People’s Education Society’s (Mumbai)

P. E. S. COLLEGE OF ENGINEERING

An Autonomous Institute

Nagsen Vana, Chhatrapati Sambhajinagar, Maharashtra,
431002 Tel. No. (+91) 240 2400031
Web: www.pescoe.ac.in

CURRICULUM FOR POST GRADUATE PROGRAMME

Department of Computer Science & Engineering (Cyber Security)

In line with National Education Policy 2020 Guidelines
[With Effect from the Academic Year 2025-2026]

				1.00
Chairman Board of Studies	Dean Academics	Chairman Academic Council	Date of Release	Version

Department Vision

To become centre of excellence in computer education to create globally competitive graduate with moral and social responsibilities

Department Mission

The CSE department is committed to create computer engineers with updated professional competencies to work in various domains and having moral and social attributes leading to global competency by providing advance technical infrastructure and learning environment.

M.TECH. CSE(Cyber Security) PROGRAM STRUCTURE

First Year Teaching and Evaluation Scheme

Semester-I

Sr. No.	Course Category	Course Code	Course Title	Teaching Scheme			Evaluation Scheme				
				L	**T**	**P**	**CA**	**MSE**	**ESE**	**Total**	**Credit**
1	PCC	MTPESCS101T	Information Security and Privacy Policies and Standards	4	0	0	20	20	60	100	4
2	PCC	MTPESCS102T	Research Methodology and IPR	4	0	0	20	20	60	100	4
3	PCC	MTPESCS103T	Operating System Security	4	0	0	20	20	60	100	4
4	PCC	MTPESCS104T	Cloud Security	4	0	0	20	20	60	100	4
5	PEC	MTPESCS105T	Program Elective I*	4	0	0	20	20	60	100	4
6	PCC LAB	MTPESCS101L	Cloud Security Lab	0	0	2	60	-	$40^{\&}$	100	1
7	ELC	MTPESCS102L	Seminar $^{\$}$	0	0	2	100	-	$100^{\&}$	200	2
			Total	**20**	**0**	**4**	**260**	**100**	**440**	**800**	**23**

NOTE:

* Refer to Program Elective Bucket

$ Students are required to actively participate in seminar sessions as part of the course. Each student should select a topic for presentation related to latest development in Cyber Security, give presentation and submit seminar repoer in given format.

& Practical/Oral evaluation at the end of the semester.

M.TECH. CSE(Cyber Security) PROGRAM STRUCTURE

First Year Teaching and Evaluation Scheme

Semester-II

Sr. No.	Course Category	Course Code	Course Title	Teaching Scheme			Evaluation Scheme				
				L	**T**	**P**	**CA**	**MSE**	**ESE**	**Total**	**Credit**
1	PCC	MTPESCS201T	Advanced Computer Network & Security	4	0	0	20	20	60	100	4
2	PCC	MTPESCS202T	Cyber Forensics and Cyber Laws	4	0	0	20	20	60	100	4
3	PCC	MTPESCS203T	Database Security	4	0	0	20	20	60	100	4
4	PEC	MTPESCS204T	Program Elective II*	4	0	0	20	20	60	100	4
5	PCC Lab	MTPESCS201L	Database Security Lab	0	0	2	60	-	40[&]	100	1
6	ELC	MTPESCS202L	Mini Project	0	0	2	60	-	40[&]	100	1
7	OE	MTPESCS205T	Open Elective I ** [@]	3	0	0	20	20	60	100	3
			Total	**19**	**0**	**4**	**260**	**100**	**440**	**800**	**21**

NOTE:

* Refer to Program Elective Bucket

** Refer to Open Elective Bucket

@NPTEL Courses (NPTEL Credit will be transferred)

# Refer to IKS Bucket

& Practical/Oral evaluation at the end of the semester.

M.TECH. CSE(Cyber Security) PROGRAM STRUCTURE

Second Year Teaching and Evaluation Scheme

Semester-III

Sr. No.	Course Category	Course Code	Course Title	Teaching Scheme			Evaluation Scheme				
				L	T	P	CA	MSE	ESE	Total	Credit
1	MDM	MTPESCS301T	MDM Bucket [$@]	3	0	0	20	20	60	100	3
2	HSSM	MTPESCS302T	Entrepreneurship Essentials [@]	3	0	0	20	20	60	100	3
3	ELC	MTPESCS301L	Project I	0	0	4	100	-	100[&]	200	10
			Total	**6**	**0**	**4**	**140**	**40**	**220**	**400**	**16**

NOTE:

@ NPTEL Courses (The students who give NPTEL exam for the course their exam Credits will be transferred)

$ Refer to Multidisciplinary Minor Bucket(Opt any one course)

& Practical/Oral evaluation at the end of the semester.

M.TECH. CSE(Cyber Security) PROGRAM STRUCTURE

Second Year Teaching and Evaluation Scheme

Semester-IV

Sr. No.	Course Category	Course Code	Course Title	Teaching Scheme			Evaluation Scheme				
				L	T	P	CA	MSE	ESE	Total	Credit
1	ELC	MTPESCS401L	Project II	0	0	4	100	-	100$^{\&}$	200	20
			Total	**0**	**0**	**4**	**100**	**0**	**100**	**200**	**20**

NOTE:

& Practical/Oral evaluation at the end of the semester.

Course Code Abbreviations: MTPESCSYXXT/L (only for the reference).

Where:

MT- Master of Technology

PES- Institute Name

CS- Branch name

Y- Semester

XX- Serial no. For Theory or Practical

T/L- Theory subject or Laboratory subject

Semester wise Credit Distribution

Sr. No.	Semester	L	T	P	CA	MSE	ESE	Total	Credit
1	Semester-I	20	0	4	260	100	440	800	23
2	Semester-II	19	0	4	260	100	440	800	21
3	Semester-III	6	0	4	140	40	220	400	16
4	Semester-IV	0	0	4	100	-	100	200	20
	Total	**45**	**0**	**16**	**760**	**240**	**1200**	**2200**	**80**

List of Courses for Minor in Computer Science & Engineering (Cyber Security)

Sr. No.	Semester	Course Code	Course Title	Teaching Scheme			Evaluation Scheme				
				L	T	P	CA	MSE	ESE	Total	Credit
1	III	MTPESCS301TA	Introduction to Industry 4.0 and Industrial Internet of Things	3	0	0	20	20	60	100	3
2	III	MTPESCS301TB	Business Intelligence & Analytics	3	0	0	20	20	60	100	3
			Total	**3**	**0**	**0**	**20**	**20**	**60**	**100**	**3**

Program Elective I

Sr. No.	Semester	Course Code	Course Title	Teaching Scheme			Evaluation Scheme				
				L	T	P	CA	MSE	ESE	Total	Credit
1	I	MTPESCS105TA	Secured Software Architecture and Design	4	0	0	20	20	60	100	4
2	I	MTPESCS105TB	Mobile Application Security	4	0	0	20	20	60	100	4
3	I	MTPESCS105TC	AI in Cyber Security	4	0	0	20	20	60	100	4
			Total	**4**	**0**	**0**	**20**	**20**	**60**	**100**	**4**
Program Elective II											
1	II	MTPESCS204TA	Blockchain	4	0	0	20	20	60	100	**4**
2	II	MTPESCS204TB	Ethical Hacking	4	0	0	20	20	60	100	**4**
3	II	MTPESCS204TC	Digital Forensics	4	0	0	20	20	60	100	**4**
			Total	**4**	**0**	**0**	**20**	**20**	**60**	**100**	**4**

Open Elective Bucket

Sr. No.	Semester	Course Code	Course Title	Teaching Scheme			Evaluation Scheme				
				L	T	P	CA	MSE	ESE	Total	Credit
1	II	MTPESCS205TA	Product Design & Innovation	2	0	0	20	20	60	100	2
2	II	MTPESCS205TB	Educational Leadership	2	0	0	20	20	60	100	2
			Total	**2**	**0**	**0**	**20**	**20**	**60**	**100**	**2**

Semester-I

MTPESCS101T	**Information Security and Privacy Policies and Standards**	**PCC**	**4L-0T-0P**	**4 Credit**
Evaluation Scheme	**CA-20 Marks**	**MSE-20 Marks**	**ESE-60 Marks**	**ESE Time Duration 3 Hrs**

Course Objectives	
1	To comprehend and differentiate between various policy components such as definitions, standards, guidelines, and procedures, and to understand how business objectives align with security goals and international security standards.
2	To Audit vulnerabilities based on the IT security standards
3	To gain the ability to design and document effective security policies addressing key organizational areas such as network security, authentication, access control, contingency planning, and secure communication practices.

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Remember basics of policy document writing for securing network connection and interfaces.	K1
CO2	Understand the standards, guidelines, Procedures, and key roles of the organization	K2
CO3	Apply the procedure to write, monitor, and review policy document	K3
CO4	Explore privacy, confidentiality, and ethical data handling supported by privacy engineering principles.	K4
CO5	Examine international frameworks and best practices for designing robust information security architectures.	K4

Unit 1	Preamble: Significance and Scope of the course, Importance of the course in societal, political and economic growth of the nation, Impact of the course on societal and ethical issues and career perspective. Introduction to Information Security Policies: About Policies, why Policies are Important, When policies should be developed, How Policy should be developed, Policy needs, Identify what and from whom it is being protected, Data security consideration, Backups, Archival storage and disposal of data, Intellectual Property rights and Policies, Incident Response and Forensics, Management Responsibilities, Role of Information Security Department, Security Management and Law Enforcement, Security awareness training and support.	7 Hours
Unit 2	Policy Definitions, Standards, Guidelines, Procedures with examples, Policy Key elements, Policy format and Basic Policy Components, Policy content considerations, Program Policy Examples, Business Goal Vs Security Goals, Computer Security Objectives, Mission statement Format, Examples, Key roles in Organization, Business Objectives, Standards: International Standards.	7 Hours
Unit 3	Writing The Security Policies: Computer location and Facility construction, Contingency Planning, Periodic System and Network Configuration Audits, Authentication and Network Security, Addressing and Architecture, Access Control, Login Security, Passwords, User Interface, Telecommuting and Remote Access, Internet Security Policies, Administrative and User Responsibilities, WWW Policies, Application Responsibilities, E-mail Security Policies.	7 Hours

Unit 4	Privacy & Online Rights - Privacy as Confidentiality, Data Confidentiality Cryptography-based access control, Obfuscation-based inference control , Metadata Confidentiality , Privacy as Control ,Support for privacy settings configuration , Support for privacy policy negotiation ,Support for privacy policy interpretability , Privacy as Transparency , Feedback-based transparency , Auditbased transparency, Privacy Technologies and Democratic Values, Privacy technologies as support for democratic political systems , Censorship resistance and freedom of speech ,Privacy Engineering	7 Hours
Unit 5	The Information Security Blueprint: The ISO 27000 Series, NIST Security Models, IETF Security Architecture Baselining and Best Business Practices, Design of Security Architecture	7 Hours

Text Book	
1	Scott Barman, “Writing Information Security Policies”, Sams Publishing 2002.
2	Rashid, A., Martin, A. et. all, “The Cyber Security Body of Knowledge”, Oct 2019, Version 1.0. U.K.: National Cyber Security Centre.
3	Michael E. ,Whitman, “Principles of Information Security”, 2012, Fourth Edition, Cengage Learning publication

Reference Book	
1	Thomas R Peltier, Justin Peltier et.all , “Information Security Fundamentals”,2005, CRC Press, .
2	Harold F. Tipton and Micki Krause, “Information Security Management”, 5th Edition, 2005, Handbook Auerbach publications

NPTEL Link	
1	https://onlinecourses.nptel.ac.in/noc23_cs127/preview
2	https://nptel.ac.in/courses/106106248

MTPESCS102T	Research Methodology and IPR		PCC	4L-0T-0P	4 Credit
Evaluation Scheme	**CA-20 Marks**	**MSE-20 Marks**	**ESE-60 Marks**		**ESE Time Duration 3 Hrs**

Course Objectives	
1	To comprehend the fundamental concepts of research methodology, including problem definition, literature review, research design, data analysis, and report writing.
2	To explain various forms of Intellectual Property Rights (IPR), their relevance, business impact, and the leading international instruments and Indian acts concerning IPR.

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Understand the research process, including problem definition, literature review, and the ethical considerations in research and academic integrity.	K2
CO2	Understand the research designs, sampling designs, and data collection methods.	K2
CO3	Apply and analyze various statistical techniques for hypothesis testing and data optimization.	K3
CO4	Apply statistical hypothesis testing, chi-square analysis, and optimization techniques to analyze data, interpret results, and effectively communicate findings through well-structured reports.	K3
CO5	Demonstrate the ability to prepare and present research reports and understand, apply, and evaluate intellectual property rights (IPR) laws and international frameworks relevant to research and innovation.	K3

Unit 1	Introduction to Research Methodology: Meaning, Objectives, Motivation, Types of Research, Research Approaches, Significance, Research Methods versus Methodology, Research Process, Criteria of Good Research. Defining the Research Problem: Research Problem, Selecting the Problem, Necessity of Defining the Problem, Technique Involved in Defining a Problem. Ethics in Research: Engineering Ethics, Code of Ethics, Academic Integrity and Plagiarism.	7 Hours
Unit 2	Reviewing the Literature: Place of the literature review in research, Functions, Searching the existing literature , Reviewing the selected literature. Frameworks: Developing a Theoretical Framework and a Conceptual Framework. Research Design: Meaning, Need, Features of a Good Design, Important Concepts, Different Research Designs (Exploratory, Descriptive, Experimental), Basic Principles of Experimental Designs.	7 Hours
Unit 3	Design of Sampling: Introduction, Sample Design, Sampling and Non-sampling Errors, Types of Sampling Designs. Measurement and Scaling: Qualitative and Quantitative Data, Classifications of Measurement Scales (Nominal, Ordinal, Interval, Ratio), Goodness of Measurement Scales, Scaling Techniques. Data Collection: Experimental and Surveys, Collection of Primary Data (Survey Research Methods), Collection of Secondary Data, Selection of Appropriate Method (Case Study Method).	7 Hours
Unit 4	Testing of Hypotheses: Hypothesis, Basic Concepts, Procedure for Hypothesis Testing, Test Statistics and Critical Region, Hypothesis Testing for Mean, Proportion, Variance, Difference of Two Means/Proportions/Variances, P-Value approach. Chi-square Test: Test of Difference of more than Two Proportions, Test of Independence of Attributes, Test of Goodness of Fit. Optimization Techniques: Two-parameter optimization methods (Monte Carlo, Simplex), Multi-parameter optimization methods, The cost function. Interpretation and Report Writing: Meaning and Technique of Interpretation, Significance of Report Writing, Different Steps in Writing Report	7 Hours

Unit 5	Research Reporting: Layout of the Research Report, Types of Reports, Thesis Structure and Style, Oral Presentation, Mechanics of Writing a Research Report, Precautions. Research Presentation . Intellectual Property Rights (IPR): The Concept, Competing Rationales for Protection of IPRs. IPR in India: Patents Act, 1970, Trade Mark Act, 1999, The Designs Act, 2000, Copyright Act, 1957. Leading International Instruments Concerning IPR: World Intellectual Property Organization , TRIPS Agreement Paris Convention, Berne Convention.	7 Hours

Text Book	
1	C.R. Kothari, Gaurav Garg, “Research Methodology: Methods and Techniques” 4th Edition, 2018,New Age International.
2	David V. Thiel, “Research Methods for Engineers”, ISBN: 978-1-10761019-4, 2014,Cambridge University Press

Reference Book	
1	Ranjit Kumar, “Research Methodology: A Step-by-Step Guide for Beginners” , 4th Edition, 2014,SAGE Publications Ltd.
2	Caroline Whitbeck, “Ethics in Engineering Practice and Research”, 2nd Edition, ISBN: 978-1-107-66847-8, 2011, Cambridge University Press.

NPTEL Link	
1	https://archive.nptel.ac.in/courses/127/106/127106227
2	https://nptel.ac.in/courses/121106007

MTPESCS103T	Operating System Security		PCC	4L-0T-0P	4 Credit
Evaluation Scheme	**CA-20 Marks**	**MSE-20 Marks**	**ESE-60 Marks**		**ESE Time Duration 3 Hrs**

Course Objectives	
1	To provide comprehend knowledge of the fundamental security principles and models applicable to modern operating systems.
2	To enable students to study vulnerabilities, identify threats (including malware), and design effective security mechanisms for various operating system environments.

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Remember Foundational Concepts of security requirements andOS Architecture	K1
CO2	Understand various access control mechanism to enforce a principle of least privilege in a computing environment.	K2
CO3	Apply procedures to Design and implement mechanisms for process isolation and memory protection to secure critical operating system components.	K3
CO4	Identify, analyze, and mitigate various types of malware and common system vulnerabilities like buffer overflows.	K4
CO5	Analyze advanced security challenges in virtualization, operating systems, and intrusion detection, and evaluate real-world case studies to apply best practices for securing computing environments.	K4

Unit 1	Foundational Concepts and OS Architecture: Introduction to System Security: Security Goals and Principles: Confidentiality, Integrity, and Availability. Security policies and security mechanisms, Operating System Fundamentals: Comprehensive review of OS core components: Processes and Threads, Memory Management , and File Systems, Security Architecture: Design and components of a secure operating system. Trusted Computing Base , Security Kernels, and the theoretical role of a Reference Monitor. Hardware and firmware security mechanisms	7 Hours
Unit 2	Access Control Mechanisms: Concepts of protection domains and access matrices. Discretionary Access Control : capabilities and access control lists .Mandatory Access Control : security labels and clearance levels. Role-Based Access Control : roles, permissions, and session management, Formal Security Models: Detailed study of the Bell-LaPadula Model , the Biba Model , and the Chinese Wall Model ,Authentication and Authorization: User authentication techniques, Robust password management systems. Multi-factor authentication and its implementation.	7 Hours
Unit 3	Protection Mechanisms and OS Hardening: Process and Memory Protection: Techniques for achieving Process Isolation , Memory Protection mechanisms: base and bounds registers, tagged architecture, and hardware-enforced Data Execution Prevention and Address Space Layout Randomization, File System Security: Advanced access control lists, permission management in Unix/Linux and Windows. Secure file operations and data sanitization, Trusted Operating Systems: Introduction to security-enhanced operating systems. Concepts of Linux Security Modules. Detailed case studies of SELinux and AppArmor for fine-grained access control.	7 Hours

Unit 4	Malware and System Vulnerability Analysis: Malware Taxonomy and Mechanisms: Detailed study of Types of Malware, Malware propagation and infection techniques, Software Vulnerability Analysis: Classic vulnerabilities: Buffer Overflows , format string exploits, Techniques for finding vulnerabilities: Fuzzing and automated testing, Malware Analysis and Detection: Tools and techniques for static and dynamic analysis of malicious software. Introduction to sandboxing environments for safe analysis.	7 Hours
Unit 5	Advanced Topics and Real-World Case Studies : Virtualization and Cloud Security: Security issues and threats in hypervisors and virtual machines. VM es cape and inter-VM attacks. Security best practices in virtualization, Operating System Hardening: Strategies for Secure System Configuration and minimizing the attack surface, Security of the booting process , Auditing and Intrusion Detection: System call monitoring and security event logging. Design and implementation of Host-based Intrusion Detection Systems , Case Studies: Security features and common vulnerabilities in Windows Security , Linux Security , and Mobile OS Security .	7 Hours

Text Book:	
1	Charles P. Pfleeger, Shari Lawrence Pfleeger, “Security in Computing” , 5th Edition, 2015, Prentice Hall.
2	Trent Jaeger, Morgan &amp, “Operating System Security”, 2008, Claypool Publishers.

Reference Book	
1	Matt Bishop, “Computer Security: Art and Science” , 2018, Addison-Wesley,
2	Ross Anderson, “Security Engineering: A Guide to Building Dependable Distributed Systems”, 3rd Edition, ISBN 978-1-119-64278-7, 2020, Indianapolis, IN: John Wiley & Sons.

NPTEL Link	
1	https://onlinecourses.nptel.ac.in/noc25_cs94
2	https://onlinecourses.nptel.ac.in/noc21_cs30
3	https://archive.nptel.ac.in/courses/106/106/106106141

MTPESCS104T	Cloud Security		PCC	4L-0T-0P	4 Credit
Evaluation Scheme	**CA-20 Marks**	**MSE-20 Marks**	**ESE-60 Marks**		**ESE Time Duration 3 Hrs**

Course Objectives	
1	To Identify the security risks, challenges, and threat factors specific to Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) environments.
2	To Implement effective mechanisms for identity management, access control, and data protection across leading public cloud platforms to ensure confidentiality, integrity, and availability.
3	To Establish cloud security governance models and compliance frameworks that align with recognized industry standards, organizational policies, and legal or regulatory requirements.

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Describe cloud architecture, service/deployment models, shared responsibility model, and major threats like account hijacking and data leakage.	K2
CO2	Explain and apply encryption methods, cloud KMS/HSM usage, and secure data lifecycle management in cloud storage.	K3
CO3	Implement IAM policies, federation models, and analyze network-level protections like firewalls, NACLs, and DDoS prevention.	K4
CO4	Analyze risk assessment methods and evaluate compliance frameworks (ISO 27017, GDPR, HIPAA) and CSA STAR standards.	K4
CO5	Apply advanced cloud-native security practices, including container and serverless security, DevSecOps integration, and cloud incident response and forensics, to secure modern cloud environments.	K3

Unit 1	Cloud Fundamentals & Threat Model: NIST Cloud Definition, Service Models (IaaS, PaaS, SaaS), Deployment Models. Shared Responsibility Model (Critical Concept). Virtualization Security (Hypervisor risks, VM escape). CSA Top Threats (Account Hijacking, Data Leakage).	7 Hours
Unit 2	Data Security & Encryption: Data Lifecycle Security in Cloud. Data Encryption (At rest, in transit, in use). Cloud Key Management Service (KMS) and Hardware Security Modules (HSM). Cloud Storage Security (S3, Blob). Homomorphic Encryption basics.	7 Hours
Unit 3	Access Management & Network Controls: Identity and Access Management (IAM): Users, Groups, Roles, Policies. Federation (SAML, OAuth). Network Security: Cloud Firewalls, Security Groups/NACLs, VPC/VNet architecture, DDoS protection. Zero Trust Architecture principles.	7 Hours
Unit 4	Governance, Risk & Compliance (GRC): Cloud Governance framework. Risk Assessment in cloud. Compliance: ISO 27017, GDPR (Data Privacy), HIPAA. Cloud Audit and logging mechanisms. Cloud Security Alliance (CSA) STAR program.	7 Hours
Unit 5	Advanced & Cloud-Native Security: Container Security (Docker, Kubernetes): Image scanning, Admission controllers. Serverless Security (FaaS) challenges. DevSecOps principles and integration into CI/CD pipeline. Cloud Incident Response and Forensics basics.	7 Hours

Text Book	
1	Dr. Kumar Saurabh, “Cloud Computing”, 4th Edition 2017, ISBN-13: 978-8126570966, Wiley India,
2	Thomas Erl, Ricardo Puttini &amp; Zaigham Mahmood,“Cloud Computing: Concepts, Technology &amp; Architecture” , 2014, ISBN-13: 978-9332535923,Pearson India (Indian edition),
3	Tim Mather, Subra Kumaraswamy &amp; Shahed Latif, “Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance”,2009. published by O’Reilly Media in

Reference Book	
1	Ben Malisow and Mike Chapple, “(ISC)^2 CCSP Official Study Guide” ,3rd Edition (2022), ISBN: 978-1119861157, Sybex/Wiley,

NPTEL Link	
1	https://nptel.ac.in/courses/106105167
2	https://nptel.ac.in/courses/106106129

MTPESCS105TA	Secured Software Architecture and Design		PEC	4L-0T-0P	4 Credit
Evaluation Scheme	**CA-20 Marks**	**MSE-20 Marks**	**ESE-60 Marks**		**ESE Time Duration 3 Hrs**

Course Objectives	
1	To establish a clear understanding of the principles, models, and best practices for integrating security controls into the entire Software Development Life Cycle (SDLC) from requirements gathering to deployment.
2	To equip students with the ability to assess software architectures against established security standards, identify and mitigate architectural-level risks, and employ advanced threat modeling techniques to design robust, secure, and resilient systems

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Understand Foundations of secure software architectural, secure software development life cycle.	K2
CO2	Apply the knowledge of architectural patterns and security mechanisms for identifying the attack.	K3
CO3	Analyze the risks and threat modeling.	K4
CO4	Evaluate design patterns on the basis of security aspects.	K5
CO5	Evaluate security merics for security architecture for cloud DevOps and its Governance.	K5

Unit 1	Foundations of Secure Software Architecture: Introduction to Software Security vs. Software Reliability. The Secure Software Development Lifecycle . Security Architecture Goals: Confidentiality, Integrity, Availability, Authentication, Authorization, Non-repudiation. Security Design Principles: Least Privilege, Fail Securely, Separation of Privilege, Secure Defaults, Defense in Depth, Complete Mediation. Introduction to Security Frameworks: OWASP SAMM and Microsoft SDL.	7 Hours
Unit 2	Architectural Patterns and Security Mechanisms: Security Architectural Patterns: Gatekeeper Pattern, Policy Enforcement Point, Broker, Service-Oriented Architecture and Microservices Security. Trust Boundaries and identifying the Attack Surface. Security Mechanisms at Architectural Level: Firewalls, IDS/IPS, WAFs, Hardware Security Modules . Security Quality Requirements Engineering and Elicitation of Security Requirements.	7 Hours
Unit 3	Threat Modeling and Risk Analysis: Introduction to Threat Modeling, Why model threats, when to model. Data Flow Diagrams for system decomposition. STRIDE methodology. DREAD for risk ranking. Creation of Attack Trees and Attack Libraries. Mitigating identified threats and verifying controls.	7 Hours
Unit 4	Secure Coding and Design Patterns: Secure Design Patterns, Identity and Access Management , Session Management, Input Validation/Sanitization. Secure Coding Practices for common languages . Secure APIs and Web Services: REST API security, JSON Web Tokens , OAuth 2.0 and OpenID Connec,. Use of Static Application Security Testing and Dynamic Application Security Testing in the pipeline.	7 Hours

Unit 5	Advanced Topics: Cloud, DevOps, and Governance: Security in DevOps (DevSecOps), Integrating security into CI/CD pipelines, Security as Code, Infrastructure as Code (IaC) security. Cloud Security Architecture,hared Responsibility Model, Security Groups, Network Segmentation, Identity Federation. Governance and Compliance, Auditing secure software architecture, aligning design with regulations. Security Metrics for software architecture.	7 Hours

Text Book	
1	Charles P. Pfleeger and Shari Lawrence Pfleeger, “Security in Computing”, 5th Edition, 2015, Prentice Hall.
2	Dominic Chell, Tyrone Erasmus et all , “The Mobile Application Hacker’s Handbook”, 2015, Wiley Publication
3	Loren Kohnfelder, “Designing Secure Software: A Guide for Developers, Architects, and Leaders”, 2021, O’Reilly Media

Reference Book	
1	Len Bass, Paul Clements et.all, “Software Architecture in Practice”, 4th Edition, 2021, Addison-Wesley Professional
2	Adam Shostack, “Threat Modeling: Designing for Security”, ISBN: 978-1-118-80999-0, 2014, John Wiley & Sons
3	Robert C. Seacord, “Secure Coding in C and C++”, 2nd Edition, 2013, Addison- Wesley Professional,

MTPESCS105TB	Mobile Application Security		PEC	4L-0T-0P	4 Credit
Evaluation Scheme	**CA-20 Marks**	**MSE-20 Marks**	**ESE-60 Marks**		**ESE Time Duration 3 Hrs**

Course Objectives	
1	To provide students with a deep understanding of the architecture, threats, and security models of major mobile operating systems (Android and iOS).
2	To equip students with the practical skills necessary to perform mobile application penetration testing, vulnerability analysis, and forensic analysis.

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Critically analyze the security architectures of Android and iOS platforms, identifying design-level security weaknesses.	K4
CO2	Identify Vulnerabilities: Identify and classify common security vulnerabilities in mobile applications (e.g., those listed in OWASP Mobile Top 10).	K2
CO3	Perform hands-on static and dynamic analysis (SAST/DAST), and penetration testing of mobile applications using industry-standard tools.	K3
CO4	Analyze mobile operating system vulnerabilities and malware, apply exploit development techniques, and evaluate defense mechanisms to secure mobile applications and platforms.	K4
CO5	Apply mobile forensic techniques to acquire, preserve, and analyze digital evidence from mobile devices for incident response and investigation.	K3

Unit 1	Mobile Platform Security Fundamentals: Mobile Ecosystem Overview: Evolution of mobile platforms (GSM, GPRS, 3G/4G, 5G), Mobile Device and Application landscape,Mobile OS Architectures, Detailed analysis of Android Security Architecture and iOS Security Architecture,Mobile Device Security, Boot process security, Device encryption, Hardware-based security, Mobile Device Management (MDM) and Mobile Application Management concepts.Mobile Network Security,Cellular network security , Wi-Fi and Bluetooth security issues.	7 Hours
Unit 2	Mobile Application Security & OWASP Mobile Top 10: Threat Modeling, Principles and methodology for threat modeling mobile applications.OWASP Mobile Top 10,Detailed study and case studies for the latest OWASP Mobile Top 10 risks: Insecure Data Storage, Insecure Communication, Insecure Authentication/Authorization, Poor Cryptography, Client-Side Injection, Improper Platform Usage, etc,Application Development Security, Secure data handling , Input validation, Session management, Transport Layer Security.API Security for Mobile, Understanding the security challenges of mobile back-end APIs, Broken Object Level Authorizatio in mobile contexts.	7 Hours
Unit 3	Static and Dynamic Analysis: Static Analysis, Tools and techniques for analyzing application code without executing it; Decompilation and Reverse Engineering fundamentals; Understanding Dalvik bytecode, Smali, and Objective-C/Swift binaries, Dynamic Analysis , Setting up a Mobile Pentesting Environment,Runtime Manipulation, Tools for dynamic instrumentation and hooking , bypassing root/jailbreak detection and SSL pinning,Tampering and Repackaging, Techniques for application tampering, logic manipulation, and securing apps against repackaging attacks.	7 Hours

Unit 4	Advanced Mobile Exploitation and Malware: Operating System Vulnerabilities, Exploits targeting the mobile OS kernel, privilege escalation, and zero-day threats in mobile platforms, Mobile Malware, Classification and analysis of mobile malware,Malware analysis methodology , ExploitDevelopment, Understanding common exploit methods like buffer overflows, race conditions, and memory corruption in the context of mobile applications/libraries, DefenseTechniques,Code obfuscation, Anti-debugging, Anti-tampering, and application shielding techniques.	7 Hours
Unit 5	Mobile Forensics and Incident Response: Digital Forensics Overview, Mobile forensics process model ,Data Acquisition,Logical vs. Physical acquisition techniques for both Android and iOS devices; Bypassing lock screens and device encryptions,Forensic Analysis,Analysis of file systems, call logs, SMS, application data , web artifacts, and location data; Using standard forensic tools.	7 Hours

Text Book:	
1	Nina Godbole and Sunit Belapure, “Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives”, 2011, Wiley India Pvt. Ltd.
2	Dominic Chell, Tyrone Erasmus et.all, “The Mobile Application Hacker’s Handbook”, 2015, Wiley publication.

Reference Book:	
1	Michael Sikorski and Andrew Honig, “Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software”, 2012,Michael Sikorski and Andrew Honig, No Starch Press.
2	Nikolay Elenkov, “Android Security Internals: An In-Depth Guide to Android’s Security Architecture”, Nikolay Elenkov, 2014, No Starch Press,

MTPESCS105TC	AI in Cyber Security		PEC	4L-0T-0P	4 Credit
Evaluation Scheme	**CA-20 Marks**	**MSE-20 Marks**	**ESE-60 Marks**		**ESE Time Duration 3 Hrs**

Course Objectives	
1	To introduce the fundamental concepts of Artificial Intelligence (AI), its history, and its applications in the field of cybersecurity
2	To develop the ability to apply machine learning and deep learning techniques for solving various security problems such as intrusion detection, anomaly detection, and malware analysis
3	To explore advanced AI-based security topics including adversarial machine learning, privacy-preserving techniques, and AI-driven threat detection and authentication systems.

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Explain the fundamental concepts, history, and applications of Artificial Intelligence in cybersecurity	K2
CO2	Analyze intelligent agent architectures and apply search-based, logic-based, and optimization approaches for security problem-solving.	K4
CO3	Apply knowledge representation techniques such as logic, ontologies, and expert systems for effective threat modeling and reasoning in cybersecurity.	K3
CO4	Evaluate machine learning and deep learning models for anomaly detection, intrusion detection, and malware classification.	K5
CO5	Demonstrate understanding of advanced AI-based security mechanisms such as adversarial learning, privacy-preserving AI, and AI-driven authentication systems.	K5

Unit 1	AI Foundations for Security: Introduction to Artificial Intelligence, history, and applications in cybersecurityIntelligent agents and problem-solving approaches: search-based (uninformed/informed),logic-based reasoning, and optimization algorithms Knowledge representation: propositional and first-order logic, ontologies, semantic networks,and expert systems for threat modelling	7 Hours
Unit 2	Machine Learning for Security Supervised, unsupervised, and reinforcement learning with focus on security use-cases, e.g., anomaly detection, network intrusion detection, and malware classificationnita+1 Anomaly detection in logs and network traffic; feature engineering; model evaluation in adversarial environments Neural network basics, deep learning for cyber threat detection, sequence modeling (HMMs, LSTMs) for malicious pattern discovery nita+1	7 Hours
Unit 3	Specialized Security AI Topics Adversarial machine learning: model stealing, evasion attacks, and security hardening for AI Models Privacy-preserving machine learning: differential privacy, federated learning in forensic data collection Automated phishing and malware detection using AI-powered NLP and pattern recognitionphddirection+1 AI-driven secure authentication (behavioral biometrics, continuous authentication)	7 Hours
Unit 4	Projects and Practical Applications Building AI-based intrusion detection systems (IDS), phishing detection tools, and malware analysis frameworkscoursera+1 Hands-on applications such as network traffic analysis, incident response automation, and threat intelligence miningstationx+1	7 Hours
Unit 5	Deep Learning and Advanced AI Techniques Deep neural networks for advanced malware and network intrusion detection, Use of Generative Adversarial Networks (GANs) for simulating adversarial threat, Sequential models (e.g., HMMs, LSTMs) for behavioral threat analyticsnita+1	7 Hours

Reference Book	
1	Bishop , “Pattern Recognition and Machine Learning”, 2008
2	Stuart Russell, “Artificial Intelligence: A Modern Approach” , 1995, Peter Norvig,
3	Soma Halder, Sinan Ozdemir, “Hands- On Machine Learning for Cybersecurity”, 2018
4	Alessandro Parisi, “Hands- On Artificial Intelligence for Cybersecurity” , 2019
5	Gupta, “Machine learning for computer and cyber security: principle, algorithms, and Practices”, 2021, Sheng

NPTEL Link	
1	https://onlinecourses.nptel.ac.in/noc23_cs127/preview

MTPESCS101L	Cloud Security Lab	PCC		0L-0T-2P	1 Credit
Evaluation Scheme	**CA-60 Marks**		**ESE-40 Marks**		**ESE Time Duration 3 Hrs**

Course Objectives	
1	To provide skills for designing and analyzing cloud Concepts.
2	To prepare students to work on various cloud platforms.
3	To provide skills to work towards solution of real-life problems

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Implement secure cloud environments by defining foundational security policies and implementing IAM and RBAC to enforce the principle of least privilege.	K3
CO2	Design and deploy secure network topologies with VPCs, subnets, and firewall rules to control and monitor traffic flow.	K6
CO3	Apply encryption mechanisms and key management strategies to protect data at rest and in transit.	K3
CO4	Perform continuous security assessments using vulnerability scanning, container image analysis, and cloud posture management tools to detect and remediate security risks.	K3
CO5	Configure centralized logging, auditing, and alerting systems to ensure traceability and rapid response to security incidents.	K6

List of Experiment	
1	Setting up a Secure Cloud Environment: Creating an Organization/Project/Account, defining foundational security policies.
2	IAM and Role-Based Access Control (RBAC): Creating users, groups, and service roles with custom permissions to enforce the principle of least privilege.
3	Secure Network Configuration: Deploying a Virtual Private Cloud (VPC/VNet) with public and private subnets, configuring Network Security Groups (Firewalls) to restrict traffic.
4	Data at Rest Encryption: Setting up object storage (S3/Blob/Cloud Storage) and configuring encryption using a Cloud Key Management Service (KMS) with customer- managed keys.
5	Virtual Machine Hardening (IaaS Security): Deploying a Linux VM, implementing security best practices (secure SSH, patching, intrusion detection), and monitoring security logs.
6	Web Application Security: Deploying a simple web application behind a Web Application Firewall (WAF) and testing common OWASP Top 10 vulnerabilities (e.g., SQLi, XSS)
7	Serverless Function Security: Deploying a simple serverless function (e.g., Lambda/Azure Function) and securing its execution role and environment variables.
8	Vulnerability Scanning and Posture Management: Using a CSPM tool (e.g., Cloud Security Hub, Azure Security Center, a third-party tool) to scan the deployed cloud environment for misconfigurations and remediating critical findings
9	Container Image Security: Utilizing a container registry to scan a Docker image for known vulnerabilities and implementing a secure build process.
10	Cloud Auditing and Logging: Configuring centralized logging and monitoring (e.g., CloudTrail, Azure Monitor) and creating alerts for critical security events (e.g., policy changes, root login).

Recommended Tools and Platforms	
1	Cloud Platforms: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP).
2	IaC Tools: Terraform, CloudFormation/ARM Templates.
3	Security Tools: Wireshark, Nmap, Cloud-native vulnerability scanners, Open-source tools like ScoutSuite or Prowler (for security auditing).
4	Containers:

Web References:	
1	Cloud Academy Security Labs Details: https://cloudacademy.com/learning-paths/awssecurity-services-42/ 2.
2	Udemy Certification on AWS security fundamentals: https://www.udemy.com/course/aws-hands-on-labs-2020-step-by-step-for-beginnersnew/?utm_source=adwords&utm_medium=udemyads&utm_campaign=LongTail_la.EN_cc.INDIA&utm_content=deal4584&utm_term=_._ag_77882236223_._ad_533093955804_._kw__._de_c_._dm__._pl__._ti_dsa1007766171032_._li_9062044_._pd__._&matchtype=&gclid=Cj0KCQiA1sucBhDgARIsAFoytUtbiwTaUqvVRLrS0glkHq0HrOBbBayvYat0B6_p35i5MeOUdfA9ZuMaAiPP EALw_wcB

NPTEL Link	
1	https://onlinecourses.nptel.ac.in/noc24_cs17/preview
2	https://onlinecourses.nptel.ac.in/noc25_cs16/preview

Semester-II

MTPESCS201T	Advanced Computer Network & Security		PCC	4L-0T-0P	4 Credit
Evaluation Scheme	CA-20 Marks	MSE-20 Marks	ESE-60 Marks		ESE Time Duration 3 Hrs

Course Objectives	
1	To learn the fundamentals of cryptography.
2	To learn the key management techniques and authentication approaches.
3	To explore the network and transport layer security techniques.

Course Outcome: At the end of this course, the students will be able to:		Bloom's Taxonomy Level
CO1	Understand the basics of cryptography	K2
CO2	Illustrate the key management technique and authentication.	K3
CO3	Apply the security techniques to network and transport layer	K3
CO4	Apply and analyse security concepts for electronic mail security	K3
CO5	Apply security practices for real time applications.	K3

Unit 1	Introduction: Basics of cryptography, conventional and public-key cryptography, hash functions, authentication, and digital signatures.	7 Hours
Unit 2	Key Management and Authentication: Key Management and Distribution: Symmetric Key Distribution, Distribution of Public Keys, X.509 Certificates, Public-Key Infrastructure. User Authentication: Remote User-Authentication Principles, Remote User-Authentication Using Symmetric Encryption, Kerberos Systems, Remote User Authentication Using Asymmetric Encryption.	7 Hours
Unit 3	Access Control and Security:Network Access Control: Network Access Control, Extensible Authentication Protocol, IEEE 802.1X Port-Based Network Access Control – IP Security – Internet Key Exchange (IKE). Transport-Level Security: Web Security Considerations, Secure Sockets Layer, Transport Layer Security, HTTPS standard, Secure Shell (SSH) application.	7 Hours
Unit 4	Application Layer Security: Electronic Mail Security: Pretty Good Privacy, S/MIME, Domain Keys Identified Mail. Wireless Network Security: Mobile Device Security	7 Hours
Unit 5	Security Practices: Firewalls and Intrusion Detection Systems: Intrusion Detection Password Management, Firewall Characteristics Types of Firewalls, Firewall Basing, Firewall Location and Configurations. Blockchains, Cloud Security and IoT security	7 Hours

Text Book	
1	M. Speciner, R. Perlman, C. Kaufman, “Network Security: Private Communications in a Public World”, 2002 , Prentice Hall,
2	Michael Goodrich, Roberto Tamassia, “Introduction to Computer Security”, Pearson publications, 2nd edition, 2021, ISBN-13: 978-0133575477.
3	Michael Rash, “Linux Firewalls”, ISBN: 978-1-59327-141- 1, October 2007, No Starch Press.

Reference Book	
1	J. Michael Stewart, Jones, “Network Security, Firewalls And VPNs,” ISBN-10: 1284031675, ISBN-13: 978-1284031676, 2013,Bartlett Learning,
2	Michael Gregg, “The Network Security Test Lab: A Step-By-Step Guide,” 2015, ISBN-10:8126558148, ISBN-13: 978-8126558148, Dreamtech Press

NPTEL Link	
1	https://onlinecourses.nptel.ac.in/noc23_cs35/preview

MTPESCS202T	Cyber Forensics and Cyber Laws		PCC	4L-0T-0P	4 Credit
Evaluation Scheme	**CA-20 Marks**	**MSE-20 Marks**	**ESE-60 Marks**		**ESE Time Duration 3 Hrs**

Course Objectives	
1	To gain knowledge of the various aspects of cyber security and law aspects
2	To Learn various acts related to cyber security world
3	To examine issues in detection and investigation of Cyber Crime

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Understand the importance of cyber forensics for economical political growth	K2
CO2	llustrate evidence collection and legal challenges	K3
CO3	Apply tools and Analyze the cybercrime with the support tools and methods.	K3,K4
CO4	Design/ set computer forensics laboratory using special tools and techniques of forensics	K6
CO5	Understand the Security Policies and Cyber Lawsc	K2

Unit 1	Introduction: Significance and Scope of the course, Importance of the course in societal, political and economic growth of the nation, Impact of the course on societal and ethical issues and career perspective. Introduction to Cybercrime: Definition and Origins of the Word, Classifications of Cybercrimes, An Indian Perspective, Cybercrime and the Indian ITA 2000, A Global Perspective on Cybercrimes, Cybercrime Era: Survival Mantra for the Netizens. How Criminals Plan Cyberoffenses, Attacks, Social Engineering, Cyberstalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector, Cloud Computing.	7 Hours
Unit 2	Cybercrime: Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones,	7 Hours
Unit 3	Tools and Methods Used in Cybercrime: Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks. Phishing and Identity Theft: Introduction, Phishing, Identity Theft (ID Theft).	7 Hours
Unit 4	Understanding Computer Forensics: Introduction, Historical Background of Cyber-forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber-forensics and Digital Evidence, Forensics Analysis of E-Mail, Digital Forensics Life Cycle, Chain of Custody Concept, Network Forensics, Approaching a Computer Forensics Investigation, Setting up a Computer Forensics Laboratory: Understanding the Requirements, Computer Forensics and Steganography,	7 Hours
Unit 5	Introduction to Security Policies and Cyber Laws: Need for An Information Security Policy, Information Security Standards – Iso, Introducing Various Security Policies and Their Review Process, Introduction to Indian Cyber Law, Objective and Scope of the it Act, 2000, Intellectual Property Issues, Overview of Intellectual - Property - Related Legislation in India, Patent, Copyright, Law Related to Semiconductor Layout and Design, Software License.	7 Hours

Reference Book	
1	Thomas J. Mowbray, “Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions” , 2013, John Wiley & Sons, .

Text Book	
1	Sunit Belapure and Nina Godbole, “Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives”, 2013, Wiley India Pvt Ltd.
2	Surya Prakash Tripathi, Ritendra Goyal, Praveen Kumar Shukla, “Introduction to information security and cyber laws”, 2015, Dream tech Press

NPTEL Link	
1	https://onlinecourses.swayam2.ac.in/cec21_ge10/preview

MTPESCS203T	Database Security		PCC	4L-0T-0P	4 Credit
Evaluation Scheme	**CA-20 Marks**	**MSE-20 Marks**	**ESE-60 Marks**		**ESE Time Duration 3 Hrs**

Course Objectives	
1	To describe the principles, models, and key techniques involved in securing databases against unauthorized access and misuse.
2	To Implement database protection mechanisms through encryption, access control, authentication, and auditing processes to maintain data confidentiality, integrity, and availability.
3	To implement strategies to identify, prevent, and mitigate security threats and vulnerabilities in contemporary database environments.

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Understand the CIA triad and layered database security architecture to identify threats, vulnerabilities, and common attacks.	K2
CO2	Apply DAC, MAC, and RBAC models to control database access and enforce roles, sessions, and separation of duties.	K3
CO3	Implement inference risks, auditing mechanisms, and privacy frameworks to protect sensitive database information.	K3
CO4	Implement application-level security using SQL injection prevention, input validation, encryption, and fine-grained access controls.	K3
CO5	Evaluate security challenges in cloud, NoSQL, and emerging databases, and apply techniques like forensics, watermarking, and blockchain for data integrity.	K5

Unit 1	Fundamentals and Security Architecture: Security Foundations: Concepts of Data Confidentiality, Integrity, and Availability (CIA Triad). Non-repudiation and Accountability. Threats and Vulnerabilities: Threat modeling, Risk assessment, and classification of database assets. Vulnerabilities (unpatched systems, isconfiguration). Basic attacks (uncontrolled access, privilege escalation, DoS). Layered Security Architecture: Defense-in-Depth principle and its necessity. Security across Physical, Operating System (OS), Network, DBMS, and Application layers.	7 Hours
Unit 2	Database Access Control Models: Discretionary Access Control (DAC): Ownership, GRANT and REVOKE privileges in SQL. Limitations and the "Trojan Horse" problem. Mandatory Access Control (MAC): Security labels and system-wide policies. Bell-LaPadula Model (Confidentiality: no read up, no write down). Biba Model (Integrity: no read down, no write up). Role-Based Access Control (RBAC): Users, Roles, Permissions, and Role Hierarchies. Role activation and Sessions. Separation of Duties (SoD): Implementation of Static and Dynamic SoD constraints to prevent fraud.	7 Hours
Unit 3	Inference, Auditing, and Data Privacy: Inference Problem: Deducing sensitive data from aggregate queries. Query restriction techniques (e.g., query-set-size control). Statistical Database Protection: Noise addition (Data Perturbation) and its impact on utility. Micro-aggregation and Data Swapping as anonymization techniques. Audit Logs and Intrusion Detection: Database Audit Trails (logging DDL, DML, user activity). Signature-based IDS for detecting known attacks. Database forensics principles. Privacy Frameworks: Principles of Hippocratic Databases. Compliance requirements and database implications of GDPR and HIPAA.	7 Hours

Unit 4	Application Security and Data Protection TechniquesApplication Vulnerabilities and Defense: Preventing SQL Injection (SQLi) attacks (all variants). Parameterized Queries (Prepared Statements) as the primary defense. Secure Coding Practices: Server-side Input Validation, type checking, and whitelisting. Encryption Techniques: Storage/Transparent Data Encryption (TDE). Column-level Encryption and advanced key management. Virtual Private Databases (VPD): Implementing Fine-Grained Access Control (FGAC). Dynamic row-level and column-level security policies.	7 Hours
Unit 5	Advanced Topics and Emerging Database Technologies: Cloud Database Security: Understanding the Shared Responsibility Model (IaaS, PaaS, SaaS). Security controls for multi-tenancy and data isolation in the cloud. NoSQL Database Security: Security models for Document, Key-Value, and Graph databases. Authentication and access control challenges in distributed NoSQL architectures. Data Tracking and Forensics: Advanced analysis of transaction logs in Database Forensics. Data watermarking for tracing and attribution of data leakage. Blockchain for Integrity: Application of blockchain for immutable logging and creating a tamper-proof audit trail for critical transactions.	7 Hours

Text Book	
1	Sushil Jajodia, Pierangela Samarati, Ravi Sandhu, and Elisa Bertino, “Database Security: Concepts, Approaches, and Challenges”,2005, ISBN 978-0387233762,Springer.
2	Sabrina Castano, Mariagrazia Fugini, Giancarlo Martella, and Pierangela Samarati, “Database Security”, 1995, ISBN 978-0201594072Addison-Wesley.
3	Ron Ben Natan,“Implementing Database Security and Auditing”, 2005, ISBN 978-1555583347,Elsevier.

Reference Book	
1	Abraham Silberschatz, Henry F. Korth, and S. Sudarshan,“Database System Concepts”, 7th Edition, 2019, ISBN 978-9354601515, McGraw Hill Education.
2	David Litchfield, Chris Anley,John Heasman, and Bill Grindlay, “The Database Hacker’s Handbook: Defending Database Servers”, 2005, ISBN 978-0764578014,Wiley.
3	Sushil Jajodia and Ravi Sandhu,“Database Security: Advances and Challenges”,1995, ISBN 978-1852339745,Springer.

NPTEL Link	
1	https://onlinecourses.nptel.ac.in/noc25_cs116/preview
2	https://onlinecourses.nptel.ac.in/noc22_cs90/preview

MTPESCS203T	Blockchain		PEC	4L-0T-0P	4 Credit
Evaluation Scheme	**CA-20 Marks**	**MSE-20 Marks**	**ESE-60 Marks**		**ESE Time Duration 3 Hrs**

Course Objectives	
1	To introduce the fundamental architecture, principles, and components of blockchain technology, emphasizing its decentralized, immutable, and secure nature.
2	To develop an understanding of cryptographic mechanisms, consensus algorithms, and smart contracts that enable trust and transparency in blockchain systems.
3	To explore the application of blockchain in cybersecurity domains such as secure identity management, digital forensics, data integrity, and privacy-preserving systems.

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Remember and understand the fundamental architecture, evolution, and features of blockchain systems, and differentiate them from traditional databases.	K1,K2
CO2	Apply cryptographic algorithms such as SHA-256, Merkle Trees, and PKI for data integrity and security in blockchain. Explain wallet creation, key management, and transaction verification.	K3
CO3	Implement PoW, PoS, DPoS, PBFT, and PoA consensus algorithms. Design and implement simple smart contracts in Solidity while identifying common vulnerabilities and applying secure coding practices.	K3
CO4	Analyze blockchain's role in cybersecurity, financial systems, IoT, and supply chain management. Explore tokenization, NFTs, and blockchain integration with cloud and AI technologies.	K4
CO5	Evaluate and design solutions for blockchain scalability, privacy (ZKPs, zk-SNARKs), interoperability (Polkadot, Cosmos), and forensic investigation. Assess ethical and regulatory implications.	K5

Unit 1	Introduction to Blockchain Technology: Evolution of blockchain: Bitcoin and beyond. Basic concepts: Blocks, chains, nodes, miners, and distributed ledgers. Features: Decentralization, transparency, immutability, and security. Blockchain architecture: Structure of blocks and transactions. Hash functions and digital signatures. Public vs. private blockchains. Types of nodes: full node, light node, miner node. Types of blockchains: Public, Private, Consortium, and Hybrid. Difference between blockchain and traditional databases.	7 Hours
Unit 2	Cryptographic Foundations: Cryptographic hash functions: Properties: determinism, preimage resistance, collision resistance, avalanche effect. Algorithms: SHA-256, SHA-3 (Keccak), and their usage in block generation. Merkle Trees and Merkle Proofs for data verification. Public Key Infrastructure (PKI), digital signatures, and certificates. Symmetric and asymmetric cryptography in blockchain operations. Wallets and keys: private keys, public keys, address generation, and key management. Transaction verification and digital trust mechanisms. Role of cryptography in ensuring data confidentiality and integrity.	7 Hours

Unit 3	Consensus Mechanisms and Smart Contracts: Consensus Models: Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS). Practical Byzantine Fault Tolerance (PBFT), Proof of Authority (PoA). Comparative analysis of consensus algorithms (energy, latency, security). Smart Contracts: Concept, features, and benefits. Lifecycle of a smart contract. Writing simple smart contracts using Solidity. Security concerns: reentrancy, overflow/underflow, timestamp dependency. Smart Contract Security: Common vulnerabilities: reentrancy, integer overflow/underflow, timestamp dependency, gas misuse. Security best practices and testing tools (Mythril, Remix IDE).	7 Hours
Unit 4	Blockchain Applications and Integration: Blockchain in Cyber Security: Secure identity management. Immutable logging for database and network security. Data provenance and audit trails. Blockchain in Financial Services: Cryptocurrencies, payment gateways, DeFi. Blockchain in Supply Chain Management and IoT. Integration with Cloud and AI for enhanced data trust. Tokenization and Non-Fungible Tokens (NFTs): concepts and use cases. Government and enterprise adoption challenges.	7 Hours
Unit 5	Advanced Topics and Emerging Trends: Blockchain scalability and performance issues. Layer-2 solutions: Sidechains, Lightning Network, and State Channels. Interoperability between blockchains (Polkadot, Cosmos). Privacy in blockchain: Zero-Knowledge Proofs (ZKP), zk-SNARKs, zk-STARKs. Confidential transactions and privacy coins (Monero, Zcash). Blockchain Forensics: tracing transactions and analyzing blockchain crimes. Regulatory and ethical aspects of blockchain and cryptocurrency.	7 Hours

Text Book	
1	Imran Bashir, “Mastering Blockchain”, 4th Edition, 2023, ISBN 978-1803241067, Packt Publishing.
2	Arshdeep Bahga and Vijay Madisetti, “Blockchain Applications: A Hands-On Approach”,2017, ISBN 978-0996025558, VPT (Universities Press).
3	Melanie Swan, “Blockchain: Blueprint for a New Economy”,1st Edition, 2015, ISBN 978-1491920497,O’Reilly Media.

Reference Book	
1	Andreas M. Antonopoulos, “Mastering Bitcoin” ,2nd Edition, 2017, ISBN 978-1491954386, O’Reilly Media.
2	Daniel Drescher, “Blockchain Basics: A Non-Technical Introduction in 25 Steps”, 1st Edition, 2017, ISBN 978-1484226032, Apress, .

NPTEL Link	
1	https://nptel.ac.in/courses/106105235
2	https://nptel.ac.in/courses/106105184

MTPESCS204TB	**Ethical Hacking**		**PEC**	**4L-0T-0P**	**4 Credit**
Evaluation Scheme	**CA-20 Marks**	**MSE-20 Marks**	**ESE-60 Marks**		**ESE Time Duration 3 Hrs**

Course Objectives	
1	To Recognize how attacker plans for attack through data collection
2	To Perform security scan to test the application and network for vulnerability.

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Identify basics of Ethical Hacking, cyber laws and responsibilities of Ethical Hacker.	K1
CO2	Explain Ethical Hacking types, acking, Password Cracking Techniques, types of intrusions and Malware Analysis Techniques	K2
CO3	Analyse database exploitation types and Techniques for extracting information from common databases	K4
CO4	Analyse the various attacks.	K4
CO5	Describe various encryption techniques	K2

Unit 1	Introduction to Ethical Hacking: Introduction to Ethical Hacking,Cyber Ethics and Laws, Difference between Ethical Hacking, Hacking, and Cracking,Attacker, Defining the responsibilities and ethics of an ethical hacker, different categories of hackers and their roles, Five stages of hacking:Reconnaissance(Survey), Probing, Actualattack, maintainingpresence, Coveringattacktracks, Cyber Ethics and Laws (HIPAA, GDPR, etc.), Defining the responsibilities and ethics of an ethical hacker.	7 Hours
Unit 2	System Hacking and Malware Threats: ethical hacking types,system hacking, password cracking techniques (rainbow tables, brute-force, dictionary), authentication bypass, privilege escalation (linux/windows), rootkits, steganography, malware analysis,understanding viruses, worms, trojans, ransomware, and spyware. basic static and dynamic malware analysis techniques (e.g., sandboxing, debugging). anti-virus evasion.	7 Hours
Unit 3	Database Exploitation Types: injection, broken authentication , sensitive data exposure, xml external entities (xxe), broken access control , security misconfiguration, cross-site scripting xss, insecure deserialization, using components with known vulnerabilities, insufficient logging & monitoring. database hacking,techniques for extracting information from common databases	7 Hours
Unit 4	Network, Wireless, and Denial of Service (DoS) Attacks: TCP/IP–Checksums P Spoofing, port scanning, DNS Spoofing. DoS attacks, SYN attacks, Smurf attacks, UDP flooding, DDOS Models. Firewalls and its types, Password hacking, A study on various attacks: input validation,SQL injection, Buffer overflow, Privacy attacks,	7 Hours
Unit 5	Cryptography: Introduction to cryptography, private-key encryption, public-key encryption. Cryptographic hash functions, digital signature and certificate, applications. Steganography, biometric authentication, network-based attacks, DNS, and Email security.	7 Hours

Text Book:	
1	Mark Rhodes-Ousley, “Information Security: The Complete Reference”, 2013, 2nd Edition, McGraw-Hill Education, .
2	Dafydd Stuttard and Marcus Pinto, “The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws”, 2011, 2nd Edition, Wiley Publishing

Reference Book	
1	AnkitFadia, “EthicalHacking”, 2006, 2ndEdition MacmillanIndiaLtd,
2	Michael T. Simpson, Nicholas Antill, and Kent Backman, “Ethical Hacking and Network Defense”, 2022, 4th Edition, Cengage Learning,
3	C.H.Wu and J.D.Irwin, “Introduction to Computer Networks and Cybersecurity”, 2013, CRC Press,
4	William Stallings, “Network Security: Principles and Practice”, 2023 ,8th Edition, Pearson Education

NPTEL Link	
1	https://onlinecourses.nptel.ac.in/noc25_cs142

MTPESCS204TC	Digital Forensics		PEC	4L-0T-0P	4 Credit
Evaluation Scheme	**CA-20 Marks**	**MSE-20 Marks**	**ESE-60 Marks**		**ESE Time Duration 3 Hrs**

Course Objectives	
1	To comprehend fundamentals of the principles, methodology, and legal framework governing the science of digital forensics, ensuring evidence integrity and legal admissibility.
2	To study techniques for the acquisition, preservation, analysis, and reporting of digital evidence from various sources like computer systems, networks, and mobile devices.

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Remember the fundamentals of digital forensics, process and legal framework.	K1
CO2	Understand various file systems, processes in file system forensics	K2
CO3	Analyze Network & Malware: Conduct network forensics by capturing and analyzing network traffic and perform malware analysis (static and dynamic) to identify attack vectors and malicious intent	K4
CO4	Examine challenges in mobile colud and Email forensics.	K5
CO5	Analyze various types of malware using static and dynamic tools, apply steganography detection techniques, and produce professional forensic reports while understanding the ethical and legal responsibilities of expert testimony.	K4

Unit 1	Fundamentals of Digital Forensics and Legal Framework : Introduction: Definition, Historical background, Types of Digital Forensics, Digital Forensics Process: Identification, Preservation, Collection, Examination, Analysis, and Presentation. The role of the first responder. Forensic Readiness, Legal and Ethical Issues: Overview of the Information Technology Act, 2000 (India) and its amendments. Rules for admissibility of digital evidence in court. Understanding Chain of Custody and its significance. Ethical guidelines for digital forensic professionals, Digital Evidence: Characteristics of digital evidence, Types of evidence.	7 Hours
Unit 2	Computer and File System Forensics: Data Acquisition and Duplication: Hardware and software write blockers. Forensic imaging ,types of images ,Best practices for remote acquisition, File System Analysis: In-depth study of common file systems: FAT, NTFS, Ext4. Understanding metadata, slack space, unallocated space, and swap files. Data and partition hiding techniques, Operating System Artifacts: Analyzing artifacts from Windows and Linux, Timeline Analysis.	7 Hours
Unit 3	Network Forensics and Live System Acquisition: Introduction to network evidence, Sources of network logs, Network Forensics Monitoring. Capturing and Analyzing Network Traffic: tools like Wireshark, tcpdump. Understanding common protocols and their logs Investigating Network Attacks: Analyzing logs from Firewalls, IDS/IPS, and Routers to trace attacks. Locating and analyzing evidence of intrusion,	7 Hours
Unit 4	Mobile, Cloud, and Email Forensics : Mobile Forensics: Challenges in mobile forensics. Data acquisition techniques: Physical acquisition, Logical acquisition, File system acquisition. Tools for mobile forensics . Analysis of SMS, Call Logs, GPS data, and application data from Android and iOS devices, Cloud Forensics: Challenges and legal issues in Cloud forensics. Evidence from SaaS, PaaS, and IaaS models. Acquisition and analysis of logs and data from cloud services ,Email Forensics: Email tracking and tracing. Analyzing email headers. Investigation of email crimes .	7 Hours

Unit 5	Malware and Report Generation: Malware Analysis: Types of malware. Static Analysis and Dynamic Analysis Tools: IDA Pro, OllyDbg, Cuckoo Sandbox, Steganography and Watermarking: Detecting hidden data within images, audio, and video files. Techniques for Steganalysis, Forensic Report Writing and Testimony: Structure of a professional forensic report. Writing technical and non-technical summaries. Ethical and legal duties of an Expert Witness. Courtroom procedures and testimony preparation.	7 Hours

Text Book	
1	Bill Nelson, Amelia Phillips, “Guide to Computer Forensics and Investigations”, 5th Edition, 2018, Cengage Learning/Thomson Learning,
2	Gerard Johansen, “Digital Forensics and Incident Response: Next-Generation Skills and Tools for Effective Incident Response and Cyber Threat Hunting”, 2nd Edition, 2020, Packt Publishing,

Reference Book	
1	son Luttgens, Matthew Pepe et all, “Incident Response &amp; Computer Forensics”, 3rd Edition, 2014, McGraw-Hill Education.
2	Rohit Tamma, Oleg Skulkin et.all, “Practical Mobile Forensics: Forensically Investigate and Analyze iOS, Android, and Windows 10 Devices”, 4th Edition, 2021, Packt Publishing.
3	Michael Hale Ligh, Andrew Case, “The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory”, 2014, Wiley .

MTPESCS201L	Database Security Lab		PCC	0L-0T-2P	1 Credit
Evaluation Scheme	**CA-60 Marks**	**ESE-40 Marks**			**ESE Time Duration 3 Hrs**

Course Objectives	
1	Students will be able to identify and explain key security threats and vulnerabilities in database systems and analyze common attack techniques such as SQL injection and buffer overflow.
2	To implement cryptographic techniques, data masking methods, and auditing mechanisms to protect sensitive data and ensure compliance with standards like GDPR and HIPAA.
3	To explore advanced database security topics, such as secure data warehousing, secure transaction processing, and privacy-preserving data publishing, while adhering to professional ethics and cybersecurity best practices.

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Implement Discretionary Access Control (DAC) and Role-Based Access Control (RBAC) to manage users, roles, and privileges in a database system.	K3
CO2	Perform vulnerability assessment and demonstrate SQL injection attacks to analyze database security weaknesses.	K4
CO3	Apply SQL injection mitigation techniques such as parameterized queries and input validation to secure web–database interactions.	K3
CO4	Configure database auditing, Transparent Data Encryption (TDE), and Row-Level Security (RLS) to enhance data protection and accountability.	K3, K4
CO5	Evaluate NoSQL database security mechanisms and analyze a real-world database breach case to propose a secure database architecture.	K5

List of Experiment	
1	Basic DAC(Discretionary Access Control) Implementation: Setting up users, roles, and fine-grained privileges using SQL (GRANT/REVOKE).
2	Implementing RBAC (Role-Based Access Control): Creating and managing roles, assigning roles to users, and setting up role hierarchies.
3	Vulnerability Assessment: Performing basic vulnerability scanning on a database instance using open-source tools.
4	SQL Injection Attacks: Performing and demonstrating various types of SQL Injection attacks (e.g., Error-based, Blind SQLi) on a vulnerable web application/database interface.
5	SQLi Mitigation: Implementing parameterized queries (Prepared Statements) and input validation to prevent SQLi.
6	Database Auditing: Configuring and analyzing audit trails for specific user actions (e.g., DDL, DML operations).
7	Transparent Data Encryption (TDE): Implementing and managing TDE for sensitive data tables.
8	Row-Level Security (RLS) Implementation: Setting up policies or views to implement Row-Level/Fine-Grained Access Control (VPD).
9	NoSQL Security Demonstration: Exploring basic authentication and authorization in a NoSQL database (e.g., MongoDB, Cassandra).
10	Case Study: Analyzing a real-world database breach incident and proposing a security architecture to prevent similar attacks.

Recommended Tools and Platforms	
1	Access Control: Tools like PAM enforce least-privilege access, ensuring users and applications only have the permissions absolutely necessary to perform their tasks.
2	Protection of Data: Encryption and masking tools render the data useless to unauthorized users, even if the underlying database files are compromised.
3	Detection and Response: DAM and Auditing tools act as security watchdogs, logging every significant action and generating alerts for suspicious activities (e.g., a massive data export, a SQL injection attempt, or a change in configuration).
4	Proactive Hardening: Vulnerability scanners help IT teams proactively find and fix security gaps before an attacker can exploit them.

NPTEL Link	
1	https://onlinecourses.nptel.ac.in/noc22_cs91/preview

MTPESCS202L	**Mini Project**	**ELC**	**0L-0T-2P**	**1 Credit**
Evaluation Scheme	**CA-60 Marks**		**ESE-40 Marks**	**ESE Time Duration 3 Hrs**

Course Objectives	
1	To encourage students to apply theoretical knowledge to small-scale practical problems, fostering creativity, teamwork, and hands-on experience in real-world scenarios.

Instructions / Guidelines:	
1	Student should undertake mini project individually by using latest cyber security tools.
2	Evaluation will be continuous, based on progress, implementation, report submission, and final demonstration.
3	A concise technical report in standard format must be submitted at the end of the term.

MTPESCS205TA	Product Design & Innovation		OE	2L-0T-0P	2 Credit
Evaluation Scheme	**CA-20 Marks**	**MSE-20 Marks**	**ESE-60 Marks**		**ESE Time Duration 3 Hrs**

Course Objectives	
1	To gain the knowedge of fundamental concepts of product design and innovation, and their role in contemporary industries
2	To acquire knowledge of user-centered design processes and techniques for identifying and analyzing user needs.
3	To utilize human factors and ergonomic principles to enhance usability, safety, and comfort in product design.

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Understand the key principles of product design and innovation, and explain different types of innovation (incremental, radical, and disruptive) and their relevance to product development.	K2
CO2	Understand the user need and problem.	K2
CO3	Apply the human central desin principles in product design.	K3
CO4	Develop innovative product concepts using creative thinking techniques and construct prototypes through CAD tools and rapid prototyping methods.	K5
CO5	Evaluate user–product interactions using testing and feedback mechanisms and integrate sustainability, manufacturability, and innovation management principles into product design.	K5

Unit 1	Introduction to Product Design and Innovation Definition, importance and scope of innovation ,Types of innovation: incremental, radical, and disruptive ,Design-inspired and user-centered innovation , Overview of product design process , Case studies of innovative product design	5 Hours
Unit 2	User Research and Need Identification User study methods: observation, interviews, surveys ,Contextual enquiry and ethnographic research , Identification of user needs and problems , Creating user personas and scenarios , Translating needs into design requirements	5 Hours
Unit 3	Human Factors and Ergonomics Introduction to ergonomics and human factors , Physical, cognitive, and emotional ergonomics , Anthropometric data and product usability , Human-centered design principles ,Aesthetic and functional balance in design	5 Hours
Unit 4	Concept Generation and Prototyping Creative thinking and idea generation techniques (brainstorming, TRIZ, morphological analysis) , Concept sketching and modeling, Rapid prototyping tools and techniques , Product visualization and computer-aided design (CAD) ,Concept evaluation and selection methods	5 Hours
Unit 5	Evaluation, Testing, and Design for Innovation Evaluation of user–product interaction , Testing and feedback mechanisms , Design for sustainability and manufacturability , Innovation management and intellectual property in design ,Case studies: Successful innovative products	5 Hours

Text Book	
1	Karl T. Ulrich and Steven D. Eppinger, “Product Design and Development”, 5th Edition, 2015, McGraw-Hill Education.
2	N. F. M. Roozenburg and J. Eekels, “Product Design: Fundamentals and Methods”, 1st Edition, 1995, Wiley.

Reference Book	
1	Mark S. Sanders and Ernest J. McCormick, “Human Factors in Engineering and Design”, 7th Edition, 1993, McGraw-Hill Education..
2	W. Green and Patrick W. Jordan, “Human Factors in Product Design: Current Practice and Future Trends”, 1st Edition, 1999, Taylor &amp; Francis.
3	William Lidwell, Kritina Holden, and Jill Butler, “Universal Principles of Design”, 1st Edition, 2003, Rockport Publishers.

NPTEL Link	
1	https://nptel.ac.in/courses/107103082

MTPESCS205TB	Educational Leadership		OE	2L-0T-0P	2 Credit
Evaluation Scheme	**CA-20 Marks**	**MSE-20 Marks**	**ESE-60 Marks**		**ESE Time Duration 3 Hrs**

Course Objectives	
1	To provide a comprehensive understanding of foundational leadership theories, ethical frameworks, and the core management functions necessary for effective educational administration.
2	To equip participants with advanced skills in strategic planning, leveraging digital technologies, managing diverse human resources, and leading institutional change in alignment with national and global policy imperatives.

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Analyze the differences between educational management and instructional leadership, and apply various established leadership theories (e.g., Transformational, Authentic) to specific institutional contexts.	K4
CO2	Understand and study professional development plans for faculty, fostering a culture of reflective practice, critical thinking, and high professional ethics and values.	K2
CO3	Evaluate organizational dynamics, including emotional intelligence, diversity, and team effectiveness, to build inclusive and high-performing educational communities.	K5
CO4	Formulate strategic plans for technology integration (digital pedagogy, online assessment) and institutional turnaround, responding effectively to 21st-century challenges and the 'New Normal' in education.	K3
CO5	Study national policies (like the National Education Policy 2020) and global sustainability goals (UNESCO SDGs), and design strategies for leading change and promoting lifelong learning.	K2

Unit 1	Foundations and Theories of Leadership: Concepts and Challenges, Differentiating Educational Management vs. Leadership, Current issues in the education sector, Classical Leadership Theories, Trait, Behavioral, and Situational models, Modern Leadership Models, Transformational, Transactional, and Charismatic leadership approaches, The Authentic Leader, Key challenges and development of authentic leadership.	5 Hours
Unit 2	Instructional Leadership and Change Management: Curriculum and Pedagogy ,The leader's role in curriculum design, evaluation, and instructional supervision, Innovative Pedagogy & Technology, Utilizing technology and innovative teaching practices to enhance learning outcomes, Leading Organizational Change, Models and processes for managing change in educational institutions, Turnaround Leadership, Strategies for improving performance and effectiveness in struggling institutions.	5 Hours
Unit 3	Human Resources, Teams, and Ethical Practice: Professional Ethics and Values, Upholding professional ethics and the code of conduct for academic leaders and faculty. Emotional Intelligence , Impact of EI on effective leadership, decision-making, and organizational climate. Professional Development: The leader as a Reflective Practitioner; nurturing continuous professional development for staff. Team Effectiveness and Dynamics: Group dynamics, team formation, and the leader's role in fostering high-performance teams.	5 Hours

Unit 4	Policy, Administration, and Governance: The Policy Landscape: Analysis and implementation of major national educational policies. Educational Governance: Understanding administrative structures and decentralized management at different levels. Stakeholder Management: Building relationships and multi-stakeholder partnerships. Resource and Conflict Management: Overview of managing resources, negotiation skills, and conflict resolution in academic settings.	5 Hours
Unit 5	Future-Ready Leadership and Global Context: Managing Diversity and Inclusion: Leadership for creating equitable, diverse, and inclusive educational environments. Global Citizenship & SDGs: Connecting local educational goals to UNESCO Sustainable Development Goal 4 for quality education. Transformative Learning: Theory and practice of transformative learning; paradigm shifts for the education system. Sustainable Leadership: Developing long-term, ethical, and resilient leadership practices for the future.	5 Hours

Text Book	
1	Patrick Duignan“Educational Leadership: Key Challenges and Ethical Tensions”,2012, Cambridge University Press.
2	Margaret Preedy, Nigel Bennett et,all,“Educational Leadership Context, Strategy and Collaboration”, 2012, Christine Wise SAGE Publications.

Reference Book	
1	Richard L. Hughes, Robert C. Ginnett et.all ,“Leadership: Enhancing the Lessons of Experience”, 9th Edition, 2018, McGraw Hill Education,.
2	Tony Bush, “Theories of Educational Leadership and Management”, 4th Edition,2011, SAGE Publications.

NPTEL Link	
1	https://nptel.ac.in/courses/109105122

Semester-III

MTPESCS301TA	**Introduction to Industry 4.0 and Industrial Internet of Things**	**MDM**	**3L-0T-0P**	**3 Credit**
Evaluation Scheme	**CA-20 Marks**	**MSE-20 Marks**	**ESE-60 Marks**	**ESE Time Duration 3 Hrs**

Course Objectives	
1	To provide a comprehensive understanding of the concepts, architecture, and enabling technologies of Industry 4.0 and the Industrial Internet of Things (IIoT).
2	To develop the ability to design and integrate smart systems using cyber-physical systems, cloud/edge computing, and data analytics for intelligent manufacturing.
3	To introduce industrial standards, cybersecurity practices, and emerging applications in the context of digital transformation and smart industries.

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Explain the evolution, concepts, and enablers of Industry 4.0 and Industrial IoT.	K2
CO2	Analyze cyber-physical systems, sensors, and communication protocols for smart industries.	K3
CO3	Design and integrate cloud/edge architectures and digital twins for industrial data management.	K4
CO4	Apply machine-learning and analytics techniques for process optimization and predictive maintenance.	K4
CO5	Evaluate cybersecurity, standards, and future trends in Industry 4.0 applications.	K5

UNIT 1	Introduction to Industry 4.0 and IIoT: Evolution of Industry 1.0 → 4.0; drivers, components, and architecture. Key pillars: Cyber-Physical Systems (CPS), IoT, Big Data, Cloud, AI, Robotics. Smart factory concept, value chain transformation, and Indian context (Smart Manufacturing Mission). Industrial use cases and business models.	6 Hours
UNIT 2	Cyber-Physical Systems, Sensors and Industrial Communication: CPS architecture, embedded controllers, edge devices, PLCs, and RTOS overview. Sensors, actuators, signal conditioning, and gateway design. Industrial communication protocols – Modbus, Profibus, OPC UA, MQTT, CoAP. Network standards for IIoT – Ethernet/IP, LoRaWAN, 6LoWPAN, TSN.	6 Hours
UNIT 3	Cloud, Edge and Digital Twin Platforms: Cloud vs Edge vs Fog computing reference architectures and deployment models. IIoT middleware and data ingestion frameworks. Digital twin concepts modeling, real-time synchronization, use cases in manufacturing. Case studies on smart factory integration and data pipelines.	6 Hours

UNIT 4	Data Analytics and AI for Smart Manufacturing: Data acquisition and pre-processing for sensor data. Machine learning methods: classification, regression, anomaly detection, time-series forecasting. Predictive maintenance, process optimization, Quality 4.0 applications. Edge AI deployment and model monitoring.	6 Hours
UNIT 5	Cybersecurity, Standards and Emerging Applications: Security challenges in CPS and IIoT – attack surfaces, authentication, secure communication. Standards and frameworks – ISA-95, OPC UA Security, ISO/IEC 27001, IEC 62443. Privacy, ethics, and governance in Industry 4.0. Additive manufacturing, robotics, AR/VR, blockchain in Industry 4.0 ecosystem. Implementation challenges and Indian initiatives (Smart Cities, Digital India).	6 Hours

Text Book	
1	Alasdair Gilchrist, “Industry 4.0: The Industrial Internet of Things”, Apress (Springer Nature), 2016. ISBN: 978-1-4842-2046-7

Reference Book	
1	Sabina Jeschke, Christian Brecher et. all, “Industrial Internet of Things: Cybermanufacturing Systems”, Springer, 2017. ISBN: 978-3-319-42558-0
2	Sudip Misra, Anandarup Mukherjee, Chandana Roy, “Introduction to Industrial Internet of Things and Industry 4.0”, CRC Press (Taylor & Francis Group), 2021. ISBN: 978-0-367-61110-2
3	Klaus Schwab, “The Fourth Industrial Revolution”, Crown Business (Penguin Random House), 2017. ISBN: 978-1-5247-5886-8
4	Wolfgang Wahlster (Ed.), “Foundations of Artificial Intelligence for Industry 4.0”, Springer, 2018. ISBN: 978-3-030-03317-0

NPTEL Link	
1	https://onlinecourses.nptel.ac.in/noc25_cs146/preview

MTPESCS301TB	Business Intelligence & Analytics		MDM	3L-0T-0P	3 Credit
Evaluation Scheme	CA-20 Marks	MSE-20 Marks	ESE-60 Marks		ESE Time Duration 3 Hrs

Course Objectives	
1	To study the foundational concepts of Business Intelligence (BI) and analytics, including drivers, architecture, and core vocabulary.
2	To Gain technical knowledge of BIA systems, including data management, OLTP/OLAP systems, data warehousing, and relational databases.
3	To study real-world business problems through case studies, and communicate actionable insights derived from analytics.

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Explain the role of BIA in modern organizations and identify its key components and technical architecture.	K2
CO2	Apply SQL queries to extract, manipulate, and analyze data from relational databases.	K3
CO3	Visualize data using descriptive statistics and dashboards to support business decision-making.	K3
CO4	Build decision trees and ensemble models for predictive modeling and understand the theory behind pruning and purity measures.	K3
CO5	Study machine learning models, including neural networks, for tasks such as forecasting and customer analytics.	K2
CO6	Study text mining workflows, including sentiment analysis, using R and Python.	K2

Unit 1	Introduction to Business Intelligence & Analytics (BIA), drivers of BIA, types of analytics: descriptive to prescriptive, vocabulary of business analytics, course plan and resource, Technical architecture of BIA, case analysis of AT&T Long distance, fundamentals of data management, OnLine Transaction Processing (OLTP), design process of databases	6 Hours
Unit 2	Relational databases, normalisation, SQL queries, ShopSense case of management questions, data warehousing, OnLine Analytical Processing (OLAP), data cube, Descriptive analytics, and visualization, customer analytics, survival analysis, customer lifetime value	6 Hours
Unit 3	Data mining process, introduction to statistical learning, data pre-processing, data quality, overview of data mining techniques, case study using regression analysis, Introduction to classification, classification techniques, scoring models, classifier performance, ROC and PR curves	6 Hours
Unit 4	Introduction to decision trees, tree induction, measures of purity, tree algorithms, pruning, ensemble methods, Tree implementation in Python: problem of targeted mailing	6 Hours
Unit 5	Cluster analysis, measures of distance, clustering algorithms, K-means and other techniques, cluster quality, A store segmentation case study using clustering, implementation in Python, profiling clusters, cluster interpretation and actionable insights, RFM sub- segmentation for customer loyalty	6 Hours
Unit 6	Machine learning, Artificial Neural Networks (ANN), topology and training algorithms, back propagation, financial time series modelling using ANN, implementation in Python, Text mining, process, key concepts, sentiment scoring, text mining using R-the case of a movie discussion forum	6 Hours

Text Book	
1	Efraim Turban, Ramesh Sharda, Jay Aronson, David King,“Decision Support and Business Intelligence Systems” 9th Edition 2009, Pearson Education.

Reference Book	
2	Ramesh Sharda, Dursun Delen, Efraim Turban,“Business Intelligence, Analytics, and Data Science” 4th Edition 2018 ,Pearson Education.

NPTEL Link	
1	https://onlinecourses.nptel.ac.in/noc25_cs09/preview

MTPESCS302T	Entrepreneurship Essentials		HSSM	3L-0T-0P	3 Credit
Evaluation Scheme	**CA-20 Marks**	**MSE-20 Marks**	**ESE-60 Marks**		**ESE Time Duration 3 Hrs**

Course Objectives	
1	To Explore the stages of entrepreneurship from discovery, ideation, and prototyping to commercialisation and scaling.
2	To Cultivate a problem-solving and opportunity-seeking mindset necessary for successful entrepreneurial ventures.
3	To explore the role of entrepreneurship in job creation and economic development.

Course Outcome: **At the end of this course, the students will be able to:**		**Bloom's Taxonomy Level**
CO1	Explain the fundamentals of entrepreneurship, including entrepreneurial qualities, myths, mission and vision, and apply the Business Model Canvas to develop a value-driven business idea.	K2
CO2	Analyze market opportunities and apply concepts of competitive advantage, lean start-up, and marketing management to design an effective business strategy.	K4
CO3	Apply the basic financial statements to develop a comprehensive business plan supported by go-to-market and pitching strategies.	K3
CO4	Understand the tools such as Design Thinking and TRIZ with knowledge of funding sources, incubation, and legal aspects to formulate strategies for launching and scaling start-ups.	K2
CO5	Apply financial, strategic, and human resource factors influencing start-up success or failure and formulate strategies for sustainable growth and risk management.	K3

Unit 1	Introduction: Dhirubhai Ambani & Sofia, Myths & Realities about entrepreneurship, entrepreneurial qualities, Why start-ups fail?, Mission, vision, entrepreneurial qualities, Value proposition, Business Model canvas, Business model generation	6 Hours
Unit 2	Competitive advantage, Lean start-up, Team and early recruit, Legal forms of business, Marketing management, Market research, Market research – Example	5 Hours
Unit 3	Introduction to financial statements, Profit & Loss statement, Balance sheet, Cash flow Example , Cost-volume-profit & Bread-Even analysis, Capital budgeting, Business plans, Pitching, Go-to-market strategies, Does & Don'ts	6 Hours
Unit 4	How to innovate, Design Thinking, Design-Driven Innovation, Systems thinking, Open innovation, TRIZ, How to start a start-up?, Government incentives for entrepreneurship, Incubation, acceleration Funding new ventures – bootstrapping, crowd sourcing, angel investors, VCs, debt financing (3), due diligence, Legal aspects of business (IPR, GST, Labour law)	6 Hours

Unit 5	Cost, volume, profit and break-even analysis, Margin of safety and degree of operating leverage, Capital budgeting for comparing projects or opportunities, Product costing, Product pricing, Funding new ventures – bootstrapping, crowd sourcing, Human Resource management in startups, Pivoting, Entrepreneurial cases, Risk assessment and analysis, Strategy management for entrepreneurial ventures, Factors driving success and failure of ventures	Hours

Books and references	
1	Robert D. Hisrich Veland Ramadani, “Effective Entrepreneurial Management: Strategy, Planning, RiskManagement, and Organization” , 2017, Springer
2	Kuratko &Hodgetts, Thompson South, “Entrepreneurship- Theory, Process Practice”, 6th edition 2004, Western Publication
3	Robert D. Hisrich, “Entrepreneurship”, 2012, Edition-9 McGraw-Hill Education

NPTEL Link	
1	https://onlinecourses.nptel.ac.in/noc20_ge08/preview

MTPESCS301L	Project I	ELC	0L-0T-4P	10 Credit
Evaluation Scheme	**CA-100 Marks**		**ESE-100 Marks**	**ESE Time Duration 3 Hrs**

Course Objectives	
1	To develop the ability to identify, define, and solve cyber security problems using appropriate tools and methodologies learned in Sem1 and Sem2.

Instructions / Guidelines:	
➢	Students should undertake a project individually and submit project report in the proper format including objective, problem definition, functional non functional requirements, system architecture and system design.
➢	A project proposal with objectives, scope, and methodology must be submitted and approved by the department.
➢	Evaluation will be continuous, based on progress, implementation, report submission, and final demonstration.

MTPESCS401L	**Project II**	**ELC**	**0L-0T-4P**	**20 Credit**
Evaluation Scheme	**CA-100 Marks**		**ESE-100 Marks**	**ESE Time Duration 3 Hrs**

Course Objectives	
1	To develop the ability to identify, define, and solve cyber security problems using appropriate tools and methodologies learned in whole curriculum.

Instructions / Guidelines:	
➢	Students should undertake a project individually and submit project report in the proper format including objective, problem definition, functional non functional requirements, system architecture and system design with implementation.
➢	A project proposal with objectives, scope, and methodology must be submitted and approved by the department.
➢	Evaluation will be continuous, based on progress, implementation, report submission, and final demonstration.
➢	Student should show live demonstration of their project during asessment