NOIDA INSTITUTE OF ENGINEERING & TECHNOLOGY, GREATER NOIDA, GAUTAM BUDDH NAGAR
(AN AUTONOMOUS INSTITUTE)

NIET
Greater Noida
Autonomous Institute
Estd.2001
Get Future Ready

Affiliated to

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

Evaluation Scheme & Syllabus

For

Bachelor of Technology
Computer Science & Engineering (Cyber Security)
Third Year

(Effective from the Session: 2024-25)

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

(AN AUTONOMOUS INSTITUTE)

Bachelor of Technology

Computer Science & Engineering (Cyber Security)

Evaluation Scheme

SEMESTER-V

S. 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	ACSE0503	Design Thinking-II	Mandatory	2	1	0	30	20	50		100		150	3
2	ACSCY0501	Cyber Security Essentials	Mandatory	3	1	0	30	20	50		100		150	4
3	ACSCY0502	Ethical Hacking	Mandatory	3	1	0	30	20	50		100		150	4
4		Departmental Elective I	Departmental Elective	3	0	0	30	20	50		100		150	3
5		Departmental Elective II	Departmental Elective	3	0	0	30	20	50		100		150	3
6	ACSE0505	Web Technology	Mandatory	3	0	0	30	20	50		100		150	3
7	ACSCY0551	Cyber Security Essentials Lab	Mandatory	0	0	2				25		25	50	1
8	ACSCY0552	Ethical Hacking Lab	Mandatory	0	0	2				25		25	50	1
9	ACSE0555	Web Technology Lab	Mandatory	0	0	2				25		25	50	1
10	ACSE0559	Internship Assessment-II	Mandatory	0	0	2				50			50	1
11	ANC0501/ ANC0502	Constitution of India, Law and Engineering/ Essence of Indian Traditional Knowledge	Compulsory Audit	2	0	0	30	20	50		50		100	NA
		*Massive Open Online Courses (For B.Tech. Hons. Degree)	*MOOCs											
		TOTAL											**1100**	**24**

*** List of Recommended MOOCs (Massive Open Online Courses) for Third Year B. Tech Students (Semester-V)**

S.No.	Subject Code	Course Name	University / Industry Partner Name	No of Hours	Credits
1	AMC0271	Cyber Security and Hacker Tactics Awareness Training	Infosys Wingspan (Infosys Springboard)	14h 24m	1
2	AMC0229	ReactJS	Infosys Wingspan (Infosys Springboard)	61h 2m	4
3	AMC0287	Digital Forensics Essentials	EC-Council	11hrs	0.5
4	AMC0288	Network Defense Essentials	EC-Council	14hrs	1

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 – ANC0501/ANC0502)**
  - 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.

List of Departmental Electives

Sl. No.	Subject Codes	Subject Name	Type of Subject	Bucket Name	Branch	Semester
1	ACSE0511	CRM Fundamentals	Departmental Elective-I	CRM-RPA	AI	5
2	ACSE0513	CRM Administration	Departmental Elective-II		AI	5
3	ACSAI0512	Data Analytics	Departmental Elective-I	Data Analytics	AI	5
4	ACSAI0519	Business Intelligence and Data Visualization	Departmental Elective-II		AI	5
5	ACSE0512	Python Web Development with Django	Departmental Elective-I	Full Stack Development	AI	5
6	ACSE0514	Design Patterns	Departmental Elective-II		AI	5
7	ACSAI0515	Mobile Application Development	Departmental Elective-I	Mobility Management	AI	5
8	ACSAI0521	Development in Swift Fundamentals	Departmental Elective-II		AI	5

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

(AN AUTONOMOUS INSTITUTE)

Bachelor of Technology

Computer Science & 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	ACSCY0601	Digital Forensics	Mandatory	3	1	0	30	20	50		100		150	4
2		Departmental Elective III	Departmental Elective	3	0	0	30	20	50		100		150	3
3		Departmental Elective IV	Departmental Elective	3	0	0	30	20	50		100		150	3
4		Open Elective I	Open Elective	3	0	0	30	20	50		100		150	3
5	ACSE0603	Software Engineering	Mandatory	3	0	0	30	20	50		100		150	3
6	ACSCY0602	Cloud Security and Privacy	Mandatory	3	0	0	30	20	50		100		150	3
7	ACSCY0651	Digital Forensics Lab	Mandatory	0	0	2				25		25	50	1
8	ACSE0653	Software Engineering Lab	Mandatory	0	0	2				25		25	50	1
9	ACSCY0652	Cloud Security and Privacy Lab	Mandatory	0	0	2				25		25	50	1
10	ACSE0659	Mini Project	Mandatory	0	0	2				50			50	1
11	ANC0602/ ANC0601	Essence of Indian Traditional Knowledge/ Constitution of India, Law and Engineering	Compulsory Audit	2	0	0			50		50		100	NA
		*Massive Open Online Courses (For B.Tech. Hons. Degree)	*MOOCs											
		TOTAL											**1100**	**23**

*** List of Recommended MOOCs (Massive Open Online Courses) for Third Year B. Tech Students (Semester-VI)**

S. No.	Subject Code	Course Name	University / Industry Partner Name	No of Hours	Credits
1	AMC0234	Exploratory Data Analysis	Infosys Wingspan (Infosys Springboard)	7h 13m	0.5
2	AMC0323	Cyber Security and Applied Ethical Hacking	Infosys Wingspan (Infosys Springboard)	12h 59m	1

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 – ANC0601/ANC0602)**
  - 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

List of Departmental Electives

Sl. No.	Subject Codes	Subject Name	Type of Subject	Bucket Name	Branch	Semester
1	ACSE0611	CRM Development	Departmental Elective-III	CRM-RPA	AI	6
2	ACSE0613	Robotics Process Automation (RPA)	Departmental Elective-IV		AI	6
3	ACSAI0617	Programming for Data Analytics	Departmental Elective-III	Data Analytics	AI	6
4	ACSAI0622N	Social Media Analytics	Departmental Elective-IV		AI	6
5	ACSAI0612	Advanced Java Programming	Departmental Elective-III	Full Stack Development	AI	6
6	ACSE0614	Web Development using MEAN Stack	Departmental Elective-IV		AI	6
7	ACSAI0614	Development in Swift Explorations and Data Collections	Departmental Elective-III	Mobility Management	AI	6
8	ACSAI0620	Augmented Reality and Virtual Reality	Departmental Elective-IV		AI	6

NOIDA INSTITUTE OF ENGINEERING & TECHNOLOGY, GREATER NOIDA, GAUTAM BUDDH NAGAR
(AN AUTONOMOUS INSTITUTE)

A student will be eligible to get Under Graduate degree with Honours only, if he/she completes the additional MOOCs courses such as Coursera 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 Coursera 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

B. TECH THIRD YEAR 5th SEMETER (DS/AI/AIML/IoT/CS)			
Course code	**ACSE0503**	**L T P**	**Credits**
Course title	**DESIGN THINKING II**	**2 1 0**	**3**

Course Objectives: The objective of this course is to upgrade Design Thinking skills by learning & 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

Pre-requisites: Student must complete Design Thinking-I course.

Course Contents / Syllabus

UNIT-I	**INTRODUCTION**	**10 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 it's 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.

UNIT-II	**REFINEMENT AND PROTOTYPING**	**8 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.

UNIT-III	**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

UNIT-IV	**INNOVATION, QUALITY AND LEADERSHIP**	**6 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.

UNIT-V	**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.

Course outcome: After completion of this course, students will be able to

CO 1	Learn sophisticated design tools to sharpen their problem-solving skills	K2
CO 2	Construct innovate ideas using design thinking tools and converge to feasible idea for breakthrough solution	K6
CO 3	Implement storytelling for persuasive articulation	K3
CO 4	Understanding the nature of leadership empowerment	K2
CO 5	Understand the role of a human being in ensuring harmony in society and nature.	K2

Textbooks:

1. Arun Jain, UnMukt : Science & Art of Design Thinking, 2020, Polaris
2. Gavin Ambrose and Paul Harris, Basics Design 08: Design Thinking, 2010, AVA Publishing SA

3. R R Gaur, R Sangal, G P Bagaria, A Foundation Course in Human Values and Professional Ethics, First Edition, 2009, Excel Books: New Delhi

Reference Books:

1. Jeanne Liedta, Andrew King and Kevin Benett , Solving Problems with Design Thinking – Ten Stories of What Works, 2013, Columbia Business School Publishing.
2. Dr Ritu Soryan, Universal Human Values and Professional Ethics, 2022, Katson Books.
3. Vijay Kumar, 101 Design Methods: A Structured Approach for Driving Innovation in Your Organization, 2013, John Wiley and Sons Inc, New Jersey.
4. Roger L. Martin, Design of Business: Why Design Thinking is the Next Competitive Advantage, 2009, Harvard Business Press, Boston MA.
5. Tim Brown, Change by Design, 2009, Harper Collins.
6. Pavan Soni, Design your Thinking : The Mindsets, Toolsets and Skill Sets for Creative Problem-Solving, 2020, Penguin Books.

Links: NPTEL/ YouTube/ Web Link:

Unit I https://www.youtube.com/watch?v=6_mHCOAAEI8
https://nptel.ac.in/courses/110106124
https://designthinking.ideo.com/
https://blog.experiencepoint.com/how-mcdonalds-evolved-with-design-thinking

Unit II https://www.coursera.org/lecture/uva-darden-design-thinking-innovation/the-ibm-story-iq0kE
https://www.coursera.org/lecture/uva-darden-design-thinking-innovation/the-meyouhealth-story-part-i-what-is-W6tTs
https://onlinecourses.nptel.ac.in/noc19_mg60/preview

Unit III https://nptel.ac.in/courses/109/104/109104109/
https://www.d-thinking.com/2021/07/01/how-to-use-storytelling-in-design-thinking/

Unit IV https://www.worldofinsights.co/2020/10/infographic-8-design-thinking-skills-for-leadership-development/

Unit V https://www.youtube.com/watch?v=hFGVcx1Us5Y

B. TECH THIRD YEAR 5th SEMETER (CYS)			
Course code	**ACSCY0501**	**L T P**	**Credits**
Course title	**CYBER SECURITY ESSENTIALS**	**2 3 1 2**	**4**

Course Objectives: To provide a comprehensive understanding of key cybersecurity concepts and tools by covering the identification and response to various cyber-attacks, the design and deployment of VPN networks using OpenVPN, and analysis of network traffic with Wireshark.

Pre-requisites: Basic understanding of networking, operating systems and programming.

Course Contents / Syllabus

UNIT-I	**CYBER SECURITY ATTACKS**	**6 HOURS**

Cybersecurity & its key principles, Cyber security threats landscapes, Attacks on different Devices, Attacks on Personal Computers and Laptops, Network attacks, IOT attacks ,Industry Controlled Systems attacks, Server & Cloud attacks, POS attacks, Smart Vehicles attacks

UNIT-II	**VIRTUAL PRIVATE NETWORKS AND OPENVPN CONFIGURATION**	**4 HOURS**

Introduction to Virtual Private Networks (VPNs), VPN protocols and encryption algorithms, OpenVPN installation and configuration, Secure communication using OpenVPN .

UNIT-III	**NETWORK SECURITY WITH WIRESHARK**	**4 HOURS**

Incident Response and Forensic Analysis with Wireshark, Protocol Analysis, Wireshark Scripting and Automation, Secure Communication Analysis, IoT Security Analysis, Wireless Network Security Analysis

UNIT-IV	**INTRODUCTION TO OSI MODEL SECURITY AND KALI LINUX**	**4 HOURS**

Physical security measures for hardware, Protection against tampering and unauthorized access
Data Link layer: MAC address filtering. VLANs for traffic. segmentation.
Network Layer - Access control lists (ACLs) and firewalls. Virtual Private Networks (VPNs). Secure routing protocols.
Transport Layer (Layer 4): SSL/TLS encryption. Firewalls and traffic policies.
Session & Presentation Layer: Authentication and authorization.
Session encryption. Data compression and encryption
Application Layer: Web application security
Overview of Kali Linux and its features, Kali Linux installation and setup, Basic commands and tools in Kali Linux.

UNIT-V	**PASSWORD SECURITY AND CRACKING TECHNIQUES**	**4 HOURS**

Password security principles and best practices, Password cracking techniques and methods
Introduction to John the Ripper password-cracking tool

Course outcome: After completion of this course, students will be able to		
CO 1	Apply basic defensive strategies by acquiring foundational understanding of cybersecurity principles and cyber-attacks on different devices	K2
CO 2	Configure secure remote access solutions using OpenVPN, ensuring confidentiality, integrity, and authenticity of network communication.	K3
CO 3	Apply techniques for capturing, analyzing, and interpreting network traffic using Wireshark, enabling them to identify security vulnerabilities, troubleshoot network issues, and detect malicious activities.	K4
CO 4	Develop proficiency in Kali Linux tools for vulnerability assessment along with security at different levels of OSI model	K3
CO 5	Apply various password-cracking techniques, understand password security, and acquire the skills to assess password vulnerabilities and implement more robust security measures	K3

Textbooks:

1."Kali Linux Revealed: Mastering the Penetration Testing Distribution"

2."Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems"

3. How to Set Up an OpenVPN Server using Amazon's Free Tier

4. Ethical Password Cracking: Crack any code using John the Ripper, Hashcat, and advanced methods for password breaking

Reference Books:

5. Cyber Security: The Essential Guide

6. Cyber Security Essentials: Understanding Risk And Controls

7. The Essential Guide To Cybersecurity For Smbs (English, Paperback, Hayslip Gary)

8. Cyber Security : Learn All The Essentials And Basic

Links: NPTEL/ YouTube/ Web Link:

Unit 1	https://youtu.be/lpa8uy4DyMo?list=PL9ooVrP1hQOGPQVeapGsJCktzIO4DtI4_
Unit 2	https://youtu.be/5Dw8iAUJoVc?list=PLTI5OvNLkI8VWWWl6Av4GICTzg5BZsn6z
Unit 3	https://youtu.be/hXSFdwIOfnE
Unit 4	https://youtu.be/D4fYyu305jg
Unit 5	https://youtu.be/RNwMeijExjg

B. TECH THIRD YEAR 5th SEMETER (CYS)			
Course code	**ACSCY0502**	**L T P**	**Credits**
Course title	**ETHICAL HACKING**	**3 1 2**	**4**

Course Objectives: To equip students with the skills and knowledge to identify and exploit vulnerabilities in computer systems ethically, and to understand the legal responsibilities of ethical hacking.

Pre-requisites: Basic understanding of computer networks, operating systems, cybersecurity fundamentals and programming concepts.

Course Contents / Syllabus

UNIT-I	**INTRODUCTION TO ETHICAL HACKING**	**6 HOURS**

Understanding the concept of ethical hacking, History and evolution of hacking, Scope and importance of ethical hacking in cybersecurity, Legal and ethical considerations in ethical hacking, Common terminologies and tools used in ethical hacking

UNIT-II	**FOOTPRINTING AND RECONNAISSANCE**	**4 HOURS**

Introduction to Cuckoo Sandbox, Basic Usage of Cuckoo Sandbox, Malware Analysis with Cuckoo Sandbox, Integrating Cuckoo Sandbox with Security Operations, Footprinting concepts and methodologies.
Passive and active reconnaissance techniques
Information gathering through search engines, social media, and WHOIS lookup, Network scanning and enumeration techniques, Vulnerability scanning and analysis

UNIT-III	**WEB APPLICATION SECURITY**	**4 HOURS**

Introduction to web application security, Common web vulnerabilities (SQL injection, XSS, CSRF, etc.)
Web application reconnaissance and Footprinting, Web application scanning and enumeration
Secure coding practices and web application hardening

UNIT-IV	**SCANNING AND ENUMERATION**	**2 HOURS**

Port scanning techniques (TCP, UDP), Service enumeration and version detection
OS fingerprinting, Vulnerability assessment and analysis, Using scanning tools like Nmap, Nessus, and OpenVAS.

UNIT-V	**SYSTEM HACKING**	**4 HOURS**

Wifi Password cracking techniques, Escalating privileges and gaining unauthorized access, Exploiting system vulnerabilities
Malware analysis and reverse engineering, Countermeasures and defensive strategies against system hacking

Course outcome: After completion of this course, students will be able to

CO 1	Understand the concept of hacking and perform hacking related activities ethically	K2
CO 2	Acquire knowledge and skills of various tools used in footprints, port scanning, and reconnaissance techniques and will apply in cybersecurity.	K3
CO 3	Identify, analyze, and mitigate security vulnerabilities in web applications using tool	K4
CO 4	Develop the ability to conduct comprehensive scanning and enumeration to identify network resources, services, and potential vulnerabilities effectively using openVAS.	K3
CO 5	Execute and defend against system hacking techniques, including gaining unauthorized access, escalating privileges, and maintaining persistent control.	K3

Textbooks:

1. "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy" by Patrick Engebretson, 2013
2. "CEH Certified Ethical Hacker All-in-One Exam Guide" by Matt Walker, 2019
3. "Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto, 2016

Reference Books:

1. Penetration Testing: A Hands-On Introduction to Hacking" by Georgia Weidman, 2017
2. "OWASP Testing Guide" by OWASP Foundation,2020
3. "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning" by Gordon Fyodor Lyon, 2018

Links: NPTEL/ YouTube/ Web Link:

Unit 1	https://www.youtube.com/watch?v=3Kq1MIfTWCE&list=PLWKjhJtqVAbnklGh3FNRLECx_2D_vK3mu
Unit 2	https://www.youtube.com/watch?v=6d0VY37lNfA&list=PL1dx_7g6scPKn5_x2NJ6pONit1dJ1OaYU
Unit 3	https://www.youtube.com/watch?v=AnwgxRtWXLI&list=PLhfrWIlLOoKMe1Ue0IdeULQvEgCgQ3a1B
Unit 4	https://www.youtube.com/watch?v=vK4Mno4QYqk
Unit 5	https://www.youtube.com/watch?v=3FNYvj2U0HM

B. TECH THIRD YEAR 5th SEMETER (CYS)			
Course Code	**ACSE0505**	**L T P**	**Credits**
Course Title	**WEB TECHNOLOGY**	**3 0 0**	**3**

Course objective: This course covers different aspect of web technology such as HTML, CSS, Java Script and provide fundamental concepts of Internet, Web Technology and Web Programming**.** Students will be able to build a proper responsive website.

Pre-requisites: Basic Knowledge of any programming language like C/C++/Python/Java. Familiarity with basicconcepts of Internet.

Course Contents / Syllabus

UNIT-I	**Basics of Web Technology & Testing**	**8 Hours**

History of Web and Internet, connecting to Internet, Introduction to Internet services and tools, Client-Server Computing, Protocols Governing Web, Basic principles involved in developing a web site, Planning process, Typesof Websites, Web Standards and W3C recommendations, Web Hosting Basics, Types of Hosting Packages,Introduction to Web testing, Functional Testing,
Usability & Visual Testing, Performance & Load Testing.

UNIT-II	**Introduction to HTML & XML**	**8 Hours**

HTML, DOM- Introduction to Document Object Model, Basic structure of an HTML document, Mark up Tags, Heading-Paragraphs, Line Breaks, Understand the structure of HTML tables. Lists, working with Hyperlinks, Image Handling, Understanding Frames and their needs, HTML forms for User inputs. New form Elements- date, number, range, email, search and data list, Understanding audio, video and article tags XML Syntax, Elements, Attributes, Namespaces, Display, HTTP request, Parser, DOM, XPath, XSLT, XQuerry, XLink, Validator, DTD and XML Schema.

UNIT-III	**Concepts of CSS3 & Bootstrap**	**8 Hours**

Creating Style Sheet, CSS Properties, CSS Styling (Background, Text Format, Controlling Fonts), Working with blockelements and objects, Working with Lists and Tables, CSSId and Class,
BoxModel (Introduction, JavaScript Border properties, Padding Properties, Margin properties) CSS Advanced (Grouping, Dimension, Display, Positioning,

Floating, Align, Pseudo class,NavigationBar,ImageSprites,Attributesector),CSSColor,CreatingpageLayoutandSite. Bootstrap Features & Bootstrap grid system, Bootstrap Components, Bootstrap Plug-Ins.

UNIT-IV	**JavaScript and ES6**	**8 Hours**

Introduction to Java Script, Javascript Types, Var, Let and Const Keywords, Operators in JS, Conditional Statements,Java Script Loops, JS Popup Boxes JS Events, JS Arrays, Working with Arrays, JS Objects, JS Functions Validation of Forms, Arrow functions and default arguments, Template Strings, Strings methods, Callback functions, Object de-structuring, Spread and Rest Operator, Typescript fundamentals, Typescript OOPs- Classes, Interfaces, Constructor etc. Decorator and Spread Operator, Asynchronous Programming in ES6, Promise Constructor, Promise with Chain, Promise Race.

UNIT-V	**Introduction to PHP**	**8 Hours**

Basic Syntax of PHP, Variables & Constants, Data Type, Operator & Expressions, Control flow and Decision makingstatements, Functions, Strings, Arrays, Understanding file& directory, Opening and closing, a file, Copying, renamingand deleting a file, working with directories, Creating and deleting folder, File Uploading &Downloading. Introductionto Session Control, Session Functionality What is a Cookie, Setting Cookies with PHP. Using Cookies with Sessions,Deleting Cookies, Registering Session variables, Destroying the variables and Session.

Course outcome: After completion of this course students will be able to

CO 1	Identify the basic facts and explaining the basic ideas of Web technology and internet.	K1, K2
CO 2	Applying and creating various HTML5 semantic elements and application with working on HTML forms for user input.	K3, K6
CO 3	UnderstandingandapplyingtheconceptsofCreatingStyleSheetCSS3 and bootstrap.	K2, K3
CO 4	Analysing and implementing concept of JavaScript and its applications.	K4, K6
CO 5	Creating and evaluating dynamic web pages using the concept of PHP.	K5, K6

Text books:

1. C Xavier, “Web Technology and Design”, 1nd Edition 2003, New Age International.
2. Raj Kamal, “Internet and Web Technologies”, 2nd Edition 2017,Mc Graw Hill Education.
3. Oluwafemi Alofe, “Beginning PHP Laravel”,2nd Edition 2020, kindle Publication.

Reference Books:

1. Burdman, Jessica, “Collaborative Web Development” 5th Edition 1999, Addison Wesley Publication.
2. Randy Connolly, “Fundamentals of Web Development”,3rd Edition 2016,
3. Ivan Bayross,” HTML, DHTML, Java Script, Perl & CGI”, 4th Edition 2010 BPB Publication

NPTEL/ YouTube/Web Link:

Unit1	https://youtu.be/96xF9phMsWAhttps://youtu.be/Zopo5C79m2k https://youtu.be/ZliIs7jHi1s https://youtu.be/htbY9-yggB0
Unit2	https://youtu.be/vHmUVQKXlVohttps://youtu.be/qz0aGYrrlhU https://youtu.be/BsDoLVMnmZs https://youtu.be/a8W952NBZUE
Unit 3	https://youtu.be/1Rs2ND1ryYc https://youtu.be/vpAJ0s5S2t0 https://youtu.be/GBOK1-nvdU4 https://youtu.be/Eu7G0jV0ImY
Unit 4	https://youtu.be/-qfEOE4vtxE https://youtu.be/PkZNo7MFNFghttps://youtu.be/W6NZfCO5SIk https://youtu.be/DqaTKBU9TZk
Unit 5	https://youtu.be/_GMEqhUyyFMhttps://youtu.be/ImtZ5yENzgE https://youtu.be/xIApzP4mWyA https://youtu.be/qKR5V9rdht0

B. TECH THIRD YEAR 5th SEMETER (CYS)			
Course Code	**ACSCY0551**	**L T P**	**Credit**
Course Title	**CYBER SECURITY ESSENTIALS LAB**	**0 0 2**	**1**
List of Experiments			
Sr. No.	**Name of Experiment**		**CO**
1	Analyze the behavior of different malware types using tools like Wireshark, Process Monitor, and a sandbox environment.		CO1
2	Detect and remove the keylogger using anti-malware tools and system logs.		CO1
3	Create a simple vulnerable app. Task: Perform static and dynamic analysis on the app to identify security flaws.		CO1
4	Setup a router with default credentials and insecure configurations. Task: Exploit the default settings to gain unauthorized access, then secure the router.		CO1
5	Provide firmware images from IoT devices. Task: Use tools like Binwalk and Firmware Analysis Toolkit to identify vulnerabilities.		CO1
6	Provide a web applied Task: Perform an SQL injection attack and extract data, then apply fixes to prevent the vulnerability.		CO1
7	Provide a PoS system with simulated malware. Task: Analyze the malware's behavior and impact, then clean and secure the system.		CO1
8	Identify and exploit the misconfigurations, then secure the cloud environment.		CO1
9	To set up a basic OpenVPN server and client.		CO1
10	To configure OpenVPN with user authentication using a username and password.		CO1
11	To configure OpenVPN to use TLS for additional security.		CO1
12	To configure an OpenVPN server to handle multiple client connections.		CO1
13	To configure and monitor OpenVPN logs for security and troubleshooting.		CO1
14	Basic Packet Capture and Analysis using Wireshark		CO2

15	To understand the differences between HTTP and HTTPS traffic by capturing and analyzing them.	CO2
16	To identify common network attacks such as ARP spoofing, DoS attacks, or port scanning using Wireshark.	CO2
17	To capture and analyze DNS queries and responses.	CO2
18	To capture and analyze FTP traffic, highlighting the vulnerabilities of unencrypted FTP.	CO2
19	Write kali linux command to implement file management, file navigation and password cracking.	CO2
20	Write kali linux commands to perform network scanning and network configuration	CO2
21	Write kali linux commands to identify vulnerable access points in a network, file integrity and analysis	CO2
22	Write kali linux command to automate vulnerability scanning of a website, shell scripting, process management	CO2
23	Write kali linux command to exploit a known vulnerability in a target system, service management, search files, permission management	CO2
24	Develop a program to crack password hashes using various techniques supported by John the Ripper.	CO3
25	Create a program to generate custom wordlists for password cracking.	CO3
26	Design a program to perform a brute-force attack on a given password-protected file.	CO 3
27	Build a program to assess the strength of user passwords based on a given policy.	CO 3
28	Develop a program to create and apply custom rules for password cracking using John the Ripper.	CO 3
Lab Course Outcome: After the completions of this course students will be able to		
CO 1	Apply basic defensive strategies by acquiring foundational understanding of cybersecurity principles and cyber-attacks on different devices	K2
CO2	Configure secure remote access solutions using OpenVPN, ensuring confidentiality, integrity, and authenticity of network communication.	K3
CO3	Apply techniques for capturing, analyzing, and interpreting network traffic using Wireshark, enabling them to identify security vulnerabilities, troubleshoot network issues, and detect malicious activities.	K4
CO4	Develop proficiency in Kali Linux tools for vulnerability assessment along with security at different levels of OSI model	K3

CO5	Apply various password-cracking techniques, understand password security, and acquire the skills to assess password vulnerabilities and implement more robust security measures	K3

B. TECH THIRD YEAR 5th SEMETER (CYS)			
Course Code	**ACSCY0552**	**L T P**	**Credit**
Course Title	**ETHICAL HACKING LAB**	**0 0 2**	**1**
List of Experiments			
Sr. No.	**Name of Experiment**		**CO**
1	Install and configure a hypervisor (such as VMware Workstation or VirtualBox0		CO1
2	Perform file and directory management tasks (e.g., create, move, delete files/directories on LINUX).		CO1
3	Install and demonstrate tools like Wireshark, Nmap, and Metasploit.		CO1
4	Participate in a capture the flag (CTF) exercise using a platform like Hack The Box.		CO1
5	Analyze real-world case studies involving hacking incidents.		CO1
6	Set up a target virtual machine with vulnerable services for reconnaissance.		CO2
7	Perform passive reconnaissance using open-source intelligence (OSINT) tools.		CO2
8	Perform DNS interrogation and ping sweeps using tools like nslookup and fping.		CO2
9	Conducting information gathering through search engines, social media, and WHOIS lookup		CO2
10	Performing network scanning and enumeration using tools like Nmap		CO2
11	Prepare a virtualized lab for various practical exercises.		CO3
12	Install and use tools like Burp Suite, OWASP ZAP, and Nikto to scan a web application.		CO3
13	Exploit vulnerabilities like SQL injection and XSS on a vulnerable web application.		CO3
14	Discussion and analysis of lab results to reinforce learning outcomes and address any questions or		CO3

	concerns	
15	Setting up a virtualized environment for scanning and enumeration activities	CO3
16	Hands-on practice with different port scanning techniques using Nmap	CO3
17	Use Nmap and Netcat to enumerate services on a target machine.	CO3
18	OS fingerprinting demonstration using Nmap or Xprobe2	CO3
19	Vulnerability assessment lab using Nessus or OpenVAS, analysing scan results, and prioritizing vulnerabilities	CO3
20	Setup of virtualized lab environment for practical exercises.	CO3
21	Step-by-step guidance on using password cracking tools, privilege escalation techniques, and exploit frameworks.	CO3
22	Supervised practice sessions allowing students to perform password cracking, privilege escalation, vulnerability exploitation, malware analysis, and reverse engineering tasks.	CO3
23	Discussion and analysis of lab results to reinforce learning outcomes and address any questions or concerns.	CO3
Lab Course Outcome: After the completions of this course students will be able to		
CO 1	Demonstrate proficiency in ethical hacking techniques including information gathering (footprinting and reconnaissance), network scanning and enumeration, system hacking, exploitation of vulnerabilities, privilege escalation, and maintaining access while adhering to legal and ethical guidelines.	K3
CO2	Conduct thorough vulnerability assessments on networks and web applications, identifying common vulnerabilities such as SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF) using various automated tools and manual techniques.	K3
CO3	Develop practical expertise in system hacking, scanning, and enumeration to detect, exploit, and mitigate security vulnerabilities in networked environments.	K3

B. TECH THIRD YEAR 5th SEMETER (CYS)			
Course Code	**ACSE0555**	**L T P**	**Credit**
Course Title	**WEB TECHNOLOGY LAB**	**0 0 2**	**1**
List of Experiments			
Sr. No.	**Name of Experiment**		**CO**
1.	Write HTML program to display your CV in navigator, your Institute website, Department Website and Tutorial website for specific subject.		CO2
2.	Write a program in XML for creation of DTD, which specifies set of rules. Create a style sheet in CSS/ XSL & display the document in internet explorer.		CO2
3.	Write a program to show the use of XML Schema.		CO2
4.	Write a CSS program to show use of Inline, Internal and External CSS.		CO3
5.	Write a program for CSS Box Model.		CO3
6.	Write a program to show the use of Bootstrap components and Grid System		CO3
7.	Write HTML program to design Registration form and Validate it using JavaScript.		CO1,CO4
8.	Write JavaScript program to show the use of Dialogue Boxes i.e. Alert, Confirm andPrompt Boxes.		CO4
9.	Write a program to show various types of JavaScript Events.		CO4
10.	Write a program in PHP to find the factorial of given number.		CO5
11.	Write a program in PHP to perform file handling.		CO5
12.	Write a PHP program to show the use of Session & Cookies.		CO5
Lab Course Outcome: After completion of this course students will be able to			
CO 1	Implementing the concepts and creating pages of HTML		K3
CO 2	Implementing the concepts and creating HTML and XML pages.		K3, K6
CO 3	Implementing the concepts of CSS and Bootstrap and Creation of various types ofstyle sheets.		K3, K6

CO 4	Implementing JavaScript and creating Client Side Pages with functionalities.	K3, K6
CO 5	Implementing the concepts of PHP and creating Server Side Pages.	K3, K6

B. TECH THIRD YEAR 6th SEMETER (CYS)			
Course Code	**ACSCY0601**	**L T P**	**Credits**
Course Title	**DIGITAL FORENSICS**	**3 1 0**	**4**
Course objective: To equip students with the skills to investigate and analyse 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			
Pre-requisites: : Fundamental knowledge of computer networks, operating systems, and cybersecurity principles.			
Course Contents / Syllabus			
UNIT-I	**INTRODUCTION TO DIGITAL FORENSICS**		**6 Hours**
Overview of Digital Forensics, Legal and Ethical Issues, Digital Evidence, Forensic Tools and Software			
UNIT-II	**COMPUTER FORENSICS**		**6 Hours**
Computer Forensics Basics, Forensic Analysis Techniques, Operating System Artifacts, Reporting and Documentation OpenVAS Tool: Vulnerability Assessment and Management, Installation and Configuration, Scanning and Reporting			
UNIT-III	**MOBILE FORENSICS**		**6 Hours**
Introduction to Mobile Forensics, Mobile Data Acquisition, Analyzing Mobile Data, Challenges in Mobile Forensics			
UNIT-IV	**NETWORK FORENSICS**		**6 Hours**
Network Forensics Fundamentals, Capturing Network Traffic, Network Attack Analysis, Advanced Network Forensics			
UNIT-V	**CLOUD AND EMERGING TECHNOLOGIES FORENSICS**		**6 Hours**
Cloud Forensics, IoT Forensics, AI and ML Forensics, Cryptocurrency Forensics, Future Trends and Research in Forensics			

Course outcome: After completion of this course students will be able to		
CO 1	Understand the fundamental principles of digital forensics, including the legal and ethical considerations involved in handling digital evidence.	K2
CO2	Implement forensic analysis on computer systems, recover data, and document findings in a comprehensive forensic report.	K3
CO3	Analyse data from mobile devices using industry-standard tools and techniques.	K4
CO4	Analyse network traffic to identify and investigate network-based attacks and anomalies.	K4
CO5	Apply forensic techniques and investigations in emerging technologies such as Cloud Computing, IoT and big data.	K3

Text books:

1. Computer Forensics: Computer Crime Scene Investigation, John Vacca ,2015 [only one edition]
2. Practical Digital Forensics: Forensic Lab Setup, Evidence Analysis, and Structured Investigation Across Windows, Mobile, Browser, HDD, and Memory, Akashdeep Bhardwaj, Keshav Kaushik, 2023

Reference Books:

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

Links: NPTEL/ YouTube/ Web Link:

Unit1	https://www.youtube.com/watch?v=5e5KdbY-xzE
Unit2	https://www.youtube.com/playlist?list=PLa2xctTiNSCiTGuejkc05zsr-G5t9AuH8
Unit 3	https://www.youtube.com/playlist?list=PLJu2iQtpGvv-2LtysuTTka7dHt9GKUbxD
Unit 4	https://www.youtube.com/watch?v=uCqeNnH1EpQ
Unit 5	https://www.youtube.com/watch?v=MnzHF_jygws

B. TECH THIRD YEAR 6th SEMETER (CYS)

Course code	ACSE0603	L T P	Credits
Course title	SOFTWARE ENGINEERING	3 0 0	3

Course objective:

To teach the students all phases of the Software Development Life Cycle(SDLC) and their role in software development through theory as well as practice." Students will be able to apply the scientific knowledge in systematicway to create and build cost effective software solutions.

Pre-requisites: Basic knowledge about software and its types. Basic knowledge of OOPs concepts.

Course Contents / Syllabus

UNIT-I	INTRODUCTION	8 Hours

Introduction: Evolving role of software, Software Characteristics, Software crisis, Silver bullet, Software myths, Software Engineering Phases, Team Software Process (TSP), emergence of software engineering, Software process,project and product, Software Process Models: Waterfall Model, Prototype Model, Spiral Model, Iterative Model, Incremental Model, Agile Methodology: Scrum Sprint, Scrum Team, Scrum Master, Product Owner.

UNIT-II	SOFTWARE REQUIREMENT	8 Hours

Software Requirement Specifications (SRS): Requirement Engineering Process: Elicitation, Analysis, Documentation, Review and Management of User Needs, Feasibility Study, Information Modelling, Use Case Diagram, Data Flow Diagrams, Entity Relationship Diagrams, Decision Tables, SRS Document, IEEE Standards forSRS. Software Quality Assurance (SQA): Quality concepts, SQA activities, Formal approaches to SQA; Statistical software quality assurance; CMM, The ISO standard.

UNIT-III	SOFTWARE DESIGN	8 Hours

Software Design: Design principles, the design process; Design concepts: refinement, modularity: Cohesion, Coupling, Effective modular design: Functional independence, Design Heuristics for effective modularity, Softwarearchitecture: Function Oriented Design, Object Oriented Design: OOPs concepts-Abstraction, object, classification,inheritance, encapsulation, UML Diagrams-Class Diagram, Interaction diagram, Activity Diagram, control hierarchy: Top-Down and Bottom-Up Design, structural partitioning, software procedure.

UNIT-IV	SOFTWARE TESTING	8 Hours

Software Testing: Testing Objectives, 7 Principals of Testing, Levels of Testing: Unit Testing, System Testing, Integration Testing, User Acceptance Testing, Regression Testing, Testing for Functionality and Testing forPerformance, Top Down and Bottom-Up Testing Strategies: Test Drivers and Test Stubs, Structural Testing (WhiteBox Testing), Functional Testing (Black Box Testing), Test Data Suit Preparation, Alpha and Beta Testing of Products. Functional Testing(DAO, BO) Static Testing Strategies: Formal Technical Reviews (Peer Reviews), WalkThrough, Code Inspection, Compliance with Design and Coding Standards.

UNIT-V	**PROJECT MAINTENANCE AND MANAGEMENT CONCEPTS**	**8 Hours**

Project management concepts, Planning the software project, Estimation: Software Measurement and Metrics, Various Size Oriented Measures-LOC based, FP based, Halestead's Software Science, Cyclomatic Complexity Measures: Control Flow Graphs, Use-case based, empirical estimation COCOMO- A Heuristic estimation techniques, staffing level estimation, team structures, risk analysis and management. Configuration Management, Software reengineering: reverse engineering, restructuring: forward engineering, Clean Room software engineering.Case Tools, Software Maintenance: Preventive, Corrective and Perfective Maintenance, Cost of Maintenance, Needof Maintenance.

Course outcome: After completion of this course students will be able to

CO 1	Identify, formulate, analyse, and solve problems, as well as identify thecomputing requirements appropriate to their solutions. The ability to work in one or more significant application domains	K2, K4, K5
CO 2	Design, implement, and evaluate software-based systems, components, orprograms of varying complexity that meet desired needs, satisfy realistic constraints, and demonstrate accepted design and development principles.	K2, K3, K4, K6
CO 3	Apply knowledge of computing, mathematics, science, and engineering appropriate to the discipline, particularly in the modelling and design of software systems and in the analysis of trade-offs inherent in design decisions.	K3, K4
CO 4	Formulate testing strategies for software system, apply various testingtechniques such as unit testing, test driven development and functional testing.	K3
CO 5	Understand ability to engage in life-long maintenance and continuing Software development using various software management tools.	K2, K5

Text books:

1. KK Aggarwal and Yogesh Singh, Software Engineering, New Age International Publishers 3RDEdition(December 11, 2008)
2. RS Pressman, Software Engineering: A Practitioners Approach, McGraw Hill. 7thEdition.(14-Jan-2022)
3. Rajib Mall, Fundamentals of Software Engineering, PHI Publication.4th Edition.(1 January 2014)

Reference Books:

1. Pankaj Jalote, Software Engineering, Wiley. (1 January 2010)

2. Ghezzi, M. Jarayeri, D. Manodrioli, Fundamentals of Software Engineering, PHI Publication. 2nd Edition. (1 January 2007)
3. Kassem Saleh, “Software Engineering”, Cengage Learning. (2009)
4. Ian Summerville, Software Engineering, Addison Wesley. 9th Edition.(29 October 2017)

Links: NPTEL/ YouTube/ Web Link:

Unit 1	https://youtu.be/x-jqSXYE4S4
Unit 2	https://youtu.be/mGkkZoFc-4I
Unit 3	https://youtu.be/sGxgZxwuHzc
Unit 4	https://youtu.be/BNk7vni-1Bo
Unit 5	https://youtu.be/8swQr0kckZI

B. TECH THIRD YEAR 6th SEMETER (CYS)

Course code	ACSCY0602	L T P	Credits
Course title	CLOUD SECURITY AND PRIVACY	3 0 0	3

Course objective:

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.

Pre-requisites: Familiarity with networking concepts, cybersecurity principles, and mobile application development.

Course Contents / Syllabus

UNIT-I	INTRODUCTION TO CLOUD AND MOBILE SECURITY	6 Hours

Overview of Cloud Computing. Importance of Security in Cloud and Mobile Environments.
Threat Landscape: Common Security Risks and Vulnerabilities, Security Principles and Best Practices

UNIT-II	CLOUD SECURITY FUNDAMENTALS	4 Hours

Cloud Service Models: IaaS, PaaS, SaaS Shared Responsibility Model in Cloud Security. Identity and Access Management (IAM) in Cloud Environments.
Data Encryption and Key Management. Securing Cloud Infrastructure: Virtualization, Containers,and Orchestration

UNIT-III	PRIVACY PRESERVATION	6 Hours

Anonymization techniques: Generalization, Suppression,Perturbation, Pseudonymization.
Anonymization algorithms: Datafly, 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-IV	MOBILE SECURITY BASICS	6 Hours

Mobile Operating Systems: IOS, and AndroidArchitecture and its Security,
Secure Mobile Development Practices: Authentication and Authorization in Mobile Applications
Data Protection on Mobile Devices: Encryption, SecureStorages.

UNIT-V	PROJECT MAINTENANCE AND MANAGEMENT CONCEPTS	6 Hours

Mobile Device Management (MDM) and MobileApplication Management (MAM)
Mobile Threat Defense: Detection and Prevention Strategies
Secure Communication on Mobile Devices: VPNs, TLSBiometric Security on Mobile Devices,
Mobile Security Case Studies

Course outcome: After completion of this course students will be able to

CO 1	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

Text books:

1. Debasish Mandal, Penetration Testing for Jobseekers: Perform Ethical Hacking across Web Apps, Networks, Mobile Devices using Kali Linux, Burp Suite, MobSF, and Metasploit
2. Gerardus Blokdyk, Mobile Device Management MDM A Complete Guide - 2020
3. Tim Speed and Joseph Downs, "Mobile Security: How to Secure, Privatize, and Recover Your Devices"

Reference books:

1. Bill Phillips and Chris Stewart, "Android Programming: The Big Nerd Ranch Guide"
2. Christian Keur, Aaron Hillegass, "iOS Programming: The Big Nerd Ranch Guide"

Links: NPTEL/ YouTube/ Web Link:

Unit 1	**https://www.youtube.com/playlist?list=PLVHgQku8Z934QrhnpXGXdfE63w7Qj9eJn**
Unit 2	**https://www.youtube.com/playlist?list=PLOspHqNVtKACfjqfEwR3iKz1gJILKj5Tn**
Unit 3	**https://www.youtube.com/playlist?list=PL-JvKqQx2AtfQ8cGyKsFE7Tj2FyB1yCkd**
Unit 4	**https://www.youtube.com/playlist?list=PLBV6VAQlom0kA8gpvOkHmT2VQ39vRkXQ2**
Unit 5	**https://www.youtube.com/playlist?list=PLVHgQku8Z934QrhnpXGXdfE63w7Qj9eJn**

B. TECH THIRD YEAR 6th SEMETER (CYS)

Course Code	ACSCY0651	L T P	Credit
Course Title	DIGITAL FORENSICS LAB	0 0 2	1

List of Experiments

Sr. No.	Name of Experiment	CO
1.	Using tools to identify and collect digital evidence	CO1
2.	Installation and basic usage of forensic tools	CO1
3.	Analyzing 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.	Analyzing system artifacts from different OS	CO1
8.	Installing OpenVAS, performing scans, and generating reports	CO1
9.	Extracting data logically from various mobile devices	CO2
10.	Extracting data physically from various mobile devices	CO2
11.	Analyzing extracted data from mobile devices	CO2
12.	Identifying and reporting on challenges in mobile forensics	CO2
13.	Capturing and analyzing network packets	CO2
14.	Using tools like tcpdump to capture network traffic	CO2
15.	Detecting and analyzing network-based attacks	CO2
16.	Performing deep packet inspection and correlating events	CO2
17.	Extracting and analyzing data from cloud platforms	CO3
18.	Performing forensic analysis on various IoT devices	CO3
19.	Research and document emerging trends in forensics	CO3

Lab Course Outcome: After completion of this course students will be able to

CO 1	Apply digital evidence collection techniques and analyze forensic tool usage by and utilizing OpenVAS for vulnerability scanning.	K3
CO 2	Analyze digital evidence in mobile devices and conduct network forensics investigations, applying forensic techniques to extract valuable insights.	K4

CO 3	Analyze digital evidence in cloud and emerging technology environments, applying forensic techniques to conduct investigations and ensure compliance with legal and ethical standards.	K4

B. TECH THIRD YEAR 6th SEMETER (CYS)

Course code	ACSE0653	L T P	Credit
Course title	SOFTWARE ENGINEERING LAB	0 0 2	1

List of Experiments

Sr. No.	Name of Experiment	CO
1.	Team formation and allotment of Mini project: Problem statement, Literaturesurvey, Requirement analysis.	CO1
2.	Draw the use case diagram: specify the role of each of the actors, Data FlowDiagram (DFD): All levels.	CO2
3.	Design an ER diagram for with multiplicity.	CO2
4.	Prepare a SRS document in line with the IEEE recommended standards.	CO2
5.	Create a Software Design Document (SDD): Object and Class diagram.	CO3
6.	Create Interaction diagram: sequence diagram, collaboration diagram for SDD.	CO3
7.	Create Activity diagram and Component diagram for SDD	CO4
8.	Estimation of Test Coverage Metrics and Structural Complexity.	CO5
9.	Design test suite for equivalence class partitioning.	CO5
10.	Design test cases for Boundary value analysis	CO5
11.	Mini Project with CASE tools.	CO5
12.	Mini Project with CASE tools.	CO4

Lab Course Outcome: After completion of this course students will be able to

CO1	Develop python programs to work on Data sets and Implement ArtificialNeural Network Techniques.	K6
CO2	Explore different types of tensor and perform exploratory data analysis on different data sets.	K4
CO3	Apply Automatic Image Captioning with Keras ---Facial Recognition.	K3

B. TECH THIRD YEAR 6th SEMETER (CYS)

Course code	ACSCY0652	L T P	Credit
Course title	CLOUD SECURITY AND PRIVACY LAB	0 0 2	1

List of Experiments

Sr. No.	Name of Experiment	CO
1.	Basic Understanding of AWS Platform	CO1
2.	Analyze potential security risks and prioritize them.	CO1
3.	Create threat models for cloud-based systems and mobile apps.	CO1
4.	Configure IAM roles and policies for access control.	CO1
5.	Encrypt data and manage encryption keys securely.	CO1
6.	Deploy containerized applications securely.	CO1
7.	Understand how to securely store sensitive data in Amazon S3 using encryption and access controls.	CO1
8.	Learn how to implement data masking to protect sensitive information in Amazon RDS databases	CO2
9.	Learn how to anonymize dataset without affecting its utility using DataFly algorithm	CO2
10.	Learn how to anonymize dataset without affecting its utility using Incognito Algorithm	CO2
11.	Learn how to monitor and audit AWS resources to ensure compliance with privacy regulations.	CO2
12.	Explore differential privacy techniques for preserving privacy in data analytics scenarios.	CO2
13.	Analyze mobile app security using MobSF and OWASP guidelines.	CO2
14.	Encrypt mobile devices and configure security settings.	CO3
15.	Simulate mobile security incidents and respond to threats.	CO3
16.	Implement biometric authentication in a sample app.	CO3

Lab Course Outcome: After completion of this course students will be able to

CO1	Summarize Security risks and vulnerabilities and apply security measures within cloud and mobile environments to ensure robust protection for digital assets.	K5

CO2	Implement data anonymization techniques and analyze differential privacy methods to ensure data privacy andregulatory adherence.	K4
CO3	Analyze mobile app security, encrypt devices, simulate security incidents, and implement biometric authentication.	K4