NOIDA INSTITUTE OF ENGINEERING & TECHNOLOGY, GREATER NOIDA, GAUTAM BUDDH NAGAR

(AN AUTONOMOUS INSTITUTE)

Estd.2001
Get Future Ready

NIET
Greater Noida
An Autonomous Institute

Affiliated to

DR. A.P.J. ABDUL KALAM TECHNICAL UNIVERSITY, LUCKNOW

Evaluation Scheme & Syllabus

For

Bachelor of Technology

Computer Science and Engineering (Cyber Security)

Third Year

(Effective from the Session: 2026-27)

NOIDA INSTITUTE OF ENGINEERING & TECHNOLOGY, GREATER NOIDA

(An Autonomous Institute)

Computer Science and Engineering (Cyber Security)

Evaluation Scheme

SEMESTER –V

Sl. No.	Subject Codes	Subject Name	Type of Subject	Periods			Evaluation Schemes				End Semester		Total	Credit
				L	T	P	CT	TA	TOTAL	PS	TE	PE		
1	BCSE0502B	Computer Networks and Networks Programming	Mandatory	3	1	0	30	20	50		100		150	4
2	BCSCY0501	Digital Forensic	Mandatory	3	1	0	30	20	50		100		150	4
3		Departmental Elective II	Departmental Elective	3	0	0	30	20	50		100		150	3
4		Departmental Elective III	Departmental Elective	3	0	0	30	20	50		100		150	3
5	BCSE0552B	Computer Networks and Networks Programming Lab	Mandatory	0	0	4				50		50	100	2
6	BCSCY0551	Digital Forensic Lab	Mandatory	0	0	2				25		25	50	1
7		Departmental Elective II Lab.	Departmental Elective	0	0	2				25		25	50	1
8	BCSCY0555	Machine Learning for Cyber Security	Mandatory	0	0	6				50		100	150	3
9	BCSCC0501Y	Design Thinking II	Mandatory	2	0	0	60	40	100				100	2
10	BCSCC0552	Research Methodology, Ethics and Writing	Mandatory	0	0	2				50			50	1
11	BCSE0559X	Internship II	Mandatory	0	0	2				50			50	1
12	BVAC0551	Professional Practice and Employability I	Compulsory Audit	0	0	6				50			50	NA
13		MOOCs (For B.Tech. Hons. Degree)												
		TOTAL		**14**	**2**	**24**	**180**	**120**	**300**	**250**	**400**	**200**	**1150**	**25**

*** List of MOOCs Based Recommended Courses for Third year B. Tech Students**

S. No.	Subject Code	Course Name	University/ Industry Partner Name	N. of Hours	Credits
1.	BMC0067	AWS Certified Security Specialty 2024 [NEW]	Infosys Wingspan (Infosys Springboard)	38 h	3
2.	BMC0082	Introduction to AI & ML	Infosys Wingspan (Infosys Springboard)	64h13m	4
3.	BMC0114	Cyber Security Essential	NASSCOM	70h	4

PLEASE NOTE: -

- **A 3-4 weeks Internship shall be conducted during summer break after semester-IV and will be assessed during semester-V.**
- **Compulsory Audit (CA) Courses (Non-Credit - BVAC0551)**
  - All Compulsory Audit Courses (a qualifying exam) do not require any credit.
  - The Total and obtained marks are not added in the Grand Total.

Abbreviation Used:

L: Lecture, T: Tutorial, P: Practical, CT: Class Test, TA: Teacher Assessment, PS: Practical Sessional, TE: Theory End Semester Exam.
CE: Core Elective, OE: Open Elective, DE: Departmental Elective, PE: Practical End Semester Exam, CA: Compulsory Audit,
MOOCs: Massive Open Online Courses.

NOIDA INSTITUTE OF ENGINEERING & TECHNOLOGY, GREATER NOIDA

(An Autonomous Institute)

List of Department Elective II & III: -

Sr. No	Subject code	Subject Name	Types of Subjects	Bucket Name	Branch	Sem.
1	BCSAI0512	Advance Java Programming	DE II	Full Stack	CYS	V
2	BCSAI0512P	Advance Java Programming Lab	DE II	Full Stack	CYS	V
3	BCSCY0512N	Malware Analysis and Reverse Engineering	DE II	Cyber Security	CYS	V
4	BCSCY0512P	Malware Analysis and Reverse Engineering Lab	DE II	Cyber Security	CYS	V
5	BCSE0514	Design Pattern	DE III	Full Stack	CYS	V
6	BCSCY0514	IoT Security and Forensic	DE III	Cyber Security	CYS	V

NOIDA INSTITUTE OF ENGINEERING & TECHNOLOGY, GREATER NOIDA
(An Autonomous Institute)

Computer Science and Engineering (Cyber Security)
Evaluation Scheme
SEMESTER VI

Sl. No.	Subject Codes	Subject Name	Type of Subject	Periods			Evaluation Schemes				End Semester		Total	Credit
				L	T	P	CT	TA	TOTAL	PS	TE	PE		
1	BCSCY0603	Network Security and Cryptography	Mandatory	3	1	0	30	20	50		100		150	4
2	BCSCY0602N	Cloud Security and Privacy	Mandatory	3	1	0	30	20	50		100		150	4
3		Departmental Elective IV	Departmental Elective	3	0	0	30	20	50		100		150	3
4		Departmental Elective V	Departmental Elective	3	0	0	30	20	50		100		150	3
5		Open Elective I	Elective	2	0	0	30	20	50		50		100	2
6	BCSCY0653	Network Security and Cryptography Lab	Mandatory	0	0	4				50		50	100	2
7	BCSCY0652N	Cloud Security and Privacy Lab	Mandatory	0	0	4				50		50	100	2
8	BCS0501	Departmental Elective IV Lab	Departmental Elective	0	0	2				25		25	50	1
9	BCSCY0652	Penetration Testing	Mandatory	0	0	6				50		100	150	3
10	BCSE0659X	Applied Research with Mini Project	Mandatory	0	0	2				50			50	1
11	BVAC0651	Professional Practice and Employability II	Compulsory Audit	0	0	6	60	40	100					NA
12		MOOCs (For B.Tech. Hons. Degree)												
		TOTAL		**14**	**2**	**18**	**150**	**100**	**250**	**225**	**450**	**225**	**1150**	**25**

***List of MOOCs Based Recommended Courses for Third year B. Tech Students**

S. No.	Subject Code	Course Name	University/ Industry Partner Name	N. of Hours	Credits
1.	BMC0095	ReactJS	Infosys Wingspan (Infosys Springboard)	61h 2m	4
2.	BMC0073	Cyber Security and Applied Ethical Hacking	Infosys Wingspan (Infosys Springboard)	13h	1
3.	BMC0117	An Introduction to world of AI with Machine Learning	NASSCOM	30h	2

PLEASE NOTE: -

- **A 3-4 weeks Internship shall be conducted during summer break after semester-VI and will be assessed during Semester-VII**
- **Compulsory Audit (CA) Courses (Non-Credit - BVAC0651)**
  - All Compulsory Audit Courses (a qualifying exam) do not require any credit.
  - The Total and obtained marks are not added in the Grand Total.

Abbreviation Used:

L: Lecture, T: Tutorial, P: Practical, CT: Class Test, TA: Teacher Assessment, PS: Practical Sessional, TE: Theory End Semester Exam.
CE: Core Elective, OE: Open Elective, DE: Departmental Elective, PE: Practical End Semester Exam, CA: Compulsory Audit,
MOOCs: Massive Open Online Courses.

NOIDA INSTITUTE OF ENGINEERING & TECHNOLOGY, GREATER NOIDA

(An Autonomous Institute)

List of Department Elective IV & V: -

Sr. No	Subject code	Subject Name	Types of Subjects	Bucket Name	Branch	Sem.
1	BCSE0614	Web Development Using Mean Stack	DE IV	Full Stack	CYS	VI
2	BCSE0614P	Web Development Using Mean Stack Lab	DE IV	Full Stack	CYS	VI
3	BCSCY0612N	Blockchain And Cryptocurrency Security	DE IV	Cyber Security	CYS	VI
4	BCSCY0612P	Blockchain And Cryptocurrency Security Lab	DE IV	Cyber Security	CYS	VI
5	BCSCY0614	Security Risk Management	DE V	Cyber Security	CYS	VI
6	BCSE0615	Web Development Using Mern Stack with Devops	DE V	Full Stack	CYS	VI

NOIDA INSTITUTE OF ENGINEERING & TECHNOLOGY, GREATER NOIDA

(An Autonomous Institute)

AICTE Guidelines in Model Curriculum:

A student will be eligible to get Under Graduate degree with Honours only, if he/she completes the additional MOOCs courses such as Infosys Springboard/NASSCOM/CISCO (as applicable) certifications, or any other online courses recommended by the Institute (Equivalent to 20 credits). During Complete B.Tech. Program Guidelines for credit calculations are as follows.

1. For 6 to 12 Hours =0.5 Credit
2. For 13 to18 =1 Credit
3. For 19 to 24 =1.5 Credit
4. For 25 to 30 =2 Credit
5. For 31 to 35 =2.5 Credit
6. For 36 to 41 =3 Credit
7. For 42 to 47 =3.5 Credit
8. For 48 and above =4 Credit

For registration to MOOCs Courses, the students shall follow Infosys Springboard/NASSCOM/CISCO (as applicable) registration details as per the assigned login and password by the Institute these courses may be cleared during the B. Tech degree program (as per the list provided). After successful completion of these MOOCs courses, the students shall provide their successful completion status/certificates to the Controller of Examination (COE) of the Institute through their coordinators/Mentors only.

The students shall be awarded Honours Degree as per following criterion.

i. If he / she secures 7.50 as above CGPA.
ii. Passed each subject of that degree program in the single attempt without any grace.
iii. Successful completion of MOOCs based 20 credits

SYLLABUS - SEMESTER V

Course Code: BCSE0502B	Course Name: Computer Network and Network Programming	L	T	P	C
Course Offered in: CSE(CYS)		3	1	0	4

Prerequisite: The student should have a basic knowledge of data communication and programming.

Course Objectives:

The objective of the course is to present an introduction of TCP/IP protocol, packet switching and message switching, sliding window protocol, CDMA, network layer protocols (IPv4, ARP, RARP), routing, TCP and UDP, congestion control, quality of service, and network applications such as DNS, FTP, TELNET, and remote logging.

Course Outcome: After completion of this course students will be able to		Bloom's Knowledge Level (KL)
CO1	Build an understanding of the Layered Architecture of computer networking and the physical layer.	K2
CO2	Understand the properties of link and network layer and analyze the solutions for error control, flow control, and addressing, for networks.	K4
CO3	Understand the duties of the transport layer and the addressing and functions of sockets.	K2
CO4	Implement and analyze network connections using programming skills.	K4
CO5	Understand and analysed the different protocols used at application layer.	K4

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	2	2	2	2	1	1	-	-	1	2	2	1	1
CO2	3	3	2	3	3	1	2	-	-	1	2	3	2	1
CO3	3	3	3	3	3	2	2	-	1	2	2	3	3	2
CO4	3	3	3	2	3	2	2	-	2	2	1	3	3	2
CO5	3	2	2	3	2	2	1	1	1	2	2	2	3	2

Course Contents / Syllabus

Unit 1 **Introduction to Networking** **10 hours**

Goals and applications of networks, Categories of networks, Organization of the Internet, ISP, The OSI reference model, TCP/IP protocol suite, Network devices and components, Mode of communications, Physical Layer: Network topology design, Types of connections, LAN, MAN and WAN, Transmission media, Signal transmission and encoding, Network performance and transmission impairments, multiplexing, IEEE standards.

Unit 2 **Data Link and Network Layer** **9 hours**

Framing, Error Detection and Correction, Flow control (Elementary Data Link Protocols, Sliding Window protocols). Medium Access Control and Local Area Networks: Channel allocation, Multiple access protocols, LAN standards, Link layer switches & bridges. Network Layer: Point-to-point networks, logical addressing, Basic internetworking (IP, CIDR, ARP, RARP, DHCP, ICMP), IPv4, IPv6, Routing, forwarding and delivery, Static and dynamic routing, Routing algorithms and protocols, Congestion control

Unit 3 **Transport Layer** **9 hours**

Process-to-process delivery, Transport layer protocols (UDP and TCP), Connection management, Flow control and retransmission, Window management, TCP Congestion control, and Quality of service. Introduction to Socket Programming: Introduction to sockets, network programming concepts and applications, client-server architecture and communication model, socket address structures, socket APIs and system calls, TCP socket programming, UDP socket programming, unicast communication, broadcast communication and multicast communication using sockets, TCP three-way handshake and connection termination, concurrent client-server communication concepts, file transfer using TCP sockets, error handling in socket programming, and packet analysis

using Wireshark.

Unit 4	**Network Connection**	**9 hours**

Network Programming Libraries and Frameworks, Byte ordering and Byte manipulation functions, socket presentation functions, socket options, and configuration. Establish connections and send and receive data using sockets, timeout mechanisms and socket configuration parameters. Advanced Socket Programming Concepts: Concurrent server design, Introduction to raw sockets, packet generation

Unit 5	**Application Layer**	**8 hours**

Domain Name System, World Wide Web and Hyper Text Transfer Protocol, Electronic mail, File Transfer Protocol, Remote login, Network Management, Data compression, VPN, Firewalls.

	Total Lecture Hours	**45 hours**

Textbook:

	Author
1. "Data Communication and Networking" Fourth Edition-2006, Tata McGraw Hill	Behrouz Forouzan,
2. UNIX Network Programming: The sockets networking API, Vol 1	

Reference Books:

	Author
1. Data and Computer Communication", Eighth Edition-2008, Pearson.	William Stallings,
2. Computer Networks", Fifth Edition-2011, Prentice Hall.	Andrew Tanenbaum
3. Computer Networking- A Top-Down Approach", Eighth Edition-2021, Pearson.	Kurose and Ross

Self-Study Content Links:		Duration (in Hrs)
MOOCs	1. Java Network Programming Recipes - TOC | Infosys Springboard	5 Hrs 12 Min
Video Lectures	1. https://onlinecourses.nptel.ac.in/noc21_cs18/preview 2. https://nptel.ac.in/courses/106105081 3. https://elearn.nptel.ac.in/shop/nptel/computer-networks-and-internet-protocol/	8 Hrs 5 Hrs 2 Hrs
References	https://nptel.ac.in/courses/106105183?utm_source=chatgpt.com https://www.netacad.com/courses/packet-tracer?utm_source=chatgpt.com https://www.wireshark.org/docs/?utm_source=chatgpt.com	6Hrs 2 Hrs 2 Hrs

Course Code: BCSCY0501	Course Name: Digital Forensics	L	T	P	C
Course Offered in: CSE (CYS)		3	1	0	4

Prerequisite: Fundamental knowledge of computer networks, operating systems, and cyber security principles

Course Objectives:

To equip students with the skills to investigate and analyze digital devices and mobile platforms. Students will learn to recover and examine data from computers, smartphones, and other digital media. The course covers methods for detecting cybercrimes, collecting digital evidence, and understanding legal procedures.

Course Outcome: After completion of this course, students will be able to:		Bloom's Knowledge Level (KL)
CO1	Understand the fundamental principles of digital forensics, including the legal and ethical considerations involved in handling digital evidence.	K2
CO2	Perform forensic analysis on computer systems, recover data, and document findings in a comprehensive forensic report.	K3
CO3	Analyze the data from mobile devices using industry-standard tools and techniques.	K4
CO4	Analyze network traffic to identify and investigate network-based attacks and anomalies.	K4
CO5	Conduct forensic investigations in cloud environments and apply forensic techniques to emerging technologies such as IoT and big data.	K3

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	2	3	2	3	-	-	2	2	1	2	3	1	2
CO2	3	3	3	2	2	-	1	2	1	1	2	3	1	1
CO3	3	2	3	2	3	1	1	2	2	2	2	3	2	1
CO4	3	3	2	2	3	1	1	2	2	2	2	3	1	2
CO5	2	2	3	2	2	1	-	1	2	1	2	1	1	2

Course Contents / Syllabus

Unit 1	Introduction to Digital Forensics	10 hours

Overview of Digital Forensics, Legal and Ethical Issues, Digital Evidence, Forensic Tools and Software, Forensic Process Model & Chain Custody.

Unit 2	Computer Forensics.	10 hours

Computer Forensics Basics, Forensic Analysis Techniques, Operating System Artifacts, Reporting and Documentation, Disk Imaging and File System Analysis, Memory Forensics Basics.

Unit 3	Mobile Forensics	9 hours

Introduction to Mobile Forensics, Mobile Data Acquisition (Logical, Physical, Cloud-based), Analyzing Mobile Data, Challenges in Mobile Forensics, Mobile Device Architecture and File Systems, Mobile Application Analysis.

Unit 4	Network Forensics	8 hours

Network Forensics Fundamentals, Capturing Network Traffic, Network Attack Analysis, Advanced Network Forensics, Log Analysis and Intrusion Detection, Introduction to SIEM Tools		
Unit 5	***Cloud and Emerging Technologies Forensics***	***8 hours***
Cloud Forensics, IoT Forensics, Role of AI in Forensics, Cryptocurrency Forensics, Future Trends and Research in Forensics, Anti-Forensics Techniques.		
	Total Lecture Hours	**45 hours**

Textbook:

	Author
1. Computer Forensics: Computer Crime Scene Investigation, 2nd Edition (2015), Charles River Media.	John Vacca
2. Practical Digital Forensics: Forensic Lab Setup, Evidence Analysis, and Structured Investigation Across Windows, Mobile, Browser, HDD, and Memory, 1st Edition (2023), BPB Publication.	Akashdeep Bhardwaj, Keshav Kaushik,

Reference Books:

	Author
1. Mastering Network Forensics: A practical approach to investigating and defending against network attacks, 1st Edition (2024), BPB Publication	Nipun Jaswal
2. Ethical Hacking and Network Analysis with Wireshark: Exploration of network packets for detecting exploits and malware, 1st Edition (2023), BPB Publication.	Manish Sharma

Self-Study Content Links:		Duration (in Hrs)
MOOCs	212 Digital Forensics KSAT Advanced NCWF Journey - TOC | Infosys Springboard	14 hr 27 Min
Video Lectures	1. https://www.youtube.com/watch?v=5e5KdbY-xzE **2.** https://www.youtube.com/playlist?list=PLa2xctTiNSCiTGuejkc05zsr-G5t9AuH8 **3.** https://www.youtube.com/playlist?list=PLJu2iQtpGvv-2LtysuTTka7dHt9GKUbxD 4. https://www.youtube.com/watch?v=uCqeNnH1EpQ 5. https://www.youtube.com/watch?v=MnzHF_jygws	(40 Min 52 Sec 13 Lecture 44 Lecture 21 Min 49 Sec 25 Min 16 Sec) Total 16 Hrs.
Web References	• SANS Digital Forensics and Incident Response • NIST Computer Forensics Resource Center • Autopsy Digital Forensics • The Sleuth Kit • Volatility Foundation • Magnet Forensics • Cellebrite • DFIR Training • Cyber Triage	

Course Code: BCSAI0512	Course Name: Advance Java Programming	L	T	P	C
Course Offered in: CSE(AI)/CSE(AIML)/CSE(DS)/CSE(CS)/CSE(CYS)/CSE(IOT)/CSE(M		3	0	0	3

Pre-requisite: Basic knowledge of Core Java (OOP, exception handling, collections), multithreading, and fundamentals of SQL/database operations.

Course Objectives:

To equip students with in-depth knowledge of server-side programming using Java technologies such as Servlets, JSP, JDBC, and frameworks like Spring and Hibernate. The aim of this course is to enable students to build dynamic web applications and enterprise-level solutions with real world project exposure.

Course Outcome: After completion of the course, the student will be able to		Bloom's Level
CO1	Apply JDBC to integrate Java applications with relational databases for dynamic data handling and managing server-side programming using Servlets for handling web requests and responses.	K3
CO2	Analyze the use of JSP scripting elements, expression language, and directives to determine their effectiveness in dynamic web page rendering and maintainability.	K4
CO3	Implement modular, maintainable Java applications using advanced dependency injection techniques within the Spring Ecosystem.	K3
CO4	Design modular loosely coupled web applications by implementing the MVC architecture using Spring MVC and Spring Boot.	K6
CO5	Deploy JPA to map, store, retrieve, and update data from java objects to relational databases and vice versa with RESTful APIs to enable scalable and maintainable services.	K6

CO-PO Mapping (Scale: 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	3	2	2	2	2	1	1	1	1	2	2	2	1
CO2	3	2	3	2	2	2	1	1	1	1	2	2	2	1
CO3	3	3	3	2	3	2	1	1	1	1	2	1	2	2
CO4	3	3	2	3	3	1	2	2	2	1	2	2	1	2
CO5	3	3	3	3	3	1	2	2	2	2	3	2	2	1

Course Contents / Syllabus

Module 1	**JDBC & Servlets**	**9 hours**

JDBC: Introduction, JDBC Driver, DB Connectivity, Connection, Statement, Result Set, Prepared Statement, Transaction Management, Stored Procedures. **Servlet:** Servlet Overview, Servlet Life Cycle, Servlet API, Generic Servlet, HTTP Servlet, Redirect requests to other resources using Request Dispatcher, sendRedirect, Session Tracking: Using cookies, URL rewriting, and HttpSession.

Module 2	**JSP**	**9 hours**

JSP: Introduction, Life Cycle of JSP, JSP to Servlet Conversion, JSP Scripting Elements , JSP Implicit Objects, JSP Directives, Expression Language, Servlet-JSP-JDBC Integration, Login and registration system using JSP and Servlet.

Module 3	**Spring Framework**	**9 hours**

Spring: Overview of Spring Ecosystem, Spring Modules, IOC container, Types of Dependency Injection (DI): Constructor Injection, XML based Configuration, Setter Injection, Field Injection, Configuration Approaches: Java-based Configuration, Component Scanning, Annotation-based Configuration, Spring JDBC, Spring Project Setup using Maven.

Module 4	**Spring MVC & Spring Boot**	**9 hours**

Spring MVC: Overview of Spring MVC architecture, Controllers in Spring MVC, Passing Data Between Controller and View, JSP in Spring MVC, Integration with Spring JDBC. **Spring Boot:** Introduction, Creating a Spring Boot project using Spring

Initializer, Spring Boot Annotations & Auto Configuration, Spring Data JPA, Serving HTML pages and static content, Handling HTTP methods, H2 databased Integration, Project Lombok.		
Module 5	**JPA**	**9 hours**
JPA: Introduction to ORM & JPA, JPA Annotations, JPA Relationships, RESTful API, CRUD with Spring Data JPA, Repository Interfaces: Jpa Repository, Crud Repository, JSON/XML handling, Postman testing and deployment.		
Total Lecture Hours		**45 hours**

Textbook:

S.No	Book Title
1	B. Basham, K. Sierra, and B. Bates, Head First Servlets and JSP, 2nd ed. Sebastopol, CA, USA: O'Reilly Media, 2008.
2	H. Bergsten, Java Server Pages, 3rd ed. Sebastopol, CA, USA: O'Reilly Media, 2003.
3	C. Walls, Spring in Action, 6th ed. Shelter Island, NY, USA: Manning Publications, 2022.
4	C. Walls, Spring Boot in Action, 1st ed. Shelter Island, NY, USA: Manning Publications, 2016.
5	M. Pollack and O. Gierke, Spring Data: Modern Data Access for Enterprise Java, 1st ed. Sebastopol, CA, USA: O'Reilly Media, 2012.

Reference Books:

S.No	Book Title
1	M. Hall and L. Brown, Core Servlets and JavaServer Pages, Volume 1: Core Technologies, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2003.
2	M. Hall and L. Brown, Core Servlets and JavaServer Pages, Volume 2: Advanced Technologies, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2004.
3	C. Ho, R. Harrop, and C. Schaefer, Pro Spring 6, 1st ed. New York, NY, USA: Apress, 2023.
4	M. Keith and M. Schincariol, Pro JPA 2 in Java EE 8, 3rd ed. New York, NY, USA: Apress, 2018.

Self Study Content Link:

MOOCs	1. https://nptel.ac.in/courses/106105191 2. https://www.coursera.org/specializations/spring-framework	12 Weeks 50 hrs
Video Lectures	1. https://www.youtube.com/playlist?list=PLlhM4lkb2sEjVsbbZ_kiixY5CcR84IQUg 2. https://www.youtube.com/playlist?list=PL-XjHn7CHrmQhMkVC6KCfmsPHdklvUlQr 3. https://www.youtube.com/playlist?list=PL9ooVrP1hQOEfi91PCFQMawtBJrPpir7y 4. https://www.youtube.com/playlist?list=PL-XjHn7CHrmQhMkVC6KCfmsPHdklvUlQr 5. https://www.youtube.com/playlist?list=PLGRDMO4rOGcNSBOJOlrgQqGpIgo6_VZgR	13 hrs 1 hrs 18 hrs 50 Min 25 hrs
Web References	1. https://spring.io/guides 2. https://docs.oracle.com/javase/tutorial/	

Course Code: BCSCY0512N	Course Name: Malware Analysis and Reverse Engineering	L	T	P	C
Course Offered in: CSE (CYS)		3	0	0	3

Prerequisite: Computer Networks, Operating Systems, C/C++ or Python Programming

Course Objectives:

This course introduces techniques for analyzing and understanding malware behavior and reverse engineering malicious software. It equips students with skills to dissect malware through static and dynamic analysis and understand countermeasures and detection techniques.

Course Outcome: After completion of the course, the student will be able to		Bloom's Knowledge Level (KL)
CO1	Demonstrate an understanding of malware, its types, lifecycle, and behavioral characteristics.	K2
CO2	Apply static analysis techniques to examine file structures, metadata, and signatures of malware.	K3
CO3	Perform dynamic analysis to observe runtime behavior and system interaction of malware in isolated environments.	K4
CO4	Detect evasion and obfuscation techniques employed by malware to bypass security mechanisms.	K4
CO5	Develop comprehensive malware analysis reports including IOCs, attack vectors, and mitigation recommendations.	K4

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	2	2	3	2	3		3	1	-	1	3	-	2	1
CO2	2	3	3	3	3		3	1	-	1	3	2	3	2
CO3	2	2	3	3	3	1	3	2	1	1	3	3	3	3
CO4	3	2	3	3	3	1	2	2	1	2	2	2	3	3
CO5	3	3	3	2	3	1	3	2	1	2	3	2	2	3

Course Contents / Syllabus

Unit 1	Introduction to Malware	10 hours

Definition and classification of malware: viruses, worms, Trojans, ransomware, spyware, , bots and fileless malware. Malware attack vectors and lifecycle: infection, persistence, execution, command and control (C2), and data exfiltration. Motivation behind malware: cybercrime, hacktivism, cyber espionage, and cyber warfare. Overview of living-off-the-land attacks and script-based malware (PowerShell/macros). Legal and ethical considerations in malware research and responsible handling of malicious software.

Unit 2	Static Analysis Techniques	10 hours

Analyzing executable file formats: (Windows) and ELF (Linux) structure. Analyzeing executable headers and attributes using tools such as PEStudio, Detect It Easy (DIE), and Exeinfo PE. Extracting and analyzing strings using Strings and FLOSS, File fingerprinting using SHA-256 hashing and reputation analysis with VirusTotal. Detecting and unpacking packed binaries, . Introduction to YARA rules for malware identification and classification.

Unit 3	Dynamic Analysis Techniques	10 hours

Setting up isolated malware analysis environments using VirtualBox/VMware. Monitoring process behaviour using Process Explorer and Process Monitor, observing network activity using Wireshark, and FakeNet-NG, . Identifying system changes: file system, registry, services, and persistence mechanisms. Introduction to automated malware analysis platforms such as Cuckoo Sandbox, Hybrid Analysis or Any. Run. Behavioural indicators and basic malware evasion techniques.

Unit 4	Reverse Engineering Essentials	8 hours
Overview of x86 architecture and assembly fundamentals. Understanding program control flow (: loops, branches, function calls) and stack operations. Disassembling binaries using IDA Pro and Ghidra Recognizing common library functions and reconstructing, program logic. Debugging malware using x64dbg breakpoints, stepping, memory inspection,. Introduction to code obfuscation and anti-disassembly techniques.		
Unit 5	**Advanced Topics & Reporting**	**7 hours**
Code injection and hooking techniques: DLL injection, and API hooking,. Memory forensics using Volatility framework for malware investigation. Anti-analysis techniques: anti-debugging, anti-VM, detection and code obfuscation. Extracting Indicators of Compromise (IOC): IPs, domains, registry keys, file paths, and hashes, Mapping malware behaviour to the MITRE ATT&CK framework. Preparation of professional malware analysis reports including attack summary, indicators and mitigation strategies. Case studies of real-world malware such as WannaCry, Emotet, and Zeus).		
Total Lecture Hours		**45 hours**

Textbook:	
	Author
1. Practical Malware Analysis, Michael Sikorski,, 1st Edition (2012), No Starch Press.	Andrew Honig
2. IDA Pro Book,, 2nd Edition, No Starch Press.	Chris Eagle
3. The Art of Memory Forensics, Michael Hale Ligh,, 1st Edition (2014), John Wiley & Sons / Wiley.	Andrew Case, Jamie Levy, Aron Walters
Reference Books:	
	Author
1. Practical Reverse Engineering, Bruce Dang,, Sebastien Josse, 1st Edition, Wiley.	Alexandre Gazet, Elias Bachaalany
2. Reversing: Secrets of Reverse Engineering, Eldad Eilam, 1st Edition, Wiley Publishing.	
3. Malware Analyst's Cookbook and DVD, Michael Hale Ligh, Steven Adair, Blake Hartstein, 1st Edition, Wiley.	Matthew Richard,
4. Learning Malware Analysis, 1st Edition, Packt Publishing.	Monnappa K. A
5. Mastering Malware Analysis,, 1st Edition, Packt Publishing.	Alexey Kleymenov, Amr Thabet
6. The Ghidra Book,, 1st Edition, No Starch Press.	Chris Eagle, Kara Nance
7. Windows Internals, Part 1 & 2, Pavel Yosifovich, Mark Russinovich,, Alex Ionescu, 7th Edition, Microsoft Press.	David Solomon
8. Rootkits and Bootkits, Alex Matrosov, Eugene Rodionov, , 1st Edition, No Starch Press.	Sergey Bratus
9. The Shellcoder's Handbook, Chris Anley, John Heasman, Felix Lindner, , 2nd Edition, Wiley.	Gerardo Richarte
10. Malware Data Science, 1st Edition, No Starch Press.	Joshua Saxe, Hillary Sanders,
11. Windows Kernel Programming, , 2nd Edition, Leanpub.	Pavel Yosifovich
12. Rootkits: Subverting the Windows Kernel, , 1st Edition, Addison-Wesley	Greg Hoglund, James Butler

Self-Study Content Links:		**Duration (in Hrs)**
MOOCs	**1. Advanced Malware Analysis - TOC | Infosys Springboard**	**5 Hrs 3 Min**
Video Lectures	**1. OpenSecurityTraining.info – Reverse Engineering** **2. Malware Unicorn – https://www.malwareunicorn.org/** **3. https://bazaar.abuse.ch/**	**15 hours** **10 hours** **10 hours**
Web References		

Course Code: BCSE0514	**Course Name: Design Patterns**	**L**	**T**	**P**	**C**
Course Offered in: CSE(AI)/CSE(AIML)/CSE(DS)/CSE(CS)/ CSE(CYS)/CSE(IOT)/CSE(MCT)		3	0	0	3

Pre-requisite: Object Oriented Analysis and Design. Data structures and algorithms. Programming Language (C++ or Java)

Course Objectives:

The course objective is to familiarize the student with techniques for designing reusable combinations of Java classes and organizing their cooperation to produce modular and maintainable Java programs.

Course Outcome: After completion of the course, the student will be able to

CO	Course Outcome	Bloom's Level
CO1	Analyze, classify, and apply appropriate design patterns to solve real-world software problems, understanding their structure and selection principles.	K3
CO2	Identify, compare, and apply creational design patterns (Factory, Abstract Factory, Builder, Prototype, Singleton) to develop flexible and reusable software components.	K4
CO3	Analyze, design, and implement structural design patterns to improve flexibility, reusability, and maintainability of software systems.	K4
CO4	Analyze, design, and apply behavioral design patterns (Mediator, Memento, Observer) to manage object interactions and system behavior effectively.	K3
CO5	Analyze and implement advanced behavioral design patterns to solve common software design problems.	K4

CO-PO Mapping (Scale: 1: Low, 2: Medium, 3: High)

CO \ PO	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PSO1**	**PSO2**	**PSO3**
CO1	3	3	2	2	2	-	-	1	1	-	2	2	–	2
CO2	3	2	3	1	3	-	-	1	1	-	2	2	1	2
CO3	3	3	3	2	3	-	-	1	1	-	2	2	1	2
CO4	3	3	3	2	2	-	-	1	1	-	2	2	–	2
CO5	3	2	3	2	2	-	-	1	2	-	3	2	–	2

Course Contents / Syllabus

Module 1	**Introduction to Design Patterns**	**9 hours**

Describing Design Patterns, Design Patterns in Smalltalk MVC, The Catalog of Design Patterns, Organizing the Catalogue, Design Patterns for Solving the Real-life Problems, Selection and Use of Design patterns.

Module 2	**Creational Design Pattern**	**9 hours**

Creational Patterns: Abstract Factory, Builder, Factory Pattern, Prototype Pattern, Singleton pattern.

Module 3	**Structural Design Pattern**	**9 hours**

Structural Pattern Part-I, Adapter, Bridge, Composite. Structural Pattern Part-11, Decorator Pattern, Facade Pattern, Flyweight Pattern, Proxy Pattern.

Module 4	**Behavioural Patterns - I**	**9 hours**

Behavioural Patterns Part: I, Chain of Responsibility Pattern, Command Pattern, Interpreter Pattern, Iterator Pattern. Behavioural Patterns Part: II, Mediator, Memento, Observer Pattern.

Module 5	**Behavioural Patterns - II**	**9 hours**

Behavioral Patterns Part: III, State Patterns, Strategy, Template Patterns, Visitor, Expectation from Design Patterns Relationship between different Design Patterns.

	Total Lecture Hours	**45 hours**

Textbook:

S.NO.	**TITLE**	**Authors**
1	First Design Patterns, 2004, O'Reilly	Eric Freeman, Elisabeth Freeman, Kathy Sierra, Bert Bates Head

2	Design Patterns: Elements of Reusable Object-oriented Software Addison-Wesley, 1995.	Erich Gamma, Richard Helm, Ralph Johnson, John Vlissides
Reference Books:		
S.NO.	**TITLE**	**Authors**
1	Design Patterns Pearson Education	Erich Gamma
2	Patterns in JAVA Volume -I	Mark Grand, Wiley Dream

Self-Study Content Link:		
MOOCs	1. https://www.coursera.org/learn/design-patterns 2. https://www.udemy.com/course/soft-design-patterns/?utm_campaign=Search_DSA_Beta_Prof_la.EN_cc.India&utm_source=google&utm_medium=paid-search&portfolio=India&utm_audience=mx&utm_tactic=nb&utm_term=_._ag_160270535505_._ad_696202838334_._kw_&utm_content=g&funnel=&test=&gad_source=1&gad_campaignid=21178559974&gbraid=0AAAADROdO3wWjcAcJrZ3ow_Fcj2OFn24&gclid=Cj0KCQjw3K7RBhDJARIsAKRtP5TgfS7r7XJhzwC-gZgMsTFRkUx44pchkPY7WDXEXQyxDGeidGMqrbAaAn56EALw_wcB&couponCode=PMNVD2025	25 hrs 5 hrs
Video Lectures	1. https://www.youtube.com/watch?v=ysoC8S96pZU&list=PLBBog2r6uMCResrR48HziFtNx4-BDOmU0 2. https://www.youtube.com/playlist?list=PLmCsXDGbJHdhULIoYzIIIeFFJSo1NlMbN 3. https://www.youtube.com/watch?v=dCWuXDBRFtk&list=PL2NZAYdLkYvhFnqbvLbwf4ZM4rH99Jap6 4. https://www.youtube.com/watch?v=a4u_caEWTR8&list=PL2NZAYdLkYvg__5SpIDMlRopz-dD_KsIX	36 Min 1 hr 6 Min 8 Min 50 Sec
Web References	1. https://refactoring.guru/design-patterns 2. https://www.geeksforgeeks.org/system-design	

Course Code: BCSCY0514	Course Name: IoT Security and Forensics	L	T	P	C
Course Offered in: CSE (CYS)		3	0	0	3

Prerequisite: Basics of Networking, Cybersecurity and Programming

Course Objectives:ss

The course aims to provide a comprehensive understanding of Internet of Things (IoT) architecture, associated security challenges, and potential attack vectors. It also equips students with knowledge and skills in securing IoT systems and conducting forensic investigations in IoT environments.

Course Outcome: After completion of the course, the student will be able to		Bloom's Knowledge Level (KL)
CO1	Understand the architecture, components, and communication protocols of IoT systems.	K2
CO2	Analyze various threats, vulnerabilities, and attack surfaces in IoT environments.	K4
CO3	Apply appropriate security mechanisms, including encryption, authentication, and access control, to protect IoT systems.	K3
CO4	Demonstrate techniques for collecting, preserving, and analyzing digital evidence from IoT devices.	K3
CO5	Use forensic tools and methodologies to investigate real-world IoT security incidents and suggest mitigation strategies.	K3

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	2	-	2	2	2	-	2	-	1	-	**2**	2	-
CO2	2	3	1	1	2	3	-	2	1	1	1	**2**	2	2
CO3	3	2	3	2	2	2	1	2	1	2	2	**3**	2	2
CO4	2	3	-	3	3	1	-	2	1	1	1	**2**	2	3
CO5	2	2	2	2	3	1	-	2	2	2	1	**3**	2	3

Course Contents / Syllabus

Unit 1	Introduction to IoT and Security Landscape	10 hours

Fundamentals of IoT: Definition, evolution, components, IoT Architecture: Perception, Network, Middleware, Application layers, IoT Communication Protocols: MQTT, CoAP, AMQP, HTTP/HTTPS, Bluetooth, Zigbee, 6LoWPAN, IoT Ecosystem: Devices, Gateways, Cloud Services, Mobile Apps, IoT in different domains: Smart Home, Smart Cities, Health, Industry 4.0, Security Goals in IoT: Confidentiality, Integrity, Availability, Authentication, Privacy, IoT-specific security challenges and resource constraints. Edge and Fog Computing in IoT, Zero Trust concept in IoT environments.

Unit 2	Threat Modeling, Vulnerabilities, and Attack Surface in IoT	10 hours

Threat Modeling Techniques: STRIDE, DREAD, Vulnerability Scanning and Assessment in IoT, Physical Attacks: Side-channel attacks, device tampering, Network Attacks: DDoS, Eavesdropping, Man-in-the-Middle (MITM), Replay attacks, Software Attacks: Malware, buffer overflows, insecure firmware, remote code execution, Botnets in IoT (e.g., Mirai, Mozi), Security Risks in IoT, Lifecycle: Manufacturing, Deployment, Maintenance, OWASP Top 10 IoT Vulnerabilities. Firmware vulnerabilities and insecure APIs, Supply Chain Attacks in IoT devices.

Unit 3	IoT Security Mechanisms, Standards, and Architectures	10 hours

Authentication: Token-based, certificate-based, Authorization: Role-based, Attribute-based access control, Cryptographic Techniques: Lightweight encryption (AES-CCM, ECC), symmetric vs. asymmetric encryption, Secure Communication Protocols (TLS/DTLS for IoT), Security-by-Design: Secure Boot, Trusted Platform Unit (TPM), Secure Firmware Updates, Identity and Access Management in IoT, End-to-End Security Architectures, , Device Identity Management and PKI for IoT.

Unit 4	IoT Forensics: Principles, Tools, and Data Collection	8 hours

Basics of Digital Forensics and relevance to IoT, Forensic Readiness in IoT Systems, Evidence Sources in IoT: Devices, Network Cloud, Mobile Interfaces, Data Acquisition Techniques: Live vs. dead forensics, remote acquisition, volatile data, Chain of Custody and Integrity Verification, Anti-forensics and tamper detection in IoT, IoT Forensic Challenges: Device diversity, encryption, decentralized data, Legal, Privacy, and Ethical Issues, Logging and Monitoring strategies for forensic readiness.		
Unit 5	**Advanced IoT Forensics, Case Studies, and Emerging Trends**	**7 hours**
IoT Forensics Tools: Autopsy, Volatility, IoT-specific tools like IoT Scope, Memory Forensics for Embedded Devices Firmware Analysis and Reverse Engineering Basics, Network Traffic Analysis in IoT Forensics, Case Studies: Smart home forensics, Wearable device investigations, Industrial IoT breaches, Incident Response in IoT: Detection, Containment, Recovery. Cloud Forensics in IoT environments, Emerging Trends: AI for IoT Security, Blockchain for IoT Integrity, Edge Forensics.		
	Total Lecture Hours	**45 hours**

TextBooks:

	Authors Name
1. Internet of Things: A Hands-On Approach, 1st Edition, Universities Press	Arshdeep Bahga, Vijay Madisetti
2. Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations, , 1st Edition CRC Press / Taylor & Francis Group,	Fei Hu

Reference Books:

	Authors Name
1. Digital Forensic Investigation of Internet of Things (IoT) Devices, 1st Edition 2021 Springer Cham	Reza Montesari
2. Privacy,Security and Forensics in IoT 1st Edition (2022) Springer Cham	Fiona Carrol
3.The Iot Hackers Hand Book, 1st Edition (2019) Apress/Springer	Aditya Gupta

SeContent Links:		Duration (in Hrs)
MOOCs	1. https://infyspringboard.onwingspan.com/web/en/app/toc/lex_auth_01384661405937664051513_shared/overview 2. https://infyspringboard.onwingspan.com/web/en/app/toc/lex_auth_013094443365384192267 1_shared/overview	3Hrs 25Min 2Hrs 16Min
Video Lectures	1. https://www.youtube.com/watch?v=hDcJnsYQiEc 2. https://www.youtube.com/watch?v=MYXIw5aqYNQ 3. https://www.youtube.com/watch?v=4YAsAdCa9sU 4. https://www.youtube.com/watch?v=mN7tHGBbg_Y 5. https://www.youtube.com/watch?v=B7tTQ272OHE	54 Min 21 Sec 7 Min 1 Sec 34 Min 41 Sec 2 hr 9 Min 15 Min 24 Sec
Web References	1. https://transformainsights.com/blog/iot-security-evolving-landscape 2. https://transformainsights.com/blog/iot-security-evolving-landscape	

LAB Course Code: BCSE0552B	**LAB Course Name: Computer Network and Network Programming Lab**	**L**	**T**	**P**	**C**
Course Offered in: CSE(CYS)		**0**	**0**	**4**	**2**

Pre-requisite: The student should have a basic knowledge of data communication and programming.

Course Objectives:

The practical course aims to provide students with hands-on experience in computer networks and cybersecurity concepts using industry-relevant tools and techniques. Students will develop proficiency in network commands, socket programming, and the implementation and analysis of network protocols. The course also enables learners to use simulation tools for evaluating network performance, preparing them to address real-world networking and cybersecurity challenges effectively.

Course Outcome: After completion of the course, the student will be able to		Bloom's Knowledge Level (KL)
CO1	Apply networking concepts, IP addressing, subnetting, routing protocols, and network simulator tools to configure and establish computer networks.	K3
CO2	Analyze and implement various communication techniques, congestion control methods, routing algorithms, and packet transmission using socket programming.	K4
CO3	Evaluate client-server applications, packet capture mechanisms, and network protocol analysis using TCP/UDP sockets and network monitoring tools.	K5

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	3	3	3	3	2	2	2	2	2	1	3	3	2
CO2	3	3	2	3	3	1	1	1	2	2	1	3	3	2
CO3	3	3	3	3	3	2	2	1	2	2	1	3	3	3

List Of Practical's (Indicative & Not Limited To)	**CO**
1. Basic Networking commands.	**CO1**
2. Familiarization of network simulator software - Setting up a small network, Configure interfaces, IP addresses and routing Protocols.	**CO1**
3. Build a small network using Cisco Packet Tracer.	**CO1**
4. Setting up a Network LAN with sub-netting and CIDR concept for a specific scenario.	**CO1**
5. Configuration and simulation of static and dynamic routing protocols using Cisco Packet Tracer	**CO1**
6. Study and implementation of DNS and DHCP server configuration in a LAN environment	**CO1**
7. Implementation of Checksum	**CO2**
8. Implementation of error detection and correction techniques using CRC and Hamming Code.	**CO2**
9. Implementation of congestion control algorithms.	**CO2**
10. Implementation and simulation of algorithms for routing protocols.	**CO2**
11. Socket Programming for TCP Client-Server Communication	**CO2**
12. Socket Programming for UDP Client-Server Communication	**CO2**
13. Implementation of Unicast Communication using Socket Programming	**CO2**
14. Implementation of Broadcast Communication in Computer Networks	**CO2**

15. Implementation of Multicast Communication using UDP Sockets	**CO2**
16. Study and Analysis of TCP Three-Way Handshake using Wireshark.	**CO3**
17. Study and implementation of Socket Address Structures and Byte Ordering Functions.	**CO3**
18. Configuration and implementation of Socket Options and Timeout Mechanisms.	**CO3**
19. Development of Client-Server File Transfer Application using TCP Sockets.	**CO3**
20. Development of a chat application using TCP socket programming.	**CO3**
21. Development of Concurrent Client-Server Communication System.	**CO3**
22. Implementation of Raw Socket Programming for Packet Generation.	**CO3**
23. Development of a packet capture and filtering application using raw sockets.	**CO3**
24. Simulation and analysis of network traffic using Wireshark.	**CO3**
25. Experimental study of Application Protocols using network packet sniffers and analysers.	**CO3**
26. Implementation of a simple Network Intrusion Detection System (NIDS) using packet sniffing and traffic analysis tools.	**CO3**
Total Hours: 60 hrs.	

LAB Course Code BCSCY0551	LAB Course Name: Digital Forensics Lab	L	T	P	C
Course Offered in: CSE (CYS)		0	0	2	1

Pre-requisite: Fundamental knowledge of computer networks, operating systems, and cyber security principles

Course Objectives:

To provide hands-on experience in investigating and analyzing digital and mobile devices. Students will learn to use various forensic tools and techniques to recover, analyze, and report digital evidence. The practical's cover disk imaging, file carving, OS artefact analysis, mobile data extraction, network traffic analysis, and cloud forensics.

Course Outcome: After completion of this course, students will be able to:		Bloom's Knowledge Level (KL)
CO1	Apply digital evidence collection techniques and forensic tool usage for computer forensics	K3
CO2	Analyse digital evidence in mobile devices, network forensics investigations, and applying forensic techniques to extract valuable insights.	K4
CO3	Analyse digital evidence in cloud and emerging technology environments, applying forensic techniques to conduct investigations and ensure compliance with legal and ethical standards	K4

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	3-	2	2-	2	2	2	2	2	1	2	3	2	2
CO2	3	3	2	3	2	2	2	2	2	1	-1	3	2	2
CO3	3	3	2	2	2	2	2	2	2-	1	2	3	2	2

List Of Practical's (Indicative & Not Limited To)	**CO Mapping**

1. Using tools to identify and collect digital evidence and preserve digital evidence (with chain of custody documentation)	
2. Installation and basic usage of forensic tools	CO1
3. Analysing case studies related to legal and ethical issues	CO1
4. Research and documentation on a historical case	CO1
5. Creating and verifying disk images	CO1
6. Recovering files and data from disk images	CO1
7. Analysing system artifacts from different OS	CO1
8. Log analysis and event correlation using system/network logs (aligned with SIEM)	CO1
9. Extracting data logically from various mobile devices	CO2
10. Extracting data physically from various mobile devices	CO2
11. Analysing extracted data from mobile devices	CO2
12. Identifying and reporting on challenges in mobile forensics	CO2
13. Capturing and analysing network packets	CO2
14. Using tools like tcpdump to capture network traffic	CO2
15. Detecting and analysing network-based attacks	CO2
16. Performing deep packet inspection and correlating events	CO2
17. Basic memory forensics (analysing RAM images using tools like Volatility)	CO3
18. Extracting and analysing data from cloud platforms	CO3
19. Performing forensic analysis on various IoT devices	CO3
20. Legal and Ethical Compliance Case Study	CO3
21. Prepare forensic investigation reports while maintaining chain of custody and compliance with cyber laws and ethical standards.	CO3
Total Hours: 30 hrs.	

LAB Course Code: BCSAI0512P	LAB Course Name: Advanced Java Programming Lab	L	T	P	C
Course Offered in: CSE(AI)/CSE(AIML)/CSE(DS)/CSE(CS)/CYS/IOT/MCT		0	0	2	1

Pre-requisite: PROGRAMMING LANGUAGE PREFEREBALY JAVA

Course Objectives:

Provide hands-on experience to develop scalable, database-driven applications using Spring Boot, JPA, and RESTful APIs with proper integration and deployment practices.

Course Outcome: After completion of the course, the student will be able to

1. Students will be able to develop dynamic web applications using JDBC, Servlets, and JSP with proper database connectivity and session management.
2. Students will apply Spring Framework concepts, including IOC and Dependency Injection, to build structured and scalable applications.
3. Students will design and implement RESTful web services using Spring Boot and JPA and deploy complete full-stack applications effectively.

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	POS1	POS 2	POS 3
CO1	**3**	3	2	2	1	1	-	3	1	1	2	1	1	2
CO2	3	3	3	2	2	1	-	3	1	1	2	1	2	2
CO3	3	3	3	2	2	1	-	3	1	1	2	1	2	2

List Of Practical's (Indicative & Not Limited To)

1. Write Java program to create a demo table emp having fields, name, city and insert two rows by using JDBC.
2. Write a Java program using Statement to create a table for Students with fields id, name, age, and grade.
3. Write a Java program to demonstrate a money transfer transaction between two bank accounts. Ensure that both debit and credit operations are either committed together or rolled back in case of an error.
4. Write a Java program using PreparedStatement to delete student records where grades are below a given threshold.
5. Write a Java program to call a stored procedure that calculates the total salary of employees in a given department.
6. Write a servlet program to select the details of an employee (emp id, empname, empadd,empphone) and display on browser in appropriate format.
7. Write a GenericServlet to handle employee registration. The servlet should: Accept employee details (name, email, designation, salary) via a form (POST request). Store the details in a database (use JDBC). Display a success message after successful insertion
8. Implement a servlet program that redirects a request to Google.com.
9. Develop a Java Servlet program to demonstrate session tracking using the following techniques:

(i) Cookies
(ii) URL Rewriting
(iii) HttpSession

The program should maintain user information (such as visit count or username) and display it across multiple requests using all three session tracking methods.

10. Implement all JSP scripting elements (scriptlet, expression and declaration).

11. Implement all JSP directive elements (page, include and taglib).
12. Implement a JSP program for arithmetic exception error handling by using html page, jsp page, and errorPage, isErrorPage directives.
13. A company recruitment portal requires candidates to register before applying for jobs. Design a JSP page for registration and a Servlet to store user details in a MySQL database using JDBC. How would you implement session management in a JSP-based web application to keep users logged in across multiple pages?
14. Implement a JSP which inserts the details of the 3 or 4 users who register with the web site by using registration form. Authenticate the user when he submits the login form using the user's name and password from the database. Design and implement a simple shopping cart example with session tracking API.
15. Demonstrate the use of ApplicationContext as an IOC container to load beans. Concept: Spring IOC container usage.
16. Define multiple Spring Beans and manage them using XML-based configuration. Concept: Spring Modules and IOC in action.
17. Implement a Setter-based DI to inject a service bean into another. Concept: Using setters for bean wiring.
18. Demonstrate Field Injection using @Autowired annotation. Concept: Simplified DI using annotations.
19. Program: Configure beans using Java-based configuration with @Configuration and @Bean. Concept: Pure Java Spring configuration.
20. Program: Use Component Scanning and @Component, @Service, @Repository. Concept: Autodetection of components.
21. Program: Set up a Maven project structure for a spring app and manage dependencies using pom.xml. Concept: Maven-based project setup
22. You are designing a web application for an online bookstore. Set up a basic Spring MVC structure with Dispatcher Servlet, controller, and view." Program Goal: Create a minimal Spring MVC app showing folder structure and web.xml setup.
23. Create a basic Spring Boot application using Spring Initializer and write a program to display "Hello World" on the browser using appropriate Spring Boot annotations.
24. Develop a Spring Boot application that uses annotations like @SpringBootApplication and @RestController to create a simple REST API that returns a welcome message.
25. Build a feedback page for a college portal. Create a Spring MVC controller that returns a welcome message on accessing /feedback." Program Goal: Implement a basic controller class using @Controller and map a simple GET request.
26. Develop a Spring Boot web application for a library website that displays a homepage containing contact information and a static banner. The application should serve HTML pages from the /templates directory and load static resources such as images and CSS from the /static directory to demonstrate proper handling of dynamic views and static content.
27. Develop a Java program for a Book management system where you need to reduce boilerplate code (such as getters, setters, and constructors) in the Book class. Use Project Lombok annotations like @Data, @NoArgsConstructor, and @AllArgsConstructor to simplify the class definition. The program should create Book objects and display their details to demonstrate the use of these annotations.
28. You are designing a simple library system. Begin by creating an entity Book and use JPA to persist data to a relational database.
29. In a school database system, annotate an @Entity class Student with appropriate JPA annotations like @Id, @GeneratedValue, @Column.
30. In a hospital management system, create a one-to-one relationship between Patient and Medical Record using JPA
31. Implement CRUD operations on MYSQL database using spring data rest with POSTMAN client.
32. Develop a system for online courses where one Instructor can have many Courses. Model this using JPA annotations.
33. Develop a simple Java application using JPA to create an entity class (e.g., Student) and map it to a database table using basic JPA annotations like @Entity, @Id, and @Column.
34. Write a program using JPA to perform basic CRUD operations (insert and display) on an entity using annotations and an ORM approach.
35. Create a JPA-based application that demonstrates the use of annotations such as @Table, @GeneratedValue, and @Column for mapping an entity to a relational database.

36. Build a college management system where Students can enroll in multiple Courses. Implement many-to-many using JPA.
37. Develop an employee management system that performs Create, Read, Update, and Delete operations using JpaRepository.
38. In a bookstore app, compare the use of CrudRepository vs. JpaRepository for managing Book entities
39. Develop a RESTful web service that produces and consumes data in both JSON and XML formats and test the API using Postman.
40. Create a Simple application with a REST API for CRUD operations, demonstrate JSON/XML data handling, test it using Postman, and deploy the application on a local server.

LAB Course Code: BCSCY0512P	**LAB Course Name: Malware Analysis and Reverse Engineering Lab**	**L**	**T**	**P**	**C**
Course Offered in: CSE (CYS)		**0**	**0**	**2**	**1**

Pre-requisite: Computer Networks, Operating Systems, C/C++ or Python Programming

Course Objectives:

This course introduces techniques for analyzing and understanding malware behavior and reverse engineering malicious software. It equips students with skills to dissect malware through static and dynamic analysis and understand countermeasures and detection techniques.

Course Outcome: After completion of the course, the student will be able to		Bloom's Knowledge Level (KL)
CO1	Understand malware fundamentals, malware categories, attack vectors, executable formats, malware lifecycle, legal and ethical considerations, and basic static malware analysis techniques.	K2
CO2	Apply static and dynamic malware analysis techniques using malware analysis tools, sandboxing environments, network monitoring, and behavioral analysis utilities.	K3
CO3	Perform reverse engineering, debugging, memory forensics, IOC extraction, anti-analysis detection, and professional malware investigation and reporting.	K3

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO – PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	3	1	2	3	2	-	2	-	1	-	2	1	2
CO2	2	3	2	3	3	1	-	1	1	1	-	2	1	2
CO3	3	3	3	3	3	2	-	2	2	2	-	2	2	1

List Of Practical's (Indicve & Not Limited To)	**CO**
1. Study malware categories, lifecycle, and attack vectors using real-world malware examples	CO1
2. Analyze legal and ethical issues in malware analysis through case studies	CO1
3. Analyze PE and ELF executable structures using PEStudio and Detect It Easy	CO1
4. Perform string extraction, hashing, and VirusTotal reputation analysis	CO1
5. Detect packed malware and create basic YARA rules for malware identification	CO2
6. Configure an isolated malware analysis environment using VirtualBox/VMware	CO2
7. Monitor malware behaviour using Process Explorer and Process Monitor	CO2
8. Capture and analyze malware network traffic using Wireshark and TCPView	CO2
9. Perform automated malware analysis using Cuckoo Sandbox and observe evasion behaviour	CO2
10. Study x86 assembly instructions and analyze program control flow	CO3
11. Perform binary disassembly and debugging using IDA Pro/Ghidra and x64dbg	CO3
12. Identify obfuscation and anti-disassembly techniques in malware binaries	CO3
13. Perform memory forensics using Volatility and extract Indicators of Compromise (IOCs)	CO3
14. Prepare a professional malware analysis report with mitigation strategies and case study analysis	CO3
Total Hours: - 30 Hours	

Course Code: BCSCY0555	Course Name: Machine Learning for Cyber Security	L	T	P	C
Course Offered in: CSE (CYS)		0	0	6	3

Pre-requisite: Basic Python, Python libraries (Numpy, Pandas, Matplotlib, Seaborn), Data Structures, Cyber Security Fundamentals

Course Objectives: The course objective is to apply foundational machine learning concepts, including data preprocessing, supervised and unsupervised learning algorithms (regression, classification, clustering), and ensemble methods, to address real-world problems, evaluate model performance critically, and implement practical solutions, particularly in areas like Cyber Security applications.

Course Outcome: After completion of the course, the student will be able to		Bloom's Knowledge Level (KL)
CO1	Apply to the fundamental concepts, types, and applications of Machine Learning, particularly within the context of Cyber Security and various data preprocessing and dimensionality reduction techniques to prepare datasets for Machine Learning models.	K2
CO2	Evaluate linear regression models, optimizing them with Gradient Descent and improving their robustness using regularization techniques	K4
CO3	Explore various classification algorithms, including Logistic Regression, Decision Trees, Support Vector Machines, and K-Nearest Neighbors, to solve binary and multiclass classification problems.	K4
CO4	Apply probabilistic methods (Naive Bayes) and advanced ensemble techniques (Random Forest, AdaBoost, Gradient Boosting, XGBoost) to build robust classification models.	K4
CO5	Implement diverse unsupervised learning techniques, including K-Means, hierarchical, and DBSCAN clustering along with anomaly detection systems.	K4

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	2	1	1	1	2	2	-	1	2	2	3	2	3
CO2	3	3	1	2	2	2	3	-	2	3	2	3	2	2
CO3	2	3	2	3	3	3	2	1	3	2	2	3	3	2
CO4	2	3	2	3	3	2	2	1	2	1	2	2	2	3
CO5	2	2	3	3	3	2	2	2	2	2	3	3	2	2

Course Contents / Syllabus

Unit 1	**Introduction to ML in Cyber Security**	**15 hours**

Introduction to Machine Learning: Motivation, Definition, Applications of Machine Learning focusing on Cyber Security. Types of Machine Learning: Supervised, Unsupervised, and Reinforcement Learning. Datasets and Features: Features and their types, handing missing data, Dealing with categorical features, Feature Scaling, Feature selection, outlier detection and removal. Dimensionality reduction: Curse of Dimensionality, Principal Component Analysis (PCA) Algorithm. Cyber security challenges and need for ML, Types of cyber data (logs, network traffic, malware data)

Unit 2	**Regression and Regularization**	**14 hours**

Introduction to Regression: Regression Problem, Linear regression model (Simple, Multiple, and Polynomial). Errors: Mean Squared Error (MSE), Root Mean Squared Error (RMSE), Mean Absolute Error (MAE). Cost function: formula, intuition and visualization. Gradient Descent: Algorithm, intuition, learning rate, and Gradient Descent for linear regression. Evaluating the Accuracy of Linear Regression Model: R2 and Adjusted R2. Regularization: Bias and Variance, Overfitting and Underfitting, L1 and L2 Regularization, regularize cost function, Regularized Linear Regression

Unit 3	**Classification Algorithm**	**14 hours**

Classification: Classification problem, Binary and Multiclass Classification, Decision Boundary. Logistic regression model for binary classification, Cost function of logistic regression model, Regularized logistic regression, One Vs. All strategy for multiclass classification using logistic regression. Measuring Performance of Classification Model: Accuracy, Precision, Recall, F1-Score, ROC-AUC curve, Confusion matrix. Decision Trees: Decision Tree Classification Algorithm, Attribute Selection Measures, Variants of Decision Trees (ID3, C4.5, CART) Large Margin Classifier: Support Vector Machines Instance Based Learning: K Nearest Neighbor Algorithm

Unit 4	**Probabilistic Models and Ensembles**	**14 hours**

Probabilistic Methods for Classification: Bayesian Learning, Naive Bayes Classifier, Bayesian belief networks. Tree Ensembles: Using multiple decision trees, Bagging Vs. Boosting, Sampling with replacement, Random Forest Algorithm, Adda boost, Gradient Boosting, Xgboost Algorithm

Unit 5	**Clustering Algorithms and Anomaly Detection**	**15 hours**

Unsupervised Learning &Clustering: The problem of clustering, Distance measures. Partition Based Methods: K-Means Clustering (Intuition, Algorithm, Optimization objective, Initializing K-Means, choosing number of clusters), K-Medoids and K-Mode clustering algorithms. Hierarchical Clustering (Single Linkage, Complete Linkage, AGNES (Agglomerative Nesting), DIANA (Divisive Analysis). Density-based Clustering: DBSCAN Algorithm. Anomaly Detection: Finding unusual events, Gaussian Distribution and Gaussian Mixture Model, Anomaly Detection Algorithm, Developing and evaluating anomaly detection system.

	Total Lecture Hours	**72 hours**

Textbooks:

1. Machine Learning, Deep Learning and AI for Cybersecurity, Mark Stamp & Martin Jureček, 1st Edition (2025), Springer
2. Machine Learning, Tom Mitchell, 1st Edition (1997), McGraw-Hill Education
3. Data Mining and Machine Learning in Cybersecurity, Sumeet Dua & Xian Du, 1st Edition (2011), CRC Press

Reference Books:

1. Machine Learning: An Artificial Intelligence Approach, Volume 1, Ryszard, S., Michalski, J. G. Carbonell and Tom M. Mitchell, 1st Edition (2014), Elsevier
2. Machine Learning: An Algorithmic Perspective, Stephen Marsland, 2nd Edition (2015), CRC Press/Taylor & Francis

Self-Study Content Links:		Duration (in Hrs)
MOOCs	1. Introduction to AI & ML https://infyspringboard.onwingspan.com/web/en/app/toc/lex_auth_01424935121484185673/overview 2. Indroduction to Cybersecurity https://www.netacad.com/courses/introduction-to-cybersecurity?courseLang=en-US	64 Hrs 13 Min 6 Hrs
Video Lectures	1. https://www.youtube.com/playlist?list=PL1xHD4vteKYVpaIiy295pg6_SY5qznc77 2. https://www.youtube.com/watch?v=JxcBm7CRtI0&list=PL74sw1ohGx7GHqDHCkXZeqMQBVUTMrVLE 3. https://www.youtube.com/watch?v=OQV8WmUdeIo&list=PLbMVogVj5nJSpj5sl-8tdKARg1lw2wEa- 4. https://www.youtube.com/watch?v=TTo2kjrAuTo&list=PL05umP7R6ij2YE8rRJSb-olDNbntAQ_Bx 5. https://www.youtube.com/watch?v=5p8B2Ikcw-k&list=PLubVnfIHABZQZXwT7Nx3M4Joixwe3V824	35 Hrs 48 Min 43 Min 56 Sec 55 Min 20 Sec 1 Hrs 18 Min 32 Min 47 Sec
Web References	1. https://developers.google.com/machine-learning/intro-to-ml 2. https://scikit-learn.org/stable/ 3. https://www.tensorflow.org/ 4. https://www.kaggle.com/datasets	30 Min 2 Hrs 3 Hrs 30 Min

List Of Practical's (Indicative & Not Limited To)				
Lab No.	**Unit**	**Topic**	**Program Logic Building**	**CO Mapping**
1.1	1	Cyber Security Dataset Exploration using Anaconda & Jupyter Notebook	Use Anaconda and Jupyter Notebook to load cyber security datasets (network intrusion/malware data) from Kaggle or Sklearn. Explore dataset features, analyze attack labels, implement basic ML models using Sklearn, and study their application in cyber threat detection	CO1
1.2	1	Data Pre-processing on Cyber Security Dataset	Perform data exploration, cleaning, missing value handling, duplicate removal, outlier detection, categorical encoding, feature scaling, and correlation analysis on a cyber-security dataset.	CO1
1.3	1	Data Exploration and Cleaning	Load the dataset and perform basic data exploration. Check for missing values, remove or impute missing data using mean/median for numerical features and mode for categorical features. Handle duplicate records and detect/remove outliers using statistical methods.	CO1
1.4	1	Handling Categorical Variables	Apply encoding techniques such as One-Hot Encoding, Label Encoding, Ordinal Encoding, and Target Encoding for categorical attributes like protocol type, service, and flag features.	CO1
1.5	1	Feature Scaling	Implement feature scaling techniques including MinMaxScaler, StandardScaler, MaxAbsScaler, RobustScaler, and Normalizer to normalize numerical features for machine learning models.	CO1
1.6	1	Correlation Analysis	Perform correlation analysis using correlation matrices and heat maps to identify relationships between features and remove highly correlated or redundant attributes.	CO1
2.1	2	Principal Component Analysis (PCA)	Implement Principal Component Analysis (PCA) on a cyber-security dataset (e.g., network intrusion or malware data) to reduce high-dimensional features. Preprocess the data (handle missing values, scaling), apply PCA to extract important components, and analyze how dimensionality reduction helps in improving model performance and visualization.	CO2
2.2	2	Evaluation Metrics and Linear Regression	Implement a class for MAE, RMSE, Log Loss, R^2, and Adjusted R^2 metrics. Train a linear regression model to predict security-related numerical features.	CO2
2.3	2	Linear Regression on Cyber Security Dataset	Load and preprocess cyber-security data, train a linear regression model for predicting continuous features such as packet size or network traffic, and evaluate performance.	CO2

2.4	2	Gradient Descent Algorithm	Implement Gradient Descent for regression on cyber-security data and analyze the effect of different learning rates on convergence and optimization.	CO2
2.5	2	Under fitting, Overfitting & Hyper parameter Tuning	Demonstrate under fitting and overfitting using regression models. Apply Grid Search and Random Search techniques for hyper parameter tuning	CO2
2.6	2	Lasso and Ridge Regression	Implement regularized regression models (Lasso and Ridge) on cyber-security datasets and compare their performance to study regularization effects	CO2
3.1	3	Logistic Regression for IoT Traffic Classification	Implement Logistic Regression for binary classification of malicious and benign IoT network traffic.	CO3
3.2	3	Logistic Regression for Intrusion Detection	Preprocess cyber-security data, train a Logistic Regression model, and evaluate attack vs normal traffic classification using confusion matrix and accuracy metrics.	CO3
3.3	3	One-Hot Encoding with Logistic Regression	Perform malicious vs benign classification using One-Hot Encoding and Logistic Regression. Evaluate using accuracy, precision, recall, and confusion matrix.	CO3
3.4	3	K-Nearest Neighbors (KNN) from Scratch	Implement KNN from scratch using Euclidean distance and majority voting for attack vs normal classification on cyber-security data.	CO3
3.5	3	KNN with ROC-AUC Evaluation	Train a KNN model for malicious vs normal activity classification and evaluate performance using ROC-AUC, precision, recall, and accuracy.	CO3
3.6	3	Decision Tree using ID3 Algorithm	Build a Decision Tree using the ID3 algorithm to classify activities as malicious or benign based on network behavior features.	CO3
3.7	3	Support Vector Machine (SVM)	Train and evaluate an SVM classifier on malware or intrusion detection datasets using accuracy, precision, recall, and confusion matrix.	CO3
3.8	3	Naïve Bayes for Phishing Detection	Implement a Naïve Bayes classifier on phishing email/message datasets after preprocessing text data and evaluate performance.	CO3
3.9	3	Naïve Bayes for Intrusion Detection	Train a Naïve Bayes classifier on intrusion/login activity datasets to classify malicious and benign events.	CO3
4	4	Random Forest and XGBoost for Malware Classification	Implement Random Forest and XGBoost algorithms for malware/intrusion detection and compare performance using classification metrics.	CO4
4.1	4	Random Forest and XGBoost for Anomaly Detection	Train Random Forest and XGBoost models for malicious vs normal activity classification on anomaly	CO4

			detection datasets.	
4.2	4	K-Means Clustering for Activity Segmentation	Perform user/activity segmentation using K-Means Clustering to identify normal and anomalous behavior patterns.	CO4
4.3	4	K-Medoids Clustering for Log/Event Grouping	Apply K-Medoids clustering on system logs/security alerts to identify common attack patterns and anomalies.	CO4
5	5	Hierarchical Clustering with Dendrogram	Perform hierarchical clustering on logs or network traffic data and visualize clusters using a dendrogram.	CO5
5.1	5	DBSCAN for Anomaly Detection	Use DBSCAN clustering to identify suspicious or malicious activities as anomalies in cyber-security datasets.	CO5
5.2	5	Gaussian Mixture Model (GMM) Clustering	Perform probabilistic clustering using GMM to identify behavioral patterns and potential attack types.	CO5
5.3	5	Anomaly Detection using Isolation Forest/DBSCAN	Implement anomaly detection systems using Isolation Forest or DBSCAN to detect malicious activities in cyber-security datasets.	CO5

Course Code: BCSCC0501Y	Course Name: Design Thinking –II	L	T	P	C
Course Offered in: All computing branches		2	0	0	2

Pre-requisite: Student must complete the Design Thinking-I course.

Course Objectives:

The objective of this course is to upgrade Design Thinking skills by learning and applying advanced and contextual Design Thinking Tools. It aims to solve a Real-Life Problem by applying Design Thinking to create an impact for all the stakeholders

Course Outcome: After completion of the course, the student will be able to		Bloom's Knowledge Level (KL)
CO1	Learn sophisticated design tools to sharpen their problem-solving skills	K2
CO2	Construct innovate ideas using design thinking tools and converge to feasible idea for breakthrough solution	K6
CO3	Implement storytelling for persuasive articulation	K3
CO4	Understanding the nature of leadership empowerment	K2
CO5	Understand the role of a human being in ensuring harmony in society and nature	K2

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	2	2	2	3	3	2	2	2	3	2	3	2	-	-
CO2	3	2	3	2	3	2	2	3	2	2	2	2	3	1
CO3	3	2	3	2	3	2	2	3	2	2	2	3	3	1
C04	3	2	3	2	3	2	2	3	2	2	2	3	2	-
CO5	3	2	3	3	3	2	2	3	3	2	3	3	3	-

Course Contents/ Syllabus

Module 1	**Introduction**	**8 hours**

Design thinking & Innovation, Design Thinking Mindset and Principles, recap of 5-Step Process of Design Thinking, Design Approaches, additional in-depth examples of each design approaches. Simon Sinek's – Start with Why, The Golden Circle, Asking the "Why" behind each example (an in-class activity of asking 5-WHYS), The Higher Purpose, in-class activity for LDO & sharing insights Visualization and its importance in design thinking, reflections on wheel of life (in-class activity for visualization & Wheel of Life), Linking it with Balancing Priorities (in class activity), DBS Singapore and Bank of Americas' Keep the Change Campaign. Litter of Light & Arvind Eye Care Examples, understanding practical application of design thinking tools and concepts, case study on McDonald's Milkshake / Amazon India's Rural Ecommerce & Gillette Working on 1-hour Design problem, Applying RCA and Brainstorm on innovative solutions. Main project allocation and expectations from the project.

Module 2	**Refinement and Prototyping**	**10 hours**

Refine and narrow down to the best idea, 10-100-1000gm, QBL, Design Tools for Convergence – SWOT Analysis for 1000gm discussion. In-class activity for 10-100-1000gm & QBL Prototyping (Convergence): Prototyping mindset, tools for prototyping – Sketching, paper models, pseudo-codes, physical mockups, Interaction flows, storyboards, acting/role-playing etc, importance of garnering user feedback for revisiting Brainstormed ideas. Napkin Pitch, Usability, Minimum Viable Prototype, Connecting Prototype with 3 Laws, A/B Testing, Learning Launch. Decision Making Tools and Approaches – Vroom Yetton Matrix, Shift-Left, Up, Right, Value Proposition, Case study: Careerbuddy, You-Me- Health Story & IBM Learning Launch. In-class activities on prototyping- paper-pen / physical prototype/ digital prototype of project's 1000gm idea.

Module 3	**Storytelling, Testing and Assessment**	**8 hours**

Storytelling: Elements of storytelling, Mapping personas with storytelling, Art of influencing, Elevator Pitch, Successful Campaigns of well-known examples, in-class activity on storytelling. Testing of design with people, conducting usability test, testing as hypothesis, testing as empathy, observation and shadowing methods, Guerrilla Interviews, validation workshops, user feedback, record results, enhance, retest, and refine design, Software validation tools, design parameters, alpha &beta testing, Taguchi, defect classification, random sampling. Final Project Presentation and assessing the impact of using design thinking

Module 4	**Innovation, quality and Leadership**	**8 hours**

Innovation: Need & Importance, Principles of innovations, Asking the Right Questions for innovation, Rationale for innovation, Quality: Principles & Philosophies, Customer perception on quality, Kaizen, 6 Sigma. FinTech case study of Design Thinking application – CANVAS Leadership, types, qualities and traits of leaders and leadership styles, Leaders vs Manager, Personas of Leaders & Managers, Connecting Leaders-Managers with 13 Musical Notes, Trait theory, LSM (Leadership Situational Model), Team Building Models: Tuckman's and Belbin's. Importance of Spatial elements for innovation.

Module 5	**Understanding Human Desirability**	**8 hours**

Comprehensive human goal: the five dimensions of human endeavour (Manaviya - Vyavstha) are: Education- Right living (Sikhsa- Sanskar), Health – Self-regulation (Swasthya - Sanyam), Justice – Preservation (Nyaya- Suraksha), Production – Work (Utpadan – Karya), Exchange – Storage (Vinimya – Kosh), Darshan- Gyan-Charitra (Shifting the Thinking) Interconnectedness and mutual fulfilment among the four orders of nature recyclability and self-regulation in nature, Thinking expansion for harmony: Self-exploration (Johari's window), group behaviour, interpersonal behaviour and skills, Myers-Briggs personality types (MBTI), FIRO-B test to repair relationships.

	Total Lecture Hours	**42 hours**

Textbook:

S. No	**Book Title**	**Author**
1.	UnMukt : Science & Art of Design Thinking, 2020, Polaris	Arun Jain
2.	Basics Design 08: Design Thinking, 2010, AVA Publishing SA	Gavin Ambrose and Paul Harris
3.	A Foundation Course in Human Values and Professional Ethics, First Edition, 2009, Excel Books: New Delhi	R R Gaur, R Sangal, G P Bagaria

Reference Books:

S.No	**Book Title**	**Author**
1.	Solving Problems with Design Thinking – Ten Stories of What Works, 2013, Columbia Business School Publishing.	Jeanne Liedta, Andrew King and Kevin
2.	Universal Human Values and Professional Ethics, 2022, Katson Books.	Dr Ritu Soryan
3.	101 Design Methods: A Structured Approach for Driving Innovation in Your Organization, 2013, John Wiley and Sons Inc, New Jersey.	Vijay Kumar
4.	Design of Business: Why Design Thinking is the Next Competitive Advantage, 2009, Harvard Business Press, Boston MA.	Roger L. Martin
5.	Change by Design, 2009, Harper Collins.	Tim Brown

Self-Study Content Links:

MOOCs	1. https://www.coursera.org/specializations/design-thinking?utm_medium=sem&utm_source=gg&utm_campaign=b2c_india_x_multi_ftcof_career-academy_cx_dr_bau_gg_pmax_gc_in_all_m_hyb_24-03_desktop&campaignid=21104989118&adgroupid=&device=c&keyword=&matchtype=&network=x&devicemodel=&creativeid=&assetgroupid=6544944776&targetid=&extensionid=&placement=&gad_source=1&gad_campaignid=21104990591&gbraid=0AAAADdKX6YJHt3GyzupmRYbPOgHkEeFp&gclid=Cj0KCQjw3K7RBhDJARIsAKRtP5RBjckHBvGEYiEnTRFA8EtXpl89ha-X8id2TOYd0e4Sf9WTvVnonK4aAmqrEALw_wcB 2. https://www.coursera.org/learn/uva-darden-designbiz	4 weeks 6 hrs

Video Lectures	1. https://www.youtube.com/watch?v=6_mHCOAAEI8 https://nptel.ac.in/courses/110106124 https://designthinking.ideo.com/ 2. https://www.youtube.com/watch?v=7enWesSofhg 3. https://youtu.be/rthuFS5LSOo https://www.youtube.com/watch?v=kho6oANGu_A 4. https://www.youtube.com/watch?v=9vMpHk44XXo&list=PL1xHD4vteKYVpaIiy295pg6_SY5qznc77&index=6 5. Reinforcement Learning Tutorial | Reinforcement Learning Example Using Python | Edureka - YouTube 6. Association Rule Mining – Solved Numerical Question on Apriori 7. Algorithm(Hindi) - YouTube 8. Q Learning Explained | Reinforcement Learning Using Python | Q Learning in AI | Edureka - YouTube	7 hrs
Web References	https://blog.experiencepoint.com/how-mcdonalds-evolved-with-design-thinking	

Course Code: BCSCC0552	Course Name: Research Methodology Ethics and Writing	L	T	P	C
Course Offered in: All computing branches		0	0	2	1

Pre-requisite: Basic communication skills, engineering fundamentals

Course Objectives:

This course equips students with fundamental research skills, including problem identification, literature review, data analysis, technical documentation, and ethical publication practices, while enhancing technical writing and scientific communication for academic and professional applications.

Course Outcome: After completion of the course, the student will be able to	**Bloom's Knowledge Level (KL)**
CO1 Analyze research methodologies, experimental design principles, and literature review techniques for identifying research gaps.	**K3**
CO2 Apply quantitative and qualitative data acquisition, analytical methods, technical documentation, and scientific citation practices in research activities.	**K4**
CO3 Develop technical reports, research manuscripts, and professional presentations using standard scientific writing and ethical communication practices.	**K2**

CO-PO Mapping (Scale: 1: Low, 2: Medium, 3: High)

CO \ PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	2	–	2	1	–	–	2	–	1	–	1	1	2
CO2	2	3	1	3	2	–	–	2	1	2	–	2	1	2
CO3	2	3	2	3	2	–	–	3	2	3	1	1	1	1

Course Contents / Syllabus

Module 1	Fundamentals of Research Methodology and Literature Review	7 hours

Definition of research, objectives of research, motivation and significance of research, types of research including fundamental, applied, qualitative, quantitative, and experimental research, stages of research process, research problem identification, formulation of research questions, identification of technical gaps, literature review methodologies, use of scientific databases such as Google Scholar, Scopus, Web of Science, IEEE Xplore, and ScienceDirect, keyword selection strategies, source reliability and credibility evaluation, annotated bibliography preparation, critical analysis of published research papers, and review writing techniques.

Module 2	Data Collection, Analysis, and Technical Documentation	7 hours

Primary and secondary data sources, data gathering methods, survey techniques, questionnaire design, experimental observations, data organization, structured sampling methods including random sampling, stratified sampling, and systematic sampling, basic statistical concepts including mean, median, standard deviation, graphical data representation, data analysis techniques, spreadsheet-based analysis, technical report preparation, scientific report structure including abstract, introduction, methodology, results, discussion, and conclusion, mini-project execution, research documentation, and technical documentation practices.

Module 3	Citation Management, Publication Ethics, and Research Integrity	7 hours

Ethical research practices, scholarly publishing standards, academic reference management, citation systems including IEEE, APA, and MLA, reference management software such as Mendeley and Zotero, plagiarism awareness, similarity detection tools, responsible citation practices, authorship ethics, predatory journals, peer review systems, journal indexing, impact factors, research integrity principles, publication misconduct, ethical compliance, professional publishing standards, citation formatting exercises, plagiarism analysis, journal quality evaluation, and ethical case studies.

Module 4	Technical Writing and Research Documentation	9 hours

Scientific and technical writing skills, engineering research documentation, professional documentation practices, technical report writing, project report preparation, review paper writing, conference paper drafting, research manuscript development, scientific writing styles, report organization, abstract preparation, introduction framing, methodology documentation, results presentation, discussion development, conclusion writing, proofreading, technical editing, document formatting, visual representation of technical data using tables, charts, and figures, documentation standards, formal technical presentations, dissemination of research findings, manuscript section drafting, technical document editing, and professional written

communication.		
Total Lecture Hours		**30 hours**
Textbook:		
SNO	**Book Title**	**Author**
1.	Research Methodology: Methods and Techniques	C.R. Kothari & Gaurav Garg
2.	Research Methodology: A Step-by-Step Guide for Beginners	Ranjit Kumar
3.	The Craft of Scientific Writing	Michael Alley
4.	How to Write and Publish a Scientific Paper	Day & Gastel
5.	Research Methodology and Scientific Writing	George Thomas
Reference Materials		
SNO		
1.	IEEE Author Guidelines	
2.	Elsevier Researcher Academy Resources	
3.	Springer Author Academy	
4.	WIPO Resources for Research Documentation	
5.	University digital library resources	
Self Study Content Links:		
MOOCs Courses	1. https://www.coursera.org/learn/research-methods 2. https://researcheracademy.elsevier.com/	6 hrs 20 hrs
Video Lectures	1. https://www.youtube.com/watch?v=rz30rRfManE&list=PLdj5pVg1kHiOypKNUmO0NKOfvoIThAv4N 2. https://www.youtube.com/watch?v=HYj4Ght1_qs 3. https://www.youtube.com/watch?v=N9tJCs-czOU&list=PLnIj1GYixjfrOhcWQq_ANzLFDniGYZ_-Q 4. https://www.youtube.com/watch?v=NM53k7x_jjk	17 hrs
Web References	https://researcheracademy.elsevier.com https://authorservices.wiley.com	

SYLLABUS- SEMESTER VI

Course Code: BCSCY0603	Course Name: Network Security and Cryptography	L	T	P	C
Course Offered in: CSE (CYS) & B. Tech CSE and Emerging Branches as Department Elective		3	1	0	4

Prerequisite: Familiarity Understanding of basic Networking Terms (e.g., IP, LAN, Router), Awareness of Digital Tools (Email, Cloud, Antivirus), Fundamental Logical Thinking, Cybersecurity fundamentals

Course Objectives:

This course aims to introduce the fundamental principles and concepts of network security and cryptography, provide insights into common network-based attacks and vulnerabilities and develop the ability to design secure network architectures using modern cryptographic tools and techniques.

Course Outcome: After completion of the course, the student will be able to		Bloom's Knowledge Level (KL)
CO1	Understand the fundamentals of cryptography and its applications in network security.	K1
CO2	Analyze different encryption algorithms and cryptographic protocols.	K2
CO3	Implement secure communication protocols to protect data transmission over networks.	K3
CO4	Identify common network attacks and employ countermeasures to mitigate them.	K3
CO5	Implement secure network architectures using cryptographic techniques.	K4

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	1	-	-	1	-	-	-	-	-	-	2	3	1
CO2	3	3	1	1	2	-	-	-	-	-	-	2	3	2
CO3	2	2	3	2	3	1	-	1	1	1	1	3	2	2
CO4	2	3	2	2	2	2	1	1	-	-	-	2	2	3
CO5	3	2	3	2	3	2	1	1	1	1	2	3	3	3

Course Contents / Syllabus

Unit 1	**Cryptographic Techniques**	**10 hours**

Introduction to Cryptography, Classical Cryptographic Techniques (Caesar Cipher, Monoalphabetic Cipher), Modern Symmetric Encryption Algorithms (AES, DES), Public Key Cryptography and RSA Algorithm (Key Generation, Encryption/Decryption), Digital Signatures and Hash Functions (SHA, Message Authentication Codes)

Unit 2	**Introduction to Network Security**	**9 hours**

Overview of Network Security Principles, Goals and Objectives of Network Security, Threats, Attacks, and Vulnerabilities (e.g., Malware, DoS), Security Policies and Mechanisms (e.g., Access Control, Firewalls), Risk Management and Assessment (e.g., Risk Analysis, Mitigation Strategies).

Unit 3	**Secure Communication Protocols**	**9 hours**

Secure Socket Layer (SSL) / Transport Layer Security (TLS – handshake process, certificate-based authentication), Internet Protocol Security (IPsec – AH/ESP protocols, tunnel and transport mode), Secure Shell (SSH – key-based authentication, port forwarding), Wireless Security Protocols (WPA, WPA2 – PSK, EAP authentication), Virtual Private Networks (VPNs – site-to-site VPN, remote access VPN).

Unit 4	**Network Attacks and Defense Mechanisms**	**8 hours**

Types of Network Attacks (e.g., Denial of Service, Man-in-the-Middle), Intrusion Detection and Prevention Systems (IDS/IPS, Signature-based and Anomaly-based Detection), Secure DNS and DHCP (DNSSEC, DHCP Snooping), Introduction to OSSEC, OSSEC Architecture (Agent-based and Agentless Modes), Event Collection (Syslog, File Monitoring), Rule-Based Detection (Decoders and Rules), -Real-Time Alerting (Active Responses, Notifications).

Unit 5	Secure Network Design and Implementation	9 hours
Network Architecture Design Principles (segmentation, least privilege), Defense-in-Depth Strategy (multiple security layers, redundancy), Secure Routing Protocols (BGP security, OSPF authentication), Security Best Practices for LANs, WANs, and Wireless Networks (encryption, access control), Security Assessment and Auditing (vulnerability scanning, log analysis)		
	Total Lecture Hours	**45 hours**

Textbook:

	Author Name
1. Network Security with OpenSSL: Cryptography, published by O'Reilly Media	John Viega, Matt Messier, Pravir Chandra
2. Cryptography and Network Security: Principles and Practice, published by Pearson	William Stallings

Reference Books:

	Author Name
1. Cryptography: Theory and Practice, 4th Edition, CRC Press, taylor and Francis	Douglas Stinson

Self-Study Content Links:		Duration (in Hrs)
MOOCs	1. Python Case Study - Cryptography - TOC | Infosys Springboard	5 Hrs 47 Min
Video Lectures	1. https://www.youtube.com/watch?v=Q-HugPvA7GQ&list=PL71FE85723FD414D7 2. https://onlinecourses.nptel.ac.in/noc22_cs90/preview	59 Min 2 Sec
Web References	1. NIST Cryptographic Standards 2. NIST Computer Security Resource Center (CSRC) 3. RFC Editor Repository 4. OpenSSL Documentation 5. Wireshark Documentation 6. Cisco Networking Academy	2 Hrs 3 Hrs 15 min 1 Hrs 4 Hrs 5 Hrs 3 Hrs

Course Code: BCSCY0602N	Course Name: CLOUD SECURITY AND PRIVACY	L	T	P	C
Course Offered in: CSE(CYS)		3	1	0	4

Prerequisite: Familiarity with networking concepts, cybersecurity principles, and mobile application development.

Course Objectives:

To provide students with comprehensive knowledge and practical skills to secure cloud environments, ensure data privacy, and manage cloud- specific security challenges by implementing advanced security measures, conducting risk assessments, and complying with industry regulations.

Course Outcome: After completion of the course, the student will be able to		Bloom's Knowledge Level (KL)
CO1	Understand fundamental principles of cloud and mobile security, including threat landscapes, security architectures, and best practices for protecting data and applications in cloud and mobile environments.	K2
CO2	Implement and manage security measures to protect information systems and data from various threats.	K3
CO3	Apply advanced anonymization algorithms to ensure data privacy, critically evaluate their effectiveness, and create solutions for protecting sensitive information.	K4
CO4	Demonstrate understanding and application of industry-standard security practices in developing and deploying secure cloud-based and mobile applications, critically analyzing their effectiveness and evaluating potential risks.	K4
CO5	Gain proficiency in utilizing security tools for cloud and mobile security, applying techniques like IAM, encryption, vulnerability assessment, and threat detection.	K4

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	3	1	2	2	2	1	2	1	2	1	2	3	2
CO2	3	3	3	2	3	-	-	-	1	2	2	3	2	2
CO3	3	3	2	3	2	-	2	-	1	2	1	1	2	2
CO4	3	3	3	2	3	1	-	-	1	2	2	3	1	2
CO5	2	2	2	1	3	-	-	-	3	3	3	2	2	2

Course Contents / Syllabus

UNIT 1	INTRODUCTION TO CLOUD AND MOBILE SECURITY	8 hours

Overview of Cloud Computing. Cloud Deployment Models and Security Implications: Public, Private, Hybrid Cloud. Importance of Security in Cloud and Mobile Environments, Mobile Security. Threat Landscape: Common Security Risks and Vulnerabilities, Security Principles and Best Practices, Malware, Rogue Applications, Device Theft, Network Attacks, Security Challenges in Cloud-Mobile Integrated Applications. Trust Models in Cloud and Mobile Environments.

UNIT 2	CLOUD SECURITY FUNDAMENTALS	8 hours

Cloud Service Models: IaaS, PaaS, SaaS Shared Responsibility Model in Cloud Security. Identity and Access Management (IAM) in Cloud Environments. Multi-factor Authentication and Federated Identity Management in Cloud. Secure Configuration Management for Cloud Resources. Data Encryption and Key Management. Securing Cloud Infrastructure: Virtualization, Containers, and Orchestration Runtime Security and Image Vulnerability Management. Logging, Monitoring, and Incident Detection in Cloud Platforms.

UNIT 3	PRIVACY PRESERVATION	10 hours

Privacy Risks in Cloud Data Storage and Processing Regulatory Requirements for Cloud Privacy: General Data Protection Regulation, Health Insurance Portability and Accountability Act. Anonymization techniques: Generalization, Suppression,

Perturbation, Pseudonymization. Anonymization algorithms: Data fly, Incognito, Mondrian, Greedy K-members Clustering, K scalable anonymization, Differential Privacy Compliance and Governance in the Cloud. Cloud Security: Case Studies and Real-world Examples.

UNIT 4	**MOBILE SECURITY BASICS**	**9 hours**

Mobile Operating Systems: IOS, Android Architecture and its Security, Application Sandboxing and Permission Models in Android and iOS. Secure APIs and Backend Communication for Mobile Apps. Secure Mobile Development Practices: Authentication and Authorization in Mobile Applications. Data Protection on Mobile Devices: Encryption, Secure Storages. Mobile Application Vulnerability Assessment and Secure Coding Practices. Backup Security and Remote Wipe Mechanisms on Mobile Devices.

UNIT 5	**PROJECT MAINTENANCE AND MANAGEMENT CONCEPTS**	**10 hours**

Mobile Device Management (MDM), Mobile Application Management (MAM) and Enterprise Mobility Management (EMM) Frameworks and Policy Enforcement. Mobile Threat Defense: Detection and Prevention Strategies, Mobile Patch Management and OS Update Strategies. Secure Communication on Mobile Devices: VPNs, TLS Biometric Security on Mobile Devices, Mobile Security Case Studies Device Compliance Monitoring and Risk Assessment. Incident Response and Forensic Considerations for Mobile Devices.

	Total Lecture Hours	**45 hours**

Textbook:

	Author Name
1. Cloud Computing Security, Russell Dean Vines 1st Edition Wiley-India.	Ronald L. Krutz
2. Practical Cloud Security, 1st Edition O'Reilly Media.	Chris Dotson

Reference Books:

	Author Name
1. Computer Security: Principles and Practice, Lawrie Brown — 4th Edition	William Stallings
2. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance —— 1st Edition O'Reilly Media.	Tim Mather, Subra Kumaraswamy, Shahed Latif

Self-Study Content Links:		Duration (in Hrs)
MOOCs	https://infyspringboard.onwingspan.com/web/en/app/toc/lex_auth_0144493 76270909440246/overview	10 hrs
Video Lectures	1. **NPTEL — Cloud Computing -** YouTube Playlist ~5 hrs 2. YouTube ~4 hrs *(use first 4 hrs)* 3. **Cloud Security Architecture — An Introduction** -- YouTube - ~2 hrs 4. **Android Security Full Course Part 1** --YouTube -~2 hrs 5. **Android Application Security Testing Full Course** -- YouTube -- ~2 hrs	15 hours
Web References	1. https://www.isaca.org/resources/isaca-journal/issues/2024/volume-5/addressing-security-concerns-in-a-mobile-computing-environment 2. https://cloudsecurityalliance.org/blog/2023/10/17/the-importance-of-the-shared-responsibility-model-for-your-data-security-strategy 3. https://censinet.com/perspectives/top-frameworks-gdpr-data-de-identification 4. https://developer.android.com/privacy-and-security/security-tips 5. https://www.locknCharge.com/blog/mdm-security-strategy	5 Hrs

Course Code: BCSCY0612N	Course Name: Blockchain and Cryptocurrency Security	L	T	P	C
Course Offered in: CSE(CYS)		3	0	0	3

Pre-requisite: Computer Networks, Network Security, Operating Systems, Programming skills

Course Objectives: To explore the foundational concepts of blockchain technology and its architecture to develop secure blockchain-based applications and assess their resilience to cyber threats.

Course Outcome: After completion of the course, the student will be able to		**Bloom's Knowledge Level (KL)**
CO1	Understand the evolution, core architecture, types of blockchain, and distinguish between centralized, decentralized and distributed ledger systems and their real-world use cases across IoT, AI/ML, Data Science and other engineering domains.	K2
CO2	Explain the fundamental cryptographic concepts — hashing, Merkle trees, digital signatures, wallets and PKI — that underpin blockchain security, without requiring advanced mathematical background.	K2
CO3	Apply knowledge of consensus mechanisms, smart contract vulnerabilities and blockchain attack vectors to analyze the security and operational behavior of decentralized networks.	K3
CO4	Develop and deploy smart contracts using Solidity on Remix IDE and understand enterprise blockchain architecture using Hyperledger Fabric, demonstrating ability to write, test and interact with blockchain applications hands-on.	K4
CO5	Evaluate and map real-world blockchain applications across financial systems, supply chain, government, healthcare, IoT and AI/ML domains, and assess emerging trends such as Zero-Knowledge Proofs, Layer 2 solutions and cross-chain interoperability.	K4

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	2	2	2	2	2	1	2	1	-	-	2	2	-
CO2	3	2	1	2	2	1	1	2	1	1	-	2	1	1
CO3	3	3	2	3	2	2	1	3	2	1	-	3	3	2
CO4	3	3	3	2	3	2	1	3	2	2	-	3	2	2
CO5	2	2	2	2	2	3	2	2	2	2	1	2	2	2

Course Contents / Syllabus

UNIT 1	**Introduction to Blockchain Technology**	**08 hours**

Evolution and history of blockchain; Structure and components of a blockchain (nodes, blocks, chain, mining); Types of blockchains: Public, Private, Consortium; Centralized traditional databases vs. Decentralized databases vs. Distributed Ledger Technology (DLT), Use cases: cryptocurrency (Bitcoin), supply chain, identity management, healthcare; Digital Money to Distributed Ledgers; Blockchain Design Primitives: Protocols, Permissions (Permissioned vs. Permissionless Blockchains), Privacy For Demo: https://andersbrownworth.com/blockchain , https://blockchaindemo.io

UNIT 2	**Cryptographic Foundations**	**09 hours**

Hash functions and Merkle trees (conceptual); Digital signatures and public-key cryptography (how it works, not proofs); Wallets: types and key management; Blockchain addresses and transactions; PKI Infrastructure — conceptual overview; Two-Factor Authentication with Blockchain. Browser based tool : CyberChef (GCHQ)https://gchq.github.io/CyberChef , https://www.myetherwallet.com ,

UNIT 3	**Consensus, Contracts, and Attacks**	**10 hours**

Need for consensus in decentralized systems; Proof-of-Work (PoW) (conceptual); Proof-of-Stake (PoS), Delegated PoS; Proof-of-Authority (PoA); Practical Byzantine Fault Tolerance (PBFT);Mining and its role in blockchain security , Introduction to Bitcoin, Ethereum and altcoins; Transaction lifecycle; UTXO model vs. account-based model; Smart contracts and their working; Common vulnerabilities: reentrancy, overflow/underflow (awareness level); Attacks:51% attack, Sybil Attack, Eclipse

Attack, Routing Attack, Distributed Denial of Service (DDoS) Online Tool: https://www.blockchain.com/explorer, https://txstreet.com/		
UNIT 4	**Enterprise Blockchain and Smart Contract Development**	**09 hours**
Hyperledger Fabric — Components and Architecture; Chaincode: What it is and how it works; Introduction to Remix IDE — Interface and Setup; Writing Your First Smart Contract on Remix IDE; Smart contract development using Solidity; Deploying and Testing Smart Contracts on Remix IDE;Events, Functions and Modifiers in Solidity; ERC-20 Token Standard — Overview , Tools for auditing smart contracts (Mythril, Slither, Oyente) , (Remix IDE) https://remix.ethereum.org , https://github.com/hyperledger/fabric-samples		
UNIT 5	**Blockchain Applications and Emerging Technologies**	**09 hours**
Introduction of version control engine, use case of automated assignment grading, peer review workflow, public repositories, building portfolios, collaborating on codebases, track changes, and resolve conflicts, Version-controlled technical manuals ensure up-to-date knowledge sharing using GitHub. Regulatory and legal frameworks for cryptocurrencies (global and national perspectives) https://etherscan.io/		
	Total Lecture Hours	**45 hours**

Textbook:

	Author Name
Mastering Bitcoin: Programming the Open Blockchain , 3rd Edition, O'Reilly Media, 2023	Andreas M. Antonopoulos and David A. Harding
Blockchain Basics: A Non-Technical Introduction in 25 Steps, 1st Edition, Apress, 2017	Daniel Drescher
Mastering Ethereum: Building Smart Contracts and DApps, 1st Edition, O'Reilly Media, 2018	Andreas M. Antonopoulos and Gavin Wood

Reference Books:

	Author Name
Blockchain Technology and Applications, Pethuru Raj, 1st Edition, CRC Press / Routledge, 2020	Kavita Saini and Chellammal Surianarayanan
The Basics of Bitcoins and Blockchains, Updated Edition, Mango Media, 2021	Antony Lewis
Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, 1st Edition, Princeton University Press, 2016	Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder

Self-Study Content Links:		Duration (in Hrs)
MOOCs	1. https://infyspringboard.onwingspan.com/web/en/app/toc/lex_auth_012929490529533952761_shared/overview ~ 9 hrs OR 2. https://infyspringboard.onwingspan.com/web/en/app/toc/lex_auth_013038627363602432360_shared/overview ~ 11 hrs	10 hrs
Video Lectures	1. https://www.youtube.com/watch?v=EH6vE97qIP4 ~2.5 hrs 2. https://www.youtube.com/watch?v=PPFsG92-HiI ~2.5 hrs 3. https://www.youtube.com/watch?v=0UvVOMZqpEA ~1.5 hrs 4. https://www.youtube.com/watch?v=7Cu8KQmUhu0 ~1.5 hrs 5. https://www.youtube.com/watch?v=w7HDA8gUbpQ ~2 hrs 6. https://www.youtube.com/watch?v=JPkgJwJHYSc ~1.5 hrs 7. https://www.youtube.com/watch?v=9mZpc6sKryk ~1.5 hrs 8. https://www.youtube.com/watch?v=RGOj5yH7evk ~1 hr 9. https://www.youtube.com/watch?v=prG1DJMoqoI ~1 hr	15 hours
Web References	1. https://en.wikipedia.org/wiki/Blockchain ~1 hr 2. https://openknowledge.worldbank.org/bitstreams/5166f335-35db-57d7-9c7e-110f7d018f79/download ~1 hr 3. https://arxiv.org/html/2508.01280v1 ~1.5 hrs 4. https://hyperledger-fabric.readthedocs.io/en/latest/whatis.html ~1 hr	5 hours

Course Code: BCSE0614	**Course Name: WEB DEVELOPMENT USING MEAN STACK**	**L**	**T**	**P**	**C**
Course Offered in: All computing branches (Department Elective)		**3**	**0**	**0**	**3**

Pre-requisite: Basic knowledge of HTML, CSS and ES6 required.

Course Objectives:

This course focuses on how to design and build static as well as dynamic webpages and interactive web applications. Students examine advanced topics like Angular, nodejs, Mongodb and Express framework for interactive web applications that use rich user interfaces.

Course Outcome: After completion of the course, the student will be able to

CO	Course Outcome	Bloom's Level
CO1	Explain, analyze and apply the role of server-side scripting language like Nodejs in the workings of the web and web applications.	K3
CO2	Demonstrate web application framework i.e., Express is to design and implement typical dynamic web pages and interactive web based applications.	K4
CO3	Apply the knowledge of Typescript that are vital in understanding angular is, and analyze the concepts, principles and methods in current client-side technology to implement angular application over the web.	K3
CO4	Analyze build and develop single page application using client-side programming i.e. angular js and also develop a static web application.	K4
CO5	Understand the impact of web designing by database connectivity with Mongodb in the current market place where everyone use to prefer electronic medium for shoping, commerce, and even social life also.	K3

CO-PO Mapping (Scale: 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	2	2	3	1	3	-	-	1	3	-	3	2	2	1
CO2	2	2	3	1	3	-	-	1	-	-	2	1	2	2
CO3	2	2	2	2	2	-	-	-	2	-	2	2	1	2
CO4	2	1	2	1	2	-	-	-	1	1	2	2	1	1
CO5	2	1	3	2	3	-	-	-	3	2	3	2	1	3

Course Contents / Syllabus

Module 1	**Introduction to Nodejs**	**9 hours**

Installing Nodejs, Node in-built packages (buffer, fs, http, os, path, util, url) Node.js modules, File System Module, Json data, Http Server and Client, Error handling with appropriate HTTP, Callback function, asynchronous programing REST API's(GET, POST PUT, DELETE UPDATE), GraphQL, Promises, Promise Chaining, Introduction to template engine (EJS).

Module 2	**Express Framework**	**9 hours**

Configuring Express, Postman configuration, , Environment Variables, Routing, Defining pug templates, HTTP method of Express, URL binding, middleware function, Serving static files, Express sessions, REST full API's, FORM data in Express, document modeling with Mongoose.

Module 3	**Basics of Angular js**	**9 hours**

Typescript, Setup and installation, Power of Types, Functions, Function as types Optional and default parameters, Arrow functions, Function overloading, Access modifiers, Getters and setters, Read-only & static, Abstract classes, Interfaces, Extending and Implementing Interface, Import and Export modules.

Module 4	**Building Single Page App with Angular js**	**9 hours**

MVC Architecture, One-way and Two-way data binding, AngularJS Expressions, AngularJS Controllers, AngularJS Modules, adding controller to a module, Component, Dependency Injection, Filters, Tables, AngularJS Forms and Forms validation, Select using ng-option, AngularJS AJAX.

Module 5	Connecting Angular js with MongoDB	9 hours
Environment Setup of Mongodb, data modeling, The current SQL/NoSQL landscape, Create collection in Mongodb, CRUD Operations in MongoDB. Mongo's feature set, Introduction to Mongoose, Understanding mongoose schemas and datatypes, Connecting Angular with mongoDB using API.		
	Total Lecture Hours	**45 hours**

Text Books

S.NO	Book Title	Author
1.	"Web Application Development with MEAN", 3rd Illustrated Edition 2017, Packt Publications.	Amos Q. Haviv , Adrian Mejia , Robert Onodi
2.	"Getting MEAN with Mongo, Express, Angular, and Node", 2nd Edition 2016, Addison Wesley Publication.	Simon Holmes , Clive Herber
3.	"Comprehensive guide to learn Node.js", 1st Edition, 2018 BPB Publications.	Dhruti Shah
4.	"Learning Angular",3rd Edition,2017 Packt publications	Christoffer Noring, Pablo Deeleman

Reference Books:

S.NO	Book Title	Author
1.	"Fullstack Angular: The Complete Guide to AngularJS and Friends", 4th edition, 2020 International Publishing.	Anthony Accomazzo, Ari Lerner, and Nate Murray
2.	"Full-Stack Angular, Type Script, and Node: Build cloud-ready web applications using Angular 10 with Hooks and GraphQL", 2nd edition, 2017 Packt Publishing Limited.	David Cho
3.	"Complete node.js: The fast guide: Learn complete backend development with node.js"5th edition, 2017 SMV publication.	Richard Haltman & Shubham Vernekar
4.	"Mastering Node.js: Build robust and scalable real-time server-side web applications efficiently" 2nd edition,2016 Packt Publishing Limited.	Glenn Geenen, Sandro Pasquali , Kevin Faaborg
5.	Express & MongoDB Development ,kindle edition,2019 international publishing.	Greg Lim
6.	"AngularJS Master Angular.js with simple steps, guide and instructions" 3rd edition, 2015 SMV publication.	Daniel Perkins
7.	"MongoDB Basics", 2nd edition ,2018 International Publication.	Peter Membrey, David Hows, Eelco Plugge

Self Study Content Links:

MOOCs	1. https://www.coursera.org/professional-certificates/ibm-full-stack-cloud-developer?utm_medium=sem&utm_source=gg&utm_campaign=b2c_india_ibm-full-stack-cloud-developer_ibm_ftcof_professional-certificates_cx_dr_bau_gg_sem_pr_in_all_m_hyb_24-06_x&campaignid=21316592778&adgroupid=165695367991&device=c&keyword=courses%20for%20full%20stack%20developer&matchtype=p&network=g&devicemodel=&creativeid=700589190893&assetgroupid=&targetid=kwd-571198547272&extensionid=&placement=&gad_source=1&gad_campaignid=21316592778&gbraid=0AAAAADdKX6Y4gVe2nrA-BD75Xjo7XWZvc&gclid=Cj0KCQjw3K7RBhDJARIsAKRtP5T6KxJN_3NMwp5KCs0I8bBY35dSkaUg10Y0FBCfhLqnqqyQCAG9yzgaAonEEALw_wcB 2. https://www.udemy.com/career/full-stack-web-developer/?utm_campaign=Search_Keyword_CareerAccelerator_Prof_la.EN_cc.India&utm_source=google&utm_medium=paid-search&portfolio=CALP-India&utm_audience=mx&utm_tactic=nb&utm_term=_._ag_177463970814_._ad_749449716155_._kw_how%20to%20become%20a%20web%20developer&utm_content=g&funnel=&test=&gad_source=1&gad_campaignid=22487789892&gbraid=0AAAAADROdO0RdwZEytECk3hJ8p0YLN6Wu&gclid=Cj0KCQjw3K7RBhDJARIsAKRtP5SBLzCT5ZsRMLP4tx1IJo-2jQWUMlsGRaHabTFG0lY_G_eZuu7xmCYaAg1tEALw_wcB	40 hrs 30 hrs

Video Lectures	1. https://youtu.be/BLl32FvcdVM 2. https://youtu.be/fCACk9ziarQ 3. https://youtu.be/YSyFSnisip0 4. https://youtu.be/mGVFltBxLKU 5. https://youtu.be/bWaucYA1YRI 6. https://youtu.be/7H_QH9nipNs 7. https://youtu.be/AX1AP83CuK4 8. https://youtu.be/SccSCuHhOw0 9. https://youtu.be/lY6icfhap2o 10. https://youtu.be/z7ikpQCWbtQ 11. https://youtu.be/0LhBvp8qpro 12. https://youtu.be/k5E2AVpwsko 13. https://youtu.be/SQJkj0WYWOE.list=PLvQjNLQMdagP3OzoBMfBT48uJ-SPfSsWj 14. https://youtu.be/0eWrpsCLMJQ.list=PLC3y8-rFHvwhBRAgFinJR8KHIrCdTkZcZ 15. https://youtu.be/ZSB4JcLLrIo 16. https://youtu.be/0LhBvp8qpro 17. https://youtu.be/k5E2AVpwsko 18. https://youtu.be/SQJkj0WYWOE.list=PLvQjNLQMdagP3OzoBMfBT48uJ-SPfSsWj 19. https://youtu.be/0eWrpsCLMJQ.list=PLC3y8-rFHvwhBRAgFinJR8KHIrCdTkZcZ 20. https://youtu.be/ZSB4JcLLrIo 21. https://youtu.be/Kvb0cHWFkdc 22. https://youtu.be/pQcV5CMara8 23. https://youtu.be/c3Hz1qUUIyQ 24. https://youtu.be/Mfp94RjugWQ 25. https://youtu.be/SyEQLbbSTWg	17 hrs
Web References	1. https://angular.io 2. https://www.mongodb.com/docs	

Course Code: BCSCY0614	Course Name: Security Risk Management	L	T	P	C
Course Offered in: CSE(CYS)		3	0	0	3

Prerequisite: Familiarity Students should have a foundational understanding of networking, cybersecurity basics, operating systems, and scripting. Familiarity with risk concepts, project lifecycle, and digital ethics is also recommended.

Course Objectives:

The objective of this course is to introduce the fundamental principles of risk management, focusing on how businesses and society assess, control, regulate, and transfer risk to ensure security and resilience, exploit, and remediate vulnerabilities in real-world environments.

Course Outcome: After completion of the course, the student will be able to		**Bloom's Knowledge Level (KL)**
CO1	Explain the nature, types, and sources of risk, uncertainty, and application security concepts including OWASP Top 10 and SSDLC.	K2
CO2	Describe risk management principles, frameworks, standards, and identity & access management concepts.	K2
CO3	Classify risks using FIRM and PESTLE frameworks and explain the phases of a cyber-attack lifecycle.	K3
CO4	Apply risk assessment techniques including risk matrix, risk appetite, inherent/current risk levels, and data & endpoint security controls.	K4
CO5	Analyze operational and project risk, evaluate information security standards (ISO 27000, NIST, COBIT), and support business continuity planning.	K4

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	2	1	1	2	2	2	1	-	1	1	1	2	-	2
CO2	3	3	2	2	3	2	-	1	-	2	1	1	2	2	3
CO3	3	3	2	2	3	1	-	3	2	2	1	2	3	3	3
CO4	2	2	2	1	2	2	1	3	2	2	-	2	3	-	3
CO5	3	2	2	2	1	3	1	3	2	2	1	3	3	-	2

Course Contents / Syllabus

Unit 1	**Fundamentals of Risk and Application Security**	**08 hours**

Definition and nature of risk; risk vs. uncertainty; classification and types of risk (short, medium, long-term); sources of risk; methods for measuring and evaluating risk. Importance of application security; OWASP Top 10 web application vulnerabilities; Secure Software Development Life Cycle (SSDLC).

Unit 2	**Risk Management Principles and Identity & Access Management**	**09 hours**

Principles and importance of risk management; risk management process and lifecycle; risk management standards and protocols; risk architecture, strategy, policies, and governance. Authorization and authentication; access control and access control models; privilege levels; IAM lifecycle and activities.

Unit 3	**Risk Classification, Scoring and Cyber Attack Lifecycle**	**10 hours**

FIRM and PESTLE risk classification systems; hazard risk, control risk, opportunity risk; risk scorecards, scoring and ranking methods. Phases of a cyber-attack — Reconnaissance, Weaponize, Deliver, Exploit, Install, Command & Control, Act on Objectives (Kill Chain model).

Unit 4	**Risk Assessment and Data & Endpoint Security**	**09 hours**

Importance and approaches of risk assessment; risk matrix, risk perception, risk appetite; application of risk matrix; inherent and current risk levels; 4T's of risk response. Data security and data security controls; endpoint/host security concepts and controls.

Unit 5	**Operational Risk, Project Risk and Information Security Standards**	**09 hours**

Risk appetite, tolerance, treatment, and termination; project risk management — uncertainty, lifecycle, planning and control; operational risk — definition, challenges, measurement. Corporate security governance; Business Continuity

Planning (BCP); overview of top 20 security controls; ISO/IEC 27000 series (27001, 27002, 27005); NIST SP 800 series; COBIT; Standard of Good Practice (SoGP).

Total Lecture Hours	**45 hours**

Textbook

	Author
1. The Cybersecurity Guide to Governance Risk And Compliance, 1st Edition (2024), John Wiley & Sons	Jason Edwards and Griffin Weaver
2. Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls, 2nd Edition (2024), Kogan Page	Christopher J. Hodson,
3. Information Security Management Handbook, 1st Edition, CRC Press, 2004	Harold F. Tipton
4. Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management, 6th Edition, Kogan Page, 2022	Paul Hopkin

Reference Books:

	Author
1. Security Risk Management: Building an Information Security Risk Management Program from the Ground Up, 1st Edition, Syngress (Elsevier), 2011	Evan Wheeler
2. Managing Information Security Risks: The OCTAVE Approach, 1st Edition, Addison-Wesley Professional, 2002	Christopher Alberts and Audrey Dorofee,
3. Enterprise Security Risk Management: Concepts and Applications, 1st Edition, Rothstein Publishing, 2017	Brian J. Allen, Rachelle Loyear and Monica Bhaskaran
4. Risk Management for Computer Security: Protecting Your Network and Information Assets, 1st Edition, Butterworth-Heinemann (Elsevier), 2005	Andy Jones and Debi Ashenden
5. Management of Information Security, 6th Edition, Cengage Learning, 2021	Michael E. Whitman and Herbert J. Mattord
6. The Failure of Risk Management: Why It's Broken and How to Fix It, 2nd Edition (2020), John Wiley & Sons	Douglas W. Hubbard

Self-Study Content Links:		**Duration (in Hrs)**
MOOCs	1. Cyber Security Risk Management - TOC | Infosys Springboard 2. https://infyspringboard.onwingspan.com/web/en/app/toc/lex_auth_0142993202164285441 1/overview 3. https://infyspringboard.onwingspan.com/web/en/app/toc/lex_auth_0135015853237288961 1474/overview 4. https://infyspringboard.onwingspan.com/web/en/app/toc/lex_auth_0135015831292968961 1290/overview 5. https://infyspringboard.onwingspan.com/web/en/app/toc/lex_auth_0135015755343872001 0672/overview	4 Hrs. 7 Min 1h 19m 1h 26m 1h 52m 1h 28m
Video Lectures	1. https://www.youtube.com/watch?v=YYe0FdfdgDU 2. https://www.youtube.com/watch?v=rKEsxddOZ64 3. https://www.youtube.com/watch?v=s6XgCJ141Ww 4. https://www.youtube.com/watch?v=OnFM8MZfwyc 5. https://www.youtube.com/watch?v=MsuX_p_RJhg 6. https://www.youtube.com/watch?v=oYVYBPTe2zQ	~2 hrs ~1.5 hrs ~25 min ~45 min ~1 hr ~8 hrs
Web References	1. https://alison.com/course/iso-iec-27001-dynamics-of-information-security-management-system-isms 2. https://alison.com/course/identity-and-access-management 3. https://csrc.nist.gov/projects/risk-management/rmf-courses 4. https://www.coursera.org/learn/owasp-top-10-risks-1-5 5. https://www.coursera.org/learn/owasp-risks-6-10	5 hours

Course Code: BCSE0615	Course Name: Web Development using MERN STACK with Devops	L	T	P	C
Course Offered in: CSE/CSE(R)/IT/M.Tech Int. (CSE)		3	0	0	3

Pre-requisite: Basic knowledge of HTML, CSS, JavaScript, and fundamental programming concepts in any language.

Course Objectives:

This course aims to equip students with practical skills in building dynamic full-stack applications using React, Node.js, Express, and MongoDB. It also introduces DevOps principles, Agile methodologies, and CI/CD automation using tools like GitHub, Jenkins, Docker, and Kubernetes.

Course Outcome: After completion of the course, the student will be able to		**Bloom's Knowledge Level (KL)**
CO1	Apply the knowledge of ES6 that are vital to implement react application over the web.	K3
CO2	Implement and Understand the impact of web designing by database connectivity with Mongodb.	K3
CO3	Explain, analyze and apply the role of server side scripting language like Nodejs and Express js framework.	K4
CO4	Apply the benefits of DevOps over other software development processes to Gain insights into the DevOps environment.	K4
CO5	Demonstrate popular open-source tools with features and associated terminology used to perform Continuous Integration and Continuous Delivery.	K3

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	2	3	1	3	1	1	-	1	-	2	2	2	2
CO2	3	2	3	1	3	1	1	-	1	-	2	2	2	3
CO3	3	2	3	1	3	1	1	2	1	2	2	2	2	2
CO4	3	1	1	1	3	2	-	-	2	1	2	2	1	2
CO5	3	1	1	1	3	1	-	-	2	1	2	2	2	2

Course Contents / Syllabus

Module 1	**Modern Frontend Development with React JS**	**9 hours**

Introduction: to React, Setting up React projects, React Folder Structure, JSX, Functional Components, and React Hooks (useState, useEffect, use Context), Props vs State, Stateless vs Stateful Components, Component Lifecycle, Routing with react-router-dom Introduction to Next.js for Server-Side Rendering and SEO, Integrating APIs with axios or fetch,.

Module 2	**UI Libraries & MongoDB Integration**	**10 hours**

UI Libraries : Introduction to Google Material UI, Tailwind CSS, Theming and responsive design with MUI, Creating reusable UI components (Navbar, Toolbar, Dialogs), Introduction to MongoDB, CRUD Operations using Mongoose Indexes: Creating, Getting, Dropping, Aggregation Pipelines and Query Optimization, Data Modeling & Relationships, Auto-Sharding and Replication Concepts, Modern MongoDB tools: MongoDB Atlas, Compass.

Module 3	**Backend with Node.js & Express**	**10 hours**

Node.js: Introduction to Node.js Setting up Express applications, Routing & Middleware, Restful API Design , JWT-based Authentication & Authorization ,Working with dotenv, CORS, body-parser. Express MVC Architecture in Express, File Upload Handling with Multer, Connecting Frontend with Backend via APIs, Introduction to GraphQL.

Module 4	**DevOps Culture and Lifecycle**	**8 hours**

Introduction to DevOps: Culture & Principles, DevOps Lifecycle and Agile vs DevOps, SDLC Models: Agile, Lean, Scrum, Kanban, Scrum: Process flow, Planning, Testing, Release Management, Introduction to Site Reliability Engineering (SRE), Overview of Terraform/Ansible, Configuration Management basics

Module 5	**CI/CD, Docker & Kubernetes**	**8 hours**

Git & GitHub: Introduction to Git, GitHub, Branching strategies, CI/CD Pipelines: Jenkins, GitHub Actions, Creating Jenkins Jobs and Pipelines, Integrating Git, Maven, and SonarQube, Introduction to Docker: Images, Containers, Lifecycle ,Building custom Docker Images, Docker Compose for multi-container apps, Container orchestration with Kubernetes Creating Deployments, Services, and scaling with K8s, Basic monitoring tools: Prometheus and Grafana

Total Lecture Hours			**45 hours**
Textbook:			
S.No	**Book Title**	**Author**	
1.	Pro MERN Stack: Full Stack Web App Development with Mongo, Express, React, and Node Paperback, 2nd Edition (2017)	Vasan Subramanian	
2.	Hands-On MERN Stack Web Development: Build production-grade web apps and APIs with MERN stack ,3rd Edition (2019)	Shama Hoque	
3.	Beginning MERN Stack: Build and Deploy a Full Stack MongoDB, Express, React, Node.js App 2nd Edition (2021)	Greg Lim	
Reference Books:			
S.No	**Book Title**	**Author**	
1.	The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations 2nd Edition (2003).	Gene Kim, Jez Humble, Patrick Debois, John Willis	
2.	Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation, 2nd Edition (2004).	Jez Humble, David Farley	
3.	Test and Deploy Production-Grade Web Applications 1st Edition (2023).	Nabendu Biswas	
Self Study Content Link:			
MOOCs	1. https://www.coursera.org/learn/fullstack-web-development 2. https://www.coursera.org/professional-certificates/ibm-full-stack-cloud-developer	4 Weeks 6 Months	
Video Lectures	1. https://youtu.be/CvCiNeLnZ00 2. https://youtu.be/4nKWREmCvsE 3. https://youtu.be/f2EqECiTBL8 4. https://youtu.be/6GQRb4fGvtk 5. https://youtu.be/kTp5xUtcalw	8 hrs 25 Min 7 hrs 8 Min 6 hrs	
Web References	1. https://react.dev 2. https://docs.docker.com		

LAB Course Code: BCSCY0653	Course Name: Network Security and Cryptography Lab	L	T	P	C
Course Offered in: CSE (CYS) & B. Tech CSE and Emerging Branches as Department Elective		0	0	4	2

Pre-requisite: Understanding basic Networking Terms (e.g., IP, LAN, Router), Awareness of Digital Tools (Email, Cloud, Antivirus), Fundamental Logical Thinking, Cybersecurity fundamentals.

Course Objectives:

Objectives: This course aims to introduce the fundamental principles and concepts of network security and cryptography, provide insights into common network-based attacks and vulnerabilities and develop the ability to design secure network architectures using modern cryptographic tools and techniques. Provide hands-on experience with classical and modern cryptographic algorithms.

1. Develop understanding of encryption, decryption, and key exchange mechanisms.
2. Demonstrate the use of cryptographic hash functions and authentication techniques.
3. Enable practical knowledge in configuring secure communication protocols.
4. Introduce tools and methods for basic penetration testing and security assessment.

Course Outcome: After completion of the course, the student will be able to		Bloom's Knowledge Level (KL)
CO1	Demonstrate the implementation and analysis of classical and modern cryptographic techniques including shift cipher, monoalphabetic cipher, one-time pad, MACs, hash functions, AES, DES, RSA, and ECC for secure data communication.	K3
CO2	Configure and evaluate secure communication protocols and network security mechanisms such as SSL/TLS, TLS handshake analysis, IPsec VPNs, and firewall configurations using appropriate security tools and techniques.	K4
CO3	Analyze and perform network security assessment activities including Man-in-the-Middle (MITM) attack simulation, DoS attack simulation, and penetration testing to identify vulnerabilities and strengthen system security.	K4

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	2	1	1	2	-	-	1	-	-	-	2	3	1
CO2	3	3	2	2	3	1	-	1	1	1	1	3	2	2
CO3	3	3	1	2	2	-	-	1	-	-	-	1	3	3

List Of Practical's (Indicative & Not Limited To)	CO Level
1. Implementing Shift Cipher (Caesar Cipher).	CO1
2. Implementing Monoalphabetic Substitution Cipher.	CO1
3. Implementing Vigenère Cipher.	CO1
4. Implementing One-Time Pad and Perfect Secrecy.	CO1
5. Implementing Message Authentication Codes (MAC).	CO1
6. Implementing Cryptographic Hash Functions (SHA-256).	CO1
7. Implementation of AES Encryption Algorithm.	CO1
8. Implementation of DES Encryption Algorithm using Python.	CO1
9. Implementation of RSA Algorithm (Key Generation, Encryption/Decryption).	CO1
10. Digital Signature Generation and Verification using RSA/ECC.	CO1
11. Packet Capturing and Analysis using Wireshark.	CO2
12. Basic Firewall Configuration using IPTables/pfSense.	CO2
13. Vulnerability Scanning using Nmap/OpenVAS.	CO2
14. Risk Assessment and Security Policy Documentation for a Small Network.	CO2
15. Configuration of SSL/TLS for Secure Web Communication.	CO2
16. TLS Handshake Analysis using Wireshark.	CO2
17. Secure Remote Login using SSH and Key-Based Authentication.	CO2
18. SSH Port Forwarding and Secure Tunneling.	CO2

19. Setting up IPsec VPN for Secure Network Communication.	CO2
20. Wireless Security Configuration using WPA2/WPA3.	CO2
21. DoS Attack Simulation in a Safe Lab Environment.	CO3
22. Man-in-the-Middle (MITM) Attack Simulation.	CO3
23. Intrusion Detection using Snort IDS.	CO3
24. OSSEC Installation, Log Monitoring, and Alert Configuration.	CO3
25. Secure Network Design using VLAN Segmentation and Access Control.	CO3
26. Network Security Assessment and Penetration Testing.	CO3
Total Hours : 60 hrs.	

LAB Course Code: BCSCY0652N	LAB Course Name: Cloud Security & Privacy Lab	L	T	P	C
Course Offered in: CSE(CYS)		0	0	4	2

Pre-requisite: Basic knowledge of cloud computing (IaaS, PaaS, SaaS), networking fundamentals, operating systems, cybersecurity concepts, virtualization, basic programming/scripting.

Course Objectives: To provide students with comprehensive knowledge and practical skills to secure cloud environments, ensure data privacy, and manage cloud- specific security challenges by implementing advanced security measures, conducting risk assessments, and complying with industry regulations.

Course Outcome: After completion of the course, the student will be able to		Bloom's Knowledge Level (KL)
CO1	Summarize Security risks and vulnerabilities and apply security measures within cloud and mobile environments to ensure robust protection for digital assets.	K3
CO2	Implement data anonymization techniques and analyze differential privacy methods to ensure data privacy and regulatory adherence.	K4
CO3	Analyze mobile app security, encrypt devices, simulate security incidents, and implement biometric authentication.	K4

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	3	2	2	1	1	-	3	1	1	2	3	2	3
CO2	3	3	3	2	2	1	-	3	1	1	2	3	2	2
CO3	3	3	3	2	2	1	-	3	1	1	2	2	2	2

List Of Practical's (Indicative & Not Limited To)	CO
1. Basic Understanding of AWS Platform	CO1
2. Study of Cloud Deployment Models and Security Implications	CO1
3. Analyze Potential Security Risks and Prioritize Them	CO1
4. Create Threat Models for Cloud-Based Systems and Mobile Apps	CO1
5. Study of Shared Responsibility Model in Cloud Security	CO1
6. Configure IAM Roles and Policies for Access Control	CO1
7. Implementation of Multi-Factor Authentication (MFA) in AWS	CO1
8. Federated Identity Management in Cloud Environments	CO1
9. Encrypt Data and Manage Encryption Keys Securely using AWS KMS	CO1
10. Secure Storage of Sensitive Data in Amazon S3 using Encryption and Access Controls	CO1
11. Configure Logging and Monitoring using AWS Cloud Trail and Cloud Watch	CO1
12. Compliance Monitoring and Auditing of AWS Resources	CO1
13. Deploy Containerized Applications Securely using Docker	CO1
14. Container Vulnerability Assessment and Image Scanning	CO2
15. Secure Configuration Management for Cloud Resources	CO2
16. Implement Data Masking in Amazon RDS Databases	CO2
17. Learn and Implement Data Fly Algorithm for Dataset Anonymization	CO2
18. Learn and Implement Incognito Algorithm for Dataset Anonymization	CO2
19. Study of Mondrian and K-Anonymity Techniques	CO2
20. Explore Differential Privacy Techniques in Data Analytics	CO2
21. Study Android and iOS Architecture and Security Mechanisms	CO3
22. Analyze Mobile App Security using MobSF and OWASP Guidelines	CO3
23. Implement Secure Mobile Application Development Practices	CO3
24. Encrypt Mobile Devices and Configure Security Settings	CO3

25. Simulate Mobile Security Incidents and Perform Incident Response	CO3
26. Implement Biometric Authentication in a Sample Mobile Application	CO3
Total Hours: 60 hrs.	

LAB Course Code: BCSCY0612P	LAB Course Name: Blockchain and Cryptocurrency Security Lab	L	T	P	C
Course Offered in: CSE(CYS)		0	0	2	1

Pre-requisite: NA

Course Objectives:

To provide hands-on experience in setting up blockchain environments and understanding their structure. To enable students to implement and analyze cryptographic mechanisms used in blockchain systems. To facilitate practical understanding of consensus algorithms and cryptocurrency transaction flows. To develop skills in writing, deploying, and securing smart contracts using blockchain development tools. To expose students to real-world blockchain applications and privacy-enhancing technologies.

Course Outcome: After completion of the course, the student will be able to		Bloom's Knowledge Level (KL)
CO1 :	Illustrate the structure and components of a blockchain, explain DLT types and real-world use cases, and demonstrate hash functions, digital signatures, and wallet operations using browser-based tools.	K3
CO2 :	Develop and deploy Solidity smart contracts on Remix IDE, examine consensus mechanisms through simulation, and evaluate the impact of blockchain attack vectors such as 51%, Sybil, and Eclipse attacks.	K5
CO3 :	Build a basic blockchain application or token using Solidity, and apply GitHub workflows to manage, version, and collaborate on project code.	K6

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	2	2	3	1	3	–	–	–	1	–	–	3	2	1
CO2	3	2	3	3	2	–	–	1	1	–	–	3	2	3
CO3	3	2	3	1	3	–	–	–	2	1	1	3	1	2

List Of Practical's (Indicative & Not Limited To)	CO
1. Explore Block Chain Structure Using a Browser-Based Visualizer	CO1
2. Compare Public, Private, and Consortium Block chains	CO1
3. Build a Simple Block chain with 2–3 Blocks in Python/JavaScript	CO1
4. Simulate Adding a New Block with a Hash Link	CO1
5. Generate a SHA-256 Hash for Given Input Data	CO1
6. Create a Simple Merkle Tree for 2–4 Transactions	CO1
7. Generate a Public-Private Key Pair and Verify a Digital Signature	CO1
8. Create a Basic Wallet (Generate Keys and Store Them)	CO1
9. Implement Two-Factor Authentication Using OTP and Key Verification	CO1
10. Perform a Simple Proof-of-Work (Hash with Leading Zeros Condition)	CO2
11. Simulate a 51% Attack Scenario on a Toy Block chain	CO2
12. Set Up MetaMask Wallet and Send a Transaction on Ethereum Test net	CO2
13. View and Verify a Transaction Using a Block chain Explorer	CO2
14. Analyse and Compare Consensus Mechanisms (PoW, PoS, PBFT)	CO2
15. Write a Basic Smart Contract (Store and Retrieve a Value) in Remix	CO2
16. Deploy a Smart Contract with Events and Modifiers	CO2
17. Create a Simple Token Using Basic ERC-20 Structure	CO3
18. Demonstrate a Re-entrancy Vulnerability in a Smart Contract	CO3
19. Explore Hyper ledger Fabric Architecture Using Documentation	CO3
20. Upload a Project to GitHub (Create Repo and Push Code)	CO3
21. Collaborate Using GitHub Branching and Pull Requests	CO3
22. Track Changes and Resolve Merge Conflicts Using Git	CO3
Total Hours: 30 hrs.	

LAB Course Code: BCSE0614P	LAB Course Name: Web Development Using Mean Stack LAB	L	T	P	C
Course Offered in: All computing branches (Department Elective Lab)		0	0	2	1

Pre-requisite: Basic knowledge of HTML, CSS and ES6 required.

Course Objectives:

This course focuses on how to design and build static as well as dynamic webpages and interactive web applications. Students examine advanced topics like Angular, nodejs, Mongodb and Express framework for interactive web applications that use rich user interfaces.

Course Outcome: After completion of the course, the student will be able to		**Bloom's Level**
CO1	Develop server-side web applications using Node.js and Express framework by implementing modules, asynchronous programming, REST APIs, middleware, template engines, and document modeling with Mongoose.	K6
CO2	Design and build dynamic Single Page Applications (SPAs) using AngularJS and TypeScript by applying components, modules, data binding, controllers, dependency injection, forms, and AJAX concepts.	K6
CO3	Create and manage MongoDB databases by performing data modeling, CRUD operations, schema design using Mongoose, and integrating Angular applications with MongoDB through APIs.	K6

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	3	3	2	3	-	-	-	1	1	-	3	3	2
CO2	3	2	3	2	3	-	-	-	2	2	-	3	3	3
CO3	3	3	3	2	3	-	-	-	1	1	-	3	2	3

List Of Practical's (Indicative & Not Limited To)

1. Construct a program to demonstrate usage of Node.js fs module to read a file.	CO1
2. Construct a program to display system information using the os module.	CO1
3. Construct a program to create and export a simple Node.js module.	CO1
4. Construct a program to parse a URL using the Node.js url module.	CO1
5. Construct a program to create a basic HTTP server using Node.js	CO1
6. Construct a program to demonstrate callback-based asynchronous execution.	CO1
7. Construct a program to illustrate promise creation and resolution.	CO1
8. Construct a program to demonstrate promise chaining with multiple operations.	CO1
9. Construct a program to show JSON data parsing and stringifying.	CO1
10. Construct a program to demonstrate routing in an Express application.	CO1
11. Construct a program to demonstrate AngularJS data binding.	CO1
12. Construct a program to build a Node.js server that handles GET requests.	CO1

13. Construct a program to implement POST request handling using Express.	CO1
14. Construct a program to perform CRUD operations using Express and MongoDB.	CO1
15. Construct a program to create middleware for logging request details.	CO1
16. Construct a program to serve static files using Express.	CO1
17. Construct a program to create a MongoDB collection and insert documents.	CO1
18. Construct a program to build an AngularJS form with validation.	CO1
19. Construct a program to implement an API call using AngularJS AJAX.	CO1
20. Construct a program to compare synchronous and asynchronous file operations.	CO1
21. Construct a program to demonstrate differences between callbacks and promises.	CO1
22. Construct a program to illustrate REST API endpoints with multiple HTTP methods.	CO1
23. Construct a program to demonstrate middleware execution order in Express.	CO1
24. Construct a program to show one-way and two-way data binding in AngularJS.	CO2
25. Construct a program to analyze MongoDB document structure using Mongoose schema.	CO2
26. Construct a program to measure execution time of synchronous vs asynchronous code.	CO2
27. Construct a program to test REST API endpoints using different HTTP methods.	CO2
28. Construct a program to validate user authentication using Express sessions.	CO2
29. Construct a program to handle error responses with proper HTTP status codes.	CO2
30. Construct a program to demonstrate secure API access using middleware.	CO3
31. Construct a program to develop a RESTful API using Node.js, Express, and MongoDB.	CO3
32. Construct a program to build a single-page application using AngularJS.	CO3
33. Construct a program to integrate AngularJS frontend with Node.js backend.	CO3
34. Construct a program to implement user registration and login system.	CO3
35. Construct a program to build a full-stack application with CRUD operations and API integration.	CO3
Total Hours: 30 hrs	

Course Code: BCSCY0652	Course Name: Penetration Testing	L	T	P	C
Course Offered in: CSE(CYS)		0	0	6	3

Prerequisite: Networking basics (TCP/IP, OSI model), Operating systems (Linux & Windows), Programming/scripting (Python, Bash), Cybersecurity fundamentals

Course Objectives:

The course aims to provide students with a comprehensive understanding of penetration testing in cybersecurity. Through theoretical learning and hands-on practical exercises, students will grasp the fundamental concepts, methodologies, and ethical considerations associated with penetration testing. They will develop the skills to identify, assess, and exploit vulnerabilities in networks, web applications, mobile apps, and wireless systems. The course aims to equip students with the knowledge and tools necessary to conduct effective penetration tests and strengthen the security posture of organizations. Overall, it seeks to prepare students for roles in cybersecurity by fostering critical thinking, problem-solving, and ethical decision-making skills.

Course Outcome: After completion of the course, the student will be able to		Bloom's Knowledge Level (KL)
CO1	Students will understand the importance and ethical considerations of penetration testing in cybersecurity.	K2
CO2	Students will demonstrate proficiency in conducting network reconnaissance, vulnerability assessment, and exploitation.	K3
CO3	Students will be able to identify, assess, and exploit vulnerabilities in web applications, recommending appropriate mitigation strategies.	K4
CO4	Students will acquire the skills to perform mobile application reconnaissance, vulnerability analysis, and exploitation, ensuring secure mobile development practices.	K4
CO5	Students will learn advanced penetration testing methodologies, including wireless penetration testing and social engineering tactics, and will be able to prepare comprehensive penetration testing reports.	K3

CO-PO Mapping (Scale 1: Low, 2: Medium, 3: High)

CO-PO Mapping	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	2	1	-	-	1	3	-	3	-	1	-	-1	3	2
CO2	2	3	2	3	3	2	-	2	1	2	1	3	2	3
CO3	2	3	3	3	3	2	-	2	1	2	1	3	3	3
CO4	2	3	3	3	3	1	-	3	2	3	2	3-	2	3
CO5	2	3	2	3	3	3	1	3	2	3	3	3-	3	3

Course Contents / Syllabus

UNIT 1	Introduction to Penetration Testing	13 hours

Overview of Penetration Testing, Importance and Scope, Legal and Ethical Considerations, Types of Penetration Testing (Black-box, White-box, Grey-box), Penetration Testing Standards & Methodologies (e.g., OWASP, NIST).

UNIT 2	Network Penetration Testing	15 hours

Network Reconnaissance, Scanning and Enumeration, Exploitation Techniques, Vulnerability Assessment Tools (e.g., Nmap, Nessus), Basic Wireless Network Security Testing.

UNIT 3	Web Application Penetration Testing	16 hours

OWASP Top 10, Web Application Scanning, SQL Injection, XSS, CSRF, Authentication & Session Management Attacks, Introduction to API Security Testing (Added – modern requirement).

UNIT 4	Mobile Application Penetration Testing	16 hours

Android and iOS Security Fundamentals, Reverse Engineering, Secure Coding Practices, Mobile Application Testing Tools (e.g., MobSF), Basic Runtime Analysis & Dynamic Testing.		
Module 5	**Advanced Techniques and Reporting,**	**15 hours**
Advanced Exploitation Techniques, Reporting and Documentation, Post-Exploitation Techniques, Privilege Escalation Concepts, Basics of Social Engineering Attacks.		
	Total Lecture Hours	**75 hours**

Textbook:

	Author Name
1. "Kali Linux Revealed: Mastering the Penetration Testing Distribution", 2nd Edition (2021), Offensive Security	Raphael Hertzog
2. "Metasploit: The Penetration Tester's Guide", 1st Edition (2011), No Starch Press	David Kennedy
3. "Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide", 2nd Edition (2012), Chappell University	Laura Chappell

Reference Books:

	Author Name
1. "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws", 2nd Edition (2011), Wiley Publishing	**Dafydd Stuttard**
2. "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning", 1st Edition (2009), Nmap project	**Gordon Fydor Lyon**

Self-Study Content Links:		Duration (in Hrs.)
MOOCs	1. https://infyspringboard.onwingspan.com/web/en/app/toc/lex_auth_0130944400803_102722559_shared/overview	6Hrs 26 Min
Video Lectures	1. https://www.youtube.com/watch?v=sm8bCHyTBNg 2. https://www.youtube.com/watch?v=xP0DIBkAPqQ 3. https://www.youtube.com/watch?v=n4muxtqLhN4 4. https://www.youtube.com/watch?v=7Fl7OoIzQYY&list=PLa2xctTiNSCjVzFfxTn_UKkd-sS34EQaF (7Lecture) 5. https://www.youtube.com/watch?v=27zYf9EPhWw&t=1248s	1Hr 29 Min 1Hr 40 Min 3Hrs 34 Min 23.33Min X7 2Hrs 32Min
Web References	Penetration Testing - Software Engineering - GeeksforGeeks Cyber Security Penetration Testing Penetration Testing: Complete Guide to Process, Types, and Tools	

List Of Practical's (Indicative & Not Limited To)

Lab No.	**Unit**	**Topic**	**Program Logic Building**	**CO Mapping**
1.1	1	Simulated Network Environment	Create a simulated network environment, identify vulnerabilities, and devise ethical hacking strategies.	**CO1**
1.2	1	Network Reconnaissance	Use tools like Nmap and Wireshark to conduct network reconnaissance and analyze captured network traffic.	**CO1**
1.3	1	Legal & Ethical Aspects of Penetration Testing	Research and present case studies highlighting legal and ethical implications of penetration testing.	**CO1**
1.4	1	Penetration Testing Methodology	Develop a penetration testing methodology document outlining various phases and techniques.	**CO1**
2.1	2	Vulnerability Scanning	Perform network scans using tools like Nessus and identify active hosts, open ports, and services.	**CO2**
2.2	2	Vulnerability	Exploit vulnerabilities identified during scanning,	**CO2**

		Exploitation	gaining unauthorized access to target systems.	
2.3	2	Firewall Evasion Techniques	Design and execute firewall evasion techniques to bypass network defenses and gain access to internal systems.	**CO2**
2.4	2	Packet Capture Analysis	Analyze packet captures detecting and mitigating network-based attacks, such as DoS and DDoS attacks.	**CO2**
3.1	3	OWASP Top 10 Vulnerabilities	Identify and exploit common web application vulnerabilities outlined in the OWASP Top 10 list.	**CO3**
3.2	3	Web Application Security Testing	Utilize tools like Burp Suite to perform web application scans and identify security vulnerabilities.	**CO3**
3.3	3	SQL Injection Attacks	Execute SQL injection attacks against vulnerable web applications to extract sensitive information.	**CO3**
3.4	3	Cross-Site Scripting (XSS)	Inject malicious scripts into web applications to exploit XSS vulnerabilities and perform client-side attacks.	**CO3**
4.1	4	Android Security Architecture	Analyze Android security architecture, identify security controls, and develop secure coding practices.	**CO4**
4.2	4	iOS Security Mechanisms	Explore iOS security mechanisms, analyze secure coding guidelines, and mitigate common security threats.	**CO4**
4.3	4	Mobile Application Reverse Engineering	Reverse engineer Android and iOS applications to identify vulnerabilities and analyze application logic.	**CO4**
4.4	4	Mobile Application Security Assessment	Perform comprehensive security assessments of mobile applications, identifying and exploiting vulnerabilities.	**CO4**
5.1	5	Advanced Exploitation Techniques	Employ advanced exploitation techniques like buffer overflows and privilege escalation to gain system access.	**CO5**
5.2	5	IDS/IPS Log Analysis	Perform basic IDS/IPS log analysis for intrusion detection.	**CO5**
5.3	5	Privilege Escalation	Perform privilege escalation techniques on compromised systems.	**CO5**
5.4	5	Authentication & Session Management Testing	Test authentication and session management vulnerabilities.	**CO5**
Total Hours: 75 hrs.				

LAB Course Code: BCSE0659X	**LAB Course Name: Applied Research with Mini Project**	**L**	**T**	**P**	**C**
Course Offered in: All Computing Branches		**0**	**0**	**2**	**1**

Pre-requisite: Basic knowledge of programming, data structures, databases, and fundamental concepts of software development. Familiarity with tools and technologies for system development is desirable.

Course Objectives:

This course aims to develop the ability to design and implement solutions for real-world problems using appropriate tools and technologies. It emphasizes system integration, performance evaluation, and effective documentation, along with promoting research skills through the preparation of a structured research paper.

Course Outcome: After completion of the course, the student will be able to		Bloom's level
CO1	Identify and define a domain-specific real-world problem through literature review, objective formulation, and structured project planning suitable for research-based implementation.	K4
CO2	Design, develop, and validate a functional prototype/model/system using appropriate tools, technologies, or methodologies while considering performance, ethics, safety, and reliability.	K6
CO3	Document, analyze, and present project outcomes through a technical report and a structured research paper in IEEE/Scopus/UGC-approved format, demonstrating research communication and publication readiness.	K4

CO-PO Mapping (Scale 1: Low, 2: Medium, 3:High)

CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2	PSO3
CO1	3	3	2	2	2	-	-	1	2	2	1	3	1	3
zCO2	3	3	3	3	3	1	1	2	3	2	2	3	3	3
CO3	2	2	2	2	2	-	-	2	3	3	2	2	1	2

Module	**Common Applied Research-Based Mini Project Activities (All Branches)**	**Expected Outcomes**
Module 1: Research Foundation & Project Planning	1. Identify domain-specific problem statement relevant to the branch. 2. Define objectives, hypothesis, and expected outcomes 3. Conduct literature review 4. Select suitable tools, technologies, software, datasets, laboratory methods, or platforms. 5. Design project methodology, workflow, or system/process architecture	Clear research problem formulation, defined objectives, foundational knowledge, and structured project roadmap
Module 2: Development, Design & Implementation	6. Develop core project components, models, experiments, prototypes, or processes. 7. Integrate relevant modules such as software, hardware, simulation, experimentation, analysis, or field implementation. 8. Apply discipline-specific techniques such as coding, fabrication, experimentation, surveys, analytics, optimization, or modelling. 9. Incorporate safety, ethics, reliability, sustainability, and security considerations where applicable	Functional prototype/model/system/process with interdisciplinary implementation and practical technical skills
Module 3: Testing, Validation & Optimization	10. Perform testing, experimentation, or validation of developed work. 11. Analyze performance, efficiency, feasibility, or effectiveness. 12. Apply analytical, computational, statistical, or intelligent techniques where relevant. 13. Optimize design, methodology, process, or	Validated and optimized project demonstrating performance improvement, technical analysis, and practical feasibility

	implementation for improved outcomes	
Module 4: Documentation, Research Publication & Presentation	14. Document project design, methodology, implementation, and results. 15. Prepare technical report/project dissertation. 16. Draft a research paper in standard format (Abstract, Introduction, Methodology, Results, Conclusion, References) 17. Format manuscript according to IEEE/Scopus/UGC-approved guidelines. 18. Include proper figures, tables, graphs, citations, and references 19. Present project findings through seminar/poster/presentation. 20. Demonstrate developed system/model/prototype/process. 21. Submit final project report and research paper for evaluation/publication consideration	Complete technical documentation, publishable-quality research paper, professional presentation skills, and final project submission