LO 4**
V	Application/Code Security	• To implement Application and code security testing using snyk • To implement Static Application Security Testing using SonarQube • To implement threat models to identify threats in the system using Threat Dragon	**04**	**LO 5**

VI	Cloud and Infrastructure as a code	• To create and work with virtual machine on cloud (GCP / AWS / Azure) • To implement terraform script for deploying compute/Storage/network infrastructure on the public cloud platform (GCP / AWS / Azure)	**04**	**LO 6**

Text Books:

1. Prem Kumar Ponuthorai, Jon Loeliger, Version Control with Git, 3rd Edition,O'Reilly Media.
2. John Ferguson Smart,"Jenkins, The Definitive Guide", O'Reilly Publication.
3. Karl Matthias & Sean P. Kane, Docker: Up and Running, O'Reilly Publication.
4. Russ McKendrick, Learn Ansible, Pakt Publication.
5. Yevgeniy Brikman, Terraform: Up and Running, 3rd Edition,O'Reilly Publication.
6. G. Ann Campbell,SonarQube in Action,First Edition, Manning publication.

References:

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

Online references:

Sr. No.	Topic	Link
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-a-job-in-jenkins-using-jenkins-freestyle-project.html 2) https://k21academy.com/devops-foundation/ci-cd-pipeline-using-jenkins/
3	Docker	https://docs.docker.com/get-started/docker_cheatsheet.pdf
4	Ansible	https://docs.ansible.com/ansible/latest/index.html
5	Prometheus	https://prometheus.io/docs/introduction/overview/
6	Snyk	https://snyk.io/learn/application-security/static-application-security-testing/
7	Threatdragon	https://www.threatdragon.com/#/
8	SonarQube	https://docs.sonarqube.org/latest/
9	Terraform	https://developer.hashicorp.com/terraform/intro

Term Work: Term Work shall consist of at least 10 to 12 practicals based on the above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiment) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above syllabus.

Subject Code	Subject Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSL702	Web Application Security Lab	--	2	--	--	1	--	1

Subject Code	Subject Name	Examination Scheme						
		Theory Marks				Term Work	Oral	Total
		Internal assessment			End Sem. Exam			
		Test1	Test 2	Avg. of 2 Tests				
CSL702	Web Application Security Lab	--	--	--	--	25	25	50

Lab Objectives:

Sr. No.	Lab Objectives
1	To be familiarized with web application security tools and techniques.
2	To gain knowledge of discovering and exploiting vulnerabilities in web applications.
3	To Understand workflow of web application penetration testing
4	To understand the importance of access control, authorization and authentication in secure web applications.
5	To be familiar with various client-side vulnerabilities in web application.
6	To understand the injection attacks on datastore and web server.

Lab Outcomes:

Sr. No.	Lab Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	To configure and install various web application security tools	L1, L2,l3
2	To identify and manage vulnerabilities of web Applications and execute mitigation plans.	L1, L2, L3
3	To perform web penetration testing and organize a checklist using burp suite.	L1, L2, L3,L4
4	To identify various attacks on access control, authorization and authentication mechanisms in web applications.	L1, L2, L3,L4
5	To Examine various client -side web application security aspects.	L1,L2,L3
6	To experiment on various injection attacks on data and server in web application	L1,L2,L3

Prerequisite: Web X

DETAILED SYLLABUS:

Sr. No.	Module	-Detailed Content	Hours	LO Mapping
0	Prerequisite	Web application terminology- cookies, sessions,web client, server ,headers	--	--
I	Installation and Set up	1. Configuration of Burp Suite 2. Installation of Mutillidae 3. Installation of Kali Linux	02	LO1
II	Vulnerability Assessment	1. Crawling the web application using Burp Spider 2. Looking for web vulnerabilities using the scanner in Burp suite 3. Replaying web requests using the Repeater tab 4. Fuzzing web requests using the burp Intruder. 5. Categorize vulnerabilities based on their severity, following industry-standard frameworks like the Common Vulnerability Scoring System (CVSS).	04	LO2
III	Web Application Pen testing	1. Discovering hidden content with Burp Suite 2. Gather information and perform reconnaissance: a) Identify the target web application and gather relevant information such as the application's technology stack, URLs, endpoints, and any other publicly available information. b) Use open-source intelligence (OSINT) techniques to gather information about the application, its infrastructure, and potential vulnerabilities. 3. Generate HTML/XML Burp suite scan report.	06	LO3
IV	Authentication and Session management	Attacking Authentication and Session Management 1. Session Management Vulnerabilities in Mutillidae 2. Brute forcing the authentication of Mutillidae 3. Building a PHP Web Application with Cookies/Sessions 4. Third-Party Authentication	04	LO4
V	XSS and CSRF	Detecting XSS Vulnerabilities in web application 1. Perform reflected XSS attack and stored XSS attack using Mutillidae 2. Exploiting stored XSS using the header and Perform DOM XSS injection using Mutillidae Detecting CSRF Vulnerabilities in web application 1. Detect CSRF attack using Burp Suite 2. Prevent CSRF attacks in web applications using Javascript.	04	LO5
VI	Injection in web application	SQL Injection 1. Bypassing Authentication using SQL injection. 2. Extracting Data using the UNION attack 3. Blind SQL injection 4. Automating SQL injection with SQLMAP tool Extended SQLi, Protecting against SQLi, and SQLi Forensics 1. Reading Files from the Target Web Server 2. Writing Files into the Target Web Server 3. Reading from and Writing to the Target Web Server 4. Reading Database Password Hashes 5. Protecting against SQL injection 6. Investigating SQL injection attacks (SQLi Forensics)	04	LO6

Text Books:

1. Practical Web Penetration Testing by Gus khawaja,packt publication
2. Hands-On Application Penetration Testing with Burp Suite: Use Burp Suite and its features to inspect, detect, and exploit security vulnerabilities in your web by Carlos A. Lozano, Dhruv Shah and Riyaz Ahemed Walikar , Packt Publication
3. The Web Application Hacker's handbook, Defydd Stuttard, Wiley Publishing

References:

1. Professional Pen Testing for Web application, Andres andreu, wrox press
2. Mastering Modern Web Penetration Testing Paperback – 28 October 2016 by Prakhar Prasad, Packt Publication

Online References:

1. https://www.tutorialsfreak.com/web-application-penetration-testing-tutorial/
2. https://hackersploit.org/web-app-penetration-testing-tutorials

Term Work: Term Work shall consist of at least 10 to 12 practicals based on the suggested list in syllabus.. Also Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiment) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above syllabus.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSL703	ML & Security Lab	--	2	--	--	1	--	1

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Oral	Total
		Internal assessment			End Sem. Exam			
		Test1	Test 2	Avg. of 2 Tests				
CSL703	ML & Security Lab	--	--	--	--	25	25	50

Lab Objectives:

Sr. No.	Lab Objectives
1	To identify Python tools for AI and cybersecurity
2	To get basic hands-on experience with supervised, unsupervised machine learning methods
3	To detect Email Cybersecurity Threats with AI & ML techniques.
4	To understand how to combat malware, detect spam, and fight financial fraud to mitigate cybercrimes.
5	To predict network intrusions and detect anomalies with machine learning
6	To develop tools for cyber defense using deep learning.

Lab Outcomes:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
On successful completion of the course students will be able to,		
1	Optimize Artificial Intelligence for Cybersecurity Arsenal	L1, L2, L3, L4
2	Use machine learning algorithms with complex datasets to implement cybersecurity concepts	L1, L2, L3
3	Identify different email threats detection strategies using AI & ML techniques	L1, L2, L3, L4
4	Analyze the ML algorithms to mitigate the malware, detect spam, and fight financial fraud	L1, L2, L3, L4
5	Perform Efficient Network Anomaly Detection Using ML techniques	L1, L2, L3
6	Verify the strength of user authentication procedures with deep learning	L1, L2,L3, L4, L5

Prerequisite: Must have completed the course on Introduction to Linear Algebra and have basic familiarity with probability theory.

Hardware & Software requirements:

Hardware Specifications	Software Specifications
PC with following Configuration 1. Intel Core i3/i5/i7 2. 4 GB RAM 3. 500 GB Hard disk	Python 3.4.1- Python 3.11.3 any stable version

DETAILED SYLLABUS:

Sr. No.	Detailed Content	Hours	LO Mapping
I	Programming in Python and Basics of manipulation of Data, Enter Anaconda—the data scientist's environment of choice, Playing with Jupyter Notebook, feeding your AI arsenal—where to find data and malicious samples, learn to speed up a system using Python libraries with NumPy, Scikit-learn, and CUDA	**04**	LO1
II	Types of Regression Models, Supervised Learning using Linear regression, Unsupervised Learning using Clustering, Simple Neural Network using Perceptron	**04**	LO2
III	How to detect spam with Perceptrons, Email spam detection with support vector machines (SVMs), Phishing detection with logistic regression and decision trees, Spam detection with Naive Bayes algorithm, Spam detection adopting NLP	**04**	LO3
IV	Fraudulent emails and spoofs, Types of email fraud, Featurization techniques that convert text-based emails into numeric values, Spam detection with logistic regression	**04**	LO4
V	Get hold of information, modify information, disrupt services, perform distributed denial of service to and from the server where information is stored, Exploit using malware and viruses, Privilege escalation and credential compromise	**04**	LO5
VI	Authentication abuse prevention, Account reputation scoring, User authentication with keystroke recognition, Biometric authentication with facial recognition	**04**	LO6

Textbooks:

1. Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber-attacks and detecting threats and network anomalies, Alessandro Parisi, Packt Publishing; 1st edition, 2019

2. Hands-On Machine Learning for Cybersecurity: Safeguard your system by making your machines intelligent using the Python ecosystem, Soma Halder, Packt Publishing; 1st edition, 2018

3. Gupta, Brij B., and Quan Z. Sheng, eds. Machine learning for computer and cyber security:principle, algorithms, and practices. CRC Press, 2019.

4. Artificial Intelligence and Data Mining Approaches in Security Frameworks Editor(s): Neeraj Bhargava, Ritu Bhargava, Pramod Singh Rathore, Rashmi Agrawal, 2021.

References:

1. Tsai, Jeffrey JP, and S. Yu Philip, eds. Machine learning in cyber trust: security, privacy, and reliability. Springer Science & Business Media, 2009.

2. Machine Learning: A Probabilistic Perspective, Kevin P Murphy, MIT Press.

3. Christopher M. Bishop. Pattern Recognition and Machine Learning. Springer 2006.

4. Tom Mitchell. Machine Learning. McGraw Hill, 1997.

Online References:

1. What Is Machine Learning in Security? - Cisco

2. https://www.mdsny.com/5-top-machine-learning-use-cases-for-security/

MOOC Courses:

1. https://nptel.ac.in/courses/106/106/106106139/

2. https://nptel.ac.in/courses/106/106/106106202/

3. https://www.classcentral.com/course/independent-machine-learning-security-12651

List of Experiments/Mini-Project.

1. Implement Supervised Learning model using Linear regression.
2. Implement Unsupervised Learning model using Clustering.
3. Design and implement Simple Neural Network using Perceptron.
4. Implementation and analysis of Bayesian Spam Detector with Nltk
5. Design and implement Decision Tree Phishing Detector
6. Design a Logistic Regression based Phishing Detector
7. Perform Email spam detection using SVM.
8. Set up a Decision Tree Malware Detector
9. Implement K-means malware clustering.
10. Design and implement Random Forest Malware Classifier
11. Implementation and analysis of Gaussian Network Anomaly Detection
12. Design and implement Network Anomaly Detection model.
13. Implementation and analysis of Keystroke Detection using different classifiers.
14. Perform Malicious URL detection using linear regression model.
15. Study of SMS spam detection
16. Study of Credit card fraud detection

Term Work: Term Work shall consist of at least 10 to 12 practical's based on the above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiment) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above syllabus.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSL704	Open-Source Intelligence (OSINT) Lab	--	2	--	--	1	--	1

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Oral	Total
		Internal assessment			End Sem. Exam			
		Test1	Test 2	Avg. of 2 Tests				
CSL704	Open-Source Intelligence (OSINT) Lab	--	--	--	--	25	25	50

Lab Objectives:

Sr. No.	Lab Objectives
The course aims:	
1	To provide hands-on experiences for students to develop critical thinking, research skills
2	To incorporate ethical usage of OSINT tools.
3	To get familiar with OSINT framework and its usage on publicly available data.
4	To learn to use the OSINT tools for social media, Email, Image, or network analysis, websites and understand the usage for Digital Forensics.
5	To performs background/profile/corporate profile checks, corporate Open-Source Intelligence (OSINT) Assessment etc.
6	Identify intelligence needs and leverage a broad range of tools and sources to improve data collection, analysis, and decision making.

Lab Outcomes:

Sr. No.	Lab Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Gain knowledge about Open-Source Intelligence understand the threats and think critically about countermeasures.	L1, L2, L3
2	Conduct advanced searches to gather intelligence and apply advance OSINT search techniques and tools.	L1, L2, L4
3	Use OSINT tools for analysis fake news, image, video data	L1, L2, L3
4	Conduct advanced searches to gather intelligence from social media sites and understand the use of Public Records for corporate and business intelligence etc.	L1, L2
5	Gather information/metadata about Maps to performance detailed map profiling	L1, L2, L3
6	Get familiar with Technical Foot printing websites for mitigating various threats	L1, L2

Prerequisite:

1. Kali Linux Installation and VM deployment.
2. Networking and security fundamentals

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	LO Mapping
0	The Evolution of Open-Source Intelligence,	Open-Source Information Categories OSINT Types, Digital Data Volume, OSINT Organizations, Parties Interested in OSINT Information, International Organizations, Information Gathering Types, Benefits of OSINT, Challenges of Open-Source Intelligence Legal and Ethical Constraints	**1**	LO1
I	Introduction To Online Threats and Countermeasures	Online Threats-. Securing the Operating System: Hardening the Windows OS, Staying Private in Windows, Destroying Digital Traces General Privacy Settings- Avoiding Pirated Software, Handling Digital Files Metadata, Physically Securing Computing Devices	**1**	LO1
II	Using Search Engines to Locate Information	Search Engine Technique - Keywords Discovery and Research, - Google, Privacy-Oriented Search Engines, Other Search Engines, Business Search Sites, Metadata Search Engines, Code Search FTP Search Engines Automated Search Tools, Dorks	**2**	LO2
III	Searching for Digital Files	News Search - Customize Google News, News Websites, Fake News Detection - Document Search, Image, Video, File Extension and File Signature List, Productivity Tools	**2**	LO4
IV	People Search Engines and Public Records	Social Media Intelligence: What Is Social Media Intelligence? Social Media Content Types, General Resources for Locating Information on Social Media Sites Pastebin Sites People Search Engine, Public Records and example of Public Records, Searching for Personal Details, General People Search , Online Registries, Vital Records, Criminal and Court Search, Property Records, Tax and Financial Records, Social Security Number Search Username Check, E-mail Search and Investigation Data Compromised Repository Websites, Phone Number Search	**6**	LO4
V	Online Maps:	The Basics of Geolocation Tracking, How to Find the GPS Coordinates of Any Location on a Map How to Find the Geocode Coordinates from a Mailing Address, General Geospatial Research Tools Commercial Satellites, Date/Time Around the World, Location-Based social media, Conducting Location Searches on social media Using Automated Tools, Country Profile Information Transport Tracking	**6**	LO5
VI	Technical Foot printing:	Website History and Website Capture Website Monitoring Services - RSS Feed Investigate the Target Website, Investigate the Robots.txt File, Mirror the Target Website Extract the Links Check the Target Website's Backlinks Monitor Website Updates Check the Website's Archived Contents	**6**	LO6

		Identify the Technologies Used, Web Scraping Tools Investigate the Target Website's File Metadata, Website Certification Search, Website Statistics and Analytics Tools, Website Reputation Checker Tools, Passive Technical Reconnaissance Activities, WHOIS Lookup, Subdomain Discovery, DNS Reconnaissance, IP Address Tracking		

Textbooks:

1. Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence by Nihad A. Hassan (Author), Rami Hijazi (Author)
2. OSINT Techniques - Resources for Uncovering Online Information - 10th Edition (2023) by Michael Bazzell
3. Operator Handbook: Red Team + OSINT + Blue Team Reference by Joshua Picolet

References:

1. We Are Bellingcat: Global Crime, Online Sleuths, and the Bold Future of Newsby Eliot Higgins
2. Extreme Privacy: What It Takes to Disappear in America by Michael Bazzell

Tools:

1. https://cheatsheet.haax.fr/open-source-intelligence-osint/
2. https://inteltechniques.com/tools/
3. https://hunter.io/
4. https://www.shodan.io/
   https://github.com/laramies/theHarvester
5. https://www.osintcombine.com/osint-bookmarks
6. https://osintframework.com/
7. https://learn.baselgovernance.org/enrol/index.php?id=79
8. https://inteltechniques.com/
9. https://www.bellingcat.com//
10. https://www.tracelabs.org/

List of Experiments/Mini-Project.

Sr.No.	Detailed Content
1	• Perform Email Header Analysis for extracting valuable information like sender IP address, email servers, and routing information. • Conduct email address enumeration by attempting to verify the existence of email addresses within a target domain. Use tools like the Harvester or thehunter.io to search for email addresses associated with a specific domain. This can help identify valid email addresses within an organization. • Analyze the metadata of an email, including date and time stamps, email clients used, or the originating IP address, email's origin, potential geographic location of the sender, or possible email routing
2	• Using OSINT tool such as (Harverster) you can gather information like emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key server.
3	• Use OSINT DORKS (create and execute search queries) to verify the accuracy of the information by cross-referencing various sources and critically evaluating the reliability and credibility of the new article.
4	• To perform the reverse Image analysis for finding physical location where the content was captured. Use OSINT tool to use image metadata, landmarks, street signs, or other visual cues to identify the geolocation accurately.

5	• Using OSINT tools gather Tactical information using WHOIS lookup tools or websites like DomainTools (domain, registration details, owner's contact information, registration date, and expiration date.) Archives, Text, Reverse Image Search, Images and EXIF data, Source code, Others TLD, Mentions of target, Check info such as via RSS,SSL certificates, Robots/Sitemap, Port scans, Reverse IP lookup
6	• Utilize website crawling OSINT tools to gather a comprehensive list of URLs, internal links, and structure of the website
7	• Use OSINT Tools to identify the technologies and frameworks used by the website, such as content management systems (CMS), server software, programming languages, or analytics tools and create vulnerability reports.
8	• Determine the geolocation (country, city, or approximate location) of each IP address (at least 10) One can use online IP geolocation tools, databases, and various techniques to gather information and accurately identify the physical location associated with each IP
9	• Conduct a comprehensive OSINT investigation about well-known company and gather information about the company's history, key executives, financial data, partnerships, news mentions, and any other relevant details using online databases, news articles, corporate websites, and industry reports
10	• Analyze the company's competitors to understand their market positioning, strengths, and weaknesses. Tools like SEMrush, Similar Web, or Alexa or any other OSINT tool can provide website traffic, keyword analysis, and competitor comparisons
11	• Fake News detection - Analyze at least 5 OSINT tools to detect, verify, authenticate, fake news and report.
12	• **Example Mini Project suggestion -** **Digital Footprint Analysis using OSINT Tools:** Assess and analyze your own digital footprints wrt, Personal Information, data (full name, age, date of birth, address, phone number, and email address), images, videos (online directories, social media profiles (at least 3 social media accounts), personal websites, Online Professional Presence and analyze. 1. Posts, comments, photos, and other content that they have shared publicly or with specific privacy settings. 2. Analyze their online interactions, connections, interests, and activities. 3. Analyze the nature of the content, locations, events, or people, as it can provide insights into activities, hobbies, or relationships. 4. Analyze work experience, educational background, skills, recommendations, and any professional associations or achievements.

Term Work: Term Work shall consist of at least 10 to 12 practical's based on the above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiment) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above syllabus.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Oral	Tutorial	Total
CSP701	Major Project I	--	6#	--	--	3	--	3

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Oral	Total
		Internal assessment			End Sem. Exam			
		Test1	Test 2	Avg. of 2 Tests				
CSP701	Major Project I	--	--	--	--	25	25	50

Course Objectives:
The project work facilitates the students to develop and prove Technical, Professional and Ethical skills and knowledge gained during graduation program by applying them from problem identification, analyzing the problem and designing solutions.

Course Outcomes:

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	To develop the understanding of the problem domain through extensive review of literature.	L6
2	To Identify and analyze the problem in detail to define its scope with problem specific data.	L4
3	To know various techniques to be implemented for the selected problem and related technical skills through feasibility analysis.	L3
4	To design solutions for real-time problems that will positively impact society and environment.	L6
5	To develop clarity of presentation based on communication, teamwork and leadership skills.	L6
6	To Cultivate professional and ethical behavior.	L6

Guidelines:

- **Project Topic Selection and Allocation:**

1. Project topic selection Process to be defined and followed:
2. Project orientation can be given at the end of sixth semester.
3. Students should be informed about the domain and domain experts whose guidance can be taken before selecting projects.
4. Students should be recommended to refer papers from reputed conferences/ journals like IEEE, Elsevier, ACM etc. which are not more than 3 years old for review of literature.
5. Students can certainly take ideas from anywhere but be sure that they should evolve them in a unique way to suit their project requirements. Students can be informed to refer Digital India portal, SIH portal or any other hackathon portal for problem selection.

- Topics can be finalized with respect to following criterion:

Topic Selection: The topics selected should be novel in nature (Product based, Application based, or Research based) or should work towards removing the lacuna in currently existing systems.

Technology Used: Use of the latest technology or modern tools can be encouraged**.**

- Students should not repeat work done previously (work done in the last three years).
- Project work must be carried out by a group of at least 2 students and a maximum of 4.
- The project work can be undertaken in a research institute or organization/Industry/any business establishment. (Out-house projects)
- The project proposal presentations can be scheduled according to the domains and should be judged by faculty who are experts in the domain.
- The head of department and senior staff along with project coordinators will take decision regarding final selection of projects.
- Guide allocation should be done, and students have to submit weekly progress reports to the internal guide.
- Internal guide has to keep track of the progress of the project and also has to maintain attendance report. This progress report can be used for awarding term work marks.
- In the case of industry/ out-house projects, a visit by internal guide will be preferred and external members can be called during the presentation at various levels.

Project Report Format:

At the end of semester, each group needs to prepare a project report as per the guidelines issued by the University of Mumbai.

A project report should preferably contain at least following details:

- Abstract
- Introduction
- Literature Survey/ Existing system
- Limitation Existing system or research gap
- Problem Statement and Objective
- Proposed System
- Analysis/Framework/ Algorithm
- Design details
- Methodology (your approach to solve the problem) Proposed System
- Experimental Set up
- Details of Database or details about input to systems or selected data
- Performance Evaluation Parameters (for Validation)
- Software and Hardware Set up
- Implementation Plan for Next Semester
- Timeline Chart for Term1 and Term-II (Project Management tools can be used.)
- References

Desirable

- Students can be asked to undergo some Certification course (for the technical skill set that will be useful and applicable for projects.

Term Work:

Distribution of marks for term work shall be done based on following:

1. Weekly Log Report
2. Project Work Contribution
3. Project Report (Spiral Bound) (both side print)
4. Term End Presentation (Internal)

The final certification and acceptance of TW ensures satisfactory performance on the above aspects.

Oral and Practical:

The Oral and Practical examination (Final Project Evaluation) of Project 1 should be conducted by Internal and External examiners approved by University of Mumbai at the end of the semester.

Suggested quality evaluation parameters are as follows:

1. Quality of problem selected.
2. Clarity of problem definition and feasibility of problem solution
3. Relevance to the specialization / industrial trends
4. Originality
5. Clarity of objective and scope
6. Quality of analysis and design
7. Quality of written and oral presentation
8. Individual as well as teamwork