

RN SHETTY TRUST ®



ESTD.: 2001
An Institute with a Difference

RNS INSTITUTE OF TECHNOLOGY

Autonomous Institution affiliated to Visvesvaraya Technological University, Belagavi

Approved By AICTE, New Delhi. Accredited by NAAC 'A+' Grade

RR Nagar, Dr. Vishnuvardhan Road, Bengaluru - 560 098

Ph: (080) 28611880, 28611881 URL: www.rnsit.ac.in



Dr. R N Shetty
Founder



DEPARTMENT OF CSE - CYBER SECURITY

BACHELOR OF ENGINEERING

Scheme and Syllabus of V - VIII Semesters

2024 SCHEME



 www.rnsit.ac.in

Scheme and Syllabus Batch 2024 - 2028

(As per NEP-2020)
(Effective from the academic year 2024 – 25)

About RNSIT

RNS Institute of Technology, familiar as RNSIT was established in the year 2001. It is the brainchild of Dr. R. N. Shetty, a well-known industrialist, and a great philanthropist. The institution was established with the sole purpose of imparting quality education in Engineering, Technology and Management. Being one of the premier engineering colleges in the country RNSIT is marching towards placing itself in the global map by excelling in academics and placements.

Lush green campus, state of the art infrastructure, well equipped laboratories, hundreds of activities, numerous new initiatives, consistent VTU ranks, path breaking placements, cultural extravaganza, Sports events, 5600 + students and 300 + faculty – with all these RNSIT has become dream destination for engineering aspirants across the country.

Vision

Building RNSIT into a World Class Institution

Mission

To impart high quality education in Engineering, Technology and Management with a difference, enabling students to excel in their career by

- Attracting quality Students and preparing them with a strong foundation in fundamentals so as to achieve distinctions in various walks of life leading to outstanding contributions
- Imparting value based, need based, choice based and skill based professional education to the aspiring youth and carving them into disciplined, World class Professionals with social responsibility
- Promoting excellence in Teaching, Research and Consultancy that galvanizes academic consciousness among Faculty and Students
- Exposing Students to emerging frontiers of knowledge in various domains and make them suitable for Industry, Entrepreneurship, Higher studies, and Research & Development
- Providing freedom of action and choice for all the Stakeholders with better visibility

About CSE (Cyber Security)

The Department of CSE – Cyber Security was started with the notion of establishing a complete cyber security ecosystem. In an era of exponential digital expansion, the corporate landscape has transitioned into a digitally driven operational framework. This metamorphosis has ushered in a parallel surge in cyber threats, compelling organizations to fortify their cybersecurity posture. As the demand for cybersecurity expertise reaches new heights, our program, in collaboration with industry luminaries, offers a specialized curriculum. It equips students with cutting-edge skills, spanning cryptography, API security, software fortification, network defense, identity and access management, cloud security, hardware safeguards, malware forensics, ransomware mitigation, vulnerability assessments, penetration testing, and more. This program empowers graduates to become agile defenders against the relentless evolution of cyber threats, ensuring the security of invaluable organizational assets in the contemporary industrial landscape.

Vision

To be a global leader in imparting Cyber Security education, research & development and empowering young minds to safeguard the digital world

Mission

- Empower students with Cyber Security essentials through hands-on facilities and a strong ethical foundation.
- Facilitate collaborative learning environment, teamwork, and global certifications for real-time challenges.
- Drive innovation in Cyber Security through state-of-the-art research, fostering a culture of exploration through higher learning and entrepreneurship.
- Promote students to possess qualities of interpersonal, interdisciplinary, leadership, and societal responsibilities.

Programme Educational Objectives

A Graduate of Computer Science and Engineering (Cyber Security) will be able to:

- **PEO1:** Demonstrate technical skills and problem-solving capabilities in the field of cyber security, effectively addressing complex challenges.
- **PEO2:** Develop strong communication skills, collaborative spirit to convey technical concepts and findings effectively to stakeholders, to foster employability in cyber security and related fields.

- **PEO3:** Incorporate ethical, legal, and social aspects into their professional practice, recognizing the implications of their actions on individuals, organizations, and society.
- **PEO4:** Actively engage in activities that foster the continuous development of their computing and cyber security skills, staying abreast of emerging technologies, best practices, and evolving threats to maintain their effectiveness as professionals in the field.

Program Outcomes (Revised)

1. **PO1: Engineering Knowledge:** Apply knowledge of mathematics, natural science, computing, engineering fundamentals and an engineering specialization as specified in WK1 to WK4 respectively to develop to the solution of complex engineering problems.
2. **PO2: Problem Analysis:** Identify, formulate, review research literature and analyze complex engineering problems reaching substantiated conclusions with consideration for sustainable development. (WK1 to WK4)
3. **PO3: Design/Development of Solutions:** Design creative solutions for complex engineering problems and design/develop systems/components/processes to meet identified needs with consideration for the public health and safety, whole-life cost, net zero carbon, culture, society and environment as required. (WK5)
4. **PO4: Conduct Investigations of Complex Problems:** Conduct investigations of complex engineering problems using research-based knowledge including design of experiments, modelling, analysis & interpretation of data to provide valid conclusions. (WK8).
5. **PO5: Engineering Tool Usage:** Create, select and apply appropriate techniques, resources and modern engineering & IT tools, including prediction and modelling recognizing their limitations to solve complex engineering problems. (WK2 and WK6)
6. **PO6: The Engineer and The World:** Analyze and evaluate societal and environmental aspects while solving complex engineering problems for its impact on sustainability with reference to economy, health, safety, legal framework, culture and environment. (WK1, WK5, and WK7).
7. **PO7: Ethics:** Apply ethical principles and commit to professional ethics, human values, diversity and inclusion; adhere to national & international laws. (WK9)
8. **PO8: Individual and Collaborative Teamwork:** Function effectively as an individual, and as a member or leader in diverse/multi-disciplinary teams.

9. **PO9: Communication:** Communicate effectively and inclusively within the engineering community and society at large, such as being able to comprehend and write effective reports and design documentation, make effective presentations considering cultural, language, and learning differences
10. **PO10: Project Management and Finance:** Apply knowledge and understanding of engineering management principles and economic decision-making and apply these to one's own work, as a member and leader in a team, and to manage projects and in multidisciplinary environments.
11. **PO11: Life-Long Learning:** Recognize the need for and have the preparation and ability for i) independent and life-long learning ii) adaptability to new and emerging technologies and iii) critical thinking in the broadest context of technological change. (WK8)

Programme Specific Outcomes (PSOs)

The CSE – Cyber Security graduates will have

1. **PSO1:** Proficiency in applying principles of software development to deliver efficient software solutions.
2. **PSO2:** Competency in securing information, systems, and networks through the implementation of cybersecurity best practices.

B.E. in CSE (Cyber Security)

Autonomous Scheme

V – VIII Semester

B. E in Computer Science and Engineering (Cyber Security): Autonomous Scheme and Syllabus
V SEMESTER

SL NO	COURSE	COURSE CODE	COURSE TITLE	TD/ PSB	TEACHING HOURS PER WEEK			Term work (TW)+ Self learning (SL) per semester	EXAMINATION				CREDITS
					THEORY LECTURE (L)	TUTORIAL (T)	PRACTICAL (P)		DURATION IN HOURS	CIE MARKS	SEE MARKS	TOTAL MARKS	
1	HSMC	BCS501	SOFTWARE ENGINEERING AND PROJECT MANAGEMENT	CSE - CY	3	2	0	45	3	50	50	100	4
2	IPCC	BCY502	COMPUTER NETWORKS AND SECURITY	CSE - CY	3	0	2	45	3	50	50	100	4
3	IPCC	BCY503	ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING	CSE - CY	3	0	2	45	3	50	50	100	4
4	PCCL	BCYL504	ADVANCED CYBER SECURITY LABORATORY	CSE - CY	0	0	2	0	3	50	50	100	1
5	PEC	BCY515X	PROFESSIONAL ELECTIVE - 1 (BUCKET LIST E)	CSE - CY	3	0	0	45	3	50	50	100	3
6	PROJ	BCY586	MINI PROJECT	CSE - CY	0	0	2	30	3	100	0	100	2
7	BSC	BENS507/ BBOE507	ENVIRONMENTAL STUDIES / BIOLOGY FOR ENGINEERS	ANY	2	0	0	30	2	50	50	100	2
8	AEC	BRMK557	RESEARCH METHODOLOGY AND IPR	ANY	2	0	0	30	2	50	50	100	2
9	MC	BNSK559	NATIONAL SERVICE SCHEME(NSS)	ANY	0	0	2	0		100	0	100	0
		BPEK559	PHYSICAL EDUCATION(PE)										
		BYOK559	YOGA										
	TOTAL									550	350	900	22

NOTE: 1st SEMESTER CHEMISTRY CYCLE SECTIONS WILL STUDY "ENVIRONMENTAL STUDIES" IN 4th SEMESTER & "Biology for Engineers" IN 5th SEMESTER

NOTE: 1st SEMESTER PHYSICS CYCLE SECTIONS WILL STUDY "Biology for Engineers" IN 4th SEMESTER & "ENVIRONMENTAL STUDIES" IN 5th SEMESTER

BUCKET LIST E			
PEC BCY515X			
BCY515A	THEORY OF COMPUTATION	BCY515D	DEVSECOPS
BCY515B	DIGITAL WATER MARKING AND STEGANOGRAPHY	BCY515E	DATA SCIENCE FOR CYBER SECURITY
BCY515C	HACKER TECHNIQUES, TOOLS AND INCIDENT HANDLING		

B. E in Computer Science and Engineering (Cyber Security): Autonomous Scheme and Syllabus
VI SEMESTER

SL NO	COURSE	COURSE CODE	COURSE TITLE	TD/PSB	TEACHING HOURS PER WEEK			Term work (TW)+ Self learning (SL) per semester	EXAMINATION				CREDITS	
					THEORY LECTURE(L)	TUTORIAL (T)	PRACTICAL (P)		DURATION IN HOURS	CIE MARKS	SEE MARKS	TOTAL MARKS		
1	IPCC	BCY601	VULNERABILITY ASSESSMENT AND PENETRATION TESTING	CSE - CY	3	0	2	45	3	50	50	100	4	
2	PCC	BCY602	CRYPTOGRAPHY AND NETWORK SECURITY	CSE - CY	3	2	0	45	3	50	50	100	4	
3	PEC	BCY613X	PROFESSIONAL ELECTIVE (BUCKET LIST F)	CSE - CY	3	0	0	45	3	50	50	100	3	
4	OEC	BXX654X	OPEN ELECTIVE (BUCKET LIST G)	CSE& ALLIED	3	0	0	45	3	50	50	100	3	
5	PROJ	BCY685	MAJOR PROJECT PHASE-1	CSE - CY	0	0	4	0	3	100	0	100	2	
6	PCCL	BCYL606	DIGITAL FORENSICS LAB	CSE - CY	0	0	2	0	3	50	50	100	1	
7	AEC/SEC	BCYT/L657X	BUCKET LIST H	CSE - CY	IF COURSE IS THEORY				2	50	50	100	1	
					1	0	0	15						
					IF COURSE IS PRACTICAL				3					
					0	0	2	0						
8	MC	BIKS608	INDIAN KNOWLEDGE SYSTEM	ANY	1	0	0	0	2	100		100	0	
9	MC	BNSK659	NATIONAL SERVICE SCHEME(NSS)	ANY	0	0	2	0	2	100		100	0	
		BPEK659	PHYSICAL EDUCATION(PE)											
		BYOK659	YOGA											
	TOTAL										600	300	900	18

BUCKET LIST F

Professional Elective BCY612X

BCY613A	BIG DATA ANALYTICS WITH SPARK	BCY613C	BLOCK CHAIN TECHNOLOGY
BCY613B	DEEP LEARNING TECHNIQUES	BCY613D	SURVEILLANCE AND VIDEO ANALYTICS

BUCKET LIST G

Open Elective BXX654X

BCS654A	INTRODUCTION TO DATA STRUCTURES	BCI654C	INTRODUCTION TO DBMS
BCY654B	FUNDAMENTALS OF OPERATING SYSTEMS	BCD654D	FOUNDATIONS OF DATA SCIENCE

BUCKET LIST H

AEC/SEC BCYT/L657X

BCYL657A	INDUSTRIAL CYBER SECURITY	BCYL657C	GENERATIVE AI
BCYL657B	REACT	BCYL657D	DATA VISUALIZATION WITH PYTHON

B. E in Computer Science and Engineering (Cyber Security): Autonomous Scheme and Syllabus
VII SEMESTER

SL NO	COURSE	COURSE CODE	COURSE TITLE	TD/PSB	TEACHING HOURS PER WEEK			Term work (TW)+ Self learning (SL) per semester	EXAMINATION				CREDITS
					THEORY LECTURE (L)	TUTORIAL (T)	PRACTICAL (P)		DURATION IN HOURS	CIE MARKS	SEE MARKS	TOTAL MARKS	
1	IPCC	BCY701	CLOUD COMPUTING AND SECURITY	CSE - CY	3	0	2	45	3	50	50	100	4
2	IPCC	BCY702	ETHICAL HACKING	CSE - CY	3	0	2	45	3	50	50	100	4
3	PCC	BCY703	MALWARE ANALYSIS	CSE - CY	3	2	0	45	3	50	50	100	4
4	PEC	BCY714X	PROFESSIONAL ELECTIVE (BUCKET LIST I)	CSE - CY	3	0	0	45	3	50	50	100	3
5	OEC	BXX755X	OPEN ELECTIVE (BUCKET LIST J)	ANY	3	0	0	45	3	50	50	100	3
6	PROJ	BCY786	MAJOR PROJECT PHASE-2	CSE - CY	0	0	12	0	3	100	100	200	6
TOTAL										350	350	700	24

BUCKET LIST I			
PROFESSIONAL ELECTIVE BCY714X			
BCY714A	VIRTUAL REALITY	BCY714C	WEB APPLICATION HACKING AND SECURITY
BCY714B	WIRELESS AND MOBILE DEVICE SECURITY	BCY714D	NATURAL LANGUAGE PROCESSING

BUCKET LIST J			
OPEN ELECTIVE BXX755X			
BCS755A	INTRODUCTION TO ALGORITHMS	BCD755C	FULL STACK WEB DEVELOPMENT
BCY755B	FOUNDATIONS OF INFORMATION SECURITY	BCI755D	INTRODUCTION TO MACHINE LEARNING

B. E in Computer Science and Engineering (Cyber Security): Autonomous Scheme and Syllabus
VIII SEMESTER

SL NO	COURSE	COURSE CODE	COURSE TITLE	TD/PSB	TEACHING HOURS PER WEEK			Term work (TW)+ Self learning (SL) per semester	EXAMINATION				CREDITS
					THEORY LECTURE (L)	TUTORIAL (T)	PRACTICAL (P)		DURATION IN HOURS	CIE MARKS	SEE MARKS	TOTAL MARKS	
1	PEC	BCY811X	PROFESSIONAL ELECTIVE (BUCKET LIST J) (ONLINE)	ONLINE	3	0	0	45	3	50	50	100	3
2	OEC	BCY852X	OPEN ELECTIVE (BUCKET LIST K) (ONLINE)	ONLINE	3	0	0	45	3	50	50	100	3
3	INT	BCY803	INTERNSHIP (INDUSTRY/RESEARCH-MINIMUM 14 WEEKS)	CSE - CY	0	0	20	0	3	100	100	200	10
TOTAL										200	200	400	16

BUCKET LIST K	
PROFESSIONAL ELECTIVE BCY801X	
BCY811X	BOS WILL PUBLISH COURSES BASED ON THE AVAILABILITY
BUCKET LIST L	
OPEN ELECTIVE BXX802X	
BCY852A	BOS WILL PUBLISH COURSES BASED ON THE AVAILABILITY

B. E in Computer Science and Engineering (Cyber Security): Autonomous Scheme and Syllabus
SCHEME - A - VII SEMESTER (Swappable VII and VIII SEMESTER)

SL NO	COURSE	COURSE CODE	COURSE TITLE	TD/PSB	TEACHING HOURS PER WEEK			Term work(TW)+ Self learning (SL) per semester	EXAMINATION				CREDITS
					THEORY LECTURE (L)	TUTORIAL (T)	PRACTICAL (P)		DURATION IN HOURS	CIE MARKS	SEE MARKS	TOTAL MARKS	
1	IPCC	BCY701	CLOUD COMPUTING AND SECURITY	CSE - CY	3	0	2	45	3	50	50	100	4
2	IPCC	BCY702	ETHICAL HACKING	CSE - CY	3	0	2	45	3	50	50	100	4
3	PCC	BCY703	MALWARE ANALYSIS	CSE - CY	3	2	0	45	3	50	50	100	4
4	PEC	BCY714X	PROFESSIONAL ELECTIVE (BUCKET LIST H)	CSE - CY	3	0	0	45	3	50	50	100	3
5	OEC	BXX755X	OPEN ELECTIVE (BUCKET LIST I)	ANY	3	0	0	45	3	50	50	100	3
6	PROJ	BCY786	MAJOR PROJECT PHASE-2	CSE - CY	0	0	12	0	3	100	100	200	6
TOTAL										350	350	700	24

BUCKET LIST H			
PROFESSIONAL ELECTIVE BCY714X			
BCY714A	REALITY	BCY714C	WEB APPLICATION HACKING AND SECURITY
BCY714B	WIRELESS AND MOBILE DEVICE SECURITY	BCY714D	NATURAL LANGUAGE PROCESSING
BUCKET LIST I			
OPEN ELECTIVE BXX755X			
BCS755A	INTRODUCTION TO ALGORITHMS	BCD755C	FULL STACK WEB DEVELOPMENT
BCY755B	FOUNDATIONS OF INFORMATION SECURITY	BCI755D	INTRODUCTION TO MACHINE LEARNING

T: Tutorial, P: Practical, S= SDA: Skill Development Activity, CIE: Continuous Internal Evaluation, SEE: Semester End Evaluation. TD : Teaching Department, PSB: Paper setting department, OEC: Open Elective Course, PEC: Professional Elective Course. PROJ: Project work
Note: VII and VIII Semesters of IV Years of the Program (1) Institutions can swap the VII and VIII semester Schemes of Teaching and Examinations to accommodate research internships/Industry internships after the VI semester. (2) Credits earned for the courses of VII and VIII Semester Schemes of Teaching and Examinations shall be counted against the corresponding semesters whether the VII or VIII semesters is completed during the beginning of the IV year or the later part of IV years of the program.

B. E in Computer Science and Engineering (Cyber Security): Autonomous Scheme and Syllabus
SCHEME - A - VIII SEMESTER (Swappable VII and VIII SEMESTER)

SL NO	COURSE	COURSE CODE	COURSE TITLE	TD/PSB	TEACHING HOURS PER WEEK			Term work(T W)+ Self learning (SL) per semester	EXAMINATION				CREDITS
					THEORY LECTURE (L)	TUTORIAL (T)	PRACTICAL (P)		DURATION IN HOURS	CIE MARKS	SEE MARKS	TOTAL MARKS	
1	PEC	BCY811X	PROFESSIONAL ELECTIVE (BUCKET LIST J)(ONLINE)	ONLINE	3	0	0	45	3	50	50	100	3
2	OEC	BCY852X	OPEN ELECTIVE (BUCKET LIST K)(ONLINE)	ONLINE	3	0	0	45	3	50	50	100	3
3	INT	BCY803	INTERNSHIP (INDUSTRY/RESEARCH-MINIMUM 14 WEEKS)	CSE - CY	0	0	20	0	3	100	100	200	10
TOTAL										200	200	400	16

BUCKET LIST J	
Professional Elective BCY801X	
BCY811X	BOS WILL PUBLISH COURSES BASED ON THE AVAILABILITY
BUCKET LIST K	
Open Elective BXX802X	
BCY852A	BOS WILL PUBLISH COURSES BASED ON THE AVAILABILITY

L: Lecture, T: Tutorial, P: Practical, S= SDA: Skill Development Activity, CIE: Continuous Internal Evaluation, SEE: Semester End Evaluation. TD - Teaching Department,
PSB: Paper setting department, OEC: Open Elective Course, PEC: Professional Elective Course. PROJ: Project work ,
INT: Industry Internship/ Research Internship/ Rural Internship
Note: VII and VIII semesters of IV years of the programs
Swapping Facility
* Institutions can swap VII and VIII Semester Scheme of Teaching and Examinations to accommodate research internships/ industry internships/ Rural Internship after the VI semester.
*Credits earned for the courses of VII and VIII Semester Schemes of Teaching and Examinations shall be counted against the corresponding semesters whether VII
or VIII semesters is completed during the beginning of the IV year or the later part of IV years of the program.
Note: Courses similar to earlier or later Semester Courses should not be offered

B. E in Computer Science and Engineering (Cyber Security): Autonomous Scheme and Syllabus
SCHEME - B - VI SEMESTER (for the candidates who seek a two - semester internship with project work/Start - up)

SL. NO.			COURSE TITLE	TD/PSB	TEACHING HOURS PER WEEK			Term work(TW)+ Self learning(SL) per semester	EXAMINATION				CREDITS
	COURSE	COURSE CODE			THEORY LECTURE(L)	TUTORIAL (T)	PRACTICAL (P)		DURATION IN HOURS	CIE MARKS	SEE MARKS	TOTAL MARKS	
1	IPCC	BCY601	VULNERABILITY ASSESSMENT AND PENETRATION TESTING	CSE - CY	3	0	2	45	3	50	50	100	4
2	PCC	BCY602	CRYPTOGRAPHY AND NETWORK SECURITY	CSE - CY	3	2	0	45	3	50	50	100	4
3	PEC	BCY613X	PROFESSIONAL ELECTIVE (BUCKET LIST F)	CSE - CY	3	0	0	45	3	50	50	100	3
4	OEC	BXX654X	OPEN ELECTIVE (BUCKET LIST G)	CSE & ALLIED	3	0	0	45	3	50	50	100	3
5	PCCL	BCYL606	DIGITAL FORENSICS LAB	CSE - CY	0	0	2	0	3	50	50	100	1
6	AEC/SEC	BCYT/L65X	PROVIDE BUCKET LIST H	CSE - CY	IF COURSE IS THEORY				2	50	50	100	1
					1	0	0	15					
					IF COURSE IS PRACTICAL				3				
					0	0	2	0					
7	MC	BNSK658	National Service Scheme (NSS)	ANY	0	0	2	0	2	100		100	0
		BPEK658	Physical Education (PE)										
		BYOK658	Yoga										
8	IKS	BIKS609	Indian Knowledge System	ANY	1	0	0		1				
									TOTAL	400	300	700	16

BUCKET LIST F			
Professional Elective BCY612X			
BCY613A	BIG DATA ANALYTICS WITH SPARK	BCY613C	BLOCK CHAIN TECHNOLOGY
BCY613B	DEEP LEARNING TECHNIQUES	BCY613D	SURVEILLANCE AND VIDEO ANALYTICS
BUCKET LIST G			
Open Elective BXX654X			
BCS654A	INTRODUCTION TO DATA STRUCTURES	BCI654C	INTRODUCTION TO DBMS
BCY654B	FUNDAMENTALS OF OPERATING SYSTEMS	BCD654D	FOUNDATIONS OF DATA SCIENCE

BUCKET LIST H			
AEC/SEC BCYT/L657X			
BCYL657A	INDUSTRIAL CYBER SECURITY	BCYL657C	GENERATIVE AI
BCYL657B	REACT	BCYL657D	DATA VISUALIZATION WITH PYTHON

Note: Courses similar to earlier or later Semester Courses should not be offered

B. E in Computer Science and Engineering (Cyber Security): Autonomous Scheme and Syllabus
SCHEME - B - VII and VIII SEMESTERS (for the candidates who seek an internship with project work)

SL NO	COURSE	COURSE CODE	COURSE TITLE	TD/PSBs	TEACHING HOURS PER WEEK			Term work (TW)+ Self learning (SL) per semester	EXAMINATION				CREDITS
					THEORY LECTURE (L)	TUTORIAL (T)	PRACTICAL (P)		DURATION IN HOURS	CIE MARKS	SEE MARKS	TOTAL MARKS	
1	IPCC	BCY701	CLOUD COMPUTING AND SECURITY	CSE - CY	3	0	2	45	3	50	50	100	4
2	IPCC	BCY702	ETHICAL HACKING	CSE - CY	3	0	2	45	3	50	50	100	4
3	PCC	BCY703	MALWARE ANALYSIS	CSE - CY	3	2	0	45	3	50	50	100	4
4	PEC	BCY714X	PROFESSIONAL ELECTIVE COURSE (MOOC COURSES)	ONLINE	3	0	0		3	50	50	100	3
5	OEC	BXX755X	OPEN ELECTIVE COURSES (MOOC COURSES)	ONLINE	3	0	0		1	50	50	100	3
1	PEC	BCY811X	PROFESSIONAL ELECTIVE (BUCKET LIST J) (ONLINE)	ONLINE	3	0	0		3	50	50	100	3
2	OEC	BCY852X	OPEN ELECTIVE (BUCKET LIST K) (ONLINE)	ONLINE	3	0	0		3	50	50	100	3
3	PROJ	BCY883	PROJECT-OUTCOME OF TRAINING	CSE - CY	0	0	12		3	100	100	200	9
4	INT	BCY804	INTERNSHIP (INDUSTRY/RESEARCH) (02 SEMESTERS)	CSE - CY	0	0	12		3	100	100	200	10
TOTAL										200	200	400	42

Professional Elective BCY801X	
BCY714X	BOS WILL PUBLISH COURSES BASED ON THE AVAILABILITY
Open Elective BXX802X	
BXX755X	BOS WILL PUBLISH COURSES BASED ON THE AVAILABILITY
Professional Elective BXX801X	
BCY811X	BOS WILL PUBLISH COURSES BASED ON THE AVAILABILITY
Open Elective BXX802X	
BCY852X	BOS WILL PUBLISH COURSES BASED ON THE AVAILABILITY

B.E. in CSE (Cyber Security)

Autonomous Syllabus

V – VIII Semester



RN Shetty Trust ®

RNS INSTITUTE OF
TECHNOLOGY

An Autonomous Institution, Affiliated to VTU,
Accredited with NAAC A+ Grade

Department of CSE (Cyber Security)

Autonomous Scheme (Effective from Academic Year
2024 – 25)



V SEMESTER SUBJECTS

ESTD : 2001

An Institute with a Difference

B.E. (CSE and Allied Branches) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – V			
Course Title:	SOFTWARE ENGINEERING AND PROJECT MANAGEMENT		
Course Code:	BCS501	CIE MARKS	50
(L :T : P) + SL	(3:2:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	4	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Understand the Fundamentals of Software Engineering, Principles of Software Engineering, Software Processes, and Process Models Used in Software Development. 2. Perform Requirements Engineering Activities and Develop Appropriate Software Requirement Models for Software Systems. 3. Apply Agile Development Practices, Scrum, Principles that Guide Practice, Mobility and Agile Change Management Techniques for Effective Software Development. 4. Plan and Manage Software Projects by Applying Project Management, Cost-Benefit Analysis, Risk Evaluation, and Stakeholder Management Techniques. 5. Assess Software Quality and Estimate Software Cost and Effort Using Software Quality Models, Testing Techniques, Reliability Concepts, Function Point Analysis and COCOMO.			
Module-1			9 Hours
Software and Software Engineering: The Nature of Software, Defining the Discipline, The Software Process, Software Engineering Practice. Process Models: A generic process model, Defining a Framework Activity, Identifying a Task Set, Prescriptive Process Models, Product and Process. Textbook 1: Chapter-1 (1.1 - 1.4), Chapter-2 (2.1 - 2.3, 2.5 - 2.6)			
Module-2			9 Hours
Understanding Requirements: Requirements Engineering, Establishing the Groundwork, Requirements Gathering, Developing Use Cases, Building Analysis Model, Negotiating Requirements, Requirements Monitoring, Validating Requirements. Requirements Modelling - A Recommended Approach: Requirement Analysis, Scenario-Based Modelling, Class-Based Modelling, Functional Modelling, Behavioural Modelling. Textbook 1: Chapter-7 (7.1 - 7.8), Chapter-8 (8.1 - 8.5)			
Module-3			9 Hours
Agility and Process: What is Agility? Agility and the Cost of Change. What is an Agile Process? Scrum, Other Agile Framework. Principles that Guide Practice: Core Principles, Principles That Guide Each Framework Activity. Software Configuration Management: Mobility and Agile Change Management. Textbook 1: Chapter-3 (3.1 - 3.5), Chapter-6 (6.1 - 6.2), Chapter-22 (22.6)			

Module-4	9 Hours
Introduction to Software Project Management: Introduction, Why is Software Project Management Important? What is a Project? Software Project versus Other Types of Project, Contract Management and Technical Project Management, Activities Covered by Software Project Management, Plans, Methods and Methodologies, Some Ways of Categorizing Software Projects, Stakeholders, Setting Objectives, The Business Case, Project Success and Failure, What is Management? Management Control, Traditional versus Modern Project Management Practices. Project Evaluation and Programme Management: Evaluation of Individual Projects, Cost-Benefit Evaluation Techniques, Risk Evaluation. Textbook 2: Chapter-1 (1.1 - 1.15), Chapter-2 (2.4 - 2.6)	
Module-5	9 Hours
Software Quality: Introduction, The Place of Software Quality in Project Planning, The Importance of Software Quality, Defining Software Quality, Product Versus Process Quality Management, Process Capability Models, Techniques to Help Enhance Software Quality, Testing, Software Reliability, Quality Plans. Software Effort Estimation: Software Effort Estimation Techniques, Bottom-up Estimating, The Top-down Approach and Parametric Models, Expert Judgement, Albrecht Function Point Analysis, COSMIC Full Function Points, COCOMO II: Parametric Productivity Model, Cost Estimation, Staffing Pattern. Textbook 2: Chapter-13 (13.1 - 13.4, 13.7, 13.9 - 13.13), Chapter-5 (5.5 - 5.8, 5.10, 5.12 - 5.15)	

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Describe the Fundamental Concepts of Software Engineering, Software Processes, Process Models, and Software Engineering Practices Used in Software Development.
CO2	Summarize Software Requirements and model them Using Requirements Engineering Techniques, Use Cases and Analysis Models.
CO3	Apply Agile Software Development Methodologies, Software Engineering Principles, and Software Configuration Management Practices for Mobility, Effective Software Development and Change Management.
CO4	Analyze Software Project Management Concepts by Applying Project Management Principles, Risk Analysis, Cost-Benefit Evaluation, and Stakeholder Management Techniques.
CO5	Assess Software Quality and Estimate Software Development Effort Using Software Quality Models, Testing Strategies, Reliability Measures, Function Point Analysis, COSMIC Function Points, and COCOMO II Estimation Models.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Continuous and Comprehensive Evaluation (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks.
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Marks shall be the sum of marks scored in Components A, B and C.
The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE.			

Textbooks:

1. Roger S. Pressman & Bruce R. Maxim, Software Engineering: A Practitioner's Approach, 9th Edition, McGraw Hill 2023 July.
2. Bob Hughes, Mike Cotterell, Rajib Mall, Software Project Management, 5th Edition 2009.

Reference Books:

1. Pankaj Jalote: An Integrated Approach to Software Engineering, Wiley India.
2. Hans van Vliet, Software Engineering: Principles and Practice, 3rd Edition, Wiley India 2008.

Web links:

1. <https://www.geeksforgeeks.org/software-engineering/software-engineering/>
2. <https://www.geeksforgeeks.org/business-studies/project-management/>
3. <https://www.geeksforgeeks.org/software-engineering/scrum-software-development/>
4. <https://confluence.atlassian.com/jira>
5. <https://shorturl.at/Cfjxd>

Self – Study topics:

1. **DevOps:** Learn about continuous integration/continuous delivery (CI/CD) pipelines, containerization (Docker), and infrastructure as code.
2. **Agile Methodologies:** Study agile frameworks like Scrum and Kanban for iterative and collaborative software development.



ESTD : 2001

An Institute with a Difference

B.E. (Computer Science and Engineering (Cyber Security))
Outcome Based Education (OBE) and Choice Based Credit System (CBCS)
SEMESTER – V

Course Title:	COMPUTER NETWORKS AND SECURITY		
Course Code:	BCY502	CIE MARKS	50
(L :T : P) + SL	(3:0:2) + (45 Hours/Sem)	SEE MARKS	50
Credits:	4	EXAM HOURS	3

COURSE LEARNING OBJECTIVES:

The purpose of the course is to facilitate the learner to:

1. Demonstration of application layer protocols.
2. Discuss transport layer services and understand UDP and TCP protocols.
3. Learn routers, IP and Routing Algorithms in network layer.
4. Disseminate the Wireless and Mobile Networks covering IEEE 802.11 Standard.
5. Illustrate concepts of Multimedia Networking, Security and Network Management.

Module-1

9 Hours

Application Layer: Principles of Network Applications: Network Application Architectures, Processes Communicating, Transport Services Available to Applications, Transport Services Provided by the Internet, Application-Layer Protocols. The Web and HTTP: Overview of HTTP, Non-persistent and Persistent Connections, HTTP Message Format, User-Server Interaction: Cookies, Web Caching, The Conditional GET, File Transfer: FTP Commands & Replies, Electronic Mail in the Internet: SMTP, Comparison with HTTP, Mail Message Format, Mail Access Protocols. Socket Programming: creating Network Applications: Socket Programming with UDP, Socket Programming with TCP.

Textbook 1: Chapter-2 (2.1-2.4, 2.7)

Module-2

9 Hours

Transport Layer : Introduction and Transport-Layer Services: Relationship Between Transport and Network Layers, Overview of the Transport Layer in the Internet, Multiplexing and Demultiplexing: Connectionless Transport: UDP, UDP Segment Structure, UDP Checksum, Principles of Reliable Data Transfer: Building a Reliable Data Transfer Protocol, Pipelined Reliable Data Transfer Protocols, Go-Back-N, Selective repeat, Connection-Oriented Transport TCP: The TCP Connection, TCP Segment Structure, Round Trip Time Estimation and Timeout, Reliable Data Transfer, Flow Control, TCP Connection Management, Principles of Congestion Control: The Causes and the Costs of Congestion, Approaches to Congestion Control, Network-assisted congestion-control example, ATM ABR Congestion control, TCP Congestion Control: Fairness.

Textbook 1: Chapter- 3 (3.1- 3.7)

Module-3	9 Hours
The Network layer: What's Inside a Router? Input Processing, Switching, Output Processing, Where Does Queuing Occur? Routing control plane, IPv6, A Brief foray into IP Security, Routing Algorithms: The Link-State (LS) Routing Algorithm, The Distance-Vector (DV) Routing Algorithm, Hierarchical Routing, Routing in the Internet, Intra-AS Routing in the Internet: RIP, Intra-AS Routing in the Internet: OSPF, Inter/AS Routing: BGP, Broadcast Routing Algorithms and Multicast. Textbook 1: Chapter-4 (4.3-4.7)	
Module-4	9 Hours
Network Security: Overview of Network Security: Elements of Network Security , Classification of Network Attacks ,Security Methods ,Symmetric-Key Cryptography :Data Encryption Standard (DES),Advanced Encryption Standard (AES) , Public-Key Cryptography :RSA Algorithm ,Diffie-Hellman Key-Exchange Protocol , Authentication :Hash Function , Secure Hash Algorithm (SHA) , Digital Signatures , Firewalls and Packet Filtering ,Packet Filtering , Proxy Server . Textbook 2: Chapter-10 (10.1-10.6, 10.8)	
Module-5	9 Hours
Multimedia Networking: Properties of video, properties of Audio, Types of multimedia Network Applications, Streaming stored video: UDP Streaming, HTTP Streaming, Adaptive streaming and DASH, content distribution Networks Voice-over-IP :Limitations of the Best-Effort IP Service ,Removing Jitter at the Receiver for Audio ,Recovering from Packet Loss Protocols for Real-Time Conversational Applications , RTP , SIP. Textbook 1: Chapter-7 (7.1 - 7.4)	

PRACTICAL COMPONENT OF IPCC

PART A
Program 1: Error Detection in Data Link Layer using CRC-CCITT
Scenario: A logistics company uses a computer network to transmit shipment information between its regional warehouses and the central server. During transmission, data packets may be corrupted due to noise and interference on the communication channel. To ensure data integrity, the company decides to implement the CRC-CCITT (16-bit) error detection technique before accepting any received packet.
Program 2: Sliding Window Protocol for Reliable Data Transmission
Scenario: A multimedia streaming company provides live online lectures to thousands of students across different locations. To ensure smooth and reliable delivery of video data, the company uses a Sliding Window Protocol at the Data Link Layer. This protocol allows multiple frames to be sent before receiving acknowledgments, thereby improving channel utilization and transmission efficiency.

Program 3: Detecting Negative-Weight Cycles in a Regional Routing Network

Scenario:

A telecommunications company is designing a routing system for a regional network consisting of multiple routers connected through communication links. Each link between routers has an associated cost representing factors such as delay, bandwidth usage, or transmission expense. Due to changing network conditions, some links may have negative costs (representing incentives or optimized routes), but the network should be checked for routing loops caused by negative-weight cycles.

Program 4: TCP/IP Client-Server File Retrieval System

Scenario:

A university maintains a centralized document server that stores laboratory manuals, assignment files and course materials. Students access these resources through a client application running on their computers. When a student needs a specific file, the client sends the file name to the server over a TCP/IP network connection. The server checks whether the requested file exists in its repository. If the file is found, the server sends the contents of the file back to the client. Otherwise, it sends an appropriate error message indicating that the file is unavailable.

Program 5: Socket-Based client-server communication using UDP

Scenario:

A regional weather monitoring center broadcasts important weather alerts to remote observation stations located across different districts. Since the alerts are short text messages and need to be delivered quickly, the system uses a connectionless communication model based on UDP datagram sockets. An operator at the central server types weather updates and the connected monitoring stations receive and display the messages immediately.

Program 6: Leaky Bucket Algorithm for Network Traffic Congestion Control

Scenario:

A multimedia streaming company provides live online lectures to thousands of students simultaneously. During peak hours, the server receives bursts of data packets generated by video streams, user interactions and real-time notifications. If these packets are transmitted directly onto the network without regulation, congestion may occur, resulting in packet loss, increased delays and poor Quality of Service (QoS). To ensure smooth network operation, the company decides to implement a Leaky Bucket Algorithm, where incoming packets are temporarily stored in a finite-capacity bucket (buffer) and transmitted at a constant rate. Any packets arriving when the bucket is full are discarded.

PART B

Program 7: Network Configuration Testing and Routing Algorithms in Packet Tracer

Scenario:

Test and verify Network configurations using Packet Tracer and explore static and dynamic routing algorithms.

Program 8: DHCP Service Configuration in a Simulated Network Topology

Scenario:

Design a simple network topology and configure DHCP services using Cisco Packet Tracer.

Program 9: LAN Simulation and FTP Server Configuration

Scenario:

Design and simulate a Local Area Network (LAN) using Cisco Packet Tracer and configure an FTP server to allow file transfer between the server and client systems.

Program 10: TCP/UDP Packet Sniffing Using Wireshark

Scenario:

A network administrator is troubleshooting communication issues between a client and a server. To analyze the network traffic, the administrator uses Wireshark to capture both TCP and UDP packets. Capture the packets, apply appropriate filters to view TCP and UDP traffic, identify the source and destination IP addresses and port numbers and compare the communication characteristics of both protocols.

OPEN ENDED EXPERIMENTS

Program 11: HTTP Packet Sniffing Using Wireshark

Scenario:

A web administrator wants to analyze the communication between a web browser and a web server to understand how HTTP requests and responses are exchanged. Using Wireshark, capture HTTP packets, apply an HTTP display filter, identify the request and response messages, source and destination IP addresses, port numbers and analyse the HTTP communication.

Program 12: NAT Configuration for Private-to-Public IP Translation

Scenario:

Design and simulate a network using Cisco Packet Tracer and configure NAT services on a router to translate private IP addresses into public IP addresses

Program 13: Inter-VLAN Routing Configuration

Scenario:

Configure Inter VLAN network using Packet Tracer.

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Describe the principles of application layer protocols.
CO2	Recognize transport layer services and infer UDP and TCP protocols.
CO3	Classify routers, IP and Routing Algorithms in network layer.
CO4	Illustrate the Wireless and Mobile Networks covering IEEE 802.11 Standard.
CO5	Apply Multimedia Networking and Network Management concepts.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE- IA Tests (A)	20	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 20 marks.
Continuous and Comprehensive Evaluation (B)	10	-	Any one Assessment methods as per 24RNBE4.2 scaled to 10 marks.
Total CIE Theory (A+B)	30	12	Marks of Tests and Assignments awarded for a maximum of 30.
CIE Practical	12	-	Marks awarded for Weekly Conduction of Experiments and Submission of Laboratory records, scaled to 12 marks.
CIE Practical Test	8	-	Average of marks of Two tests, each conducted for 100 marks covering all experiments, scaled to 8.
Total CIE Practical (C)	20	8	Marks of Experiments, Record and Test awarded for a maximum of 20 marks.
CIE: Theory + Practical (A + B + C)	50	20	CIE Evaluation is done for a maximum of 50 marks.
SEE (D)	50	18	SEE is a theory exam, conducted for 100 marks and scaled down to 50 marks. Exam duration shall be 3 hours.
CIE+SEE (A+B+C+D)	100	40	Final marks shall be the sum of marks scored in Components A, B, C and D
The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE. The laboratory component of the IPCC shall be for CIE only. However, in SEE, the questions from the laboratory component shall be included in their respective modules only.			

Text Books:

1. James F Kurose and Keith W Ross, Computer Networking, A Top-Down Approach, Sixth edition, Pearson, 2017 .

2. Nader F Mir, Computer and Communication Networks, 2nd Edition, Pearson, 2014.

Reference Books :

1. Behrouz A Forouzan, Data and Communications and Networking, Fifth Edition, McGraw Hill, Indian Edition.
2. Larry L Peterson and Bruce S Davie, Computer Networks, fifth edition, ELSEVIER.
3. Andrew S Tanenbaum, Computer Networks, fifth edition, Pearson.
4. Mayank Dave, Computer Networks, Second edition, Cengage Learning.

WebLinks:

1. <https://www.digimat.in/nptel/courses/video/106105183/L01.html>
2. <http://www.digimat.in/nptel/courses/video/106105081/L25.html>
3. <https://nptel.ac.in/courses/10610>
4. https://onlinecourses.nptel.ac.in/noc25_cs125/preview
5. <https://www.coursera.org/learn/introduction-to-networking-nvidia>

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning:

1. Certifications (Skill based): industry recognized certifications (NPTEL, CISCO, Infosys Springboard).
2. Quiz/Assignments.
3. Group Activities/Peer Learning.

Self – Study topics:

1. Analyze various error detection and correction techniques.
2. Compare Distance Vector and Link State approaches, including Bellman-Ford and OSPF, with respect to convergence, scalability, and routing efficiency.
3. Performance characteristics of TCP and UDP protocols and examine their suitability for different network applications such as real-time streaming and reliable data transfer.

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – V			
Course Title:	ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING		
Course Code:	BCY503	CIE MARKS	50
(L :T : P) + SL	(3:0:2) + (45 Hours/Sem)	SEE MARKS	50
Credits:	4	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Understands the basics of AI, history of AI and its foundations, basic principles of AI for problem solving. 2. Explore the basics of Machine Learning & Machine Learning process, understanding data. 3. Understand the Working of Artificial Neural Networks.			
Module-1			9 Hours
Introduction: What is AI, The foundation of Artificial Intelligence. Intelligent Agents: Agents and Environments, Good Behaviour: The concept of rationality, the nature of Environments, the structure of Agents. Problem solving by searching: Problem solving agents, Example problems, Searching for solutions. Textbook 1: Chapter-1(1.1-1.2), Chapter-2(2.1-2.4), Chapter-3(3.1-3.3)			
Module-2			9 Hours
Problem solving by searching: Uniformed search strategies, Informed search strategies, Heuristic functions. Beyond Classical Search: Local search algorithms and optimization problems, Local search in continuous spaces Textbook 1: Chapter-3(3.4-3.6), Chapter-4 (4.1-4.2)			
Module-3			9 Hours
Introduction to machine learning: Machine Learning Explained, Types of Machine Learning. Challenges of Machine Learning, Machine Learning Process. Understanding Data: What is data, Big data analytics and types of analytics, Big data analytics framework, Descriptive statistics, univariate data analysis and Visualization, Bivariate Data and Multivariate data, Multivariate Statistics, Feature engineering and dimensionality reduction techniques. Textbook 2: Chapter-1 (1.2, 1.4-1.6), Chapter- 2 (2.1 to 2.7, 2.10)			

Module-4	9 Hours
Basics of Learning Theory: Design of learning system, Introduction concept learning, Modelling in Machine Learning. Similarity-based learning: Nearest neighbour learning, weighted k- Nearest - Neighbour algorithm. Regression Analysis: Introduction to Regression. Regression, Introduction to Linear Regression, Multiple Linear Regression, Polynomial Regression, Logistic Textbook 2: Chapter-3 (3.3, 3.4, 3.6), Chapter-4 (4.2-4.3), Chapter-5 (5.1-5.3, 5.5-5.7)	
Module-5	9 Hours
Bayesian Learning: Introduction to Probability-based Learning, Fundamentals of Bayes Theorem, Classification Using Bayes Model, Naïve Bayes Algorithm for Continuous Attributes, Other popular types of Naïve Bayes classifiers. Artificial Neural Network: Introduction, Biological neurons, Artificial neurons, Perceptron and learning theory, types of Artificial neural Network, popular applications of Artificial Neural Networks, Advantages and Disadvantages of ANN, Challenges of ANN. Textbook 2: Chapter-8, Chapter-10 (10.1-10.5, 10.9-10.11)	

PRACTICAL COMPONENT OF IPCC

SL. No.	EXPERIMENTS
1	Implement and Demonstrate Depth First Search Algorithm on Water Jug Problem.
2	Implement and Demonstrate Best First Search Algorithm on Missionaries-Cannibals Problems.
3	Develop a program to create histograms for all numerical features and analyze the distribution of each feature. Generate box plots for all numerical features and identify any outliers. Use California Housing dataset.
4	Develop a program to Compute the correlation matrix to understand the relationships between pairs of features. Visualize the correlation matrix using a heatmap to know which variables have strong positive/negative correlations. Create a pair plot to visualize pairwise relationships between features. Use California Housing dataset.
5	Develop a program to implement Principal Component Analysis (PCA) for reducing the dimensionality of the Iris dataset from 4 features to 2.
6	For a given set of training data examples stored in a .CSV file, implement and demonstrate the Find-S algorithm to output a description of the set of all hypotheses consistent with the training examples.

7	Develop a program to implement k-Nearest Neighbour algorithm to classify the randomly generated 100 values of x in the range of [0,1]. Perform the following based on dataset generated. 1. Label the first 50 points $\{x_1, \dots, x_{50}\}$ as follows: if $(x_i \leq 0.5)$, then $x_i \in \text{Class1}$, else $x_i \in \text{Class2}$ 2. Classify the remaining points, $x_{51}, \dots, x_{100}$ using KNN. Perform this for $k=1,2,3,4,5,20,30$.
8	Implement the non-parametric Locally Weighted Regression algorithm to fit the data points. Select appropriate data set for your experiment and draw graphs.
9	Develop a program to demonstrate the working of Linear Regression and Polynomial Regression. Use Boston Housing Dataset for Linear Regression and Auto MPG Dataset (for vehicle fuel efficiency prediction) for Polynomial Regression.
10	Develop a program to demonstrate the working of the decision tree algorithm. Use Breast Cancer Data set for building the decision tree and apply this knowledge to classify a new sample.

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Apply the basics of Artificial Intelligence for suitable search strategy to solve problems.
CO2	Use machine learning and mathematical methods to engineer features and reduce dimensions for better model performance
CO3	Develop similarity-based learning models and regression models for solving classification
CO4	Build probabilistic learning models and design neural network models using perceptrons

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE- IA Tests (A)	20	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 20 marks.
Continuous and Comprehensive Evaluation (B)	10	-	Any one Assessment methods as per 24RNBE4.2 scaled to 10 marks.

Total CIE Theory (A+B)	30	12	Marks of Tests and Assignments awarded for a maximum of 30.
CIE Practical	12	-	Marks awarded for Weekly Conduction of Experiments and Submission of Laboratory records, scaled to 12 marks.
CIE Practical Test	8	-	Average of marks of Two tests, each conducted for 100 marks covering all experiments, scaled to 8.
Total CIE Practical (C)	20	8	Marks of Experiments, Record and Test awarded for a maximum of 20 marks.
CIE: Theory + Practical (A + B + C)	50	20	CIE Evaluation is done for a maximum of 50 marks.
SEE (D)	50	18	SEE is a theory exam, conducted for 100 marks and scaled down to 50 marks. Exam duration shall before 3 hours.
CIE+SEE (A+B+C+D)	100	40	Final marks shall be the sum of marks scored in Components A, B, C and D.
The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE. The laboratory component of the IPCC shall be for CIE only. However, in SEE, the questions from the laboratory component shall be included in their respective modules only.			

Text Books :

1. Stuart Russel, Peter Norvig: “Artificial Intelligence A Modern Approach”, 3rd Edition, Pearson Education, 2015.
2. S.Sridhar, MVijayalakshmi “Machine Learning”. Oxford University Press, 2021.

Reference Books :

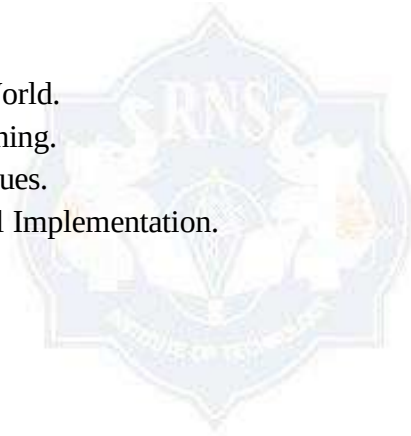
1. Elaine Rich, Kevin Knight: “Artificial Intelligence”, 3rd Edition, Tata McGraw Hill, 2009, ISBN-10: 0070087709.
2. Nils J. Nilsson: “Principles of Artificial Intelligence”, Elsevier, 1980, ISBN: 978-3-540 11340-9
3. Murty, M. N., and V. S. Ananthanarayana. Machine Learning: Theory and Practice, Universities Press, 2024.

WebLinks:

1. [Problem solving agent: https://www.youtube.com/watch?v=KTPmo-KsOis](https://www.youtube.com/watch?v=KTPmo-KsOis)
2. https://www.youtube.com/watch?v=X_Qt0U66aH0&list=PLwdnzlV3ogoXaceHrrFVZCJkbm_laSH_cH
3. <https://www.javatpoint.com/history-of-artificial-intelligence>
4. <https://www.tutorialandexample.com/problem-solving-in-artificial-intelligence>
5. <https://techvidvan.com/tutorials/ai-heuristic-search/>
6. <https://www.analyticsvidhya.com/machine-learning/>
7. <https://www.hackerearth.com/practice/machine-learning/machine-learning-algorithms/mldecision-tree/tutorial/>
8. <https://www.javatpoint.com/unsupervised-artificial-neural-networks>

Self – Study topics:

1. Ethical & Responsible AI.
2. AI Applications in Real World.
3. Introduction to Deep Learning.
4. Model Evaluation Techniques.
5. AI/ML Tools and Practical Implementation.



ESTD : 2001

An Institute with a Difference

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – V			
Course Title:	ADVANCED CYBER SECURITY LABORATORY		
Course Code:	BCYL504	CIE MARKS	50
L : T : P	0:0:2	SEE MARKS	50
Credits:	01	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. To learn core concepts and techniques of network, web, and application penetration testing. 2. To identify and exploit common vulnerabilities such as XSS, SQLi, Command Injection, File Upload, Session Attacks, and XXE. 3. To use industry-standard tools (Nmap, Wireshark, Burp Suite, Hashcat, etc.) for reconnaissance and exploitation. 4. To understand securities risks and apply mitigation through secure coding and defensive practices.			
SL No.	Experiments		
1	Network Scanning using Nmap / Zenmap Objective: To learn network discovery, port scanning, service detection, OS fingerprinting, and identifying open attack surfaces. Tools: Nmap, Zenmap (GUI).		
2	Packet Capture & Traffic Analysis using Wireshark Objective: To capture and analyze network traffic, understand network protocols and detect suspicious packets. Tools: Wireshark.		
3	Password Cracking Objective: To understand password vulnerabilities and the importance of strong passwords Tools: Hashcat, John the Ripper.		
4	Cross-Site Scripting (XSS) Objective: To identify and exploit XSS vulnerabilities and understand corresponding mitigation techniques. Tools: DVWA.		
5	File Upload Vulnerability Objective: To understand the risks associated with insecure file uploads and how attackers bypass validation to upload malicious files. Tools: DVWA, Burp Suite, vulnerable web application.		
6	Command Injection Objective: To learn how command injection attacks work and understand input validation and secure coding practices.		

	Tools: DVWA, Burp Suite, custom vulnerable web application.
7	Man-in-the-Middle(MITM) Attack Objective: To understand how MITM attacks works and how attackers intercept or manipulate traffic. Tools: Ettercap, Wireshark.
8	Session Hijacking and Fixation Objective: To learn how session hijacking and fixation attacks work. Tools: DVWA, Burp Suite, Browser developer tools.
9	SQL Injection using BurpSuite Objective: To identify and exploit SQL injection vulnerabilities using Burp Suite (Proxy, Repeater, and Intruder). Tools: BurpSuite, DVWA.
10	XML External Entity (XXE) Injection Objective: To learn about XXE vulnerabilities and how to exploit them. Tools: Burp Suite, Vulnerable XML-based application.

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Demonstrate the use of fundamental network scanning and traffic analysis techniques to assess system exposure.
CO2	Identify and exploit common web and system vulnerabilities.
CO3	Perform password attacks and injection-based exploitation.
CO4	Recommend mitigation techniques and secure coding practices to prevent cyber threats.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE Practical (A)	30	-	Marks awarded for Weekly Conduction of Experiments and Submission of Laboratory records, scaled to 30 marks.
CIE Practical Test (B)	20	-	Average of marks of Two tests, each conducted for 100 marks covering all experiments, scaled to 20.

Total CIE Practical (A+B)	50	20	Sum of Marks of Experiments, Record and Test shall be CIE marks awarded for a maximum of 50.
SEE (C)	50	20	SEE is a lab exam, conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE.			

Self – Study topics:

1. Core Textbooks (Highly Recommended)

- The Web Application Hacker's Handbook** – Dafydd Stuttard & Marcus Pinto.
⇒ <https://portswigger.net/wahh>
- Practical Web Penetration Testing** – Gus Khawaja (Packt).
⇒ <https://www.packtpub.com/en-us/product/practical-web-penetration-testing-9781788628723>
- OWASP Web Security Testing Guide.**
⇒ <https://owasp.org/www-project-web-security-testing-guide/latest/>

2. Official Tool Documentation

- Burp Suite Documentation (Official)**
⇒ <https://portswigger.net/burp/documentation>

3. High-Quality Tutorials & Training

- PortSwigger Web Security Academy**
⇒ <https://portswigger.net/web-security>
- OWASP Cheat Sheets**
⇒ <https://cheatsheetseries.owasp.org/>
- freeCodeCamp – Password Cracking with John the Ripper**
⇒ <https://www.freecodecamp.org/news/crack-passwords-using-john-the-ripper-pentesting-tutorial/>

4. Trusted YouTube Education Channels

- HackerSploit**
⇒ <https://www.youtube.com/@HackerSploit>
- David Bombal**
⇒ <https://www.youtube.com/@davidbombal>

- **CryptoCat**

⇒ https://www.youtube.com/@_CryptoCat

5. Reliable Academic Reference

- **NIST Cybersecurity Framework (CSF)**

⇒ <https://www.nist.gov/cyberframework>



ESTD : 2001

An Institute with a Difference

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – V			
Course Title:	THEORY OF COMPUTATION		
Course Code:	BCY515A	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	03	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Introduce core concepts in Automata and Theory of Computation. 2. Identify different Formal Language Classes and their Relationships. 3. Learn concepts of Grammars and Recognizers for different formal languages. 4. Prove or disprove theorems in automata theory using their properties. 5. Determine the decidability and intractability of Computational problems.			
Module-1			9 Hours
Introduction to Finite Automata, Structural Representations, Automata and Complexity. The Central Concepts of Automata Theory. Deterministic Finite Automata, Nondeterministic Finite Automata, An Application: Text Search, Finite Automata with Epsilon-Transitions. Textbook: Chapter-1(1.1- 1.5), Chapter-2(2.2-2.5)			
Module-2			9 Hours
Regular Expressions, Finite Automata and Regular Expressions, Proving Languages not to be Regular. Closure Properties of Regular Languages, Equivalence and Minimization of Automata, Applications of Regular Expressions. Textbook: Chapter- 3(3.1, 3.2, 3.3), Chapter- 4(4.1, 4.2, 4.4)			
Module-3			9 Hours
Context-Free Grammars, Parse Trees, Ambiguity in Grammars and Languages, Ambiguity in Grammars and Languages, Definition of the Pushdown Automaton, The Languages of a PDA, Equivalence of PDA's and CFG's, Deterministic Pushdown Automata. Textbook: Chapter- 5(5.1, 5.2, 5.4), Chapter -6(6.1,6.2,6.3.1,6.4)			
Module-4			9 Hours
Normal Forms for Context-Free Grammars, The Pumping Lemma for Context-Free Languages, Closure Properties of Context-Free Languages. Textbook: Chapter-7(7.1, 7.2, 7.3)			

Module-5	9 Hours
Introduction to Turing Machines: Problems That Computers Cannot Solve, The Turing Machine, Programming Techniques for Turing Machines, Extensions to the Basic Turing Machine, Undecidability: A Language That Is Not Recursively Enumerable.	
Textbook: Chapter-8(8.1,8.2, 8.3,8.4), Chapter -9(9.1, 9.2)	

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Apply the fundamental concepts of automata theory to construct DFA, NFA, and ϵ -NFA, and perform conversions between these models.
CO2	Analyze the properties of regular languages using regular expressions and formal reasoning techniques.
CO3	Design context-free grammars (CFGs) and develop corresponding pushdown automata (PDAs) for given formal languages.
CO4	Construct and evaluate Turing machines to solve computational problems and assess their correctness.
CO5	Differentiate between decidable and undecidable problems with appropriate theoretical justification.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Alternate Assessment (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.

CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
The minimum marks to be secured in CIE are 20 out of allotted 50 marks to appear for SEE, with minimum 40 % scored in every component of CIE.			

Text Books:

1. John E Hopcroft, Rajeev Motwani, Jeffrey D. Ullman,” Introduction to Automata Theory, Languages and Computation”, Second Edition, Pearson.

Reference Books:

1. Elain Rich, “Automata, Computability and complexity”, 1st Edition, Pearson Education, 2018.
2. K.L.P Mishra, N Chandrashekar, 3rd Edition, ‘Theory of Computer Science’, PHI, 2012.
3. Peter Linz, “An introduction to Formal Languages and Automata “, 3rd Edition, Narosa Publishers, 1998.
4. Michael Sipser : Introduction to the Theory of Computation, 3rd edition, Cengage learning, 2013.
5. John C Martin, Introduction to Languages and The Theory of Computation, 3rd Edition, Tata McGraw –Hill Publishing Company Limited, 2013.

Weblinks:

1. <https://nptel.ac.in/courses/106/106/106106049/#>
2. <https://www.jflap.org/>

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning Mini Project:

Group Activities, quizzes, Puzzles and presentations

Self – Study topics:

1. Concept Exploration.
2. Real-World Application.
3. Automata Simulation.
4. Tool-Based learning(JFLAP).
5. TOC in Compiler design

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – V			
Course Title:	DIGITAL WATERMARKING AND STEGANOGRAPHY		
Course Code:	BCY515B	CIE MARKS	50
(L :T : P) + SL	(3:0:0)+(45 Hours/Sem)	SEE MARKS	50
Credits:	03	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. To understand the basic principles, and characteristics of digital watermarking and steganography. 2. Examining multiple techniques and real-world implementations used in digital watermarking and steganography. 3. Using watermarking methods as a verification mechanism for secure online content distribution. 4. Employing steganography processes for hidden and confidential message exchange. 5. Gaining knowledge of counter-techniques such as steganalysis to inspect and evaluate data-hiding systems.			
Module-1			9 Hours
Introduction: Digital Watermarking, Digital Steganography, Differences between Watermarking and Steganography. Classification of Digital watermarking: Classification Based on Characteristics, Classification Based on Applications. Mathematical Preliminaries: Least-Significant-Bit Substitution, Discrete Fourier Transform, Discrete Cosine Transform. Textbook 1: Chapter-1(1.1-1.3), Chapter-2(2.1, 2.2), Chapter-3(3.1,3.2,3.3)			
Module-2			9 Hours
Digital Watermarking Fundamentals: Spatial Domain Watermarking., Frequency Domain Watermarking, Fragile Watermarks, Robust Watermarks. Watermarking Attacks and Tools: Image-Processing Attacks, Geometric Attacks, Cryptographic Attacks, Protocol Attack, Watermarking Tools. Textbook 1: Chapter-4(4.1- 4.4), Chapter-5(5.1-5.5)			
Module-3			9 Hours
Watermarking Based on Genetic Algorithms: Introduction to Genetic Algorithms, Concept of GA-Based Watermarking, GA-Based Rounding Error Correction Watermarking, Applications to Medical Image Watermarking, Authentication of JPEG Images Based on Genetic Algorithms Reversible Image Authentication Scheme Based on Chaotic Fragile Watermark. Textbook 1: Chapter-7(7.1-7.5)			

Module-4	9 Hours
Steganography – Introduction: Steganographic Communication, Information-Theoretic Foundations of Steganography, Minimizing the Embedding Impact, Types of Steganography, Applications of Steganography, Examples of Steganographic Software. Textbook 2: Chapter-12(12.1,12.3,12.5) Textbook 1: Chapter-11(11.1.1, 11.1.2, 11.1.4)	
Module-5	9 Hours
Steganalysis: Steganalysis Scenarios- Detection, Forensic Steganalysis, The Influence of the Cover Work on Steganalysis. IQM-Based Steganalytic System, Frequency Domain Steganalytic System, LSB Embedding and the Histogram Attack, Sample Pairs Analysis. Blind Steganalysis of JPEG Images Using Calibration, Blind Steganalysis in the Spatial Domain. Textbook 2: Chapter-13(13.1, 13.1.2, 13.1.3, 13.2.1, 13.2.2, 13.2.3 ,13.2.4) Textbook 1: Chapter-11(11.2.3, 11.2.5)	

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Acquire comprehensive knowledge of principles, characteristics and performance measures of digital watermarking systems.
CO2	Develop an understanding of watermarking techniques, classifications and associated attack models.
CO3	Gain proficiency in genetic algorithm-based and reversible watermarking approaches for authentication and integrity verification.
CO4	Build conceptual clarity on steganographic methods for secure concealment of information in digital media.
CO5	Formulate robust data hiding mechanisms capable of resisting steganalysis techniques.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.

Continuous and Comprehensive Evaluation (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
- The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE. If any courses of 3 credits are of Integrated Course type, for such courses the method suggested for 4 credits IPCC shall be followed.			

Suggested Learning Resources:

Text Books

1. Frank Y. Shih, Digital Watermarking and Steganography Fundamentals and Techniques, 2020, 2nd Edition. CRC Press, United States. (ISBN No: 9780367656430).
2. J. Cox, M. L. Miller, J. A. Bloom, T. Kalker, and J. Fridrich, Digital Watermarking and Steganography, 2008, 2nd Edition. Amsterdam: Morgan Kaufmann Publishers In, United States. (ISBN No: 978-0-12- 372585-1).

Reference Books

1. J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, 2010, 1st Edition. Cambridge: Cambridge University Press, United Kingdom. (ISBN No.: 978-0-52-119019-0).
2. P. Wayner, Disappearing Cryptography: Information hiding: Steganography and Watermarking, 2008, 3rd Edition. Amsterdam: Morgan Kaufmann Publishers In, United States. (ISBN No. : 978-0-08- 092270-6).

Web links and Video Lectures (e-Resources):

- <https://www.sciencedirect.com/topics/computer-science/digital-watermarking>
- https://link.springer.com/Chapter/10.1007/978-981-19-1412-6_39

- https://www.researchgate.net/publication/264048994_A_Survey_of_Digital_Watermarking_Techniques_and_its_Applications
- https://link.springer.com/Chapter/10.1007/978-981-10-8536-9_32
- <https://youtu.be/8MW094OkSpU?feature=shared>
- <https://youtu.be/zQ15474JACs?feature=shared>

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

- Demonstration of tools of watermarking and steganography.
- Implementation of different algorithms in watermarking and steganography.
-

Self-Study Topics

- Comparative study of visible, invisible and zero-watermarking techniques.
- Watermarking solutions for copyright protection in multimedia and social media platforms.
- Machine learning and deep learning techniques in steganography and steganalysis.
- Review of recent research publications and real-world applications in digital watermarking.

Alternate Assessment Methods

1. Certifications (Skill-Based) -industry-recognized certifications (e.g. CISCO, NPTEL, Infosys Springboard).
2. Assignments / Problem Solving Sheets.
3. Quiz.
4. Mini Projects.
5. Group Activities / Peer Evaluation.
6. Presentations / Tech Talks.

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – V			
Course Title:	HACKER TECHNIQUES, TOOLS, AND INCIDENT HANDLING		
Course Code:	BCY515C	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	03	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Understand ethical hacking, penetration testing, and the attacker mindset. 2. Applyfoot printing, scanning, enumeration, and OSINT tools for information gathering. 3. Analyze system, wireless, web, and database-level attack techniques. 4. Understand malware types, sniffing techniques, session hijacking, and DoS attacks. 5. Explain incident response processes, defensive technologies, and security best practices.			
Module-1			9 Hours
Hacking: The Next Generation: Profiles and Motives of Different Types of Hackers, History of Computer Hacking, Ethical Hacking and Penetration Testing, Common Hacking Methodologies, Performing a Penetration Test, The Role of the Law and Ethical Standards. Physical Security: Basic Equipment Controls, Physical Area Controls, Facility Controls, Personal Safety Controls, Physical Access Controls, Avoiding Common Threats to Physical Security, Defense in Depth. Textbook1: Chapter-1, Chapter-4			
Module-2			9 Hours
Footprinting Tools and Techniques: The Information-Gathering Process, The Information on a Company Website, Discovering Financial Information, Google Hacking, Exploring Domain Information Leakage, Tracking an Organization's Employees, Exploiting Insecure Applications, Using Social Networks, Using Basic Countermeasures. Port Scanning: Determining the Network Range, Identifying Active Machines, Mapping Open Ports, OS Fingerprinting, Mapping the Network, Analyzing the Results. Textbook1: Chapter- 5, Chapter-6			
Module-3			9 Hours
Enumeration and Computer System Hacking: Windows Basics, Commonly Attacked and Exploited Services, Enumeration, System Hacking, Types of Password Cracking, Using Password Cracking, Using PsTools, Rootkits, Covering Tracks.			

Wireless Vulnerabilities: The Importance of Wireless Security, Working with and Securing Bluetooth, Working with Wireless LANs, Threats to Wireless LANs, Internet of Things (IoT), Wireless Hacking Tools, Protecting Wireless networks.

Textbook 1: Chapter-7, Chapter-8

Module-4

9 Hours

Malware: Malware, Viruses and How they Function, Worms and How they Function, Significance of Trojans, Detection of Trojans and Viruses, Trojan Tools, Distribution Methods, Trojan Construction Kits, Backdoors, Covert Communication, Spyware, Adware, Scareware, Ransomware.

Sniffers, Session Hijacking, and Denial of Service Attacks: Sniffers, Session Hijacking, Distributed Denial of Service (DDoS) Attacks, Botnets and the Internet of Things (IoT).

Textbook 1: Chapter-10, Chapter-11

Module-5

9 Hours

Incident Response: What is Security Incident? The Incident Response Process, Incident Response Plans, Planning for Disaster and Recovery, Evidence Handling and Administration, Requirements of Regulated Industries.

Defensive Technologies: Defense in Depth, Intrusion Detection Systems, The Purpose of Firewalls, Honeypots / Honeynets, The Role of Controls, Security Best Practices.

Textbook 1: Chapter-14, Chapter-15

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Describe hacking, ethical issues, penetration testing methodologies, and cryptographic fundamentals.
CO2	Identify common information-gathering tools and techniques and analyze how port scanning and fingerprinting are used by hackers.
CO3	Analyze how enumeration is used in conjunction with system hacking and analyze wireless network vulnerabilities exploited by hackers.
CO4	Classify various types of malware, Trojans, backdoors, covert and comommunication techniques.
CO5	Perform incident handling using appropriate procedures and compare defensive technologies.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Continuous and Comprehensive Evaluation (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
The minimum marks to be secured in CIE are 20 out of allotted 50 marks to appear for SEE, with minimum 40 % scored in every component of CIE.			

Textbooks:

1. Sean-Philip Oriyano, Michael G Solomon “Hacker Techniques, Tools, and Incident Systems”, Third Edition, Jones & Bartlett Learning, 2020.

Reference Books:

1. Abhinav Ojha, “Beginners Guide to Ethical Hacking and Cyber Security”, Notion Press, 2020.
2. Hugo Hoffman, “Ethical Hacking with Kali Linux-Learn Fast how to Hack like a Pro”, 2020.

Weblinks:

1. <https://www.techtarget.com/whatis/feature/17-free-cybersecurity-tools-you-should-know-about>
2. <https://www.coursera.org/learn/introduction-cybersecurity-cyber-attacks>

3. <https://www.youtube.com/watch?v=mOOIv8-IuEo>
4. <https://www.youtube.com/watch?v=R0up9SZJqyQ>
5. <https://archive.nptel.ac.in/courses/106/105/106105217/>

Self-Study Topics:

1. Analyze real-world cyber-attack case studies and map them to penetration testing methodology and legal aspects.
2. Perform footprinting, OSINT, and port scanning using tools like Nmap in a controlled lab environment.
3. Practice enumeration, password cracking, and wireless security analysis using safe lab setups.
4. Analyze phishing emails by examining email headers, links, attachments, and social engineering indicators in a controlled lab environment.
5. Study and compare malware types, sniffing techniques, and DDoS attack mechanisms with practical demonstrations.
6. Develop a basic incident response plan and evaluate defensive technologies such as IDS, firewalls, and honeypots.



ESTD : 2001

An Institute with a Difference

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – V			
Course Title:	DEVSECOPS		
Course Code:	BCY515D	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	03	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. To understand the transition from Waterfall/Agile to DevOps and finally to DevSecOps. 2. To master the "Shift-Left" security philosophy and its implementation in the infinite loop. 3. To gain technical proficiency in Application, Infrastructure, and Container security. 4. To explore automation frameworks, Policy-as-Code, and threat modeling for modern software.			
Module-1			9 Hours
Product Development Processes: Evolution from Waterfall to Agile and DevOps. The Shift: Integrating Security into the DevOps infinite loop. Core Concepts: Shift-left security, Key changes in DevSecOps roles, Security controls, and Threat modeling. Infrastructure Security: Introduction to securing the environment before code deployment. Textbook 1: Chapter-1			
Module-2			9 Hours
Cloud Application Security: Identity and Access Management (IAM), Session management, and PKI. Vulnerability Landscape: OWASP Top 10 overview and mitigation. Pipeline Security: Building secure CI/CD pipelines, Web Application Firewalls (WAF), and continuous vulnerability monitoring. Textbook 1: Chapter-2			
Module-3			9 Hours
IaC Concepts: Cloud platforms overview (AWS, Azure, GCP). Security Automation: Implementing security checks for Terraform/Ansible. Continuous Compliance: Automating audit requirements, Secret management (Vaults), and integration with legacy systems. Textbook 1: Chapter-3			
Module-4			9 Hours
Container Basics: Docker and Kubernetes architecture security. Secure Lifecycle: Vulnerability scanning for images, RBAC (Role-Based Access Control), and Network Policies. Best Practices: Secrets management in K8s, secure container builds, and runtime protection.			

Textbook 1: Chapter 4

Module-5

9 Hours

Security as Code: Policy-as-Code, Monitoring-as-Code, and automated security workflows. **Supply Chain Security:** Managing third-party risks and Software Bill of Materials (SBOM). **Compliance Frameworks:** Aligning DevSecOps with NIST, ISO, and SOC2. Developing a DevSecOps culture.

Textbook 1: Chapter-5 and 6 (Page No:164 to 173)

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Differentiate between traditional security and the integrated DevSecOps approach.
CO2	Identify and mitigate web vulnerabilities using OWASP standards and CI/CD tools.
CO3	Secure cloud infrastructure using automated IaC scanning and secret management.
CO4	Implement robust security policies for Docker containers and Kubernetes clusters.
CO5	Architect automated compliance and monitoring workflows (Security-as-Code).

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Continuous and Comprehensive Evaluation (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.

- The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE.
- **If any courses of 3 credits are of Integrated Course type, for such courses the method suggested for 4 credits IPCC shall be followed.**

Textbooks:

1. **Ashwini Kumar Rath**, *Concepts and Practices of DevSecOps*, 2024, BPB Publications. (ISBN: 9789355519320).

Reference Books:

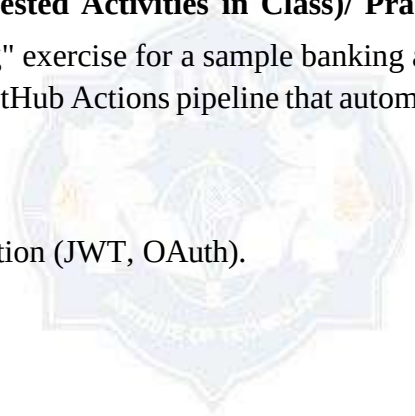
1. **Vandana Verma Sehgal**, *Implementing DevSecOps Practices*, Packt Publishing.
2. **Steve Suehring**, *DevSecOps*, O'Reilly Media.

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning Lab:

1. Perform a "Threat Modeling" exercise for a sample banking application.
2. **Project:** Create a Jenkins/GitHub Actions pipeline that automatically fails if a high-severity vulnerability is found in an NPM package.

Self-Study Topics:

1. Authentication & Authorization (JWT, OAuth).
2. Trivy.
3. Clair.
4. SonarQube.
5. Semgrep.



ESTD : 2001

An Institute with a Difference

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – V			
Course Title:	DATA SCIENCE FOR CYBER SECURITY		
Course Code:	BCY515E	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	03	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Understand the role of data science and machine learning in cyber security domains. 2. Apply classification, clustering, and anomaly detection techniques for threat detection. 3. Analyze malware, network traffic, and intrusion data using data-driven approaches. 4. Design and evaluate machine learning-based security systems for real-world applications.			
Module-1			9 Hours
Introduction to Data Science in Cyber Security: Cyber Threat Landscape, Cyber Attacker's Economy, What is Machine Learning, What ML is NOT, Adversaries Using ML, Real-world Applications, Spam Fighting: An Iterative Approach, Limitations of Machine Learning in Security. Textbook 1: Chapter-1 (Page 1 – 24)			
Module-2			9 Hours
Classification Techniques Machine Learning: Problems and Approaches, Machine Learning in Practice: A Worked Example, Model Families, Loss Functions, Optimization, Logistic Regression, Decision Trees, Random Forest, Support Vector Machines. Textbook 1: Chapter-2 (Page 25 – 49)			
Module-3			9 Hours
Advanced ML and Clustering: Naïve Bayes, k-NN, Neural Networks, Feature Selection, Overfitting & Underfitting, Model Evaluation, Clustering Algorithms, Cluster Evaluation. Introduction to Anomaly Detection: When to Use Anomaly Detection Versus Supervised Learning, Intrusion Detection with Heuristics, Data-Driven Methods. Textbook 1: Chapter-2 (Page 49-78), Chapter-3 (Page 79-85)			
Module-4			9 Hours
Anomaly Detection & Malware Analysis: Feature Engineering, Host & Network Detection, Web Application Intrusion Detection, Forecasting (Supervised Machine Learning), Statistical Metrics, Unsupervised Machine Learning Algorithms, Density Based Methods. Malware Basics: Understanding Malware, Defining Malware Classification, Malware: Behind the Scenes. Textbook 1: Chapter-3 (Page 86-145)			
Module-5			9 Hours

Network Security and Consumer Web Protection: Theory of Network Defense, Detecting In-Network Attackers, Machine Learning and Network Security, Threats in the Network, Botnets and You, Monetizing the Consumer Web.

Textbook 1: Chapter-5: Page 183-203, Chapter-5: Page 236-256

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Describe the role of data science in identifying cyber threats.
CO2	Apply classification and clustering techniques for security problems.
CO3	Analyze anomalies and detect intrusions using ML models.
CO4	Evaluate malware and network traffic using data-driven techniques.
CO5	Design secure and scalable ML-based cyber security systems.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Alternate Assessment (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks.
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
The minimum marks to be secured in CIE are 20 out of allotted 50 marks to appear for SEE, with minimum 40 % scored in every component of CIE.			

Textbooks:

1. Clarence Chio, David Freeman, “**Machine Learning and Security: Protecting Systems with Data and Algorithms**”, O’Reilly, 2018.

Reference Books:

1. Ian Goodfellow – *Deep Learning*.
2. Christopher Bishop – *Pattern Recognition and Machine Learning*.
3. Hastie, Tibshirani – *Elements of Statistical Learning*.

Weblinks:

1. <https://mlsec.net>
2. <https://scikit-learn.org>
3. <https://www.kaggle.com>
4. <https://owasp.org>

Self-Study Topics:

1. Python Libraries for Security (Scikit-learn, Pandas).
2. SIEM Tools & Log Analysis.
3. Real-world Datasets (Kaggle, CICIDS).
4. Case Study: Spam Detection System.
5. AI in Threat Intelligence.

Alternate Assessment Methods:

1. **Certifications (Skill-Based)** -industry-recognized certifications (e.g. CISCO, NPTEL, Infosys Springboard).
2. **Assignments / Problem Solving Sheets.**
3. **Quiz.**
4. **Mini Projects.**
5. **Group Activities / Peer Evaluation.**
6. **Presentations / Tech Talks.**

B.E. (Common to All Branches) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – V			
Course Title:	ENVIRONMENTAL STUDIES		
Course Code:	BENS507	CIE MARKS	50
(L :T : P) + SL	(2:0:0) + (30 Hours/Sem)	SEE MARKS	50
Credits:	2	EXAM HOURS	2
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Introduce the basic concepts of ecology and ecosystem functioning, including biodiversity and biogeochemical cycles. 2. Understand various types of environmental pollution, their sources, impacts, and preventive measures. 3. Explore causes of environmental degradation and methods of conservation with special emphasis on Indian biodiversity. 4. Create awareness about climate change, global warming, environmental legislation, and significant environmental movements in India.			
Module-1			6 Hours
Ecology: Basic concepts of ecosystem. Ecosystems (structure and function)- forest, desert, wetlands, river, oceanic and lake. Biotic and Abiotic components; Food chain; Ecological pyramid. Biogeochemical Cycles: carbon cycle, nitrogen cycle, phosphorus cycle, water cycle. Sustainability: 17 Sustainable Development Goals (SDG)- history, targets, implementation, capacity development.			
Module-2			6 Hours
Environmental Pollution: Surface and ground water pollution, noise pollution, soil pollution, air pollution and marine pollution - sources, impacts on living beings, impacts on environment, preventive measures. case-study on marine pollution. Water Chemistry: Significance and effect of pH, total dissolved solids and hardness. Case study on impact of fluoride on human health.			
Module-3			6 Hours
Environmental Degradation: Causes and effects of deforestation, desertification, soil erosion and glacier melting. Environmental Conservation: Significance and key features of national parks, wildlife sanctuaries, reserved forest and mangrove forest. Importance of western ghats as biodiversity hotspot (flora and fauna).			
Module- 4			6 Hours
Indian Monsoon and Global Warming Climate- Impact on monsoons, significance of El Nino and La Nina on India climate. Global warming: causes, greenhouse gases, effects on environment and human health. Causes and effects of acid rain and ozone depletion. Air sampler and its importance in assessing pollutants.			

Module- 5	6 Hours
Environmental Legislation: Environmental Protection Act 1984: Definition, Significance and key features. Indian Environmental Movements: Bishnoi Movement, Chipko & Appiko movement.	

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Describe the components and functions of ecosystems and explain major biogeochemical cycles and sustainability goals.
CO2	Understand various forms of pollution and environmental degradation, along with their impacts on ecosystems and human health.
CO3	Demonstrate awareness of climate issues, Indian environmental legislation, and the role of community-based movements in environmental protection.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	12	Average of Three Internal Assessment Tests each of 50 marks, scaled down to 30 marks.
Continuous and Comprehensive Evaluation (B)	20	8	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks.
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration should be for 3 hours
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
- The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE. - If any courses of 3 credits are of Integrated Course type, for such courses the method suggested for 4 credits IPCC shall be followed.			

Textbooks:

1. Benny Joseph, “Environmental studies”, 3 rd ed., Tata McGraw-Hill, 2017.
2. S M Prakash, “Environmental Studies” 3rd Edition, Elite Publishing House, Mangalore, 2018.

Reference Books:

1. M.Anji Reddy, “Textbook of environmental science and Technology”, revised ed., BS publications, 2014.
2. Dr. B.S Chauhan, “Environmental studies”, 1 st ed., University of science press, 2008



ESTD : 2001

An Institute with a Difference

B.E. (Common to All Branches) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – V			
Course Title:	BIOLOGY FOR ENGINEERS		
Course Code:	BBOE507	CIE MARKS	50
(L :T : P) + SL	2:0:0	SEE MARKS	50
Credits:	02	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Familiarize the students with the basic biological concepts and their engineering applications 2. Enable the students with an understanding of bio design principles to create novel devices and structures. 3. Provide the students an appreciation of how biological systems can be re-designed as substitute products for natural systems. 4. Motivate the students to develop interdisciplinary vision of biological engineering.			
Module-1			6 Hours
Introduction to fundamentals of life. Structure and functions of a cell. Biomolecules: Properties and functions of Carbohydrates, Nucleic acids, Proteins, Enzymes and Lipids			
Module-2			6 Hours
Introduction to applications of biomolecules, Carbohydrates in cellulose-based water filters production, PHA and PLA in bioplastics production, Nucleic acids in vaccines and diagnosis, Proteins in food production, Enzymes in biosensors fabrication, food processing, enzymes in biobleaching, Lipids in biodiesel and detergents production.			
Module-3			6 Hours
Introduction to adaptations of anatomical principles for bioengineering design, Brain as a CPU system. Eye as a Camera system. Heart as a pump system. Lungs as purification system. Kidney as a filtration system.			
Module- 4			6 Hours
Introduction to nature inspired biomaterials and mechanisms, Echolocation, Photosynthesis. Bird flying, Lotus leaf effect, Plant burrs, Shark skin, Kingfisher beak. Artificial blood - haemoglobin-based oxygen carriers (HBOCs) and perfluorocarbons (PFCs).			
Module- 5			6 Hours
Introduction to trends in bioengineering, Tissue engineering, stem cells and their applications, Bioprinting techniques and materials. Electrical tongue and electrical nose in food science, DNA origami and Biocomputing, Bioimaging and Artificial Intelligence for disease diagnosis. Bioconcrete.			

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Corroborate the concepts of biomimetics for specific requirements.
CO2	Understand the basic biological concepts for relevant industrial applications. adaptation.
CO3	Evaluate the principles of design and development, for exploring engineering knowledge in biological
CO4	Think critically towards exploring innovative biobased solutions for socially relevant problems.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Average of Three Internal Assessment Tests each of 50 marks, scaled down to 30 marks.
Continuous and Comprehensive Evaluation (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C .
The minimum marks to be secured in CIE is 20 out of allotted 50 marks to appear for SEE, with minimum 40 % scored.			

Textbooks:

1. Basuchandra's Biology for Engineers, Chandra shekara. B.M, Basavaraju B.C, 2025.
2. Biology for Engineers, Rajendra Singh C and Rathnakar Rao N, Rajendra Singh C and Rathnakar Rao N Publishing, Bengaluru, 2023.

Reference Books:

1. Human Physiology, Stuart Fox, Krista Rompolski, McGraw-Hill eBook. 16th Edition, 2022
2. Biology for Engineers, Thyagarajan S., Selvamurugan N., Rajesh M.P., Nazeer R.A., Thilagaraj W.
3. Barathi S., and Jaganthan M.K., Tata McGraw-Hill, New Delhi, 2012.
4. Biology for Engineers, Arthur T. Johnson, CRC Press, Taylor and Francis, 2011
5. Biomedical Instrumentation, Leslie Cromwell, Prentice Hall 2011.
6. Biology for Engineers, Sohini Singh and Tanu Allen, Vayu Education of India, New Delhi, 2014.
7. Biomimetics: Nature-Based Innovation, Yoseph Bar-Cohen, 1st edition, 2012, CRC Press.
8. Bio-Inspired Artificial Intelligence: Theories, Methods and Technologies, D. Floreano and C.
9. Mattiussi, MIT Press, 2008.
10. Bioremediation of heavy metals: bacterial participation, by C R Sunilkumar, N Geetha A C
11. Udayashankar Lambert Academic Publishing, 2019.



ESTD : 2001

An Institute with a Difference

B.E. (CSE and Allied Branches)
Outcome Based Education (OBE) and Choice Based Credit System (CBCS)
SEMESTER – V

Course Title:	RESEARCH METHODOLOGY AND IPR		
Course Code:	BRMK557	CIE MARKS	50
(L :T : P) + SL	(2:0:0) + (30 Hours/Sem)	SEE MARKS	50
Credits:	02	EXAM HOURS	2

COURSE LEARNING OBJECTIVES:

The purpose of the course is to facilitate the learner to:

1. Explain the fundamental concepts, objectives and types of research in engineering.
2. Apply literature review techniques, technical reading strategies and appropriate attribution and citation practices in academic research.
3. Demonstrate ethical practices and identify research misconduct in engineering research.
4. Explain the concepts and significance of Intellectual Property Rights (IPR) in engineering.
5. Understand the procedures for protecting intellectual property through patents, copyrights, trademarks, industrial designs and geographical indications.

Module-1

6 Hours

Introduction: Meaning of Research, Objectives of Engineering Research, and Motivation in Engineering Research, Types of Engineering Research, Finding and Solving a Worthwhile Problem. Ethics in Engineering Research, Ethics in Engineering Research Practice, Types of Research Misconduct, Ethical Issues Related to Authorship.

Textbook: Chapter-1 (1.1 - 1.9)

Module-2

6 Hours

Literature Review and Technical Reading: Introduction to literature review and technical reading, understanding new and existing knowledge, and techniques for analysis and synthesis of prior art. Overview of bibliographic databases such as Web of Science, Google, and Google Scholar. Effective search strategies and approaches for technical reading. Conceptualizing research through critical and creative reading practices.

Attributions and Citations: Importance of giving proper credit through attributions and citations. Functions and attributes of citations, and the role of titles and keywords in enhancing citation impact. Understanding knowledge flow through citations and the practice of citing datasets. Overview of citation styles, along with guidelines for acknowledgments and proper attribution in academic writing.

Textbook: Chapter-2 (2.1 - 2.5) Chapter-3 (3.1 - 3.9)

Module-3

6 Hours

Introduction to Intellectual Property: Role of IP in the Economic and Cultural Development of the Society, IP Governance, IP as a Global Indicator of Innovation, Origin of IP History of IP in India. Major Amendments in IP Laws and Acts in India.

Patents: Conditions for Obtaining a Patent Protection, To Patent or Not to Patent an Invention. Rights Associated with Patents. Enforcement of Patent Rights. Inventions Eligible for Patenting. Non-Patentable Matters. Patent Infringements. Avoid Public Disclosure of an Invention before Patenting. Process of Patenting.

Textbook: Chapter-4 (4.1 - 4.6) Chapter-5 (5.1 - 5.8)

Module-4

6 Hours

Process of Patenting: Prior Art Search. Choice of Application to be Filed. Patent Application Forms. Jurisdiction of Filing Patent Application. Publication. Pre-grant Opposition. Examination. Grant of a Patent. Validity of Patent Protection. Post-grant Opposition. Commercialization of a Patent. Need for a Patent Attorney/Agent. Can a Worldwide Patent be Obtained? Do I Need First to File a Patent in India? Patent Related Forms. Fee Structure.

Copyrights and Related Rights: Classes of Copyrights. Criteria for Copyright. Ownership of Copyright. Copyrights of the Author. Copyright Infringements. Copyright Infringement is a Criminal Offence. Copyright Infringement is a Cognizable Offence. Fair Use Doctrine. Copyrights and Internet. Non-Copyright Work. Copyright Registration. Judicial Powers of the Registrar of Copyrights. Fee Structure. Copyright Symbol. Validity of Copyright.

Textbook: Chapter-6 (6.1 - 6.19) Chapter-7 (7.1 - 7.16)

Module-5

6 Hours

Trademarks: Eligibility Criteria. Who Can Apply for a Trademark. Acts and Laws. Designation of Trademark Symbols. Classification of Trademarks. Registration of a Trademark is Not Compulsory. Validity of Trademark. Types of Trademark Registered in India.

Famous Case Law: Coca-Cola Company vs. Bisleri International Pvt. Ltd.

Industrial Designs: Eligibility Criteria. Acts and Laws to Govern Industrial Designs. Design Rights. Enforcement of Design Rights. Non-Protectable Industrial Designs India. International Treaties.

Famous Case Law: Apple Inc. vs. Samsung Electronics Co.

Geographical Indications: Acts, Laws and Rules Pertaining to GI. Ownership of GI. Rights Granted to the Holders. Registered GI in India. Identification of Registered GI.

Textbook: Chapter-8 (8.1 - 8.12) Chapter-9 (9.1 - 9.17) Chapter-10 (10.1 -10.5)

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Describe the fundamental concepts, objectives, classifications and methodologies of engineering research.
CO2	Analyze and apply concepts of literature review, technical reading, attribution, and citation in research contexts.
CO3	Identify ethical issues and research misconduct and demonstrate ethical practices in engineering research.

CO4	Interpret and explain the role and significance of Intellectual Property Rights (IPR) in engineering and innovation.
CO5	Differentiate between patents, copyrights, trademarks, industrial designs and geographical indications and identify their applications in intellectual property protection.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Average of Two Internal Assessment Tests (MCQs) each conducted for 30 marks
Continuous and Comprehensive Evaluation (B)	20	-	Any two Assessment methods as per 24RNBE4.2, scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks.
SEE (C)	50	18	Question papers having 50 MCQs with each question carrying 01 mark, and Exam duration shall be for 2 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.

Textbook:

1. Dr. Santosh M Nejekar, Dr. Harish Bendigeri, Research Methodology and Intellectual Property Rights, 1st Edition, Published by the Authors, 2023.

Reference Book:

1. David V. Thiel, Research Methods for Engineers, 1st Edition, Cambridge University Press, 2014
2. N.K.Acharya, Intellectual Property Rights, 6th Edition, Asia Law House.

B.E. (Common to All Branches) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – V			
Course Title:	NATIONAL SERVICE SCHEME		
Course Code:	BNSK559	CIE MARKS	100
(L :T : P)	0:0:2	SEE MARKS	0
Credits:	---	EXAM HOURS	—
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Identify the needs and problems of the community and involve the problem-solving. 2. Develop a sense of social & civic responsibility & utilize their knowledge in finding practical solutions to individual and community problems. 3. Develop competence required for group-living and sharing of responsibilities & gain skills in mobilising community participation to acquire leadership qualities and democratic attitudes.			
Module-1			
Waste management– Public, Private and Govt organization, 5 R's.			
Module-2			
Automation of local Activities.			
Module-3			
Organic farming, Indian Agriculture (Past, Present and Future), Connectivity for marketing.			
Module-4			
Spreading public awareness under rural outreach Programs.			
Module-5			
Food preservation and Packaging.			

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Understand the motto and concepts of NSS.
CO2	Develop overall personality of volunteers and make them as leaders and responsible citizens of our nation.
CO3	Analyze the environmental and societal problems/issues and will be able to design solutions for the same.
CO4	Analyze the environmental and societal problems/issues and will be able to design solutions for the same.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE - IA Tests (A)	60	-	Sum of Two Internal Assessment Tests (MCQs) each conducted for 30

			marks.
Continuous and Comprehensive Evaluation (B)	40	-	Any two Assessment methods as per 24RNBE4.2, scaled to 40 marks.
Total CIE (A+B)	100	40	CIE Evaluation is done for a maximum of 100 marks.
The minimum marks to be secured in CIE is 40 (40%) out of allotted 100 marks to Pass.			

Reference Books:

- 1) NSS Course Manual, Published by NSS Cell, VTU Belagavi.
- 2) Government of Karnataka, NSS cell, activities reports and its manual.
- 3) Government of India, NSS cell, Activities reports and its manual.

Weblinks:

1. <https://nss.gov.in/>
2. <https://pledge.mygov.in/>



ESTD : 2001

An Institute with a Difference

B.E. (Common to All Branches) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – V			
Course Title:	PHYSICAL EDUCATION		
Course Code:	BPEK559	CIE MARKS	100
(L :T : P) + SL	0:0:2	SEE MARKS	---
Credits:	---	EXAM HOURS	—
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Understand the fundamental concepts of Physical Education, games and sports skills, Health, Nutrition and Fitness. 2. Familiarization of health-related Exercises, Sports for overall growth and development 3. Participate in the competition at regional/state / national / international levels. 4. Create consciousness among the students on Health, Fitness and Wellness in developing and maintaining a healthy lifestyle.			
Module 1: Title: Athletics – Track Events – 100 & 400 Mtrs Hurdles 3 Hours			
110 Mtrs and 400Mtrs: Hurdling Technique: Lead leg Technique, Trail leg Technique. Crouch start (its variations) use of Starting Block.			
Module 2: Title: Athletics – Track 3 Hours			
High Jump A) Approach Run. B) Take-off. C) Bar Clearance (Straddle). D) Landing.			
Module 3: Title: Athletics – Throws 3 Hours			
Discuss Throw A) Holding the Discus. B) Initial Stance Primary Swing. C) Rotation. D) Release and Recovery (Rotation in the circle).			
Module 4: Title: Football 3 Hours			
A. Fundamental skills 1. Kicking: Kicking the ball with inside of the foot, Kicking the ball with Full Instep of the foot, Kicking the ball with Inner Instep of the foot, Kicking the ball with Outer Instep of the foot and Lofted Kick. 2. Trapping: Trapping- the Rolling ball, and the Bouncing ball with sole of the foot. 3. Dribbling: Dribbling the ball with Instep of the foot, Dribbling the ball with Inner and Outer Instep of the foot. 4. Heading: In standing, running and jumping condition. 5. Throw-in: Standing throw-in and Running throw-in.			

4. Tackling: Simple Tackling, Slide Tackling.
5. Goal Keeping: Collection of Ball, Ball clearance- kicking, throwing and deflecting.
6. Game practice with application of Rules and Regulations.

B. Rules and their interpretation and duties of the officials

Module 5: Title: Hockey

3 Hours

A. Fundamental skills

1. Passing: Short pass, Long pass , push pass, hit.
2. Trapping.
3. Dribbling and Dozing.
4. Penalty stroke practice.
5. Penalty corner practice.
6. Tackling: Simple Tackling, Slide Tackling.
7. Goal Keeping, Ball clearance- kicking, and deflecting.
8. Game practice with application of Rules and Regulations.

B. Rules and their interpretation and duties of the officials

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Understand and demonstrate fundamental techniques of track events including 110m and 400m hurdles, with proper use of starting blocks and hurdling skills.
CO2	Apply technical knowledge of athletic jumps , particularly high jump, including approach run, take-off, bar clearance, and landing techniques.
CO3	Develop skills and perform throwing events , specifically discus throw, with correct techniques such as grip, stance, rotation, release, and recovery.
CO4	Demonstrate fundamental skills of football such as kicking, trapping, dribbling, heading, throw-in, tackling, and goalkeeping along with understanding rules and officiating.
CO5	Exhibit basic skills and techniques in hockey , including passing, trapping, dribbling, tackling, penalty strokes/corners, and understand rules and duties of officials.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	60	---	Sum of Two Internal Assessment Tests (MCQs) each conducted for 30 marks.
Project (B)	40	---	-----
Total CIE (A+B)	100	40	CIE Evaluation is done for a maximum of 100 marks

- The minimum marks to be secured in CIE is 40 (40%) out of 100 marks allotted to Pass.

Textbooks:

1. Health and Physical Education by V.K. Sharma
2. Introduction to Physical Education, Fitness, and Sport by Daryl Siedentop
3. Physical Education Activities, Sports and Games: The Origin and Background, Rules of Play, Teaching Hints and Fundamentals by Louis E. Means

Reference Books:

1. Saraswati Health and Physical Education Textbook
2. Foundations of Physical Education, Exercise Science and Sport by Deborah A. Wuest



ESTD : 2001

An Institute with a Difference

B.E. (Common to All Branches) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – V			
Course Title:	YOGA		
Course Code:	BYOK559	CIE MARKS	100
(L :T : P) + SL	0:0:2	SEE MARKS	---
Credits:	---	EXAM HOURS	—
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Physical, Mental & spiritual Objectives of Yoga 2. Explain the meaning of Yoga. 3. Discuss the importance of the Yoga and its scope. 4. Describe the aims and objectives of Yoga. 5. Clarifythe misconceptions on Yoga			
Module-1 : Title : Suryanamaskara			3 Hours
Suryanamaskar 12 count 6 rounds a) Suryanamaskar prayer. b) Meaning, need & Importance c) Benefits of Suryanamaskara			
Module-2: Title : Yoga			3 Hours
a) Meaning and definition. b) Brief introduction of yogic practices for the common man c) Rules and regulations d) Misconceptions of Yoga			
Module-3 : Title : Asanas - Sitting & Standing			3 Hours
Need & importance of different Asana, Asana its meaning by name, technique, precautionary measures and benefits of each asana. Sitting 1. Ardha Ushtrasana 2. Yogamudra in Padmasana Standing 1. Hastapadasana 2. Utkatasana			
Module-4 : Title : Asanas - Supine line			3 Hours
Need & importance of different Asana, Asana its meaning by name, technique, precautionary measures and benefits of each asana. Supine line 1. Sarvangasana 2. Chakraasana			
Module-5: Title : Pranayama			3 Hours
1. Kapalabhati - Revision of practice 40 strokes/min - 3 rounds			

2. Pranayama :
 - i. Ujjayi
 - ii. Sheetal
3. Meaning, Need, importance of Pranayama. Different types. Meaning by name, technique, precautionary measures and benefits of each Pranayama

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Explain the meaning, definition, scope, and objectives of Yoga and its role in physical, mental, and spiritual well-being.
CO2	Demonstrate Suryanamaskara (12 counts, 6 rounds) with correct technique and understand its importance and benefits.
CO3	Apply knowledge of yogic practices, rules, and regulations while identifying and correcting common misconceptions of Yoga.
CO4	Perform sitting, standing, and supine Asanas with proper technique, precautions, and awareness of their benefits.
CO5	Practice Pranayama techniques (Kapalabhati, Ujjayi, Sheetal) to improve breathing control, concentration, and overall health.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	60	----	Sum of Two Internal Assessment Tests (MCQs) each conducted for 30 marks.
Project (B)	40	----	-----
Total CIE (A+B)	100	40	CIE Evaluation is done for a maximum of 100 marks
The minimum marks to be secured in CIE is 40 (40%) out of 100 marks allotted to Pass.			

Textbooks:

1. The Yoga Sutras of Patanjali by Sri Swami Satchidananda.
2. Light on Yoga by B.K.S Iyengar.

Reference Books:

1. The Heart of Yoga by T.K.V Desikachar.
2. Asana Pranayama Mudra Bandha by Swami Satyananda Saraswati.



RN Shetty Trust ®

RNS INSTITUTE OF
TECHNOLOGY

An Autonomous Institution, Affiliated to VTU,
Accredited with NAAC A+ Grade

Department of CSE (Cyber Security)
Autonomous Scheme (Effective from Academic Year
2024 – 25)



VI SEMESTER SUBJECTS

An Institute with a Difference

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VI			
Course Title:	VULNERABILITY ASSESSMENT AND PENETRATION TESTING		
Course Code:	BCY601	CIE MARKS	50
(L :T : P) + SL	(3:0:2) + (45 Hours/Sem)	SEE MARKS	50
Credits:	4	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Describe the ethical frameworks and methodologies involved in planning and executing a professional Vulnerability Assessment and Penetration Test (VAPT). 2. Utilize penetration testing tools (e.g., Nmap, Metasploit) to discover active hosts, identify services, and exploit vulnerabilities in a controlled environment. 3. Analyze and report on the security posture of an organization's internal and external network infrastructure, as well as its web applications, using tools like OpenVAS, Nikto, and Burp Suite. 4. Develop and execute exploits for common vulnerabilities in Linux and Windows operating systems while demonstrating an understanding of memory protections. 5. Conduct basic malware analysis and explain the mechanisms of client-side browser exploits to propose effective protection strategies.			
Module-1			9 Hours
Introduction to Ethics of Ethical Hacking: Why You Need to Understand Your Enemy's Tactics, Recognizing the Gray Areas in Security, Vulnerability Assessment and Penetration Testing. Penetration Testing and Tools: Social Engineering Attacks: How a Social Engineering Attack Works, Conducting a Social Engineering Attack, Common Attacks Used in Penetration Testing, Preparing Yourself for Face-to-Face Attacks, Defending Against Social Engineering Attacks. Textbook 1 : Chapter-1, Chapter-4			
Module-2			9 Hours
Physical Penetration Attacks: Need of Physical Penetration, Conducting a Physical Penetration, Common Ways into a Building, Defending Against Physical Penetrations. Insider Attacks: Conducting an Insider Attack, Defending Against Insider Attacks. Metasploit: The Big Picture, Getting Metasploit, Using the Metasploit Console to Launch Exploits, Exploiting Client-Side Vulnerabilities with Metasploit, Penetration Testing with Metasploit's Meterpreter, Automating and Scripting Metasploit, Going Further with Metasploit. Textbook 1 : Chapter-5, Chapter-6, Chapter-8			
Module-3			9 Hours
Managing a Penetration Test: Planning a Penetration Test, Structuring a Penetration Testing Agreement, Execution of a Penetration Test, Information Sharing During a Penetration Test, Reporting the Results of a Penetration Test.			

Basic Linux Exploits: Stack Operations, Buffer Overflows, Local Buffer Overflow Exploits, Exploit Development Process.	
Windows Exploits: Compiling and Debugging Windows Programs, Writing Windows Exploits.	
Textbook 1 : Chapter-9, Chapter-11, Chapter-15	
Module-4	9 Hours
Web Application Security Vulnerabilities: Overview of Top Web Application Security Vulnerabilities, Injection Vulnerabilities, Cross-Site Scripting Vulnerabilities, The Rest of the OWASP Top Ten, SQL Injection Vulnerabilities, Cross-Site Scripting Vulnerabilities.	
Client-Side Browser Exploits: Why Client-Side Vulnerabilities are Interesting, Internet Explorer Security Concepts, History of Client- Side Exploits and Latest Trends, Finding New Browser-Based Vulnerabilities, Heap Spray to Exploit, Protecting Yourself from Client-Side Exploit.	
Textbook 1 : Chapter-17, Chapter-23	
Module-5	9 Hours
From Vulnerability to Exploit: Exploitability, Understanding the Problem, Payload construction considerations, Documenting the problem.	
Closing the Holes: Mitigation: Mitigation Alternatives, Patching.	
Textbook 1 : Chapter-26, Chapter-27	

PRACTICAL COMPONENT OF IPCC

Sl. No	Experiments
PART-A	
1	Monitoring Network Traffic Objective: To analyze and capture network traffic to identify patterns, detect anomalies and assess overall network performance and security.
2	Host & Services Discovery using Nmap Objective: To identify active hosts and the services they are running within a network using Nmap, enabling a comprehensive understanding of the network environment.
3	Internal Penetration Testing - Mapping. - Scanning. - Gaining Access through CVEs. - Sniffing POP3/FTP/Telnet Passwords. - ARP Poisoning. - DNS Poisoning.

	Objective: To perform a thorough internal penetration test that systematically assesses the security of the organization's network infrastructure by mapping network resources, scanning for vulnerabilities, exploiting known weaknesses and demonstrating attack techniques, including credential sniffing and poisoning attacks, in order to identify and mitigate potential security risks effectively.
4	External Penetration Testing a. Evaluating External Infrastructure b. Creating Topological Map & Identifying IP Address of Target c. Lookup Domain Registry for IP Information d. Examining Use of IPv6 at Remote Location Objective: To conduct a comprehensive external penetration test aimed at evaluating the security of the organization's external infrastructure by assessing vulnerabilities, mapping the network topology, gathering IP and domain registry information, and examining the implementation of IPv6, ultimately identifying potential entry points and recommending measures to strengthen defenses against external threats.
5	Different Types of Vulnerability Scanning Objective: To explore and compare various vulnerability scanning techniques and tools, assessing their effectiveness in identifying and prioritizing security risks.
6	Vulnerability Scanning with Nessus Objective: To utilize Nessus for comprehensive vulnerability scanning, identifying security weaknesses in systems and providing recommendations for remediation.
7	Web Application Assessment with Nikto Objective: To evaluate web applications for security vulnerabilities using Nikto for identifying issues such as misconfigurations and common vulnerabilities in web applications.
8	Web Application Assessment with Burp Suite Objective: To evaluate web applications for security vulnerabilities using Burp Suite.

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Apply the ethical considerations and legal implications in conducting ethical hacking activities using appropriate tools.
CO2	Analyze social engineering, physical penetration and insider attacks using automating penetration testing processes.
CO3	Identify report penetration tests effectively to develop and execute Linux and Windows exploits, bypassing memory protections.
CO4	Illustrate web application security vulnerabilities to conduct vulnerability analysis.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE- IA Tests (A)	20	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 20 marks.
Continuous and Comprehensive Evaluation (B)	10	-	Any one Assessment methods as per 24RNBE4.2 scaled to 10 marks.
Total CIE Theory (A+B)	30	12	Marks of Tests and Assignments awarded for a maximum of 30.
CIE Practical	12	-	Marks awarded for Weekly Conduction of Experiments and Submission of Laboratory records, scaled to 12 marks.
CIE Practical Test	8	-	Average of marks of Two tests, each conducted for 100 marks covering all experiments, scaled to 8.
Total CIE Practical (C)	20	8	Marks of Experiments, Record and Test awarded for a maximum of 20 marks.
CIE: Theory + Practical (A + B + C)	50	20	CIE Evaluation is done for a maximum of 50 marks.
SEE (D)	50	18	SEE is a theory exam, conducted for 100 marks and scaled down to 50 marks. Exam duration shall before 3 hours.
CIE+SEE (A+B+C+D)	100	40	Final marks shall be the sum of marks scored in Components A, B, C and D
The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE. The laboratory component of the IPCC shall be for CIE only. However, in SEE, the questions from the laboratory component shall be included in their respective modules only.			

Text Book:

1. Gray Hat Hacking - The Ethical Hackers Handbook, Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, and Terron Williams, 3rd Edition, Tata McGraw-Hill

Reference Books:

1. The Web Application Hacker's Hand Book - Discovering and Exploiting Security flaw Dafydd Suttard, Marcus Pinto, 1st Edition, Wiley Publishing.
2. Penetration Testing: Hands-on Introduction to Hacking, Georgia Weidman, 1st Edition, Starch Press.
3. The Pen Tester Blueprint - Starting a Career as an Ethical Hacker, L. Wylie, Kim Crawly, 1st Edition, Wiley Publications.

Web links and Video Lectures (e-Resources):

1. <https://www.youtube.com/watch?v=jX0hhhaeh-g>
2. <https://www.youtube.com/watch?v=FNj8jMTOfnA>
3. <https://www.youtube.com/watch?v=U-mAqnc6ZkI>

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning:

- **Group Activity: Identify Vulnerabilities**

Scenario Setup: Provide groups with a simulated web application or network diagram.

Task: Each group identifies potential vulnerabilities based on provided documentation and visual clues.

Tools: Use a checklist or framework (e.g., OWASP Top Ten) to guide their assessment.

- **Presentation: Tools for Vulnerability Assessment**

Overview of Tools: Nessus, OpenVAS, Burp Suite, Nmap.

Demo: Show how to use one of these tools (e.g., running a scan with Nmap).

Self-Study topics:

1. AI-Driven Vulnerability Scanning.
2. Application & Multimedia Security.
3. ARP Poisoning & MITM. (Tools like Ettercap or Bettercap)
4. Top AI-Powered Tools for 2026.
5. Vulnerability Scanning using OpenVA.

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VI			
Course Title:	CRYPTOGRAPHY AND NETWORK SECURITY		
Course Code:	BCY602	CIE MARKS	50
(L :T : P) + SL	(3:2:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	4	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Apply cryptography concepts and security principles to protect information systems. 2. Analyze and implement cryptographic algorithms for secure data communication. 3. Apply public and private key cryptography techniques for authentication and confidentiality. 4. Analyze key distribution mechanisms and digital certificate-based security frameworks. 5. Apply network security approaches to safeguard computer communication systems.			
Module-1			9 Hours
A model for Network Security, Classical encryption techniques: Symmetric cipher model, Substitution ciphers-Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Hill Cipher, Polyalphabetic Ciphers, One time pad, Steganography.			
Block Ciphers and Data Encryption Standards: Traditional Block Cipher structures, data Encryption Standard (DES), A DES Example, The strength of DES, Block cipher design principles.			
Textbook 1: Chapter-1 (1.8), Chapter-3 (3.1-3.2, 3.5), Chapter-4 (4.1-4.5)			
Module-2			9 Hours
Pseudorandom number Generators: Linear Congruential Generators, Blum Blum Shub Generator.			
Public key cryptography: Principles of public key cryptosystems-Public key cryptosystems, Applications for public key cryptosystems, Requirements for public key cryptography, public key Cryptanalysis.			
Diffie-Hellman key exchange: The Algorithm, Key exchange Protocols, Man-in-the-middle Attack, ElGamal Cryptosystem.			
Elliptic Curve Cryptography: Analog of Diffie-Hellman key Exchange, Elliptic Curve Encryption/Decryption, Security of Elliptic Curve Cryptography.			
Textbook: Chapter-8 (8.2), Chapter-9 (9.1-9.2), Chapter-10 (10.1-10.2, 10.4)			
Module-3			9 Hours
Applications of Cryptographic Hash functions, Two simple Hash functions, Key management and distribution: Symmetric key distribution using symmetric encryption, Symmetric key distribution using asymmetric encryption, Distribution of public keys, X.509 Certificates, Public Key Infrastructures.			
Textbook 1: Chapter-11(11.1-11.2), Chapter-14(14.1-14.5)			

Module-4	9 Hours
User Authentication: Remote user authentication principles, Kerberos, Remote user authentication using asymmetric encryption. Web security consideration, Transport layer security. Email Threats and comprehensive email security, S/MIME, Pretty Good Privacy. Textbook 1: Chapter-15 (15.1, 15.3, 15.4) , Chapter-17 (17.1-17.2), Chapter-19 (19.3-19.5)	
Module-5	9 Hours
Domainkeys Identified Mail. IP Security: IP Security overview, IP Security Policy, Encapsulating Security Payload, Combining security associations, Internet key exchange. Textbook 1: Chapter-19 (19.9), Chapter-20 (20.1-20.5)	

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Apply classical and modern cryptographic techniques to secure data communication.
CO2	Illustrate public key cryptographic algorithms for secure communication.
CO3	Analyze authentication and access control mechanisms used in network security.
CO4	Utilize key management, key distribution, and certificate-based security mechanisms.
CO5	Apply network and email security protocols to protect communication infrastructure.

ASSESSMENT AND EVALUATION (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Alternate Assessment (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 Marks be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.

- The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE.
- If any courses of 3 credits are of Integrated Course type, for such courses the method suggested for 4 credits IPCC shall be followed.

Textbooks:

1. William Stallings, “Cryptography and Network Security”, Pearson Publication, Seventh Edition.

Reference Books:

1. Keith M Martin, “Everyday Cryptography”, Oxford University Press.
2. V.K Pachghare, “Cryptography and Network Security”, PHI, 2nd Edition.

Web links and Video Lectures (e-Resources):

- <https://nptel.ac.in/courses/106105162>
(Comprehensive video lectures covering cryptography, DES, AES, RSA, hash functions, and network security)
- <https://ocw.mit.edu/courses/6-875-cryptography-and-cryptanalysis-spring-2005/>
(Video lectures and notes covering theoretical foundations, algorithms, and cryptanalysis)
- <https://ocw.mit.edu/courses/6-875-cryptography-and-cryptanalysis-spring-2005/>
(Video lectures and notes covering theoretical foundations, algorithms, and cryptanalysis)
- <https://www.coursera.org/learn/crypto>
(Stanford Cryptography course covering block ciphers, RSA, hash functions, and protocols)
- <https://csrc.nist.gov>
(Official standards and guidelines for AES, SHA, digital signatures, and security protocols)

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning:

- Group (2 students) programming assignment to implement Cryptographic Algorithms.

Self-Study Topics:

1. Real-world security attacks (Phishing, DoS, MITM).
2. Comparison of DES, AES, and Triple DES
3. Birthday attack in hash functions.
4. Public Key Infrastructure (PKI) and digital certificate.

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VI			
Course Title:	BIG DATA ANALYTICS WITH SPARK		
Course Code:	BCY613A	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	3	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Gain clarity on Big Data principles, characteristics, evolution, and its analytical ecosystem. 2. Explore Hadoop components such as HDFS, YARN, and MapReduce for large-scale data processing. 3. Understand NoSQL concepts and utilize MongoDB for handling diverse datasets. 4. Build data workflows using Hive and Pig for querying, transformation, and distributed processing. 5. Apply Spark, text analytics, web analytics, and link analysis techniques for extracting meaningful insights from massive data sources.			
Module-1			9 Hours
Types of Digital Data: Classification of Digital Data. Introduction to Big Data: Classification of data, Characteristics, Evolution and definition of Big data, What is Big data, Why Big data, Traditional Business Intelligence Vs Big Data, Typical data warehouse and Hadoop environment. Big Data Analytics: What is Big Data Analytics, Classification of Analytics, Importance of Big Data Analytics, Technologies used in Big Data Environments, Few Top Analytical Tools. Textbook 1: Chapter-1 (1.1), Chapter-2 (2.1-2.5,2.7,2.9-2.11), Chapter-3 (3.2,3.5,3.8,3.12)			
Module-2			9 Hours
The Big Data Technology Landscape: NoSQL, Hadoop. Introduction to Hadoop: Introducing hadoop, Why hadoop, Why not RDBMS, RDBMS Vs Hadoop, History of Hadoop, Hadoop overview, Use case of Hadoop, HDFS (Hadoop Distributed File System), Processing data with Hadoop, Managing resources and applications with Hadoop YARN(Yet Another Resource Negotiator). Textbook1: Chapter-4 (4.1,4.2), Chapter-5 (5.1-,5.8, 5.10-5.12)			
Module-3			9 Hours
Introduction to Map Reduce Programming: Introduction, Mapper, Reducer, Combiner, Partitioner, Searching, Sorting, Compression. Introduction to MongoDB: What is MongoDB, Why MongoDB, Terms used in RDBMS and MongoDB, Data Types in MongoDB, MongoDB Query Language. Textbook 1: Chapter-8 (8.1 - 8.8), Chapter-6 (6.1-6.5)			

Module-4	9 Hours
Introduction to Hive: What is Hive, Hive Architecture, Hive data types, Hive file formats, Hive Query Language (HQL), RC File implementation, User Defined Function (UDF). Introduction to Pig: What is Pig, Anatomy of Pig, Pig on Hadoop, Pig Philosophy, Use case for Pig, Pig Latin Overview, Data types in Pig, Running Pig, Execution Modes of Pig, HDFS Commands, Relational Operators, Eval Function, Complex Data Types, Piggy Bank, User Defined Function, Pig Vs Hive. Textbook 1: Chapter-9 (9.1-9.6,9.8), Chapter-10 (10.1 - 10.15, 10.22)	
Module-5	9 Hours
Spark and Big Data Analytics: Spark, Introduction to Data Analysis with Spark. Text, Web Content and Link Analytics: Introduction, Text Mining, Web Mining, Web Content and Web Usage Analytics, Page Rank, Structure of Web and Analysing a Web Graph. Textbook 2: Chapter-5 (5.2,5.3), Chapter-9 (9.1-9.4)	

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Acquire fundamental knowledge of big data concepts, characteristics, ecosystems, and analytical classifications.
CO2	Develop operational familiarity with Hadoop components including HDFS, YARN, and MapReduce for large-scale data handling.
CO3	Gain working competence in managing diverse datasets using NoSQL technologies with emphasis on MongoDB.
CO4	Build structured data processing solutions using Hive and Pig in distributed computing environments.
CO5	Formulate scalable analytics solutions using Spark along with text, web, and link analytics techniques.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.

Continuous and Comprehensive Evaluation (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
• The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE. • If any courses of 3 credits are of Integrated Course type, for such courses the method suggested for 4 credits IPCC shall be followed.			

Text Books:

1. Seema Acharya and Subhashini Chellappan “Big data and Analytics” Wiley India Publishers, 2nd Edition, 2019.
2. Rajkamal and Preeti Saxena, “Big Data Analytics, Introduction to Hadoop, Spark and Machine Learning”, McGraw Hill Publication, 2019.

Reference Books:

1. Adam Shook and Donald Mine, “MapReduce Design Patterns: Building Effective Algorithms and Analytics for Hadoop and Other Systems” - O'Reilly 2012.
2. Tom White, “Hadoop: The Definitive Guide” 4th Edition, O'reilly Media, 2015.
3. Thomas Erl, Wajid Khattak, and Paul Buhler, Big Data Fundamentals: Concepts, Drivers & Techniques, Pearson India Education Service Pvt. Ltd., 1st Edition, 2016
4. John D. Kelleher, Brian Mac Namee, Aoife D'Arcy -Fundamentals of Machine Learning for Predictive Data Analytics: Algorithms, Worked Examples, MIT Press 2020, 2nd Edition.

Web links and Video Lectures (e-Resources):

1. <https://www.youtube.com/watch?v=bAyrObl7TYE&list=PLEiEAq2VkUUJqp1kg5W1mo37urJQOdCZ>
2. <https://www.youtube.com/watch?v=VmO0QgPCbZY>
3. <https://www.youtube.com/watch?v=GG-VRm6XnNk>

Self-Study Topics:

1. Big data architecture patterns used in industry-scale systems.
2. Comparative study of batch processing and stream processing frameworks.
3. Cloud-based big data platforms and managed analytics services.
4. Data governance, privacy, and ethical considerations in big data systems.
5. Case studies on large-scale analytics applications in domains such as healthcare, finance, and social media.

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning:

1. Implement MongoDB based application to store big data for data processing and analyzing the results.

Alternate Assessment Methods:

1. Certifications (Skill-Based) -industry-recognized certifications (e.g. CISCO, NPTEL, Infosys Springboard).
2. Assignments / Problem Solving Sheets.
3. Quiz.
4. Mini Projects.
5. Group Activities / Peer Evaluation.
6. Presentations / Tech Talks.

ESTD : 2001
An Institute with a Difference

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VI			
Course Title:	DEEP LEARNING TECHNIQUES		
Course Code:	BCY613B	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	3	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Understand the fundamentals of deep learning. 2. Explore how Convolutional Neural Networks and RNNs function in making decisions. 3. Illustrate the strength and weaknesses of many popular deep learning approaches. 4. Introduce major deep learning algorithms, the problem settings, and their applications to solve real world problems.			
Module-1			9 Hours
Introduction: What is a Neural Network? The Human Brain, Models of a Neuron, Neural Networks Viewed as Directed Graphs, Feedback, Network Architectures, Rosenblatt's Perceptron: Introduction, Perceptron, The Perceptron Convergence Theorem, Relation Between the Perceptron and Bayes Classifier for a Gaussian Environment. Textbook 1: Introduction 1(1-6), Chapter-1(1.1-1.4)			
Module-2			9 Hours
Multilayer Perceptrons: Introduction, Batch Learning and On-Line Learning, The Back-Propagation Algorithm, XOR Problem, Heuristics for Making the Back- Propagation Algorithm Perform Better, Back Propagation and Differentiation. Textbook 1: Chapter-4(4.1,4.3, 4.4, 4.5,4.6,4.8)			
Module-3			9 Hours
Regularization for Deep Learning: Parameter Norm Penalties - L2 Parameter Regularization, Dataset Augmentation, Semi-Supervised Learning. Optimization for Training Deep Models: Challenges in Neural Network Optimization – Ill Conditioning, Basic Algorithms. Textbook 2: Chapter-7(7.1,7.4, 7.6) , Chapter-8(8.2,8.3)			
Module-4			9 Hours
Convolution neural networks: The Convolution Operation, Motivation, Pooling, Convolution and Pooling as an Infinitely Strong Prior, Variants of the Basic Convolution Function, Structured Outputs, Data Types, Efficient Convolution Algorithms, Convolutional Networks and the History of Deep Learning. Relational Operators, Eval Function, Complex Data Types, Piggy Bank, User Defined Function, Pig Vs Hive.			

Textbook 1: Chapter-9(9.1-9.6,9.8), Chapter-10 (10.1 - 10.15, 10.22)

Module-5

9 Hours

Sequence Modelling Recurrent and Recursive Nets: Unfolding Computational Graphs, Recurrent Neural Networks, Bidirectional RNNs, Encoder-Decoder Sequence-to- Sequence Architectures, Deep Recurrent Networks, Recursive Neural Networks, The Long Short-Term Memory and Other Gated RNNs.

Textbook 2: Chapter-10(10.1-10.6, 10.10)

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Acquire foundational knowledge of neural network structures and learning paradigms used in deep learning systems.
CO2	Develop insight into learning processes and statistical behaviors governing neural network training.
CO3	Gain proficiency in building deep learning models incorporating regularization strategies and convolution-based architectures.
CO4	Establish capability to work with sequential and time-dependent data using recurrent and recursive network models.
CO5	Formulate practical solutions for real-world problems using autoencoders and related deep learning frameworks.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Continuous and Comprehensive Evaluation (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks

SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
- The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE. - If any courses of 3 credits are of Integrated Course type, for such courses the method suggested for 4 credits IPCC shall be followed.			

Suggested Learning Resources:

Text Books:

1. Simon Haykin, Neural networks and Learning Machines, Third Edition, Pearson, 2016
2. Ian Goodfellow, Yoshua Bengio and Aaron Courville, Deep Learning, MIT Press, 2016.
<http://www.deeplearningbook.org/>

Web links and Video Lectures (e-Resources):

1. <https://www.youtube.com/watch?v=VyWAvY2CF9c>
2. <https://www.youtube.com/watch?v=7sB052Pz0sQ>
3. https://www.youtube.com/watch?v=Mubj_fqiAv8
4. <https://www.coursera.org/learn/neural-networks-deep-learning>

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning:

1. Mini projects (2 to 4 students) using Deep Learning concepts

Self-Study Topics:

1. Evolution of deep learning architectures and milestone developments
2. Transfer learning and fine-tuning of pre-trained deep learning models
3. Deep learning applications in computer vision, natural language processing, and speech recognition
4. Challenges related to model interpretability, fairness, and ethical use of deep learning

Alternate Assessment Methods:

1. Certifications (Skill-Based) -industry-recognized certifications (e.g. CISCO, NPTEL, Infosys Springboard).
2. Assignments / Problem Solving Sheets.
3. Quiz.
4. Mini Projects.
5. Group Activities / Peer Evaluation.
6. Presentations / Tech Talks.



ESTD : 2001

An Institute with a Difference

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VI			
Course Title:	BLOCKCHAIN TECHNOLOGY		
Course Code:	BCY613C	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	3	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Define and Explain the fundamentals of Blockchain. 2. Illustrate the technologies of blockchain. 3. Describe the models of blockchain. 4. Analyze and demonstrate the Ethereum.			
Module-1			9 Hours
Blockchain 101: Distributed systems, the history of blockchain and bitcoin, Blockchain-Variou technical definitions of blockchains, Generic elements of a blockchain, Benefits and limitations of Block chain technology, Tiers of blockchain technology, Features of a blockchain, types of blockchain technology, Consensus in blockchain, CAP theorem and blockchain.			
Textbook 1: Chapter- 1			
Module-2			9 Hours
Decentralization : Decentralization using blockchain, Methods of decentralization, Routes to decentralization, Decentralized organizations. Symmetric cryptography: Cryptographic primitives, symmetric cryptography Public key Cryptography: Asymmetric cryptography, Public and private keys Textbook 1: Chapter- 2, Chapter-3, Chapter-4			
Module-3			9 Hours
Bitcoin: Introducing Bitcoin, Transactions, The transaction life cycle, The transaction data structure, Types of transaction, The structure of a block , The structure of a block header, The genesis block. Bitcoin network and payments: The bitcoin network, Wallets, Bitcoin payments Smart Contracts: Definition, Ricardian contracts. Textbook 1: Chapter-5, Chapter-6, Chapter-9			
Module-4			9 Hours
Smart contracts: Introduction, Ethereum blockchain, components of the Ethereum ecosystem, ETC, ETH, EVM. Textbook 1: Chapter- 10			
Module-5			9 Hours
Hyperledger : Hyperledger, Hyperledger as a protocol, Fabric, Hyperledger Fabric, Sawtooth lake, Corda.			

Textbook 1: Chapter- 15

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Describe the Blockchain terminologies with its applications.
CO2	Elaborate on the decentralization techniques and cryptography.
CO3	Demonstrate the principles and methodologies used in Bitcoin.
CO4	Develop Ethereum Network, Wallets, Nodes, Smart contract and DApps.
CO5	Make use of Hyperledger in Blockchain Based Application Architecture

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Continuous and Comprehensive Evaluation (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
- The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE. If any courses of 3 credits are of Integrated Course type, for such courses the method suggested for 4 credits IPCC shall be followed.			

Text Books :

1. Mastering Blockchain - Distributed ledgers, decentralization and smart contracts explained, Imran Bashir, Packt Publishing Ltd, Second Edition, ISBN 978-1-78712-544-5, 2017

Reference Books :

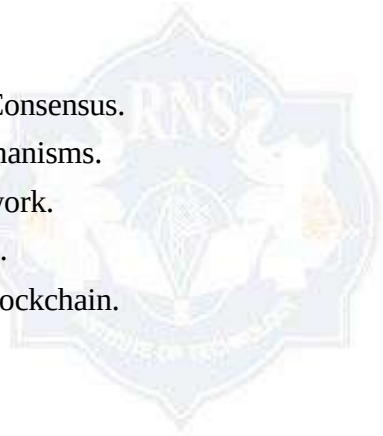
1. Bitcoin and Cryptocurrency Technologies, Arvind Narayanan, Joseph Bonneau, Edward Felten, 2016
2. Blockchain Basics: A Non-Technical Introduction in 25 Steps, Daniel Drescher, Apress, First Edition, 2017
3. Mastering Bitcoin: Unlocking Digital Cryptocurrencies, Andreas M. Antonopoulos, O'Reilly Media, First Edition, 2014

Web Links:

1. <https://nptel.ac.in/courses/106104220>
2. <https://www.geeksforgeeks.org/blockchain/>
3. <https://www.tutorialspoint.com/blockchain/index.htm>

Self-Study Topics:

1. Blockchain Architecture & Consensus.
2. Cryptographic Security Mechanisms.
3. Bitcoin Transactions & Network.
4. Ethereum & Smart Contracts.
5. Hyperledger & Enterprise Blockchain.



ESTD : 2001

An Institute with a Difference

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VI			
Course Title:	SURVEILLANCE AND VIDEO ANALYTICS		
Course Code:	BCY613D	CIE MARKS	50
(L :T : P) + SL	3:0:0	SEE MARKS	50
Credits:	3	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. To provide an understanding of the fundamental components and processes involved in video analytics. 2. To introduce various techniques for foreground extraction, segmentation, and object tracking. 3. To familiarize with different classifiers and learning methods used for video-based analysis. 4. To explore the role of video analytics in security applications such as human action recognition, behaviour analysis, and crowd monitoring. 5. To examine the use of video analytics in business intelligence and traffic monitoring for decision-making and assistance.			
Module-1			9 Hours
Video Analytic Components: Need for Video Analytics, Overview of video Analytics, Foreground extraction, feature extraction, classifier, Pre-processing, Edge detection, Smoothing, Feature space-PCA-FLD-SIFT features. Textbook: Chapter-1, Chapter-4			
Module-2			9 Hours
Foreground Extraction: Background estimation, Averaging, Gaussian Mixture Model, Optical Flow based, Image Segmentation, Region growing, Region splitting, Morphological operations, Erosion, Dilation, Tracking in a multiple camera environment. Textbook: Chapter-5, Chapter-6, Chapter -8,			
Module-3			9 Hours
Classifiers: Neural networks (back propagation), Deep learning networks, Fuzzy Classifier, Bayesian classifier, HMM based classifier. Textbook: Chapter-9, Chapter-11, Chapter-15			
Module-4			9 Hours
Video Analytics for Security: Abandoned object detection, Human behavioural analysis, Human action recognition, Perimeter security, Crowd analysis and prediction of crowd congestion. Textbook: Chapter -7, Chapter-23.			

Module-5	9 Hours
Video Analytics for Business Intelligence & Traffic Monitoring and Assistance: Video Analysis Action Recognition, Video based rendering, Context and scene understanding, Case Study: Surveillance - Advanced Driver Assistance System. Textbook: Chapter-17, Chapter-23 Textbook 1: Chapter-15	

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Explain the fundamental components and processes of video analytics.
CO2	Apply foreground extraction, segmentation, and tracking techniques to video data.
CO3	Compare and use classification approaches such as neural networks, deep learning models, fuzzy logic, Bayesian methods, and HMMs.
CO4	Evaluate video analytics approaches to recommend suitable solutions for security, business, and traffic applications.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Continuous and Comprehensive Evaluation (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.

- The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE.
- If any courses of 3 credits are of Integrated Course type, for such courses the method suggested for 4 credits IPCC shall be followed.

Textbooks:

1. Video Analytics — Dr. Lalit V. Patil, Dr. Anup Ingle, Dr. Sunita S. Dhotre, Nitin N. Sakhare, First Edition, Nirali Prakashan, 2023.

Reference Books:

1. Digital Video Processing - A. Murat Tekalp, 2nd Edition, Prentice Hall / Pearson, 2015.
2. Video-Based Surveillance Systems: Computer Vision and Distributed Processing — Edited by Graeme A. Jones, Nikos Paragios and Carlo S. Regazzoni; Publisher: Springer US (originally Kluwer / Springer), 1st Edition, 2001 (hardcover),
3. Applied Video Processing in Surveillance and Monitoring Systems — Nilanjan Dey, Amira Ashour & Suvojit Acharjee; Publisher: IGI Global (Information Science Reference, Hershey, PA, USA), first published 2016.

Web links and Video Lectures (e-Resources):

- YouTube: VideoAnalytics101
- Udemy: Video-analytics- An Introduction to Its Types, Advantages and Disadvantages

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System(CBCS) SEMESTER – VI			
Course Title:	CYBER SECURITY AND MANAGEMENT, COMPLIANCE AND GOVERNANCE		
Course Code:	BCY613E	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	3	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Understand the fundamentals of Governance, Risk, and Compliance (GRC) and their role in strategic cyber security planning. 2. Explore risk management life cycles, NIST frameworks, and best practices for cyber security program management. 3. Develop proficiency in utilizing cyber security metrics, frameworks, and risk assessment methodologies. 4. Analyze and apply cyber security controls, architectures, and risk mitigation strategies to secure organizational assets. 5. Examine emerging trends in cyber security, including cloud security, AI-powered solutions, and the impact of quantum computing.			
Module-1			9 Hours
Governance, Risk Management, and Compliance: Understanding GRC and its intersection. GRC frameworks, standards, tools, and culture. Role of GRC in strategic planning. Cybersecurity Program and Project Management: Fundamentals of program and project management. Agile project management in cybersecurity. Communication and collaboration in cybersecurity projects. Textbook 1: Chapter-1, Chapter-4			
Module-2			9 Hours
Risk Management: Understanding risk management life cycle. Third party risk management and compliance expectations. Monitoring, reporting, and risk approvals. NIST Risk Management Framework (RMF): Steps in the NIST RMF authorization process. Integrating NIST RMF into organizational risk management. Challenges and best practices in implementing RMF. Textbook 1: Chapter-7, Chapter-8			
Module-3			9 Hours
Cybersecurity Metrics: KPIs and KRIs in cybersecurity. Role of metrics in decision making, compliance, and strategy. Risk Assessments: Conducting cybersecurity risk assessments. NIST, FFIEC approaches, and best practices. Cybersecurity Frameworks: ISO/IEC 27001, COBIT, CMMC, and PCI DSS. Comparing and			

integrating multiple frameworks. Future trends in cybersecurity frameworks.

Textbook 1: Chapter-9, Chapter-10, Chapter-12

Module-4

9 Hours

NIST SP 80053: Overview and structure of NIST SP 80053 controls. Control families and their applications.

Cybersecurity Architecture: Components and layers of cybersecurity architecture. Security reference models and adapting to emerging threats.

Risk Mitigation: Basics of risk mitigation and security controls. Policies, user security controls, and physical security measures.

Textbook 1: Chapter-13, Chapter-25, Chapter-26

Module-5

9 Hours

Cloud Security: Cloud computing services, challenges, and best practices. Security tools, techniques, and future trends in cloud security.

Artificial Intelligence in Cybersecurity: AI powered cybersecurity solutions. CISO's AI preparation checklist and its role in cyber defense.

Quantum Computing: Quantum cryptography and its impact on cybersecurity. Strategic and security implications of quantum computing.

Textbook 1: Chapter-27, Chapter-28, Chapter-29

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Implement GRC principles and frameworks to enhance organizational cybersecurity and compliance.
CO2	Apply risk management strategies and integrate NIST RMF processes into organizational workflows.
CO3	Utilize metrics, assessments, and international frameworks like ISO/IEC 27001 and COBIT for effective cyber security decision-making.
CO4	Design and evaluate cyber security architectures and controls to mitigate risks and address evolving threats.
CO5	Assess emerging cyber security technologies and trends, leveraging AI and quantum computing to address future challenges.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Alternate Assessment (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.

Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
The minimum marks to be secured in CIE are 20 out of allotted 50 marks to appear for SEE, with minimum 40 % scored in every component of CIE.			

Textbooks:

1. J. Edwards and G. Weaver, The Cybersecurity Guide to Governance, Risk, and Compliance. Wiley, May 2024.

Reference Books:

1. P. Trim and Y.-I. Lee, Cyber Security Management: A Governance, Risk and Compliance Framework, 1st ed. Routledge, 2014.

Self - Study topics:

1. Cybersecurity Governance Frameworks.
Study the principles of cybersecurity governance and compare widely used governance frameworks such as COBIT, ISO/IEC 38500, and NIST Cybersecurity Framework. Understand their role in aligning cybersecurity with organizational objectives.
2. Risk Assessment and Risk Register.
Learn the process of identifying, analyzing, and evaluating cybersecurity risks. Prepare a simple risk register for a real-world organization by identifying assets, threats, vulnerabilities, and appropriate mitigation strategies.
3. Cybersecurity Compliance Standards
Explore the requirements and objectives of major cybersecurity standards and regulations including:
 - a. ISO/IEC 27001
 - b. NIST Risk Management Framework (RMF)
 - c. PCI DSS
 - d. General Data Protection Regulation (GDPR)
4. Security Controls and Zero Trust Architecture
Study different categories of security controls (Administrative, Technical, and Physical) and understand the principles of Zero Trust Architecture, including identity verification, least privilege, and continuous monitoring.
5. Emerging Trends in Cybersecurity
Investigate recent advancements in cybersecurity with a focus on:
 - a. Artificial Intelligence in Cybersecurity

- b. Cloud Security Best Practices
- c. Quantum Computing and Post-Quantum Cryptography
- d. Security Automation and Threat Intelligence

Alternate Assessment Methods:

1. **Assignments**
2. **Quiz**
3. **Case Study Discussion**
4. **Group Activities / Peer Evaluation**
5. **Presentations / Tech Talks**



ESTD : 2001

An Institute with a Difference

6TH Semester Open Elective Courses (For Other Branches)

ESTD : 2001

An Institute with a Difference

B.E. (CSE and Allied Branches) Outcome Based Education (OBE) and Choice Based Credit System(CBCS) SEMESTER – VI			
Course Title:	INTRODUCTION TO DATA STRUCTURES		
Course Code:	BCS654A	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	3	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> - Introduce elementary data structures. - Analyze Linear Data Structures: Stack, Queues, Linked list. - Analyze Non-Linear Data Structures: Trees, graphs. - Assess appropriate data structure during program development/Problem Solving.			
Module-1			9 Hours
Introduction to arrays and pointer: Introduction, Linear Arrays, Representation of Linear Arrays in Memory, Traversing Linear Arrays, Inserting and Deleting, Pointers: Pointer Arrays. Strings: Introduction, Reading and writing Strings, Operations on strings, Arrays of strings, Pointers and String. Textbook 2: Chapter-4 (4.1 - 4.5,4.10) Text book 1: Chapter-4 (4.1-4.4)			
Module-2			9 Hours
Structures and unions: Introduction, Nested Structure, Array of Structure, Self-referential Structures, Unions. Stacks: Introduction, Array representation of stacks, Operations on Stack-Push, Pop and Peek operation. Textbook 1: Chapter-5 (5.1 - 5.3,5.5,5.6), Chapter-7 (7.1 - 7.3)			
Module-3			9 Hours
Queue: Introduction, Array representation of Queues, Linked Representation of Queues, Types of Queue-Circular Queue and Deques. Linked List: Introduction, singly linked list, Circular linked list Textbook 1: Chapter-8 (8.1.8.2,8.4), Chapter-6 (6.1 - 6.3)			
Module-4			9 Hours
Linked List (Contd.): Doubly linked List-Insert and Delete operation. Trees: Introduction, Types of Trees, create a Binary Tree from a General Tree, Traversing a Binary tree, Application of Trees. Textbook 1: Chapter-6 (6.4), Chapter-9 (9.1 - 9.4,9.6)			
Module-5			9 Hours
Graph: Introduction, Graph Terminology, Representations of Graphs, Graph Traversal Algorithm, Application of Graph. Searching and Sorting- Introduction to searching, Linear Search, Binary Search, Bubble Sort, Insertion Sort. Textbook 1: Chapter-13 (13.1-13.2,13.5,13.6,13.9), Chapter-14 (14.1-14.3,14.7,14.8)			

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Implement fundamental data structures using arrays, pointers, and structure.
CO2	Apply stacks and queues to evaluate expressions and solve linear data structure problems.
CO3	Implement memory-efficient programs using singly and circular linked lists.
CO4	Analyze tree and graph structures to model hierarchical and network relationships.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks
Continuous and Comprehensive Evaluation (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be before 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
The minimum marks to be secured in CIE are 20 (40%) out of allotted 50 marks to appear for SEE.			

Textbooks

1. Reema Thareja, Data Structure using C, 3rd Edition, OXFORD University Press, 2023
2. Seymour Lipschutz, Data Structures Schaum's Outlines, Revised 1st Ed, McGraw Hill, 2014.

Reference Books:

1. Ellis Horowitz and Sartaj Sahni, Fundamentals of Data Structures in C, 2nd Ed, Universities Press, 2014.
2. E Bala Guruswamy, C Programming and data structures, 4th Edition, McGraw Hill, 2007.

Web links and Video Lectures (e-Resources):

1. https://youtu.be/S47aSEqm_0I?si=34alu47wCWGdsxwN
2. <https://ds2-iiith.vlabs.ac.in/exp/selection-sort/index.html>
3. <https://ds1-iiith.vlabs.ac.in/exp/stacks-queues/index.html>
4. <https://ds1-iiith.vlabs.ac.in/exp/linked-list/basics/overview.html>
5. <https://ds1-iiith.vlabs.ac.in/List%20of%20experiments.html>
6. <https://ds1-iiith.vlabs.ac.in/exp/tree-traversal/index.html>
7. <https://ds1-iiith.vlabs.ac.in/exp/tree-traversal/depth-first%20traversal/dft-practice.html>
8. https://onlinecourses-archive.nptel.ac.in/noc18_cs25/preview

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning:

1. Demonstration of projects developed using Linear/Non-linear data structures.

Self-Study Topics:

Applications of Data Structures

- Data structures in operating systems.
- Data structures in databases.
- Data structures in real-world problems.

Sorting Techniques

- Selection sort.
- Merge Sort.
- Quick Sort.

Advanced Tree Structure

AVL Trees, Red-Black Trees, B-Trees, B+ Trees.

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VI			
Course Title:	FUNDAMENTALS OF OPERATING SYSTEMS		
Course Code:	BCY654B	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	3	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1 Understand the fundamental concepts and architecture of operating systems, including system structure, services, and system calls. 2 Analyse and apply concepts of process, thread, and CPU scheduling, along with inter- process communication and synchronization techniques. 3 Explain and evaluate memory management strategies, including paging, segmentation, and virtual memory techniques. 4 Demonstrate knowledge of file systems, storage structures, and protection mechanisms, and use relevant system-level commands and APIs for managing OS resources			
Module-1			9 Hours
Introduction: What operating systems do, Computer System organization, Computer System architecture, Operating System operations, Resource Management. Operating System Structures: Operating System Services, User - Operating System interface, System calls; System services, Operating system design and implementation, Operating System structure. Textbook 1: Chapter-1 (1.1-1.5), Chapter-2 (2.1-2.4, 2.7-2.8)			
Module-2			9 Hours
Processes: Process concept; Process scheduling; Operations on processes; Inter process communication. Threads & Concurrency: Overview, Multithreading models Thread Libraries Threading issues. CPU Scheduling: Basic concepts, Scheduling Criteria, Scheduling Algorithms, Multiple-processor scheduling. Textbook 1: Chapter-3 (3.1-3.4), Chapter-4 (4.1,4.3,4.4,4.6), Chapter-5 (5.1 -5.3,5.5)			
Module-3			9 Hours
Synchronization Tools: Background, The critical section problem, Peterson's solution, Hardware Support for Synchronization Mutex Locks, Semaphores. Synchronization Examples: Classical problems of synchronization. Deadlocks: System model, Deadlock characterization, Methods for handling deadlocks, Deadlock prevention, Deadlock avoidance, Deadlock detection, recovery from deadlock. Textbook 1: Chapter-6 (6.1-6.6), Chapter-7 (7.1), Chapter-8 (8.1,8.3 -8.8)			

Module-4	9 Hours
Main Memory: Background, Contiguous memory allocation, Paging, Structure of page table, Swapping. Virtual Memory: Background, Demand paging, Copy-on-write, Page replacement, Allocation of frames, Thrashing. Textbook 1: Chapter -9 (9.1-9.5), Chapter-10 (10.1-10.6)	
Module-5	9 Hours
File System Interface: File concept, Access methods, Directory structure File system Implementation: File system structure, File system operations, Directory implementation, Allocation methods, Free space management. Protection: Goals of protection, Principles of protection, Domain of protection, Access matrix. Textbook 1: Chapter-13 (13.1-13.3) , Chapter-14 (14.1, 14.5), Chapter-17 (17.17.2,17.4,17.5)	

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Interpret and explain the interactions among operating system components, including kernel functions, system calls, and user interfaces, within typical system operations.
CO2	Apply CPU Scheduling algorithms and process synchronization mechanisms to manage concurrent execution.
CO3	Analyze memory management techniques such as paging and segmentation to optimize memory utilization.
CO4	Evaluate file system structures and I/O management strategies to enhance overall system performance.
CO5	Simulate key operating system functionalities and system-level tasks using software tools and utilities.

ASSESSMENT AND EVALUATION (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.

Alternate Assessment (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE+SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
The minimum marks to be secured in CIE are 20 out of allotted 50 marks to appear for SEE, with minimum 40 % scored in every component of CIE.			

Textbooks:

1. Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, Operating System Concepts, 9th Edition, Wiley-India, 2015.

Reference Books:

1. P.C.P. Bhatt, An Introduction to Operating Systems: Concepts and Practice, 4th Edition, PHI(EEE), 2015.
2. William Stallings, Operating Systems: Internals and Design Principles, 6th Edition, Pearson.
3. A.S. Tanenbaum, H. Bos, 2014, Modern Operating Systems, 4th Edition, Prentice-Hall of India, New Delhi.

Web links:

1. <https://pages.cs.wisc.edu/~remzi/OSTEP/>
2. <https://www.geeksforgeeks.org/operating-systems/>
3. https://www.tutorialspoint.com/operating_system/index.htm
4. <https://www.scaler.com/topics/operating-system/>
5. <https://www.youtube.com/watch?v=yK1uBHPdp30>
6. <https://www.youtube.com/watch?app=desktop&t=1s&v=dOiA2nNJpc0>

Self-Study Topics:

1. Virtual Machines: Study the concept of virtualization, including the architecture and functionality of virtual machines (VMs), and understand how VMs help in efficient resource utilization and system isolation.

2. Basic Linux Commands: Gain hands-on experience with essential Linux terminal commands used for file management, user permissions, process control, and system monitoring.
3. Multithreading Demonstration using Programming Languages: Implement and compare multithreading concepts using:
 - a. Java – via Thread class and Runnable interface
 - b. Python – using the threading module
4. C Programming – using POSIX threads (pthreads) Overview of Different Operating Systems: Compare architecture, scheduling, memory management, and file systems across these OS types: Linux, Windows, Unix, Android, MacOS, iOS, RTOS, Chrome OS, Solaris, Haiku OS, TinyOS



ESTD : 2001

An Institute with a Difference

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System(CBCS) SEMESTER – VI			
Course Title:	INTRODUCTION TO DBMS		
Course Code:	BCI654C	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	3	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Provide a strong foundation in database concepts, technology, and practice. 2. Practice SQL programming through a variety of database problems. 3. Understand the relational database design principles. 4. Apply normalization techniques to create well-structured relational database schemas.			
Module-1			9 Hours
Introduction to Databases: Introduction, Characteristics of database approach, Actors on the Scene, Workers behind the Scene, Advantages of using the DBMS approach, Representing Complex Relationships among Data. Overview of Database Languages and Architectures: Data Models, Schemas, and Instances. Three schema architecture and data independence, database languages, and interfaces, The Database System environment, Centralized and Client/Server Architectures for DBMSs, Classification of Database Management Systems. Textbook 1: Chapter-1 (1.1-1.6.7), Chapter-2 (2.1-2.4)			
Module-2			9 Hours
Conceptual Data Modeling using Entities and Relationships: Entity Types, Entity Sets, Attributes, and Keys Relationship Types, Relationship Sets, Roles, and Structural Constraints, Weak Entity Types, Refining the ER Design for the COMPANY Database, ER Diagrams, Naming Conventions, and Design Issues, Relationship Types of Degree Higher than Two, Another Example: A UNIVERSITY Database. Textbook 1: Chapter-3 (3.3-3.7, 3.9-3.10)			
Module-3			9 Hours
Mapping Conceptual Design into a Logical Design: Relational Database Design using ER-to-Relational mapping. Relational Model: Relational Model Concepts, Relational Model Constraints and relational database schemas, Update operations, transactions, and dealing with constraint violations. Textbook 1: Chapter-9 (9.1-9.2), Chapter-5 (5.1-5.3)			
Module-4			9 Hours
Relational Algebra: Unary Relational Operations: SELECT and PROJECT, Relational Algebra Operations from Set Theory, Binary Relational Operations: JOIN and DIVISION. additional relational operations (aggregate, grouping, etc.) Examples of Queries in relational algebra. SQL: SQL data definition and data types, Schema change statements in SQL, specifying constraints in			

SQL, retrieval queries in SQL, INSERT, DELETE, and UPDATE statements in SQL, Additional features of SQL

Textbook 1: Chapter-9 (8.1-8.5), Chapter-6 (6.1-6.5)

Module-5

9 Hours

Basics of Functional Dependencies and Normalization for Relational Databases: Informal design guidelines for relation schema, Functional Dependencies, Normal Forms Based on Primary Keys, General Definitions of Second and Third Normal Forms, Boyce-Codd Normal Form, Multivalued Dependency and Fourth Normal Form, Join Dependencies and Fifth Normal Form.

Textbook 1: Chapter-14 (14.1 to 14.7)

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Understand the fundamental concepts, architecture, and components of Database Management Systems (DBMS).
CO2	Understand real-world problem scenarios by designing Entity-Relationship (ER) models.
CO3	Apply ER-to-relational mapping techniques to transform conceptual designs into logical database schemas. Analyze and use SQL queries for efficient database definition, creation, and data manipulation..
CO4	Apply relational algebra operations to formulate SQL statements for DDL and DML.
CO5	Evaluate relational schemas using functional dependencies and apply normalization to eliminate anomalies.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Continuous and Comprehensive Evaluation (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.

CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE.			

Textbooks:

1. R. Elmasri and S. B. Navathe, Fundamentals of Database Systems, 7th Edition. Boston, MA: Pearson, 2017.

Reference Books:

1. R. Ramakrishnan and J. Gehrke, Database Management Systems, 3rd Edition. New York, NY: McGraw-Hill, 2014.
2. C. J. Date, A. Kannan, and S. Swamynathan, An Introduction to Database Systems, 8th Edition. Noida, India: Pearson, 2006.

Self – Study Topics:

- 1) Advanced Queries: Specifying constraints as assertions and action triggers, Views.
- 2) NOSQL Databases, Document-Based NOSQL Systems and MongoDB.
- 3) Column-Based NOSQL Systems and Graph Databases.
- 4) Transaction Processing, Concurrency Control, and Recovery.

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VI			
Course Title:	FOUNDATIONS OF DATA SCIENCE		
Course Code:	BCD654D	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	03	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Understand the fundamental concepts of data science. 2. Explain statistical and probabilistic concepts for data-driven decision making. 3. Apply the data science methodology and analytics life cycle to solve real-world problems. 4. Analyse and implement core machine learning techniques. 5. Explore and apply text mining and basic natural language processing techniques			
Module-1			9 Hours
Importance of Data Science: Importance of Data Science, Need for Data Science, What Is Data Science, Data Science Process, Business Intelligence and Data Science, Prerequisites for a Data Scientist, Components of Data Science, Tools and Skills Needed. Data Science Tool: Basics of Python for Data Science, Python Libraries: DataFrame Manipulation with pandas and NumPy Textbook 1: Chapter- 1 (1.1-1.8), Chapter- 7 (7.1-7.2)			
Module-2			9 Hours
Statistics and Probability: Data Types, Variable Types, Statistics, Sampling Techniques and Probability, Information Gain and Entropy, Probability Theory, Probability Types, Probability Distribution Functions, Bayes' Theorem, Inferential Statistics. Textbook 1: Chapter- 2 (2.1-2.11)			
Module-3			9 Hours
Data Science Methodology: Analytics for Data Science, Examples of Data Analytics, Data Analytics Life Cycle: Data Discovery, Data Preparation, Model Planning, Model Building, Communicate Results, operationalization. Textbook 1: Chapter - 4 (4.1-4.4)			
Module-4			9 Hours
Data Science Methods and Machine Learning: Regression Analysis, Linear Regression, Logistic regression, Multimodal logistic regression, Time-series model, Machine Learning: Decision trees, naive bayes, support vector, machines, nearest neighbour learning, clustering, Confusion matrix Textbook 1: Chapter- 5 (5.1-5.3)			

Module-5	9 Hours
Data Analysis and Text Mining: Text Analytics: Text analytics subtasks, Cleaning and parsing, searching and retrieval, Text mining, Part-of-speech tagging, Stemming, Lemmatization, Basic text analysis steps, Introduction to Natural Language Processing.	
Textbook 1: Chapter-6 (6.1-6.4)	

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Understand the fundamental concepts of Data Science, including its importance, process, components, and the role of SQL in data analysis and decision-making.
CO2	Apply statistical methods, probability distributions, and Bayes' Theorem to analyze data types and calculate metrics like Entropy and Information Gain.
CO3	Execute the Data Analytics Life Cycle, from initial data discovery and preparation to model building and the operationalization of results.
CO4	Analyze model performance using evaluation metrics such as the confusion matrix and interpret the results to assess predictive accuracy.
CO5	Demonstrate the ability to use basic Natural Language Processing (NLP) techniques and tools for real-world text analysis applications.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Continuous and Comprehensive Evaluation (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.

The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE.

Textbooks:

1. **Sanjeev J. Wagh, Manisha S. Bhende and Anuradha D. Thakare**, Fundamentals of Data Science, 1st Edition, CRC press, 2021.

Reference Books:

1. **Gareth James, Daniela Witten, Trevor Hastie, Robert Tibshirani**, An Introduction to Statistical Learning: with Applications in R, Springer, 1st edition, 2013
2. **Peter Bruce, Andrew Bruce**, Practical Statistics for Data Scientists, 2017, O'Reilly
3. **Cathy O Neil, Rachel Schutt**, Doing Data Science-Straight Talk from the Frontline, O'Reilly Media, 2013.

Web links:

1. <https://www.udemy.com/course/data-science-for-the-beginner/?couponCode=PMNVD2025>
2. <https://www.oreilly.com/library/view/doing-data-science/9781449363871/toc01.html>
3. <https://docs.python.org/3/tutorial/>
4. nptel.ac.in/courses/106106212

Self-Study Topics:

1. Difference between Data Science vs Business Intelligence vs AI
2. Central Limit Theorem (intuitive understanding)
3. CRISP-DM vs Data Analytics Life Cycle
4. Comparison of ML algorithms and analyze datasets.

B.E. (Computer Science and Engineering (Cyber Security))
Outcome Based Education (OBE) and Choice Based Credit System (CBCS)
SEMESTER – VI

Course Title:	DIGITAL FORENSICS LABORATORY		
Course Code:	BCYL606	CIE MARKS	50
(L :T : P) + SL	0:0:2	SEE MARKS	50
Credits:	01	EXAM HOURS	3

COURSE LEARNING OBJECTIVES:

The purpose of the course is to facilitate the learner to:

1. Understand the fundamental concepts, principles, and processes of digital forensics and investigation.
2. Apply forensic tools such as Autopsy, FTK, EnCase, and Sleuth Kit to perform digital evidence analysis.
3. Recover, analyze, and interpret digital evidence including deleted files, system activity, and user artifacts.
4. Examine and extract artifacts from USB devices, browsers, emails, and metadata for investigative purposes.
5. Demonstrate techniques for data hiding, file comparison, and forensic reporting to support cyber investigations.

SL No.	Experiments
1	Study of Computer Forensics & Investigation Tools Objective: To understand the fundamentals of digital forensics and various forensic tools used in investigations. Tools: EnCase, FTK, Autopsy, Sleuth Kit, Kali Linux Tools
2	Live Forensics Case Investigation using Autopsy Objective: To perform live forensic analysis on a system using Autopsy. Tools: Autopsy
3	Recovery of Deleted Files Objective: To recover deleted files from a storage device using forensic tools. Tools: FTK Imager, RecoverMyFiles
4	USB Forensics – Last Connected USB Detection Objective: To identify previously connected USB devices on a system. Tools: USBDeview
5	Viewing Last System Activity Objective: To analyze and view recent user and system activities Tools: LastActivityView

6	Browser Artifact Extraction Objective: To extract browser history, cache, cookies, and download artifacts. Tools: ChromeHistoryView, ChromeCacheView, IEHistoryView, IECacheView
7	File Comparison for Investigation Objective: To compare two files and identify differences for forensic analysis. Tools: Compare It
8	Email Evidence Collection Objective: To extract email evidence from a victim system using memory analysis. Tools: DumpIt, Bulk Extractor
9	Data Hiding and Extraction using Command Prompt Objective: To hide and extract files within image/audio files using command-line techniques. Tools: Command Prompt (copy/b), WinRAR
10	EXIF Metadata Extraction Objective: To extract and analyze EXIF metadata from image files. Tools: ExifReader

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Describe the fundamental concepts, principles, and processes of digital forensics and investigation.
CO2	Apply appropriate forensic tools to collect, analyze, and preserve digital evidence from various sources.
CO3	Analyze system activities and digital artifacts such as deleted files, browser data, USB traces, and emails for investigation.
CO4	Demonstrate techniques for data recovery, metadata extraction, file comparison, and preparation of forensic reports.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE Practical (A)	30	12	Marks awarded for Weekly Conduction of Experiments and Submission of Laboratory records, scaled to 30 marks
CIE Practical Test (B)	20	8	Average of marks of Two tests, each conducted for 100 marks covering all experiments, scaled to 20.

Total CIE Practical(A+B)	50	20	Sum of Marks of Experiments, Record and Test shall be CIE marks awarded for a maximum of 50.
SEE (C)	50	20	SEE is a lab exam, conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C .
The minimum marks to be secured in CIE are 20 out of allotted 50 marks to appear for SEE, with minimum 40 % scored in every component of CIE.			

Textbooks:

1. B. Nelson, A. Phillips, and C. Steuart, *Guide to Computer Forensics and Investigations*, 6th ed. Boston, MA, USA: Cengage Learning, 2019.
2. E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd ed. London, U.K.: Academic Press, 2011.
3. K. Mandia, M. Pepe, and J. Luttgens, *Incident Response and Computer Forensics*, 3rd ed. New York, NY, USA: McGraw-Hill, 2014.

Reference Books:

1. EC-Council, *Computer Forensics: Investigating Network Intrusions and Cybercrime*. Clifton Park, NY, USA: Delmar Cengage Learning, 2010.
2. Carrier, *File System Forensic Analysis*. Boston, MA, USA: Addison-Wesley, 2005.
3. Altheide and H. Carvey, *Digital Forensics with Open Source Tools*. Waltham, MA, USA: Syngress, 2011.

Online Resources:

1. National Institute of Standards and Technology, “Guide to Integrating Forensic Techniques into Incident Response,” Special Publication 800-86.
2. SANS Institute, Digital Forensics Resources and Whitepapers.
3. OWASP, Security Documentation and Resources.

Tools Documentation:

1. Autopsy Official Documentation.
2. FTK Imager User Guide.
3. EnCase Forensic Tool Documentation.
4. Sleuth Kit Documentation

Datasets for Practice

1. Digital Corpora, Digital Forensic Datasets.
2. CFReDS, NIST Forensic Data Repository.



ESTD : 2001

An Institute with a Difference

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VI			
Course Title	INDUSTRIAL CYBER SECURITY		
Course Code	BCYL657A	CIE MARKS	50
L: T : P	0:0:2	SEE MARKS	50
Credits	01	EXAM HOURS	3
Course Learning Objectives: <i>The purpose of the course is to facilitate the learner to:</i> 1. Demonstrate techniques for analyzing network traffic and detecting intrusions. 2. Understand security mechanisms within ICS and PLC environments. 3. Gain knowledge of configuring firewall and web system settings. 4. Perform incident response simulations and assess potential risks.			
SL No.	Experiments		
1	Network Traffic Analysis in ICS/SCADA Systems Scenario: A manufacturing plant experiences intermittent communication issues between its SCADA system and field devices. IT suspects abnormal traffic patterns are overwhelming the network. Objective: Use Wireshark to capture and analyze network traffic to detect anomalies such as unauthorized Modbus commands or excessive network scanning. Tools: Wireshark Deliverables: A detailed report of the traffic analysis, highlighting malicious or unusual traffic patterns and recommendations for mitigation.		
2	Configuring and Testing an Intrusion Detection System (IDS) Scenario: An oil refinery has deployed an IDS in its control room but has not tested its effectiveness. Simulated attacks are needed to evaluate the IDS's detection capability. Objective: Configure Snort with custom rules to detect unauthorized login attempts, PLC command injections, or DoS attacks on the refinery's network. Tools: Snort Deliverables: A configured IDS, attack simulation results, and a performance evaluation report.		
3	Vulnerability Assessment of a Simulated ICS Network Scenario: A power plant is transitioning to a new ICS network. The cybersecurity team must perform a vulnerability assessment before the network goes live. Objective: Scan the simulated ICS network for open ports, outdated software, and misconfigurations. Tools: Nmap, OpenVAS Deliverables: A vulnerability assessment report listing critical issues, potential exploitation risks, and suggested fixes.		

4	Securing a PLC Environment Scenario: A water treatment facility reports unauthorized access to its PLCs, leading to erroneous water treatment settings. Students are tasked to secure the PLC environment. Objective: Simulate unauthorized PLC access, implement secure configurations, and monitor PLC traffic for anomalies. Tools: OpenPLC, Wireshark Deliverables: A secured PLC configuration and a log of identified unauthorized commands.
5	Simulating Cyber Attacks on ICS and Designing Defenses Scenario: An attacker compromises an engineering workstation and uses it to issue malicious commands to ICS devices. Students must simulate this attack and propose defenses. Objective: Perform simulated attacks such as PLC logic manipulation and denial-of-service, then implement measures like firewall rules or intrusion prevention systems. Tools: Metasploit Framework, Security Onion Deliverables: A report describing the attack, its impact, and the defense mechanisms implemented.
6	Web Application Security for Industrial Systems Scenario: The web-based interface of a chemical plant's ICS is suspected to have vulnerabilities that attackers could exploit to alter chemical mix ratios. Objective: Conduct a security assessment of the web interface for vulnerabilities like SQL injection, cross-site scripting, and improper authentication mechanisms. Tools: OWASP ZAP Deliverables: A vulnerability scan report with remediation recommendations for the ICS web application.
7	Securing ICS Protocols and Communication Channels Scenario: A logistics company faces unauthorized Modbus/TCP communication between its control system and conveyor belt motors, disrupting operations. Objective: Configure secure communication using encryption and analyze normal vs. malicious protocol traffic. Tools: OpenSSL, Wireshark Deliverables: Secured Modbus/TCP communication setup and a comparative analysis of traffic logs.
8	Incident Response Simulation in an ICS Environment Scenario: A simulated ransomware attack encrypts critical ICS files at a gas distribution station. Students act as the incident response team. Objective: Detect the ransomware, isolate affected systems, and recover operations using backup and monitoring tools. Tools: Security Onion, GRR Deliverables: An incident response report, including root cause analysis and recovery steps.

9	Firewall and Access Control Configuration for ICS Scenario: An unauthorized laptop connects to the ICS network at a steel factory and issues shutdown commands to operational systems. Objective: Implement access control policies and configure firewalls to block unauthorized devices and restrict communication to trusted sources. Tools: pfSense, ModSecurity Deliverables: Firewall and access control configuration files, along with a report on unauthorized device mitigation.
10	Risk Assessment and Mitigation Planning for ICS Scenario: A renewable energy plant wants to evaluate cybersecurity risks before connecting its wind turbines to the grid. Objective: Conduct a risk assessment considering hardware vulnerabilities, communication protocols, and environmental factors. Propose a mitigation plan. Tools: Custom scripts, risk assessment frameworks Deliverables: A comprehensive risk assessment report and a prioritized mitigation strategy.

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Perform network traffic analysis and identify potential intrusions.
CO2	Apply security practices within ICS and PLC environments.
CO3	Create and manage configuration files for firewall and web systems.
CO4	Conduct risk assessment and simulate incident response in ICS environments.
CO5	Evaluate system vulnerabilities and recommend appropriate mitigation strategies.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE Practical (A)	30	-	Marks awarded for Weekly Conduction of Experiments and Submission of Laboratory records, scaled to 30 marks.
CIE Practical Test (B)	20	-	Average of marks of Two tests, each conducted for 100 marks covering all experiments, scaled to 20.
Total CIE Practical (A+B)	50	20	Sum of Marks of Experiments, Record and Test shall be CIE marks awarded for a maximum of 50.

SEE (C)	50	20	SEE is a lab exam, conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE.			

Suggested Learning Resources:

Textbooks:

1. P. Ackerman, Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems. Packt Publishing, 2021.
2. T. Macaulay and B. Singer, Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS. CRC Press, 2012.

Reference Books:

1. C. Bodungen, B. Singer, A. Shbeeb, K. Wilhoit, and S. Hilt, Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions. McGraw-Hill, 2017.
2. P. A. Craig Jr., Practical Industrial Cybersecurity: IT and OT Convergence. Wiley, 2021.
3. Ginter, SCADA Security: What's Broken and How to Fix It. Waterfall Security Solutions, 2016.

Online Resources:

- National Institute of Standards and Technology, Guide to Industrial Control Systems (ICS) Security (SP 800-82).
- SANS Institute, ICS/SCADA Security Resources and Whitepapers.
- OWASP, Web Application Security Documentation (for ICS web interfaces).
- CISA, ICS Cybersecurity Guidelines and Alerts.
- MITRE, ATT&CK for ICS Knowledge Base.

Tools Documentation:

- Wireshark Official Documentation.
- Snort User Manual and Rule Writing Guide.
- OpenPLC Documentation.
- Security Onion Documentation.
- OWASP ZAP User Guide.
- pfSense Configuration Guide.
- Nmap Reference Guide.
- OpenVAS Documentation.

Datasets for Practice

- Digital Bond, SCADA/ICS Security Datasets.
- ICS-CERT, Incident Reports and Malware Analysis Data.
- Stratosphere IPS, Malware and Network Traffic Datasets.
- UNSW Canberra, UNSW-NB15 Intrusion Detection Dataset.
- Canadian Institute for Cybersecurity, CICIDS Network Security Dataset.



ESTD : 2001

An Institute with a Difference

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VI			
Course Title	REACT		
Course Code	BCYL657B	CIE MARKS	50
L: T : P	0:0:2	SEE MARKS	50
Credits	01	EXAM HOURS	3
Course Learning Objectives: <i>The purpose of the course is to facilitate the learner to:</i> 1. Enable students to develop React applications utilizing functional and class-based components, effectively managing state with hooks and lifecycle methods . 2. Introduce, how to pass data dynamically between parent and child components using props, ensuring modular and reusable component design. 3. Create dynamic and responsive applications, integrating forms, validation, task management systems, and styled components. 4. Use React Router for navigation, external API integration for dynamic data handling, and CSS styling techniques for modern UI/UX design.			
SL No.	Experiments		
1	Use create-react-app to set up a new project. Edit the App.js file to include a stateful component with use State.		
2	Develop a React application that demonstrates the use of props to pass data from a parent component to child components. The application should include the parent component named App that serves as the central container for the application. Create two separate child components, Header: Displays the application title or heading. Footer: Displays additional information, such as copyright details or a tagline. Pass data (e.g., title, tagline, or copyright information) from the App component to the Header and Footer components using props. Ensure that the content displayed in the Header and Footer components is dynamically updated based on the data received from the parent component.		
3	Create a Counter Application using React that demonstrates state management with the use State hook. Display the current value of the counter prominently on the screen. Add buttons to increase and decrease the counter value. Ensure the counter updates dynamically when the buttons are clicked. Use the use State hook to manage the counter's state within the component. Prevent the counter from going below a specified minimum value (e.g., 0). Add a "Reset" button to set the counter back to its initial value. Include functionality to specify a custom increment or decrement step value.		

4	Develop a To-Do List Application using React functional components that demonstrates the use of the use State hook for state management. Create a functional component named To Do Function to manage and display the to do list. Maintain a list of tasks using state. Provide an input field for users to add new tasks. Dynamically render the list of tasks below the input field. Ensure each task is displayed in a user-friendly manner. Allow users to delete tasks from the list. Mark tasks as completed or pending, and visually differentiate them.
5	Develop a React application that demonstrates component composition and the use of props to pass data. Create two components: Figure List: A parent component responsible for rendering multiple child components. Basic Figure: A child component designed to display an image and its associated caption. Use the Figure List component to dynamically render multiple Basic Figure components. Pass image URLs and captions as props from the Figure List component to each Basic Figure component. Style the Basic Figure components to display the image and caption in an aesthetically pleasing manner. Arrange the Basic Figure components within the Figure List in a grid or list format. Allow users to add or remove images dynamically. Add hover effects or animations to the images for an interactive experience.
6	Design and implement a React Form that collects user input for name, email, and password. Form Fields are Name, Email, Password. Ensure all fields are filled before allowing form submission. Validate the email field to ensure it follows the correct email format (e.g., example@domain.com). Optionally enforce a minimum password length or complexity. Display error messages for invalid or missing inputs. Provide visual cues (e.g., red borders) to highlight invalid fields. Prevent form submission until all fields pass validation. Log or display the entered data upon successful submission (optional). Add a "Show Password" toggle for the password field. Implement client-side sanitization to ensure clean input.
7	Develop a React Application featuring a Profile Card component to display a user's profile information, including their name, profile picture, and bio. The component should demonstrate flexibility by utilizing both external CSS and inline styling for its design. Display the following information: Profile picture, User's name, A short bio or description Use an external CSS file for overall structure and primary styles, such as layout, colors, and typography. Apply inline styles for dynamic or specific styling elements, such as background colors or alignment. Design the Profile Card to be visually appealing and responsive. Ensure the profile picture is displayed as a circle, and the name and bio are appropriately styled. Add hover effects or animations to enhance interactivity. Allow the background color of the card to change dynamically based on a prop or state.
8	Develop a Reminder Application that allows users to efficiently manage their tasks. The application should include the following functionalities: Provide a form where users can add tasks along with due dates. The form includes task name, Due date, An optional description. Display a list of tasks dynamically as they are added. Show relevant details like task name, due date, and completion status. Include a filter option to allow users to view all Tasks and Display all tasks regardless of status. Show only tasks marked as completed. Show only tasks that are not yet completed.

9	Design a React application that demonstrates the implementation of routing using the react-router-dom library. The application should include the Navigation Menu: Create a navigation bar with links to three distinct pages, Home, About, Contact. Develop separate components for each page (Home, About, and Contact) with appropriate content to differentiate them. Configure routes using react-router-dom to render the corresponding page component based on the selected link. Use Browser Router and Route components for routing. Highlight the active link in the navigation menu to indicate the current page.
10	Design a React application featuring a class-based component that demonstrates the use of lifecycle methods to interact with an external API. The component should fetch and update data dynamically based on user interactions or state changes. Use the component Did Mount lifecycle method to fetch data from an API when the component is initially rendered. Display the fetched data in a structured format, such as a table or list. Use the component Did Update lifecycle method to detect changes in the component's state or props. Trigger additional API calls to update the displayed data based on user input or actions (e.g., filtering, searching, or pagination). Implement error handling to manage issues such as failed API requests or empty data responses. Display appropriate error messages to the user when necessary. Allow users to perform actions like filtering, searching, or refreshing the data. Reflect changes in the displayed data based on these interactions.

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Illustrate React basics and state components
CO2	Develop React applications that utilize component composition, passing data through props.
CO3	Use dynamic state updates, event handling, and custom logic to increment, decrement, and reset state values.
CO4	Implement forms in React that collect and validate user input.
CO5	Demonstrate interaction with external APIs, dynamic content generation and manage state in real-time applications

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE Practical (A)	30	-	Marks awarded for Weekly Conduction of Experiments and Submission of Laboratory records, scaled to 30 marks.

CIE Practical Test (B)	20	-	Average of marks of Two tests, each conducted for 100 marks covering all experiments, scaled to 20.
Total CIE Practical (A+B)	50	20	Sum of Marks of Experiments, Record and Test shall be CIE marks awarded for a maximum of 50.
SEE (C)	50	20	SEE is a lab exam, conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE.			

Textbooks:

1. Beginning React JS Foundations Building User Interfaces with ReactJS: An Approachable Guide, Chris Minnick, Wiley publications , 2022..
2. Learning React Functional Web Development with React and Redux , Alex Banks, Eve Porcello · 2017.

Web links and Video Lectures (e-Resources):

- <https://www.youtube.com/watch?v=V9i3cGD-mts>
- <https://youtu.be/PHaECbrKgs0>
- <https://youtu.be/uvEAvxWvwOs>
- <https://www.geeksforgeeks.org/state-management-with-usestate-hook-in-react/>
- <https://youtu.be/KU-I2M9Jm68>
- https://youtu.be/H63Pd_IXkeQ
- <https://youtu.be/oTIJunBa6MA>
- <https://youtu.be/3EbYJrAOpUs>

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VI			
Course Title	GENERATIVE AI		
Course Code	BCYL657C	CIE MARKS	50
L: T : P	0:0:2	SEE MARKS	50
Credits	01	EXAM HOURS	3
Course Learning Objectives: <i>The purpose of the course is to facilitate the learner to:</i> 1. Understand the principles and concepts behind generative AI models. 2. Explain the knowledge gained to implement generative models using Prompt design frameworks. 3. Apply various Generative AI applications for increasing productivity. 4. Develop Large Language Model-based Apps.			
SL No.	Experiments		
1	Explore pre-trained word vectors. Explore word relationships using vector arithmetic. Perform arithmetic operations and analyze results.		
2	Use dimensionality reduction (e.g., PCA or t-SNE) to visualize word embeddings for Q 1. Select 10 words from a specific domain (e. g., sports, technology) and visualize their embeddings. Analyze clusters and relationships. Generate contextually rich outputs using embeddings. Write a program to generate 5 semantically similar words for a given input.		
3	Train a custom Word2Vec model on a small dataset. Train embeddings on a domain-specific corpus (e.g., legal, medical) and analyze how embeddings capture domain-specific semantics.		
4	Use word embeddings to improve prompts for Generative AI model. Retrieve similar words using word embeddings. Use the similar words to enrich a GenAI prompt. Use the AI model to generate responses for the original and enriched prompts. Compare the outputs in terms of detail and relevance.		
5	Use word embeddings to create meaningful sentences for creative tasks. Retrieve similar words for a seed word. Create a sentence or story using these words as a starting point. Write a program that: Takes a seed word. Generates similar words. Constructs a short paragraph using these words.		
6	Use a pre-trained Hugging Face model to analyze sentiment in text. Assume a real-world application, Load the sentiment analysis pipeline. Analyze the sentiment by giving sentences to input.		
7	Summarize long texts using a pre-trained summarization model using Hugging face model. Load the summarization pipeline. Take a passage as input and obtain the summarized text.		
8	Install langchain, cohere (for key), langchain-community. Get the api key(By logging into Cohere and obtaining the cohere key). Load a text document from your google drive . Create a prompt template to display the output in a particular manner.		

9	Take the Institution name as input. Use Pydantic to define the schema for the desired output and create a custom output parser. Invoke the Chain and Fetch Results. Extract the below Institution related details from Wikipedia: The founder of the Institution. When it was founded. The current branches in the institution . How many employees are working in it. A brief 4-line summary of the institution.
10	Build a chatbot for the Indian Penal Code. We'll start by downloading the official Indian Penal Code document, and then we'll create a chatbot that can interact with it. Users will be able to ask questions about the Indian Penal Code and have a conversation with it.

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Explore and analyze word embeddings, including vector arithmetic and visualization.
CO2	Apply prompt engineering for information retrieval and text generation.
CO3	Use pre-trained Hugging Face models for tasks like sentiment analysis and summarization.
CO4	Understand transformer-based architectures, their advantages, and limitations.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE Practical (A)	30	-	Marks awarded for Weekly Conduction of Experiments and Submission of Laboratory records, scaled to 30 marks.
CIE Practical Test (B)	20	-	Average of marks of Two tests, each conducted for 100 marks covering all experiments, scaled to 20.
Total CIE Practical (A+B)	50	20	Sum of Marks of Experiments, Record and Test shall be CIE marks awarded for a maximum of 50.
SEE (C)	50	20	SEE is a lab exam, conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE.			

Textbooks:

1. Modern Generative AI with ChatGPT and OpenAI Models: Leverage the Capabilities of OpenAI's LLM for Productivity and Innovation with GPT3 and GPT4, by Valentina Alto, Packt Publishing Ltd, 2023.
2. Generative AI for Cloud Solutions: Architect modern AI LLMs in secure, scalable, and ethical cloud environments, by Paul Singh, Anurag Karuparti, Packt Publishing Ltd, 2024.

Web links and Video Lectures (e-Resources):

- https://www.w3schools.com/gen_ai/index.php
- <https://youtu.be/eTPiL3DF27U>
- <https://youtu.be/je6AlVeGOV0>
- <https://youtu.be/RLVqsA8ns6k>
- <https://youtu.be/0SAKM7wiC-A>
- https://youtu.be/28_9xMyrdjg
- <https://youtu.be/8iuiz-c-EBw>
- <https://youtu.be/7oQ8VtEKcgE>
- <https://youtu.be/seXp0VWWZV0>



ESTD : 2001

An Institute with a Difference

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VI			
Course Title	DATA VISUALIZATION WITH PYTHON		
Course Code	BCYL657D	CIE MARKS	50
L: T : P	0:0:2	SEE MARKS	50
Credits	01	EXAM HOURS	3
Course Learning Objectives: <i>The purpose of the course is to facilitate the learner to:</i> 1. Demonstrate techniques for analyzing network traffic and detecting intrusions. 2. Understand security mechanisms within ICS and PLC environments. 3. Gain knowledge of configuring firewall and web system settings. 4. Perform incident response simulations and assess potential risks.			
SL No.	Experiments		
1	a) Write a python program to find the best of two test average marks out of three test's marks accepted from the user. b) Develop a Python program to check whether a given number is palindrome or not and also count the number of occurrences of each digit in the input number. Datatypes: https://www.youtube.com/watch?v=gCCVsvgR2KU Operators: https://www.youtube.com/watch?v=v5MR5JnKcZI Flow Control: https://www.youtube.com/watch?v=PqFKRqpHrjw For loop: https://www.youtube.com/watch?v=0ZvaDa8eT5s While loop: https://www.youtube.com/watch?v=HZARImviDxg Exceptions: https://www.youtube.com/watch?v=6SPDvPK38tw		
2	a) Defined as a function F as $F_n = F_{n-1} + F_{n-2}$. Write a Python program which accepts a value for N (where $N > 0$) as input and pass this value to the function. Display suitable error message if the condition for input value is not followed. b) Develop a python program to convert binary to decimal, octal to hexadecimal using functions. Functions: https://www.youtube.com/watch?v=BVfCWuca9nw Arguments: https://www.youtube.com/watch?v=ijXMGpoMkhQ Return value: https://www.youtube.com/watch?v=nuNXiEDnM44		
3	a) Write a Python program that accepts a sentence and find the number of words, digits, uppercase letters and lowercase letters. b) Write a Python program to find the string similarity between two given strings Sample Output: Original string: Python Exercises Python Exercises Similarity between two said strings:		

	1.00.967741935483871 Strings: https://www.youtube.com/watch?v=ISItwlnF0eU String functions: https://www.youtube.com/watch?v=9a3CxJyTq00
4	a) Write a Python program to Demonstrate how to Draw a Bar Plot using Matplotlib. b) Write a Python program to Demonstrate how to Draw a Scatter Plot using Matplotlib. https://www.youtube.com/watch?v=RRHQ6Fs1b8w&list=PLjVLYmrlmjGcC0B_FP3bkJJIPkV5GuZR&index=3 https://www.youtube.com/watch?v=7ABCuhWO9II&list=PLjVLYmrlmjGcC0B_FP3bkJJIPkV5GuZR&index=4
5	a) Write a Python program to Demonstrate how to Draw a Histogram Plot using Matplotlib. b) Write a Python program to Demonstrate how to Draw a Pie Chart using Matplotlib. https://www.youtube.com/watch?v=Qk7caotaQUQ&list=PLjVLYmrlmjGcC0B_FP3bkJJIPkV5GuZR&index=6 https://www.youtube.com/watch?v=PSji21jUNO0&list=PLjVLYmrlmjGcC0B_FP3bkJJIPkV5GuZR&index=7
6	a) Write a Python program to illustrate Linear Plotting using Matplotlib. b) Write a Python program to illustrate liner plotting with line formatting using Matplotlib. https://www.youtube.com/watch?v=UO98IJQ3QGI&list=PL-osiE80TeTvipOqomVEeZ1HRrcEvtZB
7	Write a Python program which explains uses of customizing seaborn plots with Aesthetic functions. https://www.youtube.com/watch?v=6GUZXDef2U0
8	Write a Python program to explain working with bokeh line graph using Annotations and Legends. a) Write a Python program for plotting different types of plots using Bokeh. https://www.youtube.com/watch?v=HDvxYoRadcA
9	Write a Python program to draw 3D Plots using Plotly Libraries. https://www.youtube.com/watch?v=cCck7hCanpw&list=PLE50-dh6JzC4onXqkv9H3HtPbBVA8M94&index=4
10	a) Write a Python program to draw Time Series using Plotly Libraries. b) Write a Python program for creating Maps using Plotly Libraries. https://www.youtube.com/watch?v=xnJ2TNrGYik&list=PLE50-dh6JzC4onXqkv9H3HtPbBVA8M94&index=5 https://www.youtube.com/watch?v=D35m2CdMhVs&list=PLE50-dh6JzC4onXqkv9H3HtPbBVA8M94&index=6

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Understanding the use of IDLE or PyCharm IDE for developing Python applications.
CO2	Developing Python programs using programming constructs to solve real-world problems.
CO3	Generating graphical representations using Matplotlib for data visualization.
CO4	Utilizing Seaborn and Bokeh for advanced and interactive visualization techniques.
CO5	Creating visualizations using Plotly for time-series data and map-based analysis.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE Practical (A)	30	-	Marks awarded for Weekly Conduction of Experiments and Submission of Laboratory records, scaled to 30 marks.
CIE Practical Test (B)	20	-	Average of marks of Two tests, each conducted for 100 marks covering all experiments, scaled to 20.
Total CIE Practical (A+B)	50	20	Sum of Marks of Experiments, Record and Test shall be CIE marks awarded for a maximum of 50.
SEE (C)	50	20	SEE is a lab exam, conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE.			

Textbook :

1. Al Sweigart, “Automate the Boring Stuff with Python”, 1st Edition, No Starch Press, 2015. (Available under CC-BY-NC-SA license at <https://automatetheboringstuff.com/>)
2. Reema Thareja “Python Programming Using Problem Solving Approach” Oxford University Press.

3. Allen B. Downey, “Think Python: How to Think Like a Computer Scientist”, 2nd Edition, Green Tea Press, 2015. (Available under CC-BY-NC license at <http://greenteapress.com/thinkpython2/thinkpython2.pdf>)
4. Jake VanderPlas “Python Data Science Handbook” 1st Edition, O’REILLY.

Online Resources:

- Python Official Documentation.
- Matplotlib Documentation and Tutorials.
- Seaborn Official Guide.
- Bokeh Documentation.
- Plotly Python Graphing Library Documentation.
- W3Schools Python and Data Visualization Tutorials.
- GeeksforGeeks Python Visualization Articles and Examples.

Tools Documentation:

- IDLE User Guide.
- PyCharm Official Documentation.
- Matplotlib API Reference.
- Seaborn Documentation.
- Bokeh User Guide.
- Plotly Python Library Guide.

Datasets for Practice:

- Kaggle Public Datasets for Visualization.
- UCIMachine Learning Repository Datasets for analysis and plotting.
- Google Dataset Search Open datasets for projects.
- World Bank Open Data for time-series visualization.
- Data.gov Public datasets for charts and maps.

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VI			
Course Title:	INDIAN KNOWLEDGE SYSTEMS		
Course Code:	BIKS608	CIE MARKS	100
(L :T : P) + SL	(1:0:0) + (15 Hours/Sem)	SEE MARKS	-
Credits:	1	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. To facilitate the students with the concepts of Indian traditional knowledge and to make them understand the Importance of roots of knowledge system. 2. To make the students understand the traditional knowledge and analyze it and apply it to their day-to-day life.			
Module-1			5 Hours
Introduction to Indian Knowledge Systems (IKS): Overview, Importance of ancient knowledge, The IKS corpus, Vedic Corpus, Philosophical systems, Character scope and importance, traditional knowledge vis-a-vis indigenous knowledge, traditional knowledge vs. western knowledge.			
Module-2			5 Hours
Fundamental concepts for science and technology: Linguistics, Numbers and measurements- Mathematics, Chemistry, Physics, Art, Astronomy, Astrology, Crafts and Trade in India and Engineering and Technology.			
Module-3			5 Hours
Traditional Knowledge in Professional Domain: Town planning and architecture, Construction, Health, wellness and Psychology-Medicine, Agriculture, Governance and Public administration			

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Provide an overview of the concept of the Indian Knowledge System and its importance.
CO2	Appreciate the need for and importance of protecting traditional knowledge.
CO3	Recognize the relevance of Traditional knowledge in different domains.
CO4	Establish the significance of Indian Knowledge systems in the contemporary world.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	40	--	Each test will be conducted for 25 Marks adding upto 50 marks. Final test marks will be reduced to 40 Marks
Experimental Learning (B)	40	---	Case Study-based Teaching-Learning. Video-based Seminar (4-5 minutes per student on a relevant IKS topic)
Quiz(C)	20	---	Each quiz is evaluated for 10 marks adding up to 20 Marks.
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
Total CIE (A+B+C)	100	40	CIE Evaluation is done for a maximum of 100 marks

Textbooks:

1. Introduction to Indian Knowledge System- concepts and applications, B Mahadevan, Vinayak Rajat Bhat, Nagendra Pavana R N, 2022, PHI Learning Private Ltd, ISBN-978-93- 91818-21-0M. M. Mano, Digital Logic and Computer Design. PHI Learning, 2008. ISBN: 978-81-203-0417-84.

Reference Books:

1. Traditional Knowledge System in India, Amit Jha, 2009, Atlantic Publishers and Distributors (P) Ltd., ISBN-13: 978-8126912230
2. Knowledge Traditions and Practices of India, Kapil Kapoor, Avadesh Kumar Singh, Vol. 1, 2005, DK Print World (P) Ltd., ISBN 81-246-0334

Suggested Web Links:

1. <https://www.youtube.com/watch?v=LZP1StpYEPm>
2. <http://nptel.ac.in/courses/121106003/>
3. <http://www.iitkgp.ac.in/departments/KS;jsessionid=C5042785F727F6EB46CBF432D7683B63>
(Centre of Excellence for Indian Knowledge System, IIT Kharagpur)
4. https://www.wipo.int/pressroom/en/briefs/tk_ip.html
5. https://unctad.org/system/files/official-document/ditcted10_en.pdf



RN Shetty Trust ®

RNS INSTITUTE OF TECHNOLOGY

An Autonomous Institution, Affiliated to VTU,
Accredited with NAAC A+ Grade

Department of CSE (Cyber Security)
Autonomous Scheme (Effective from Academic Year
2024 – 25)



6. http://nbaindia.org/uploaded/docs/traditionalknowledge_190707.pdf
7. https://unfoundation.org/what-we-do/issues/sustainable-development-goals/?gclid=EAIaIQobChMImp-Jtb_p8gIVTeN3Ch27LAmPEAAAYASAAEgIm1vD_BwE



ESTD : 2001

An Institute with a Difference

B.E. (Common to All Branches) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VI			
Course Title:	NATIONAL SERVICE SCHEME		
Course Code:	BNSK659	CIE MARKS	100
L : T : P	0:0:2	SEE MARKS	---
Credits:	---	EXAM HOURS	—
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Identify the needs and problems of the community and involve the problem solving. 2. Develop a sense of social & civic responsibility & utilize their knowledge in finding practical solutions to individual and community problems. 3. Develop competence required for group living and sharing of responsibilities & gain skills in mobilising community participation to acquire leadership qualities and democratic attitudes.			
Module-1			
Contribution to national-level initiatives of the Government of India, such as Digital India, Skill India, Swachh Bharat, Atmanirbhar Bharat, Make in India, the Mudra Scheme, and other skill development programs.			
Module-2			
Spreading public awareness through rural outreach programs. (minimum 5 programs).			
Module-3			
Innovative approaches to assist in the marketing of rural produce.			
Module-4			
Creating awareness on rainwater harvesting in Urban areas..			
Module-5			
Creating awareness on digital payment frauds to locals.			

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Identify and analyze community needs and actively participate in solving social issues through NSS activities.
CO2	Demonstrate social and civic responsibility by engaging in national initiatives and rural outreach programs.
CO3	Develop leadership qualities, teamwork skills, and the ability to mobilize community participation effectively.
CO4	Apply innovative approaches to address real-world problems such as rural development, environmental sustainability, and digital awareness.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE - IA Tests (A)	60	-	Sum of Two Internal Assessment Tests (MCQs) each conducted for 30 marks.
Continuous and Comprehensive Evaluation (B)	40	-	Any two Assessment methods as per 24RNBE4.2, scaled to 40 marks.
Total CIE (A+B)	100	40	CIE Evaluation is done for a maximum of 100 marks.
The minimum marks to be secured in CIE is 40 (40%) out of allotted 100 marks to Pass.			

Reference Books:

1. NSS Course Manual, Published by NSS Cell, VTU Belagavi.
2. Government of Karnataka, NSS cell, activities reports and its manual.
3. Government of India, NSS cell, Activities reports and its manual.

Web links:

1. National Service Scheme (NSS), Ministry of Youth Affairs and Sports.
<https://nss.gov.in/>
2. MyGov Pledge Portal, Government of India.
<https://pledge.mygov.in/>

B.E. (Common to All Branches) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VI			
Course Title:	PHYSICAL EDUCATION		
Course Code:	BPEK659	CIE MARKS	100
L: T: P: S	0:0:2	SEE MARKS	---
Credits:	---	EXAM HOURS	---
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Understand the fundamental concepts of Physical Education, games and sports skills, Health, Nutrition and Fitness. 2. Familiarization of health-related Exercises, Sports for overall growth and development. 3. Participate in the competition at regional/state / national / international levels. 4. Create consciousness among the students on Health, Fitness and Wellness in developing and maintaining a healthy lifestyle.			
Module-1			3 Hours
Title: Athletics - Track Events - Relays Relays Relay Race: Starting, Baton Holding/Carrying, Baton Exchange in between zone, and Finishing			
Module-2			3 Hours
Title: Athletics - Triple Jumps Triple Jump A) Approach Run B) Take-off C) Step, D) Flight in the Hop E) Jump and Landing			
Module-3			3 Hours
Title: Athletics - Throws Javelin Throw A) Grip B) Carry and Recovery (3/5 Impulse stride). C) Release			
Module-4			3 Hours
Title: CRICKET A. Fundamental skills 1. Batting - Forward Defense Stroke, Backward Defense Stroke, Off Drive, On 2. Drive, Straight Drive, Cover Drive, Square Cut. 3. Bowling -Out-swing, In-swing, Off Break, Leg Break and Googly. 4. Fielding: Catching - The High Catch, The Skim Catch, The Close Catch and throwing at the stumps from different angles. Long Barrier and Throw, Short Throw, Long Throw, Throwing on the Turn. 5. Wicket Keeping B. Rules and their interpretation and duties of the officials			

Module-5	3 Hours
Title: BASEBALL A. Fundamental skills 1. Player Stances – walking, extending walking, L stance, cat stance 2. Grip – standard grip, choke grip 3. Batting – swing and bunt. Pitching 4. Baseball: slider, fast pitch, curve ball, drop ball, rise ball, change up, knuckle ball, screw ball, B. Rules and their interpretation and duties of the officials	

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Demonstrate the techniques of relay races, including starting, baton holding, exchange within the zone, and finishing, along with basic skills of javelin throw.
CO2	Apply the fundamental techniques of triple jump, including approach run, take-off, hop, step, jump, flight, and landing.
CO3	Develop and perform javelin throw techniques, including grip, carry, impulse stride, release, and recovery with proper coordination.
CO4	Exhibit fundamental skills of cricket, including batting, bowling, fielding, wicket keeping, and understand rules and duties of officials.
CO5	Demonstrate basic skills and techniques in baseball, including player stances, grip, batting, pitching, and understand rules and officiating.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	60	---	Sum of Two Internal Assessment Tests (MCQs) each conducted for 30 marks.
Project (B)	40	---	-----
Total CIE (A+B)	100	40	CIE Evaluation is done for a maximum of 100 marks
The minimum marks to be secured in CIE is 40 (40%) out of 100 marks allotted to Pass.			

Textbooks:

1. Health and Physical Education by V.K. Sharma
2. Introduction to Physical Education, Fitness, and Sport by Daryl Siedentop

3. Physical Education Activities, Sports and Games: The Origin and Background, Rules of Play, Teaching Hints and Fundamentals by Louis E. Means

Reference Books:

1. Saraswati Health and Physical Education Textbook.
2. Foundations of Physical Education, Exercise Science and Sport by Deborah A. Wuest



ESTD : 2001

An Institute with a Difference

B.E. (Common to All Branches) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VI			
Course Title:	YOGA		
Course Code:	BYOK659	CIE MARKS	100
(L :T : P) + SL	0:0:2	SEE MARKS	---
Credits:	---	EXAM HOURS	—
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Physical, Mental & spiritual Objectives of Yoga. 2. Explain the meaning of Yoga. 3. Discuss the importance of the Yoga and its scope. 4. Describe the aims and objectives of Yoga. 5. Clarify the misconceptions on Yoga.			
Module-1 : Title : Suryanamaskara			3 Hours
Suryanamaskar - Revision of practice 12 count 8 rounds a) Suryanamaskar prayer. b) Meaning, need & Importance. c) Benefits of Suryanamaskara.			
Module-2 : Title : Asanas			3 Hours
Need & importance of different Asana, Asana its meaning by name, technique, precautionary measures and benefits of each asana. Sitting: 1. Bakasana. 2. Hanumanasana. 3. Yogamudra in Vajrasana. Standing: 1. Vatayanasana. 2. Garudasana.			
Module-3 : Title : Asanas			3 Hours
Need, importance of Asana. Different types, Asana by name, technique, precautionary measures and benefits of each asana Prone line 1. Bhujangasana. 2. Shalabh asana. Supine line 1. Utthita dvipadasana, 2. Ardha halasana. Balancing 1. Sheershasana.			
Module-4 : Title : Pranayama			3 Hours
Kapalabhati - Revision of Kapalabhati practice (80 strokes/min 3 rounds).			

Module-5 : Title : Pranayama	3 Hours
Pranayam 1. Bhastrika. 2. Bhramari. Meaning, need, importance of Pranayama. different types, technique, precautionary measures and benefits of each Pranayama	

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Explain the meaning, objectives, scope, and importance of Yoga, including its physical, mental, and spiritual benefits and misconceptions.
CO2	Demonstrate Suryanamaskara (12 counts, 8 rounds) with correct technique, prayer, and understanding of its need and benefits.
CO3	Perform sitting and standing Asanas (Bakasana, Hanumanasana, Yogamudra in Vajrasana, Vatayanasana, Garudasana) with proper technique, precautions, and benefits.
CO4	Execute prone, supine, and balancing Asanas (Bhujangasana, Shalabhasana, Utthita Dvipadasana, Ardha Halasana, Sheershasana) with correct body alignment and safety measures.
CO5	Practice Pranayama techniques (Kapalabhati, Bhastrika, Bhramari) with proper method, breathing control, and understanding of their importance and health benefits.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	60	----	Sum of Two Internal Assessment Tests (MCQs) each conducted for 30 marks.
Project (B)	40	----	-----
Total CIE (A+B)	100	40	CIE Evaluation is done for a maximum of 100 marks
The minimum marks to be secured in CIE is 40 (40%) out of 100 marks allotted to Pass.			

Textbooks:

1. The Yoga Sutras of Patanjali by Sri Swami Satchidananda.
2. Light on Yoga by B.K.S Iyengar.

Reference Books:

1. The Heart of Yoga by T.K.V Desikachar.
2. Asana Pranayama Mudra Bandha by Swami Satyananda Saraswati.



ESTD : 2001

An Institute with a Difference



RN Shetty Trust ®

RNS INSTITUTE OF
TECHNOLOGY

An Autonomous Institution, Affiliated to VTU,
Accredited with NAAC A+ Grade

Department of CSE (Cyber Security)
Autonomous Scheme (Effective from Academic Year
2024 – 25)



VII SEMESTER SUBJECTS

An Institute with a Difference

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VII			
Course Title:	CLOUD COMPUTING AND SECURITY		
Course Code:	BCY701	CIE MARKS	50
(L :T : P) + SL	(3:0:2) + (45 Hours/Sem)	SEE MARKS	50
Credits:	4	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Introduce the fundamental concepts, architectures, and system models of distributed and cloud computing, focusing on scalability, performance, security, and energy efficiency. 2. Provide knowledge of virtualization technologies and mechanisms, including virtual machines, CPU/memory/I/O virtualization, virtual clusters, and data center automation. 3. Expose students to Hadoop and MapReduce frameworks for large-scale data processing and cloud application design methodologies. 4. Enable students to design and develop cloud-based applications using Python, including data-intensive and analytics-driven applications. 5. Familiarize students with cloud security concepts and practices, including identity and Access management, authentication, authorization, data security, key management, and auditing.			
Module-1			9 Hours
Distributed System Models and Enabling Technologies: Scalable Computing Over the Internet, Technologies for Network Based Systems, System Models for Distributed and Cloud Computing, Software Environments for Distributed Systems and Clouds, Performance, Security and Energy Efficiency. Textbook 1: Chapter-1 (1.1, 1.2, 1.3, 1.4, 1.5)			
Module-2			9 Hours
Virtual Machines and Virtualization of Clusters and Data Centers: Implementation Levels of Virtualization, Virtualization Structure/ Tools and Mechanisms, Virtualization of CPU/Memory and I/O devices, Virtual Clusters and Resource Management, Virtualization for Data Center Automation. Textbook 1: Chapter-3 (3.1, 3.2, 3.3, 3.4, 3.5)			
Module-3			9 Hours
Hadoop & MapReduce: Apache Hadoop, Hadoop MapReduce Job Execution, Hadoop Schedulers, Hadoop Cluster Setup. Cloud Application Design: Design consideration for cloud applications, Cloud Application Design Methodologies, Data Storage Approaches. Textbook 2: Chapter-4 (4.1, 4.2, 4.3, 4.4.), Chapter-5 (5.2, 5.4, 5.5)			

Module-4	9 Hours
Cloud Application Development in Python: Design Approaches, Image Processing App, Document Storage App, MapReduce App, Social Media Analytics App.	
Module-5	9 Hours
Cloud Security: Introduction, CSA Cloud security Architecture, Authentication, Authorization, Identity & Access Management, Data Security, Key Management, Auditing. Textbook 2: Chapter-12 (12.1, 12.2, 12.3, 12.4, 12.5, 12.6, 12.7, 12.8)	

PRACTICAL COMPONENT OF IPCC

Sl. NO	Experiments
1	Virtualization & VM Setup Scenario: A startup company wants to test its software on multiple operating systems without purchasing separate physical machines. Question: As a system engineer, you are asked to install a virtualization tool and create a virtual machine (VM). Configure the VM with appropriate CPU cores, memory, storage, and network settings. Demonstrate successful VM creation by verifying OS boot-up and network connectivity (e.g., ping or internet access). Application: Used for software testing across multiple OS platforms, sandboxing untrusted apps, running legacy applications, and setting up dev/test environments without buying extra hardware.
2	Resource Monitoring in Virtualized Environment – Scenario Question Scenario: An IT administrator wants to analyze how virtual machines utilize system resources to avoid performance bottlenecks. Question: Develop a program to monitor CPU usage, memory utilization, disk space, and network statistics of a virtual machine. Record and display the performance metrics periodically to help administrators assess the efficiency of the virtualized environment. Application: Used for software testing across multiple OS platforms, sandboxing untrusted apps, running legacy applications, and setting up dev/test environments without buying extra hardware.

3	Virtual Cluster Creation Scenario: A research team requires multiple interconnected machines to simulate a distributed computing environment for experimentation. Question: Create a virtual cluster using multiple virtual machines or containers. Configure passwordless communication among the nodes and demonstrate resource sharing by executing commands or sharing files across the cluster. Application: Used to build distributed system testbeds for research/teaching, simulate clusters for Big Data / HPC / microservices, and validate parallel processing + inter-node communication before deploying on real cloud infrastructure.
4	Hadoop Installation (Pseudo-Distributed Mode) Scenario: A data analytics team wants to process large datasets using Hadoop on a single machine before moving to a full cluster. Question: Install and configure Apache Hadoop in pseudo-distributed mode. Execute a sample Hadoop job and verify the successful execution by checking the output stored in HDFS. Application: Used for local Big Data prototyping, learning Hadoop components on a single machine, validating configuration and jobs before scaling to a multi-node Hadoop cluster industry.
5	HDFS File System Operations Scenario: A cloud storage administrator is responsible for managing files and access permissions in a distributed file system. Question: Demonstrate various HDFS operations, including: - Creating directories - Uploading and downloading files - Setting file permissions - Displaying file system statistics Explain how these operations support large-scale data storage and access control. Application: Used in organizations to manage large-scale distributed storage, enforce access control & permissions, support reliable storage through replication, and enable shared data access for analytics teams.

6	MapReduce – Word Count Application Scenario: A publishing company wants to analyze the frequency of words in large text documents to identify commonly used terms. Question: Implement a MapReduce program using Hadoop to count the frequency of words in a given text file. Analyze the job execution process, including the roles of the Mapper, Reducer, and HDFS. Application: Used for text analytics such as finding trending keywords, indexing documents, log keyword frequency analysis, and building features for search engines, NLP pipelines, and content mining.
7	MapReduce – Large Dataset Analysis Scenario: An e-commerce company needs insights from massive transaction or log files to understand customer behavior. Question: Develop a MapReduce program to analyze large datasets such as log files or transaction data. Generate meaningful summary statistics such as frequency counts or top-N results, and explain how MapReduce enables scalable data processing. Application: Used for log analytics, clickstream processing, transaction summarization, fraud pattern aggregation, and generating top-N insights (top products/users/errors) from massive datasets.
8	Cloud-Based Document Storage Application Scenario: A company wants a secure cloud solution for employees to store and manage official documents online. Question: Design and implement a cloud-based document storage application using Python that supports: Uploading documents Storing documents securely Retrieving documents Deleting documents Explain how cloud storage improves accessibility and reliability. Application: Used for enterprise document management (HR, finance, academic records), secure file sharing, remote access, backup/versioning, and centralized storage for collaboration.

9	Cloud-Based Image Processing Application Scenario: Scenario: A media company needs an online service to process large numbers of images efficiently. Question: Develop a cloud-based image processing application using Python that performs operations such as image resizing, format conversion, or grayscale transformation. Demonstrate how cloud computing improves scalability and performance. Application: Used in media and e-commerce for bulk image resizing/compression, thumbnail generation, format conversions, watermarking, and scalable processing pipelines (e.g., product catalogs).
10	Cloud Security Mechanisms Scenario: Scenario: A cloud service provider must ensure that user data is protected against unauthorized access and security threats. Question: Implement cloud security mechanisms for a cloud-based application, including: Authentication Authorization Data encryption Auditing Explain how each mechanism contributes to secure cloud computing. Application: Used to protect cloud apps by ensuring only valid users access data, preventing breaches, meeting compliance (audit trails), securing sensitive data via encryption, and supporting secure multi-user cloud services.

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Interpret the concepts, architectures, and system models of distributed and cloud computing including scalability, performance, security, and energy efficiency
CO2	Analyze virtualization techniques and tools used for CPU, memory, I/O virtualization, virtual clusters, and data center automation in cloud environments.
CO3	Apply Hadoop and MapReduce frameworks to process and analyze large-scale data and perform distributed computing tasks.
CO4	Design and develop cloud-based applications using Python, incorporating appropriate cloud application design methodologies and data storage approaches.

CO5	Evaluate and implement cloud security mechanisms, including authentication, authorization, identity and access management, data security, key management, and auditing.
-----	--

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE- IA Tests (A)	20	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 20 marks.
Continuous and Comprehensive Evaluation (B)	10	-	Any one Assessment methods as per 24RNBE4.2 scaled to 10 marks.
Total CIE Theory (A+B)	30	12	Marks of Tests and Assignments awarded for a maximum of 30.
CIE Practical	12	-	Marks awarded for Weekly Conduction of Experiments and Submission of Laboratory records, scaled to 12 marks.
CIE Practical Test	8	-	Average of marks of Two tests, each conducted for 100 marks covering all experiments, scaled to 8.
Total CIE Practical (C)	20	8	Marks of Experiments, Record and Test awarded for a maximum of 20 marks.
CIE: Theory + Practical (A + B + C)	50	20	CIE Evaluation is done for a maximum of 50 marks.
SEE (D)	50	18	SEE is a theory exam, conducted for 100 marks and scaled down to 50 marks. Exam duration shall before 3 hours.
CIE+SEE (A+B+C+D)	100	40	Final marks shall be the sum of marks scored in Components A, B, C and D

- The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE. The laboratory component of the IPCC shall be for CIE only. However, in SEE, the questions from the laboratory component shall be included in their respective modules only.

Textbooks:

1. Kai Hwang, Geoffrey C Fox, and Jack J Dongarra, Distributed and Cloud Computing, Morgan Kaufmann, Elsevier 2012
2. Arshdeep Bahga, Vijay Madisetti, “Cloud Computing”, A Hands-on Approach, Universities Press

Reference Books:

1. Rajkumar Buyya, Christian Vecchiola, and Thamrai Selvi, Mastering Cloud Computing McGrawHill Education, 1st Edition, 2017 2.
2. Toby Velte, Anthony Velte, Cloud Computing: A Practical Approach, McGraw- Hill Education, 2017. 3.
3. George Reese, Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, O'Reilly Publication, 1st Edition, 2009 4.
4. John Rhoton, Cloud Computing Explained: Implementation Handbook for Enterprises, Recursive Press, 2nd Edition, 2009.

Weblinks:

1. <https://www.ibm.com/topics/cloud-computing>
2. Understanding virtualization
3. Apache Hadoop 3.4.2 – MapReduce Tutorial
4. <https://realpython.com/python-cloud-development/>
5. Cloud Security Best Practices Center | Google Cloud

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning Mini Project:

1. Cloud Architecture Case Study Discussion.
2. Students design a virtual cluster architecture for a given application scenario (e.g., e-commerce, analytics).
3. Students design Map and Reduce logic for real-life problems: Word frequency, Log analysis, Sales data aggregation.
4. Hands-on coding of mini cloud applications: Document storage, Image processing Students Analyze social media datasets.

5. Students design a virtual cluster architecture for a given application scenario (e.g., e-commerce, analytics).
6. Students design Map and Reduce logic for real-life problems: Word frequency, Log analysis, Sales data aggregation.
7. Hands-on coding of mini cloud applications: Document storage, Image processing Students Analyze social media datasets.

Self-Study Topics:

1. Cloud Computing Courses in Google Cloud Career Launchpad program.



ESTD : 2001

An Institute with a Difference

B.E. (Computer Science and Engineering (Cyber Security))
Outcome Based Education (OBE) and Choice Based Credit System (CBCS)
SEMESTER – VII

Course Title:	ETHICAL HACKING		
Course Code:	BCY702	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	4	EXAM HOURS	3

COURSE LEARNING OBJECTIVES:

The purpose of the course is to facilitate the learner to:

1. Develop awareness of ethical hacking principles, legal frameworks, and professional responsibilities in cybersecurity practices.
2. Investigate structured methodologies used in penetration testing including reconnaissance, enumeration, vulnerability assessment, and exploitation phases.
3. Examine security assessment tools such as Nmap, Metasploit, and Burp Suite for identifying weaknesses across networks and applications.
4. Formulate systematic approaches for planning and executing controlled attack scenarios aligned with organizational constraints.
5. Construct detailed technical reports that communicate vulnerabilities, risks, and mitigation strategies effectively to stakeholders.

Module-1

9 Hours

Introduction: Hacking Impacts, The Hacker

The Framework: Planning the test, Sound Operations, Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Final Analysis, Deliverable, Integration.

Security Program: The Process of Information Security, Component Parts of Information Security Program, Risk Analysis and Ethical Hacking.

Textbook: Chapter-2, Chapter-3, Chapter-5

Module-2

9 Hours

The Business Perspective: Business Objectives, Security Policy, Previous Test Results, Business Challenges.

Planning for a Controlled Attack: Inherent Limitations, Imposed Limitations, timing is Everything, Attack Type, Source Point, Required Knowledge, Multi-Phased Attacks, Teaming and Attack Structure, Engagement Planner, The Right Security Consultant, The Tester, Logistics, Intermediates, Law Enforcement.

Textbook: Chapter-6, Chapter-7

Module-3	9 Hours
Preparing for a Hack: Technical Preparation, Managing the Engagement. Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance. Textbook: Chapter-8, Chapter- 9	
Module-4	9 Hours
Enumeration: Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase. Exploitation: Intuitive Testing, Evasion, Threads and Groups, Operating Systems, Password Crackers, Rootkits, Applications, Wardialing, Network, Services and Areas of Concern. Textbook: Chapter-10, Chapter-12	
Module-5	9 Hours
The Deliverable: The Deliverable, The Document, Overall Structure, Aligning Findings, Presentation. The Integration: Integrating the Results, Integration Summary, Mitigation, Defense Planning, Incident Management, Security Policy. Textbook: Chapter-13, Chapter-14.	

PRACTICAL COMPONENT OF IPCC

SL.NO	Experiments
1	Risk Analysis and Ethical Hacking Simulation Objective: Evaluate the components of an information security program through a simulated risk analysis and ethical hacking scenario. Tools: Risk management software (like FAIR or OCTAVE), Ethical hacking documentation templates (OWASP).
2	Controlled Attack Planning Simulation Objective: Plan a controlled attack scenario, considering all factors that affect the engagement and outcomes. Tools: Engagement planning templates (e.g., from OWASP), Threat modeling tools (e.g., STRIDE).
3.	Technical Preparation and Engagement Management Objective: Understand the technical preparations necessary for conducting a penetration test and how to manage the engagement effectively.

	Tools: Kali Linux (or similar penetration testing OS), Metasploit, Burp Suite, Project management tools (e.g., Asana, Trello).
4	Reconnaissance Techniques Objective: Explore various reconnaissance techniques, including social engineering, physical security assessments, and internet reconnaissance. Tools: Social engineering tools (e.g., phishing simulation software), Online reconnaissance tools (e.g., Maltego, Shodan), Physical security assessment checklist.
5	Enumeration Techniques Objective: Gain hands-on experience with various enumeration techniques to gather detailed information about a target system or network. Tools: Kali Linux (or other penetration testing distribution), Nmap, Enum4linux, Metasploit, Wireshark, Netcat.
6	Exploitation Techniques Objective: Practice various exploitation techniques to gain unauthorized access to systems while understanding different attack vectors. Tools: Kali Linux, Metasploit, Burp Suite, Hashcat (for password cracking), DVWA (Damn Vulnerable Web Application) or OWASP Juice Shop.
7	Creating a Penetration Test Deliverable Objective: Learn how to compile findings from a penetration test into a structured and professional deliverable. Tools: Word processing software (e.g., Microsoft Word, Google Docs), Presentation software (e.g., PowerPoint, Google Slides), Templates for security reports and presentations.
8	Integrating Results into a Security Strategy Objective: Learn how to integrate findings from a penetration test into a broader security framework, focusing on mitigation and incident management. Tools: Risk management software (e.g., FAIR, OCTAVE), Security policy templates, Incident response plan templates.

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Interpret ethical hacking concepts, security frameworks, and risk analysis techniques to evaluate system vulnerabilities.
------------	---

CO2	Design structured penetration testing strategies considering business objectives, operational constraints, and security policies.
CO3	Demonstrate reconnaissance techniques including social engineering, physical inspection, and internet-based information gathering.
CO4	Execute enumeration and exploitation procedures using appropriate tools and techniques to uncover security weaknesses.
CO5	Synthesize penetration testing findings into comprehensive deliverables supporting mitigation, defense planning, and incident response.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE- IA Tests (A)	20	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 20 marks.
Continuous and Comprehensive Evaluation (B)	10	-	Any one Assessment methods as per 24RNBE4.2 scaled to 10 marks.
Total CIE Theory (A+B)	30	12	Marks of Tests and Assignments awarded for a maximum of 30.
CIE Practical	12	-	Marks awarded for Weekly Conduction of Experiments and Submission of Laboratory records, scaled to 12 marks.
CIE Practical Test	8	-	Average of marks of Two tests, each conducted for 100 marks covering all experiments, scaled to 8.
Total CIE Practical (C)	20	8	Marks of Experiments, Record and Test awarded for a maximum of 20 marks.
CIE: Theory + Practical (A + B + C)	50	20	CIE Evaluation is done for a maximum of 50 marks.

SEE (D)	50	18	SEE is a theory exam, conducted for 100 marks and scaled down to 50 marks. Exam duration shall be before 3 hours.
CIE+SEE (A+B+C+D)	100	40	Final marks shall be the sum of marks scored in Components A, B, C and D.
The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE. The laboratory component of the IPCC shall be for CIE only. However, in SEE, the questions from the laboratory component shall be included in their respective modules only.			

Textbooks:

- James S. Tiller, “The Ethical Hack: A Framework for Business Value Penetration Testing”, Auerbach Publications, CRC Press.

Reference Books:

- EC-Council, “Ethical Hacking and Countermeasures Attack Phases”, Cengage Learning.
- Michael Simpson, Kent Backman, James Corley, “Hands-On Ethical Hacking and Network Defense”, Cengage Learning.

Web links:

- <https://www.youtube.com/watch?v=fNzpcB7ODxQ>
- <https://www.youtube.com/watch?v=uHU2uajL1EE>
- <https://www.youtube.com/watch?v=K6V7fc5Hj2s>
- <https://archive.nptel.ac.in/courses/106/105/106105217/>

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning:

- Students can choose one of the following activities: Capture the Flag (CTF) Competition, SQL Injection Challenge, Phishing Simulation, Social Engineering Role-Play, Security Policy Creation, Incident Response Simulation, Cryptography Challenge, Ethics Debate etc.

Self-Study Topics:

1. Penetration Testing Frameworks and Standards

Study structured methodologies such as OWASP Testing Guide and PTES for conducting systematic security assessments.

2. Virtualization and Secure Testing Environments

Explore virtual machines and sandboxing techniques used to safely perform ethical hacking experiments.

3. Web Application Security Vulnerabilities

Analyze common vulnerabilities like SQL Injection, Cross-Site Scripting (XSS), and CSRF with real- world examples.

4. Wireless Network Security Techniques

Examine security mechanisms in Wi-Fi networks and understand common attack strategies and prevention methods.

5. Cloud Security and Ethical Hacking Practices

Investigate security challenges in cloud platforms and methods used to identify vulnerabilities in cloud- based systems.

Alternate Assessment Methods:

1. **Certifications (Skill-Based)** -industry-recognized certifications (e.g. CISCO, NPTEL, Infosys Springboard).
2. **Assignments / Problem Solving Sheets.**
3. **Quiz.**
4. **Mini Projects.**
5. **Group Activities / Peer Evaluation.**
6. **Presentations / Tech Talks.**

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VII			
Course Title:	MALWARE ANALYSIS		
Course Code:	BCY703	CIE MARKS	50
(L :T : P) + SL	(3:2:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	4	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Demonstrate the purpose of commonly used file formats. 2. Identify conditional execution constructs in disassembled files. 3. Apply debugger to monitor program execution. 4. Analyse malware samples packed using common packing techniques in GHIDRA/IDA.			
Module-1			9 Hours
BASIC ANALYSIS: Basic Static Techniques, Malware Analysis in Virtual Machines, Basic Dynamic Analysis. Textbook: Chapter-1, Chapter- 2, Chapter-3			
Module-2			9 Hours
ADVANCED STATIC ANALYSIS: A Crash Course in x86 Disassembly, IDA Pro, Recognizing C Code Constructs in Assembly. Textbook: Chapter-4, Chapter-5, Chapter-6			
Module-3			9 Hours
ADVANCED DYNAMIC ANALYSIS: Analyzing Malicious Windows Programs, Debugging, OllyDbg. Textbook: Chapter-7, Chapter-8, Chapter-9			
Module-4			9 Hours
Enumeration: Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements. MALWARE FUNCTIONALITY: Malware Behavior, Covert Malware Launching.. Textbook: Chapter-11, Chapter-12			
Module-5			9 Hours
ANTI-REVERSE-ENGINEERING: Anti-Disassembly, Anti-Debugging, Anti-Virtual Machine Techniques. Textbook: Chapter-15, Chapter-16, Chapter-17			

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Identify and categorize common executable and data file formats.
CO2	Applying assembly-level conditional constructs into their corresponding high-level programming logic.
CO3	Utilize a debugger to meticulously trace and determine the execution path of a given program
CO4	Analyze the original functionality of packed malware samples using analysis tools (GHIDRA/IDA).
CO5	Develop a comprehensive analysis report that justifies the behaviour of a monitored software artifact.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Alternate Assessment (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks.
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
The minimum marks to be secured in CIE are 20 out of allotted 50 marks to appear for SEE, with minimum 40 % scored in every component of CIE.			

Textbooks:

1. Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software” by Michael Sikorski and Andrew Honig.(published by No Starch Press, 2012)

Reference Books:

1. The IDA PRO Book: The Unofficial Guide to the World’s Most Popular Disassembler, 2nd Edition” by Chris Eagle (published by No Starch Press, 2011.

Weblinks:

1. <https://www.udemy.com/course/malware-analysis-and-reverse-engineering/>
2. <https://ringzer0.training/advanced-malware-analysis.html>
3. <https://www.youtube.com/watch?v=f-fMdnUW4X4>
4. <https://www.jaiminton.com/Tutorials/PracticalMalwareAnalysis/Chapter1/#>
5. <https://www.kea.nu/files/textbooks/humblesec/practicalmalwareanalysis.pdf> (Textbook)

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning:

1. Vulnerability testing of network using Malware analysis tools like VirusTotal and Cuckoo Sandbox, and system monitoring utilities such as Process Monitor.
2. Other tools are used for specific purposes, like the debugger x64dbg, the network analysis tool Wireshark, and the decompiler Ghidra.

Self-Study topics:

1. Biometric security.
2. Malware automatic analysis tools: Process Hacker, Ghidra.
3. Operating System Security.
4. Sandboxes & Automated Analysis. (Cuckoo Sandbox).
5. PCAP files (packet captures) to practice analyzing traffic from real-world infection.

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VII			
Course Title:	VIRTUAL REALITY		
Course Code:	BCY714A	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (40 Hours)	SEE MARKS	50
Credits:	3	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Understand the fundamental concepts of Virtual Reality including its history, system architecture, hardware components, immersive characteristics, comparison with AR and MR. 2. Apply geometric transformations, coordinate systems, projection models and optical principles in the design of virtual environments. 3. Understand human visual physiology, perception mechanisms and rendering techniques to create realistic and comfortable VR experiences. 4. Analyze motion, tracking systems, sensor technologies and system dynamics used in VR environments. 5. Evaluate VR interaction techniques, spatial audio systems, usability factors and real-world applications across various domains.			
Module-1			9 Hours
Introduction to Virtual Reality & System Overview Chapter 1: Introduction Definition of VR, history, Modern VR Experiences, History Repeats. Chapter 2: Bird's-Eye View Hardware, Software, Human Physiology and Perception. Textbook: Chapter-1, Chapter- 2			
Module-2			9 Hours
Geometry of Virtual Worlds & Optics Chapter 3: The Geometry of Virtual Worlds Coordinate systems, transformations, rotations, quaternions, view and projection geometry, stereo camera models. Chapter 4: Light and Optics Optics, lenses, distortions, field of view, optical corrections, illumination basics for VR rendering. Textbook: Chapters-3, Chapter- 4			
Module-3			9 Hours
Human Physiology, Visual Perception & Rendering Chapter 5: The Physiology of Human Vision Eye physiology, depth cues, stereopsis, accommodation, convergence, visual field. Chapter 6: Visual Perception			

Motion perception, color perception, visual processing, sensory integration.	
Chapter 7: Visual Rendering	
Rasterization, raytracing overview, shading, latency, optical distortion correction, rendering pipeline for VR.	
Textbook: Chapters-5, 6 & 7	
Module-4	9 Hours
Motion, Tracking & System Dynamics	
Chapter 8: Motion in Real and Virtual Worlds	
Vestibular system, motion cues, physical vs virtual motion, redirected walking.	
Chapter 9: Tracking	
IMUs, gyroscopes, accelerometers, optical tracking, inside-out vs outside-in tracking, SLAM fundamentals, calibration, sensor fusion.	
Textbook: Chapters-8 & 9	
Module-5	9 Hours
Interaction, Audio, Evaluation & Applications	
Chapter 10: Interaction: Locomotion techniques, manipulation, gesture interfaces, controller-based interaction, haptic feedback.	
Chapter 11: Audio	
Spatial audio, binaural rendering, HRTF, sound perception in VR.	
Chapter 14: VR Applications	
Games, medical VR, training simulation, robotics, education, industrial applications.	
Textbook: Chapters-10 ,11 & 14	

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Illustrate the fundamentals, components and architecture of Virtual Reality systems.
CO2	Demonstrate human physiology and perception in relation to VR design.
CO3	Apply geometric and rendering principles for virtual world generation.
CO4	Describe motion, tracking systems and VR interaction techniques.
CO5	Evaluate VR applications, human factors and system performance.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Alternate Assessment (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
- The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE. - If any courses of 3 credits are of Integrated Course type, for such courses the method suggested for 4 credits IPCC shall be followed.			

Textbooks:

1. Steven M. LaValle, Virtual Reality, Cambridge University Press. Free official PDF available at: <https://lavalle.pl/vr/>

Web links and Video Lectures:

1. Basics of Virtual Reality.
2. AR Core & Sceneform Basics.
3. The Future of Spatial Computing.
4. NPTEL Virtual Reality Course.

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning:

1. Capture the Flag (CTF) Competition in VR.
2. AR Treasure Hunt Challenge.
3. 3D Environment Design Simulation. Virtual Navigation Role-Play.
4. Immersive User Interface Creation.
5. Motion Sickness Analysis Experiment.

Self-Study topics:

1. **Frameworks:** Study Unity3D and Unreal Engine frameworks for VR development.
2. **Environments:** Virtual machines and sandboxing for testing immersive web (WebXR).
3. **Vulnerabilities:** Privacy risks in eye-tracking and biometric data in VR.
4. **Wireless:** Examine 5G and 6G impacts on mobile AR latency.
5. **Cloud:** Investigation of Cloud Rendering and Edge Computing for VR.

Alternate Assessments Methods:

- Certifications (Unity Certified User, NPTEL, Coursera).
- Mini Projects (Building a simple AR app for Android/iOS).
- Tech Talks on the "Metaverse" and Social VR.

ESTD : 2001

An Institute with a Difference

B.E. (Computer Science and Engineering (Cyber Security))
Outcome Based Education (OBE) and Choice Based Credit System (CBCS)
SEMESTER – VII

Course Title:	WIRELESS AND MOBILE DEVICE SECURITY		
Course Code:	BCY714B	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	3	EXAM HOURS	3

COURSE LEARNING OBJECTIVES:

The purpose of the course is to facilitate the learner to:

1. Understand the evolution of wired and wireless networks and their societal and economic impacts.
2. Learn about mobile communication technologies and associated security challenges.
3. Analyse WLAN fundamentals, vulnerabilities, and threat scenarios.
4. Explore security measures for WLANs and mobile devices.
5. Gain proficiency in risk assessment and security tools for wireless networks

Module-1

9 Hours

Evolution of Data and Wired Networking

The Evolution of Data Networks: The Dawn of Data Communication; Early Data Networks; The Internet Revolution; Advances in Personal Computers and Mobile Phones; Computers Go Mobile; Convergence of Mobile and Data Networks; Business Challenges Addressed by Wireless Networking; IP Mobility and BYOD Impact; Security Considerations and Cybercrime Evolution.

The Evolution of Wired Networking to Wireless Networking: Networking and OSI Reference Model; Layers of the OSI Model; Transition from Wired to Wireless Networking; Economic Impact of Wireless Networking; Applications in Health Care, Warehousing, Retail, and Knowledge Work; WiFi Impact on Developing Nations and IoT Introduction

Textbook 1: Chapter-1

Module-2

9 Hours

The Mobile Revolution and Security Threats

The Mobile Revolution: Cellular Communication and Coverage; Frequency Sharing and Handoff; Evolution of Mobile Networks (1G to 4G/LTE); BYOD and Economic Impact of Mobility; Business Use Cases for Mobile Networking.

Security Threats Overview: Threat Categories: Confidentiality, Integrity, Availability; Wireless and Mobile Device Threats: Data Theft, System Access; Risk Mitigation and BYOD for SMBs; Security Standards and Regulatory Compliance (ISO, NIST, PCI DSS).

Textbook 1: Chapter-2, Chapter-4

Module-3	9 Hours
WLAN Fundamentals and Threat Analysis: How Do WLANs Work? WLAN Topologies, Service Sets, and Standards; Wireless Access Points (WAPs) and Antennas; Coverage Area Determination and Site Surveys; Spectrum and Protocol Analysis. WLAN and IP Networking Threat and Vulnerability Analysis: Types of Attackers: Insiders vs. Outsiders; Physical Security, Social Engineering, and Wardriving; Rogue Access Points and Bluetooth Vulnerabilities; Malicious Data Insertion, Denial of Service, and Peer to Peer Hacking. Textbook 1: Chapter-5, Chapter-6	
Module-4	9 Hours
WLAN Security Measures Basic WLAN Security Measures: Design and Implementation for Security; Authentication, MAC Filters, VPN, and VLANs; Wired Equivalent Privacy, WPA, WPA2; Ongoing Management Considerations (Firmware, Physical Security). Advanced WLAN Security Measures: Comprehensive Security Policies; Authentication and Access Control (EAP, RADIUS); Intrusion Detection/Prevention Systems and Protocol Filtering; Advanced Data Protection: WPA2 Modes, VPN, IPsec; User Segmentation, VLANs, DMZ Segmentation; Device and Network Management. Textbook 1: Chapter -7, Chapter-8	
Module-5	9 Hours
Advanced Mobile Security and Risk Management WLAN Auditing Tools: Discovery Tools (NetStumbler, Kismet); Penetration Testing Tools (Metasploit, Aircrackng); Network Enumerators, Protocol Analyzers, and Attack Tools. WLAN and IP Network Risk Assessment: Risk Assessment Methodologies and Stages; Security Risk Analysis and Audits; Legal Requirements and IT Security Management. Mobile Communication Security Challenges: Mobile Phone Threats: Exploits, Tools, and Techniques; Security Architectures: Android, iOS, Windows Phone; BYOD and Enterprise Mobility Management. Mobile Device Security Models: Security Models: Android, iOS, Windows Phone; Device Management, Encryption, and Handoff Challenges. Textbook: Chapter-10, Chapter-11, Chapter-12	

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Analyze the evolution and impact of wired and wireless networks.
CO2	Identify and categorize security threats to wireless and mobile networks.
CO3	Design and implement security measures for WLANs and mobile devices.
CO4	Utilize security tools for auditing and penetration testing.
CO5	Develop strategies to manage risks in mobile and wireless communication systems.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Alternate Assessment (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.

The minimum marks to be secured in CIE are 20 out of allotted 50 marks to appear for SEE, with minimum 40 % scored in every component of CIE.

Textbooks:

1. J. Doherty, Wireless and Mobile Device Security. Jones & Bartlett Learning, 2nd edition Dec. 2021.

Reference Books:

1. M. S. Obaidat, A. Anpalagan, I. Woungang, and S. Misra, Security and Privacy in Wireless and Mobile Networks. MDPI, 2021.
2. M. Zinkus, T. M. Jois, and M. Green, "Data Securityon Mobile Devices: Current State of the Art, Open Problems, and Proposed Solutions," arXiv, 2021. [Online]. Available: <https://arxiv.org/abs/2105.12613>
3. J. Stevenson, Mobile Offensive Security Pocket Guide: A Quick Reference Guide for Android and iOS. Independently Published, 2022.

Weblinks:

1. https://www.youtube.com/watch?v=H7tGiGjL9bA&list=PLjGG94etKypKeb0nzyN9tSs_HCd5c4wXF
2. https://www.youtube.com/watch?v=A97j344LA1M&list=PLzUKfMcBC0HTp9qvTR_cEbYNhYzNes7BG
3. <https://arxiv.org/abs/2105.12613>

Activity Based Learning (Suggested Activities in Class) / Practical Based Learning:

1. Use any WLAN simulator tools to demonstrate the working of RADIUS protocol.
2. Students in a group of TWO or THREE are expected to prepare report on different Intrusion Detection and Prevention techniques.

Self-study Topics:

1. Advanced Wi-Fi Security & WPA3 Implementation.
2. Mobile Application Penetration Testing.
3. Mobile Malware Analysis.
4. 5G Network Security Challenges.
5. IoT and Mobile Device Security Integration.

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VII			
Course Title:	WEB APPLICATION HACKING AND SECURITY		
Course Code:	BCY714C	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	3	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Understand web application architecture and security issues. 2. Learn how vulnerabilities arise and how attackers exploit them. 3. Perform penetration testing on web applications. 4. Apply defensive mechanisms and secure coding practice.			
Module-1			9 Hours
Web Foundations & Security Basics: Evolution of Web Applications, Common Web Application Functions, Benefits of Web Applications, Web Application Security, The Core Security Problem, Key Problem Factors, The New Security Perimeter, The Future of Web Application Security, Handling User Access, Handling User Input, Approaches to Input Handling, Boundary Validation, Multistep Validation and Canonicalization, Handling Attackers, Managing the Application.			
Textbook: Chapter-1, Chapter -2: Page 1-37			
Module-2			9 Hours
Web Technologies: The HTTP Protocol, Cookies, Status Codes, HTTPS, Web Functionality, Client-Side Functionality, Document Object Model, State and Sessions, Encoding Schemes, Remoting and Serialization Frameworks, Enumerating Content and Functionality, Discovering Hidden Content, Application Pages Versus Functional Paths, Analyzing the Application, Identifying Server-Side Technologies, Identifying Server-Side Functionality, Mapping the Attack Surface.			
Textbook: Chapter-3: Page 39-71			
Module-3			9 Hours
Enumerating Content and Functionality, Discovering Hidden Content, Application Pages Versus Functional Paths, Analyzing the Application, Identifying Server-Side Technologies, Identifying Server-Side Functionality, Mapping the Attack Surface.			
Textbook: Chapter-4: Page 73-114			
Module-4			9 Hours
Session & Access Attacks: Authentication Overview, Password Attacks, Brute Force Techniques, Credential Vulnerabilities, Password Reset Issues, Session Concepts, Token Weaknesses, Session Hijacking, Prevention Techniques.			
Textbook: Chapter-6: Page 159-198			

Module-5	9 Hours
Injection & Advanced Attacks: Injection Overview, SQL Injection Basics, Exploiting SQL Injection, UNION Attacks, Data Extraction Techniques, Blind SQL Injection, Filter Bypass Technique, Prevention Methods, Case Study.	
Textbook: Chapter-9: Page 287-326	

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Describe web application security concepts and vulnerabilities.
CO2	Analyze authentication and session mechanisms.
CO3	Identify and exploit common web vulnerabilities.
CO4	Evaluate application security using testing techniques.
CO5	Apply penetration testing methodology for web applications.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Alternate Assessment (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.

The minimum marks to be secured in CIE are 20 out of allotted 50 marks to appear for SEE, with minimum 40 % scored in every component of CIE.

Textbooks:

1. The Web Application Hacker's Handbook (2nd Edition) – Dafydd Stuttard, Marcus Pinto.

Reference Books:

1. OWASP Testing Guide.
2. Web Application Security – Andrew Hoffman.
3. Network Security Essentials – William Stallings.

Weblinks:

1. <https://owasp.org>
2. <https://portswigger.net>
3. <https://hackerone.com>
4. <https://bugcrowd.com>

Self-Study Topics:

1. Burp Suite Tool Usage.
2. OWASP Top 10 Vulnerabilities.
3. Bug Bounty Platforms.
4. Secure Coding Practices.
5. Case Study: Real-world Web Attacks.

Alternate Assessment Methods:

1. Certifications (Skill-Based) -industry-recognized certifications (e.g. CISCO, NPTEL, Infosys Springboard).
2. Assignments / Problem Solving Sheets.
3. Quiz.
4. Mini Projects.
5. Group Activities / Peer Evaluation.
6. Presentations / Tech Talks.

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VII			
Course Title:	NATURAL LANGUAGE PROCESSING		
Course Code:	BCY714D	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	3	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Learn the importance of natural language modelling. 2. Understand the applications of natural language processing. 3. Study spelling, error detection and correction methods and parsing techniques in NLP. 4. Illustrate the information retrieval models in natural language processing.			
Module-1			9 Hours
Introduction: What is Natural Language Processing? Origins of NLP, Language and Knowledge, The Challenges of NLP, Language and Grammar, Processing Indian Languages, NLP Applications. Language Modeling: Various Grammar-based Language Models-Paninion Framework, Karaka theory, Statistical Language Model - N-gram model. Textbook 1: Chapter-1 (1.1-1.7), Chapter-2 (2.2-2.3)			
Module-2			9 Hours
Word Level Analysis: Regular Expressions, Finite-State Automata, Morphological Parsing, Spelling Error Detection and Correction, Words and Word Classes, Part-of Speech Tagging. Syntactic Analysis: Context-Free Grammar, Constituency, Parsing- Bottom-up Parsing, A basic Top-down parser, CYK Parser. Textbook 1: Chapter-3 (3.1-3.7), Chapter-4 (4.1-4.4)			
Module-3			9 Hours
Naive Bayes, Sentiment Classification: Naive Bayes Classifiers, Training the Naive Bayes Classifier, Worked Example, Optimizing for Sentiment Analysis, Naive Bayes for Other Text Classification Tasks, Naive Bayes as a Language Model. Textbook 2: Chapter-4 (4.1-4.6)			
Module-4			9 Hours
Information Retrieval: Design Features of Information Retrieval Systems, Information Retrieval Models – Classical Information Retrieval models, Non-classical models of IR, Alternative Models of IR - Custer model, Fuzzy model, LSI model, Evaluation of the IR System. Lexical Resources: WordNet, FrameNet, Stemmers, Parts-of-Speech Tagger, Research Corpora. Textbook 1: Chapter-9 (9.1-9.7), Chapter-12 (12.1-12.6)			

Module-5	9 Hours
Machine Translation and Encoder Decoder Models: Language Divergences and Typology, Encoder-Decoder Model, Attention, Beam Search, MT Evaluation, Bias and Ethical Issues.	
Textbook 2: Chapter-11 (11.1-11.2, 11.4-11.5, 11.8-11.9).	

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Apply the fundamental concept of NLP, grammar-based language model and statistical-based language model.
CO2	Analyze morphological processing and various parsing techniques used in natural language understanding.
CO3	Develop and apply Naïve Bayes and sentiment analysis techniques for text classification and other NLP tasks.
CO4	Apply concepts of information retrieval, lexical semantics, lexical resources, and machine translation using encoder–decoder models.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Continuous and Comprehensive Evaluation (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.

- The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE.
- **If any courses of 3 credits are of Integrated Course type, for such courses the method suggested for 4 credits IPCC shall be followed.**

Text Books:

1. Tanveer Siddiqui, U.S. Tiwary, “Natural Language Processing and Information Retrieval”, Oxford University Press.
2. Daniel Jurafsky, James H. Martin, “Speech and Language Processing, An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition”, Pearson Education, 2023.

Reference Books:

1. Akshay Kulkarni, Adarsha Shivananda, “Natural Language Processing Recipes - Unlocking Text Data with Machine Learning and Deep Learning using Python”, Apress, 2019.
2. T V Geetha, “Understanding Natural Language Processing – Machine Learning and Deep Learning Perspectives”, Pearson, 2024.
3. Gerald J. Kowalski and Mark.T. Maybury, “Information Storage and Retrieval systems”, Kluwer Academic Publishers.

Web links and Video Lectures (e-Resources):

1. <https://www.youtube.com/watch?v=M7SWr5xObkA>
2. <https://youtu.be/02QWRAhGc7g>
3. <https://www.youtube.com/watch?v=CMrHM8a3hqw>
4. https://onlinecourses.nptel.ac.in/noc23_cs45/preview
5. <https://archive.nptel.ac.in/courses/106/106/106106211>

Self-Study Topics:

1. Build an N-gram language model (unigram, bigram, trigram) using sample text data.
2. Perform POS tagging and basic morphological analysis on a given text.
3. Implement sentiment analysis using a Naive Bayes classifier.
4. Develop a simple information retrieval system using TF-IDF and WordNet.



RN Shetty Trust ®

RNS INSTITUTE OF
TECHNOLOGY
An Autonomous Institution, Affiliated to VTU,
Accredited with NAAC A+ Grade

Department of CSE (Cyber Security)
Autonomous Scheme (Effective from Academic Year
2024 – 25)



7TH Semester Open Elective Courses (For Other Branches)



ESTD : 2001

An Institute with a Difference

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VII			
Course Title:	INTRODUCTION TO ALGORITHMS		
Course Code:	BCS755A	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	3	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Understand the methods of analyzing algorithms and to analyze evaluating their performance. 2. Apply algorithm's efficiencies using asymptotic notations. 3. Analyze problems using algorithm design methods such as the brute force method, greedy method, divide and conquer, decrease and conquer, transform and conquer, and dynamic programming 4. Design the appropriate data structure and algorithm design method for a specified application			
Module-1			9 Hours
Introduction: What is an Algorithm? Fundamentals of Algorithmic Problem Solving, Important problem Types, Fundamental Data Structures. Fundamentals of the Analysis of Algorithm Efficiency: Analysis Framework, Asymptotic Notations and Basic Efficiency Classes. Textbook : Chapter-1 (1.1 - 1.4), Chapter-2 (2.1, 2.2)			
Module-2			9 Hours
Fundamentals of the Analysis of Algorithm Efficiency: Mathematical Analysis of Non- recursive Algorithms, Mathematical Analysis of Recursive Algorithms. Brute Force Approaches: Selection Sort and Bubble Sort, Sequential Search and Brute Force String Matching. Textbook : Chapter-2 (2.3,2.4), Chapter-3 (3.1,3.2)			
Module-3			9 Hours
Exhaustive Search: Travelling Salesman problem and Knapsack Problem, Depth First search and Breadth First search. Decrease-and-Conquer: Insertion Sort, Topological Sorting. Divide and Conquer: Merge Sort, Quick sort, Binary Tree Traversals. Textbook : Chapter-3 (3.4,3.5), Chapter-4 (4.1,4.2), Chapter-5 (5.1 - 5.3)			
Module-4			9 Hours
The Greedy Method: Prim's Algorithm, Kruskal's Algorithm, Dijkstra's Algorithm, Huffman Trees and Codes. Dynamic Programming: Three basic examples, The Knapsack Problem and Memory Functions. Textbook 1: Chapter-9 (9.1 – 9.4) , Chapter-8 (8.1 – 8.2)			

Module-5	9 Hours
Transform-and-Conquer: Heap and Heapsort. Space and Time Trade-offs: Sorting by Counting: Comparison counting sort, Input Enhancement in String Matching: Horspool's Algorithm. Textbook 1: Chapter-6 (6.4), Chapter-7 (7.1, 7.2)	

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Analyze algorithm efficiency using asymptotic notations and fundamental algorithmic problem-solving concepts.
CO2	Analyze brute-force, decrease-and-conquer and divide-and-conquer algorithms for sorting, searching and matrix problems.
CO3	Design algorithms for optimization problems using greedy and dynamic programming paradigms.
CO4	Apply transform-and-conquer and space-time trade-off strategies to sorting and string matching problems.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Continuous and Comprehensive Evaluation (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation maximum 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.

CIE+SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.
The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE.			

Textbooks:

1. Anany Levitin, Introduction to the Design and Analysis of Algorithms, 3rd Edition, Pearson Education, 2012

Reference Books:

1. Ellis Horowitz, Sartaj Sahni and Sanguthevar Rajasekaran, Computer Algorithms/C++, 2nd Edition, Universities Press, 2008.
2. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, Introduction to Algorithms, 3rd Edition, MIT Press, 2009.
3. A M. Padma Reddy, Design and Analysis of Algorithms, 1st Edition, Sri Nandi Publications, 2009..

Web links and Video Lectures (e-Resources):

1. <https://youtu.be/xGYsEge9Vl0>
2. <https://youtu.be/A03oI0znAoc>
3. <https://www.udemy.com/topic/algorithms/>

Self-Study Topics:

- Identify algorithms used in daily life (ATM, Google Maps).
- Compare two sorting algorithms based on time complexity.
- Write pseudocode for a simple problem.
- Trace Fibonacci / searching algorithms manually.
- Explore algorithm visualization tools online.

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VII			
Course Title:	FOUNDATIONS OF INFORMATION SECURITY		
Course Code:	BCY755B	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	03	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Provide an overview of information security concepts, threats, and defense strategies. 2. Present identification, authentication, and access control concepts for securing system access. 3. Introduce auditing, accountability, and cryptographic concepts for securing information systems. 4. Outline operations, human, and physical security concepts for protecting information systems. 5. Illustrate network and operating system security concepts for system protection.			
Module-1			9 Hours
What is Information Security? Defining Information Security, When Are You Secure? Models for Discussing Security Issues, Attacks, Defense in Depth. Textbook 1: Chapter-1 (pg: 1-20)			
Module-2			9 Hours
Identification and Authentication: Identification, Authentication, Common Identification and Authentication methods. Authorization and Access Controls: What are Access Controls? Implementing Access Controls, Access Control Models. Textbook 1: Chapter-2 (pg: 23-33), Chapter-3 (pg: 35-50)			
Module-3			9 Hours
Auditing and Accountability: Accountability, Security Benefits of Accountability, Auditing. Cryptography: The History of Cryptography, Modern Cryptographic Tools, Protecting Data at Rest, in Motion and in Use. Textbook 1: Chapter-4 (pg: 51-58), Textbook: Chapter-5 (pg: 61-77)			
Module-4			9 Hours
Operations Security: The Operations Security Process, Laws of Operation Security. Human Element Security: Gathering Information for Social Engineering Attacks, Types of Social Engineering Attacks. Physical Security: Identifying Physical Threats, Physical Security Controls, Protecting People, Protecting Data, Protecting Equipment. Textbook 1: Chapter-7 (pg: 95-100), Chapter-8 (pg: 107-116) Chapter-9 (pg: 121-132)			

Module-5	9 Hours
Network Security: Protecting Networks, Protecting Network Traffic, Network Security Tools Operating System Security: Operating System Hardening, Protecting against Malware, Operating System Security Tools. Textbook 1: Chapter-10 (pg: 133-144), Chapter-11 (pg: 145-156)	

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Demonstrate information security concepts, attack types, and defense-in-depth principles.
CO2	Apply identification, authentication, and access control mechanisms for regulated system access.
CO3	Implement auditing mechanisms and cryptographic techniques for ensuring security and data protection.
CO4	Assess operational, human, and physical security threats and controls for system protection.
CO5	Utilize network and operating system security measures to protect systems and data.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Alternate Assessment (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C.

- The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE.

Textbooks:

1. Jason. Andress, Foundations of Information Security: A Straightforward Introduction. San Francisco, CA, USA: No Starch Press, 1st edition, 2019.

Reference Books:

1. M. E. Whitman and H. J. Mattord, Principles of Information Security, 7th ed. Boston, MA, USA: Cengage Learning, 2022.
2. M. Stamp, Information Security: Principles and Practice. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2006.

Web Links:

1. https://onlinecourses.nptel.ac.in/noc25_cs16
2. https://onlinecourses-archive.nptel.ac.in/noc17_cs36
3. https://onlinecourses.nptel.ac.in/noc20_cs23
4. https://www.youtube.com/results?search_query=Cyber+Security+Full+Course+for+Beginner
5. https://www.youtube.com/results?search_query=Introduction+to+Cryptography+and+Network+Security+Neso+Academy
6. https://www.youtube.com/results?search_query=Cryptography+and+System+Security

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

1. Cryptography Demonstration Activity: Demonstration of basic encryption techniques using simple tools like Online AES / RSA demo tools.
2. Network Security Demo (Visualization Based): Demonstration of: Firewall working, Packet filtering using tools such as Cisco Packet Tracer.

Self-Study Topics:

1. Zero Trust security model and architecture.
2. Cloud security fundamentals and shared responsibility model.
3. Security standards and frameworks (ISO 27001, NIST).
4. Ethical hacking and penetration testing basics.
5. Blockchain and its role in information security.

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VII			
Course Title:	FULL STACK WEB DEVELOPMENT		
Course Code:	BCD755C	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	3	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Understand the essential JavaScript concepts for web development. 2. Distinguish different types of events and their roles in interactive web applications. 3. Utilize React JS to build front end User Interface. 4. Understand the usage of API's to create web applications using Express JS. 5. Store and model data in a no sql database.			
Module-1			9 Hours
Basic JavaScript Instructions: Statements, Comments, Variables, Data Types, Arrays, String operator, Functions, Methods & Objects, Decisions & Loops. Textbook 1: Chapter-2, Chapter-3, Chapter-4			
Module-2			9 Hours
Document Object Model: DOM, DOM Tree, Accessing Elements, Selecting Elements, Adding Elements using DOM Manipulation, Adding an element to the DOM Tree, Removing elements via DOM Manipulation, Removing elements from the DOM Tree, CROSS-SITE scripting attacks, Attribute nodes. Events: Different Types of Events, How to bind an event to an element, Event Listeners, Event Delegation. Textbook 1: Chapter-5, Chapter-6			
Module-3			9 Hours
Form enhancement and validation: Helper Functions, The form element, Form controls, Submitting forms, HTML5 elements & Attributes. Introduction: MERN, MERN components, Why MERN. Hello World: Server- Less Hello world, Express, Separate Script File, JSX Transform, Older Browsers Support, Automate. React Components: Issue Tracker, React Classes, Composing Components, Passing Data using Properties, Passing Data Using Children, Dynamic Composition. Textbook 1: Chapter-13 Textbook 2: Chapter-1, Chapter-2, Chapter-3			

Module-4	9 Hours
React State: Initial State, Async State Initialization, Updating State, Lifting State Up, Event Handling, Stateless Components, Designing Components. Express and GraphQL: Express, REST API, GraphQL. Textbook 2: Chapter-4, Chapter-5	
Module-5	9 Hours
MongoDB: MongoDB Basics, MongoDB CRUD Operations, MongoDB Node.js Driver, Schema Initialization, Reading from MongoDB, Writing to MongoDB. Modularization and Webpack: Back-End Modules, Front-End Modules and Webpack, Transform and Bundle, Libraries Bundle. Textbook 2: Chapter-6, Chapter-8	

COURSE OUTCOMES:

After successfully completing the course, the student will be able to:

CO1	Understand JavaScript to build dynamic and interactive Web projects.
CO2	Implement user interface components for JavaScript-based Web using React.JS
CO3	Apply Express/Node to build web applications on the server side.
CO4	Develop data model in an open-source NoSQL database.
CO5	Demonstrate modularization and packing of the front-end modules.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.
Continuous and Comprehensive Evaluation (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks

SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C .
- The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE. - If any courses of 3 credits are of Integrated Course type, for such courses the method suggested for 4 credits IPCC shall be followed.			

Textbooks:

1. **Jon Duckett**, JavaScript & jQuery: Interactive Front-End Web Development, 1st Edition, John Wiley & Sons, Inc., 2014.
2. **Vasan Subramanian**, Pro MERN Stack: Full Stack Web App Development with Mongo, Express, React, and Node, 2nd edition, Apress, 2019.

Web Links (e- Resources):

1. <https://github.com/vasansr/pro-mern-stack>
2. <https://nptel.ac.in/courses/106106156>
3. <https://archive.nptel.ac.in/courses/106/105/106105084/>

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning:

- Course Project: Build Web applications using MERN stack. Students (group of 2) can choose any real-world problem from domains such as finance, marketing, medical, or enterprise projects.

Self-Study Topics:

1. Microservices architecture.
2. GraphQL vs REST.
3. WebSockets (real-time apps).
4. Full-stack AI integration (LLM APIs).
5. DevOps for MERN (Docker, CI/CD).

B.E. (Computer Science and Engineering (Cyber Security)) Outcome Based Education (OBE) and Choice Based Credit System (CBCS) SEMESTER – VII			
Course Title:	INTRODUCTION TO MACHINE LEARNING		
Course Code:	BCI755D	CIE MARKS	50
(L :T : P) + SL	(3:0:0) + (45 Hours/Sem)	SEE MARKS	50
Credits:	3	EXAM HOURS	3
COURSE LEARNING OBJECTIVES: <i>The purpose of the course is to facilitate the learner to:</i> 1. Introduce the fundamental concepts and techniques of machine learning. 2. Understand the types of machine learning and the challenges faced in real world applications. 3. Familiarize the machine learning algorithms such as regression, decision trees, Bayesian models, clustering, and neural networks. 4. Explore advanced concept like reinforcement learning and provide practical insight into its applications. 5. Enable students to model and evaluate machine learning solutions for different types of problems.			
Module-1			9 Hours
Introduction to Machine Learning: Need for Machine Learning, Machine Learning Explained, Machine Learning in Relation to other Fields, Types of Machine Learning, Challenges of Machine Learning, Machine Learning Process, Machine Learning Applications. Understanding Data: Introduction, Big Data Analysis Framework, Descriptive Statistics, Univariate Data Analysis and Visualization. Textbook 1: Chapter-1 (1.1-1.7), Chapter-2 (2.1-2.5)			
Module-2			9 Hours
Understanding Data: Bivariate Data and Multivariate Data, Multivariate Statistics, Essential Mathematics for Multivariate Data, Feature Engineering and Dimensionality Reduction Techniques. Basic Learning Theory: Design of Learning System, Introduction to Concept of Learning, Modelling in Machine Learning. Textbook 1: Chapter-2 (2.6-2.8, 2.10), Chapter-3 (3.3-3.4, 3.6)			
Module-3			9 Hours
Similarity-based Learning: Nearest-Neighbour Learning, Weighted K-Nearest-Neighbor Algorithm, Nearest Centroid Classifier, Locally Weighted Regression (LWR). Regression Analysis: Introduction to Regression, Introduction to Linear Regression, Multiple Linear Regression, Polynomial Regression, Logistic Regression. Decision Tree Learning: Introduction to Decision Tree Learning Model, ID3 Tree Construction. Textbook 1: Chapter-4 (4.2-4.5), Chapter-5 (5.1-5.3, 5.5-5.7), Chapter-6 (6.1, 6.2.1)			

Module-4	9 Hours
Bayesian Learning: Introduction to Probability-based Learning, Fundamentals of Bayes Theorem, Classification Using Bayes Model, Naïve Bayes Algorithm for Continuous Attributes. Artificial Neural Networks: Introduction, Biological Neurons, Artificial Neurons, Perceptron and Learning Theory, Types of Artificial Neural Networks, Popular Applications of Artificial Neural Networks, Advantages and Disadvantages of ANN, Challenges of ANN. Textbook 1: Chapter-8 (8.1-8.4), Chapter-10 (10.1-10.5, 10.9-10.11)	
Module-5	9 Hours
Clustering Algorithms: Introduction to Clustering Approaches, Proximity Measures, Hierarchical Clustering Algorithms, Partitional Clustering Algorithm, Density-based Methods, Grid-based Approach. Reinforcement Learning: Overview of Reinforcement Learning, Scope of Reinforcement Learning, Reinforcement Learning as Machine Learning, Components of Reinforcement Learning, Markov Decision Process, Multi-Arm Bandit Problem and Reinforcement Problem Types, Model-based Learning. Textbook 1: Chapter-13 (13.1-13.6), Chapter-14 (14.1-14.7)	

COURSE OUTCOMES

After successfully completing the course, the student will be able to:

CO1	Describe the machine learning techniques, their types and data analysis framework.
CO2	Apply mathematical concepts for feature engineering and perform dimensionality reduction to enhance model performance.
CO3	Develop similarity-based learning models and regression models for solving classification and prediction tasks.
CO4	Build probabilistic learning models and design neural network models using perceptron's and multilayer architectures.
CO5	Utilize clustering algorithms to identify patterns in data and implement reinforcement learning techniques.

ASSESSMENT DETAILS (BOTH CIE AND SEE)

Assessment Type	Maximum Marks	Minimum Passing Marks	Evaluation Details
CIE – IA Tests (A)	30	-	Two tests each of 50 marks shall be conducted. Average of Two Internal Assessment Tests shall be scaled down to 30 marks.

Continuous and Comprehensive Evaluation (B)	20	-	Any two Assessment methods as per 24RNBE4.2 (*if it is project based, one assignment shall be given), scaled to 20 marks.
Total CIE (A+B)	50	20	CIE Evaluation is done for a maximum of 50 marks
SEE (C)	50	18	SEE is a theory exam conducted for 100 marks and scaled down to 50 marks. Exam duration shall be for 3 hours.
CIE + SEE (A+B+C)	100	40	Final marks shall be the sum of marks scored in Components A, B and C .
The minimum marks to be secured in CIE is 20 (40%) out of allotted 50 marks to appear for SEE.			

Textbooks:

1. S. Sridhar and M. Vijayalakshmi. Machine Learning, 1st Edition, Oxford University Press, 2021.

Reference Books:

1. M. Narasimha Murty and V. S. Ananthanarayana, Machine Learning: Theory and Practice, 1st Edition, Universities Press, 2024.
2. Tom M. Mitchell, Machine Learning, 1st Edition, McGraw-Hill Education, 1997.
3. Andriy Burkov, The Hundred-Page Machine Learning Book, 1st Edition Andriy Burkov, 2019.

Web links and Video Lectures(e-Resources):

1. <https://www.universitiespress.com/resources?id=9789393330697>
2. https://www.drssridhar.com/?page_id=1053
3. <https://www.geeksforgeeks.org/machine-learning/>
4. https://www.tutorialspoint.com/machine_learning/index.htm
5. https://onlinecourses.nptel.ac.in/noc22_cs29/preview



RN Shetty Trust ®

RNS INSTITUTE OF
TECHNOLOGY

An Autonomous Institution, Affiliated to VTU,
Accredited with NAAC A+ Grade

Department of CSE (Cyber Security)

Autonomous Scheme (Effective from Academic Year
2024 – 25)



ESTD : 2001

An Institute with a Difference



VISION

Building RNSIT into a World Class Institution.



MISSION

To impart high quality education in Engineering, Technology and Management with a difference, enabling students to excel in their career by

- Attracting quality students and preparing them with a strong foundation in fundamentals so as to achieve distinctions in various walks of life leading to outstanding contributions.
- Imparting value based, need based, choice based and skill based professional education to the aspiring youth and carving them into disciplined, World class professionals with social responsibility.
- Promoting excellence in Teaching, Research and Consultancy that galvanizes academic consciousness among Faculty and Students.
- Exposing Students to emerging frontiers of knowledge in various domains and make them suitable for Industry, Entrepreneurship, Higher studies, and Research & Development.
- Providing freedom of action and choice for all the Stakeholders with better visibility.

 www.rnsit.ac.in

follow us on:    

RR Nagar, Dr. Vishnuvardhan Road, Bengaluru - 560 098
Ph: (080) 28611880, 28611881