PAAVAI ENGINEERING COLLEGE, NAMAKKAL – 637 018 (AUTONOMOUS)

B.E – CYBER SECURITY REGULATIONS 2023

2023-2024 Onwards (CHOICE BASED CREDIT SYSTEM)

CURRICULUM AND SYLLABI

for

V SEMESTER

B.E – CYBER SECURITY

REGULATIONS 2023

SEMESTER V

S. No	Category	Course Code	Course Title	L	T	P	C
Theory							
1	PC	CY23501	Artificial Intelligence in Cyber security	3	1	0	4
2	PC	CY23502	Foundations of Data Science	3	0	0	3
3	PC	CY23503	UI and UX Design	3	0	0	3
4	PC	CY23504	Digital Forensics and Incident Response	3	0	0	3
5	PC	CY23505	Secure Software Engineering	3	0	0	3
6	PE	CY2315*	Professional Elective – I	3	0	0	3
Practical							
7	PC	CY23506	Artificial Intelligence Laboratory	0	0	4	2
8	PC	CY23507	Data Science Laboratory	0	0	2	1
9	EE	CY23508	Industrial Training	0	0	2	1
10	EE	GE23501	Professional Development III	0	0	2	1
			Total	**18**	**1**	**10**	**24**

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
05/7/25
★ AUTONOMOUS ★

PROFESSIONAL ELECTIVE COURSES – VERTICALS

VERTICAL I –BUSINESS DATA ANALYTICS AND SECURITY

S.No	Category	Course Code	Course Title	L	T	P	C
1	PE	CY23151	Data Virtualization	3	0	0	3
2	PE	CY23152	Cognitive Science and Analytics	3	0	0	3
3	PE	CY23153	Privacy Preservation in Data Mining	3	0	0	3
4	PE	CY23154	Digital Marketing and Social Media Analytics	3	0	0	3
5	PE	CY23155	Information Security Management	3	0	0	3
6	PE	CY23156	Predictive Analytics	3	0	0	3
7	PE	CY23157	Cloud Services Management	3	0	0	3

VERTICAL II – CLOUD COMPUTING AND DATA CENTRE TECHNOLOGIES

S.No	Category	Course Code	Course Title	L	T	P	C
1	PE	CY23251	E-Commerce Security	3	0	0	3
2	PE	CY23252	Data Centre Networking	3	0	0	3
3	PE	CY23253	Storage Technologies	3	0	0	3
4	PE	CY23254	Cloud Computing	3	0	0	3
5	PE	CY23255	Security and Privacy in Cloud	3	0	0	3
6	PE	CY23256	Stream Processing	3	0	0	3
7	PE	CY23257	Prompt Engineering	3	0	0	3

VERTICAL III – EMERGING TECHNOLOGIES

S.No	Category	Course Code	Course Title	L	T	P	C
1	PE	CY23351	Foundations of Virtual Reality	3	0	0	3
2	PE	CY23352	Security in Embedded Systems	3	0	0	3
3	PE	CY23353	Quantum Cryptography	3	0	0	3
4	PE	CY23354	Algorithmic Game theory	3	0	0	3
5	PE	CY23355	Introduction to Industry 4.0 and IIoT	3	0	0	3
6	PE	CY23356	Digital Twins	3	0	0	3
7	PE	CY23357	MANET and Sensor Networks	3	0	0	3

VERTICAL IV – COMPUTER NETWORKS AND SECURITY

S.No	Category	Course Code	Course Title	L	T	P	C
1	PE	CY23451	Advanced Distributed Systems	3	0	0	3
2	PE	CY23452	Mobile and Wireless Security	3	0	0	3
3	PE	CY23453	Cellular Network Security	3	0	0	3
4	PE	CY23454	Secured Network Protocols	3	0	0	3
5	PE	CY23455	Software Security	3	0	0	3
6	PE	CY23456	Intrusion Detection and Prevention	3	0	0	3
7	PE	CY23457	Virtual Private Networks	3	0	0	3

VERTICAL V – SOFTWARE DEPLOYMENT

S.No	Category	Course Code	Course Title	L	T	P	C
1	PE	CY23551	Web Technologies	3	0	0	3
2	PE	CY23552	Mobile App Development	3	0	0	3
3	PE	CY23553	Microservices	3	0	0	3
4	PE	CY23554	DevSecOps	3	0	0	3
5	PE	CY23555	Full stack development	3	0	0	3
6	PE	CY23556	Git and GitHub	3	0	0	3
7	PE	CY23557	Responsible and Safe AI systems	3	0	0	3

VERTICAL VI - DATA SECURITY AND STANDARDS

S.No	Category	Course Code	Course Title	L	T	P	C
1	PE	CY23651	Exploratory Data Analytics	3	0	0	3
2	PE	CY23652	Data Preprocessing and Wrangling	3	0	0	3
3	PE	CY23653	Biometric Security	3	0	0	3
4	PE	CY23654	Security Metrics	3	0	0	3
5	PE	CY23655	Big Data Computing	3	0	0	3
6	PE	CY23656	Social Networks	3	0	0	3
7	PE	CY23657	Security Audit and Risk Assessment	3	0	0	3

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/7/25
AUTONOMOUS

MINOR IN IOT WITH CYBER SECURITY

Course Code	Category	Course Title	L	T	P	C
CY23851	MDC	Cyber Security Essentials	3	0	0	3
CY23852	MDC	Fundamentals of Computer Forensics	3	0	0	3
CY23853	MDC	Privacy and Security in Online Social Media	3	0	0	3
CY23854	MDC	Introduction to Sensor Technologies	3	0	0	3
CY23855	MDC	IoT and its Applications	3	0	0	3
CY23856	MDC	Industrial IoT	3	0	0	3

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/7/25
★ AUTONOMOUS ★

CY23501	ARTIFICIAL INTELLIGENCE IN CYBER SECURITY	3	1	0	4

COURSE OBJECTIVES

To enable the students to

1.	understand the fundamentals of Artificial Intelligence and its relevance in cyber security.
2.	learn various AI models and techniques applied in threat detection and response.
3.	analyze the role of Convolutional Neural Networks in security domains.
4.	implement AI techniques in intrusion detection.
5.	explore real-world case studies and ethical issues in AI-driven cyber security.

UNIT I **INTRODUCTION TO ARTIFICIAL INTELLIGENCE AND CYBER SECURITY** **12**

Introduction to Artificial Intelligence – Scope – Cyber Security Challenges and Threat Landscape – Role of AI in Enhancing Cyber Security – Types of AI Models: Machine Learning, Deep Learning, Expert Systems; Rule-Based vs Learning-Based AI; Search Algorithms in AI (BFS, DFS); Knowledge Representation Techniques – Applications of AI in Security Monitoring and Automation, Cyber Defense.

UNIT II **APPLICATION OF AI TECHNIQUES IN THREAT DETECTION** **12**

Introduction to Supervised Learning – Classification Techniques: Decision Trees, Naive Bayes, SVM – Regression Techniques: Linear and Logistic Regression–Unsupervised Learning: K-Means Clustering, Hierarchical Clustering–Dimensionality Reduction and Feature Engineering – Applications- Email Threat Classification, Anomaly Detection, Spam and Phishing Detection, Zero-Day Threat Identification with AI.

UNIT III **LEARNING MODELS FOR SECURITY ANALYTICS** **12**

Introduction to Neural Networks: Perceptron, Multilayer Perception, Convolutional Neural Networks, Recurrent Neural Networks, Long and short-term memory, Training Learning Models using TensorFlow and PyTorch; Applications: Convolutional Neural Networks for Packet Inspection, LSTM for Log Analysis, Autoencoders for Intrusion Detection, Malware Generation and Defense, Malware Classification using CNNs, Adversarial Attacks and Robustness, Log Anomaly Detection.

UNIT IV **APPLICATIONS OF AI IN NETWORK INTRUSION** **12**

Introduction to Intrusion Detection Systems (IDS), Host and Network-based Behavioral Analysis using AI, AI in Ransomware Detection and Response, AI in Network Traffic Analysis, AI for Endpoint Security – Automation of Incident Response using AI, Static and Dynamic malware threat Detection using AI.

UNIT V **ETHICAL CONSIDERATIONS AND AI IN SOCIAL ENGINEERING** **12**

AI in Detecting Social Engineering Attacks, Fake Content Detection, Chatbots in Phishing Simulation and Training; Bias and Fairness in AI Algorithms, Ethical Challenges in AI Deployment for Surveillance, Legal and Regulatory Considerations, AI and Privacy-Preserving Techniques, Future

Trends and Responsible AI in Cyber Security, AI Misuse in Security Contexts.

TOTAL PERIODS **60**

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	understand the roles and applications of AI in Cyber Security.	Understanding (K2)
CO2	analyze the applications of AI in threat detection and response.	Analyzing (K4)
CO3	explain about Convolutional Neural Networks in security domains.	Analyzing (K4)
CO4	recognize AI techniques in intrusion detection.	Applying (K3)
CO5	depict ethical implications of AI in Cyber Security systems.	Analyzing (K4)

TEXTBOOKS

1. V.S. Subramanian, Handbook of Artificial Intelligence and Big Data Applications in Cybersecurity, Springer, 2021.
2. Clarence Chio, David Freeman, Machine Learning and Security, O'Reilly Media, 2018.

REFERENCES

1. Stuart J. Russell, Peter Norvig, Artificial Intelligence: A Modern Approach, 4th Edition, Pearson, 2020.
2. Claude Sammut, Geoffrey I. Webb, Encyclopedia of Machine Learning and Data Mining, Springer, 2017.
3. Pethuru Raj, Artificial Intelligence for Cybersecurity, CRC Press, 2023.
4. Sumeet Dua, Xian Du, Data Mining and Machine Learning in Cybersecurity, CRC Press, 2011.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	1	-	-	2	2	2	2
CO2	2	2	2	2	2	2	-	2	-	-	2	2	2	2
CO3	2	2	2	2	2	2	-	2	-	-	2	2	2	2
CO4	2	2	2	2	2	2	-	2	-	-	2	2	3	3
CO5	2	2	2	2	2	2	-	2	-	-	2	2	3	3

CY23502	FOUNDATIONS OF DATA SCIENCE	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the data science fundamentals and its process.
2.	describe the data for building the model along and statistical basis for AI.
3.	analyze the relationship between data using predictive model evaluation.
4.	utilize the Python libraries for Data Wrangling.
5.	interpret data using visualization libraries in Python.

UNIT I	INTRODUCTION	9

Data Science: Benefits and uses – facets of data - Data Science Process: Overview – Defining research goals – Retrieving data – Data preparation - Exploratory Data analysis – build the model– presenting findings and building applications.

UNIT II	DESCRIBING DATA	9

Types of Data - Types of Variables - Basic Statistical descriptions of Data - Describing Data with Tables and Graphs –Describing Data with Averages - Describing Variability - Normal Distributions and Standard (z) Scores.

UNIT III	DESCRIBING RELATIONSHIPS	9

Correlation –Scatter plots –correlation coefficient for quantitative data –computational formula for correlation coefficient – Regression –regression line: least squares regression line – Standard error of estimate, interpretation of r2 –multiple regression equations –regression towards the mean.

UNIT IV	PYTHON LIBRARIES FOR DATA WRANGLING	9

Basics of Numpy arrays –aggregations –computations on arrays –comparisons, masks, boolean logic – fancy indexing – structured arrays – Data manipulation with Pandas – data indexing and selection – operating on data – missing data – Hierarchical indexing – combining datasets – aggregation and grouping – pivot tables.

UNIT V	DATA VISUALIZATION	9

Importing Matplotlib – Line plots – Scatter plots – visualizing errors – density and contour plots-Histograms – legends – colors – subplots – text and annotation – customization – three-dimensional plotting - Geographic Data with Basemap - Visualization with Seaborn.

	TOTAL PERIODS	45

COURSE OUTCOMES

	At the end of the course, the students will be able to	BT MAPPED (Highest Level)
CO1	define the data science process.	Understanding (K2)
CO2	understand different types of data description for data science.	Analyzing (K4)
CO3	gain knowledge on relationships between data.	Applying (K3)
CO4	use the Python Libraries for Data Wrangling.	Applying (K3)
CO5	apply visualization Libraries in Python to interpret and explore data.	Analyzing (K4)

TEXTBOOKS

1. David Cielen, Arno D. B. Meysman, and Mohamed Ali, "Introducing Data Science", Manning Publications ,2016
2. Robert S. Witte and John S. Witte, "Statistics", Eleventh Edition, Wiley Publications, 2017.

REFERENCES

1. Jake VanderPlas, "Python Data Science Handbook", O'Reilly, 2016.
2. Auerlien Geron, Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow,3rd Edition, O'Reilly Media.
3. Allen B. Downey, "Think Stats: Exploratory Data Analysis in Python", Green Tea Press,2014.
4. Avrim Blum, John Hopcroft, Ravindran Kannan, "Foundations of Data Science", Cambridge Press, 2020.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

	PO's												PSO's	
CO's	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	-	2	2	2	2
CO2	2	2	2	2	2	2	-	-	-	-	2	2	2	2
CO3	2	2	2	2	2	2	-	-	-	-	2	3	3	3
CO4	2	2	2	2	2	2	-	-	-	-	2	3	3	3
CO5	2	2	2	2	2	2	-	-	-	-	2	3	3	3

CY23503	UI AND UX DESIGN	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	gain a sound knowledge in UI & UX.
2.	explain the need for UI and UX.
3.	extend the application of various tools and methods used in Design.
4.	explore the various interaction patterns used in UI & UX.
5.	build personas and scenarios for ideations.

UNIT I FOUNDATIONS OF DESIGN 9

UI vs. UX Design (principles, deliverables, wireframes vs. prototypes) – Core Stages of Design Thinking (Empathize: user research, Define: problem framing, Ideate: creative ideation, Prototype: low/high-fidelity, Test: usability evaluation) – Divergent & Convergent Thinking (mind mapping, Crazy 8s, affinity mapping, dot-voting) – Brainstorming & Gamestorming (structured ideation rules, brainwriting, role-play games, Six Thinking Hats) – Observational Empathy (contextual inquiry, shadowing, diary studies, empathy mapping).

UNIT II FOUNDATIONS OF UI DESIGN 9

Visual & UI Principles (visual hierarchy, balance, contrast, alignment) – UI Elements & Patterns (buttons, forms, cards, navigation, masonry/grid layouts) – Interaction Behaviors & Principles (affordances, feedback, consistency, motion design, user flows) – Branding (logo usage, color palettes, typographic hierarchy, voice and tone) – Style Guides (component libraries, design tokens, accessibility standards, versioning).

UNIT III FOUNDATIONS OF UX DESIGN 9

Introduction to User Experience -. Why You Should Care about User Experience - Understanding User Experience - Defining the UX Design Process and its Methodology - Research in User Experience Design - Tools and Method used for Research - User Needs and its Goals - Know about Business Goals

UNIT IV WIREFRAMING, PROTOTYPING AND TESTING 9

Sketching Principles - Sketching Red Routes - Responsive Design – Wireframing - Creating Wireflows - Building a Prototype - Building High-Fidelity Mockups - Designing Efficiently with Tools - Interaction Patterns - Conducting Usability Tests - Other Evaluative User Research Methods - Synthesizing Test Findings - Prototype Iteration

UNIT V DESIGN AND IDEATION 9

Identifying and Writing Problem Statements - Identifying Appropriate Research Methods - Creating Personas - Solution Ideation - Creating User Stories - Creating Scenarios - Flow Diagrams - Flow Mapping - Information Architecture

	TOTAL PERIODS	45

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/7/25
AUTONOMOUS

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	build UI for user applications.	Understanding (K2)
CO2	use UX design of any product or application.	Applying (K3)
CO3	demonstrate UX design skills in product development.	Applying (K3)
CO4	create wireframe and prototype.	Analyzing (K4)
CO5	implement personas and create user stories.	Analyzing (K4)

TEXT BOOKS

1. Joel Marsh, "UX for Beginners", O'Reilly , 2022.
2. Jon Yablonski, "Laws of UX using Psychology to Design Better Product & Services" O'Reilly 2021.

REFERENCES

1. Jenifer Tidwell, Charles Brewer, Aynne Valencia, "Designing Interface" 3rd Edition , O'Reilly 2020.
2. Steve Schoger, Adam Wathan "Refactoring UI", 2018
3. Steve Krug, "Don't Make Me Think, Revisited: A Commonsense Approach to Web & Mobile", Third Edition, 2015
4. UX Strategy: Product Strategy Techniques for Devising Innovative Digital Solutions (2nd ed.) – Jaime Levy – O'Reilly Media, 2021.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's

(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	-	2	2	2	2
CO2	2	2	2	2	2	2	-	-	-	-	2	2	2	2
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO5	2	2	2	2	2	2	-	-	-	-	2	2	3	3

CY23504	DIGITAL FORENSICS AND INCIDENT RESPONSE	3	0	0	3

COURSE OBJECTIVES	
To enable the students to	
1.	know the various types of cybercrime and benefits of digital forensics.
2.	understand the process of investigating computer crime, policies and laws.
3.	learn digital evidence investigation procedure and legal issues of computer forensics.
4.	understand the need for mobile forensics and Amendments Indian IT Act (2008).
5.	learn the incident response process and maintaining the incident response capability.

UNIT I	INTRODUCTION TO DIGITAL FORENSICS	9
Introduction - Definition of Computer Forensics, Cybercrime, Computer based crime; Evolution of Computer Forensics - Stages of Computer Forensics Process - Benefits of Computer Forensics - Uses of Computer Forensics - Role of Forensics Investigator - Forensics Readiness - Goals of Forensic Readiness, Benefits and Planning of Forensic Readiness.		
UNIT II	COMPUTER FORENSICS INVESTIGATION PROCESS	9
Introduction to Computer Crime Investigation - Assess the Situation, Review Policies and Laws, Identify Investigation Team Members, conduct a Thorough Assessment, Prepare for Evidence Acquisition; Acquire the Data - Build Computer Investigation Toolkit, Collect the Data, Store and Archive; Analyze the Data - Report the Investigation.		
UNIT III	DIGITAL EVIDENCE AND FIRST RESPONDER PROCEDURE	9
Digital Evidence - Characteristics of Digital Evidence, Stages in Digital Evidence Investigation Process; First Responder Toolkit - Issues Facing Computer Forensics - Technical Issues, Legal Issues, Administrative Issues; Types of Investigation - Techniques of Digital Forensics - Cross-drive analysis, Live analysis, Recovery of deleted files.		
UNIT IV	MOBILE DEVICE FORENSICS	9
Introduction to Mobile Forensics - Challenges in Mobile Forensics - Mobile Communication – Evidence's in Mobile Devices - Mobile Forensic Process - Forensic Acquisition Tools - Hardware acquisition tools, Software acquisition tools - Report Preparation - Expert Witness - Legal Aspects of Computing - Amendments Indian IT Act (2008).		
UNIT V	INCIDENT RESPONSE	9
Introduction - The incident response process - The role of digital forensics - The incident response framework and charter - CSIRT core team - Technical support personnel - Organizational support personnel - External resources - The incident response plan - Incident classification - The incident response playbook - Escalation procedures - Maintaining the incident response capability.		
	TOTAL PERIODS	45

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	classify the various types of cybercrime and benefits of computer forensics.	Understanding (K2)
CO2	apply the policies and laws related to forensics investigation process.	Applying (K3)
CO3	analyze digital evidence investigation procedure and legal issues of computer forensics	Analyzing (K4)
CO4	apply knowledge of mobile forensics and Indian IT Act (2008).	Understanding (K2)
CO5	apply the process of incident response plan and capability.	Applying (K3)

TEXTBOOKS

1. Dr. Ajay Prasad, Dr. Jeetendra Pande, "Digital Forensics", Uttarakhand Open University, Haldwani, Mumbai, 2019.
2. Gerard Johansen "Digital Forensics and Incident Response" Packt Publishing Ltd, Birmingham, B3 2PB, UK, 2017.

REFERENCES

1. L.T. Brown "Computer Evidence Collection &Presentation", Firewall Media. 2017.
2. Linda Volonino, Reynaldo Anzaldua; Computer Forensics for Dummies, Wiley, Publishing, Inc.2016.
3. Real Digital Forensics by Keith j.Jones, Richard Bejitlich,Curtis W.Rose ,Addison - Wesley Pearson Education. 2015
4. Computer Forensics, Computer Crime Investigation by John R,Vacca, Firewall Media, New Delhi. 2012.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's

(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	Programme Outcomes PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	2	-	2	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	2	-	-	2	2	3	3
CO3	3	3	3	3	3	3	-	2	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	2	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	2	-	-	2	2	3	3

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/7/25
AUTONOMOUS

CY23505	SECURE SOFTWARE ENGINEERING	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand foundational concepts and ethics of software engineering.
2.	explain requirements engineering, system modeling and architectural design.
3.	describe design decisions, architectural patterns and model driven approaches.
4.	learn the testing strategies and reengineering.
5.	recognize core security engineering practices, testing and assurance.

UNIT I — SOFTWARE PROCESS AND AGILE DEVELOPMENT — 9

Introduction to Software Engineering, Layered Technology, Software Process: Common process framework; Capability Maturity Mode (CMM), Perspective and Specialized Process Models: Waterfall model-Incremental Process Model-Evolutionary Process Model -Introduction to Agility-Agile process.

UNIT II — REQUIREMENTS ANALYSIS AND SPECIFICATION — 9

Software Requirements: Functional and Non-Functional, User requirements, System requirements, Software Requirements Document – Requirement Engineering Process: Feasibility Studies, Requirements elicitation and analysis, requirements validation, requirements management-Classical analysis: Structured system Analysis, Petri Nets- Data Dictionary.

UNIT III — SOFTWARE DESIGN — 9

Design process – Design Concepts-Design Model– Design Heuristic – Architectural Design and architectural styles – Architectural Mapping using Data Flow- User Interface Design: Interface analysis, Interface Design –Component level Design: Designing Class based components, traditional Components.

UNIT IV — TESTING AND MAINTENANCE — 9

Software testing fundamentals-Internal and external views of Testing-white box testing — basis path testing-control structure testing-black box testing- Regression Testing-Maintenance and re-engineering BPR model-Re-engineering process model-Reverse and Forward Engineering.

UNIT V — SECURITY TESTING & RESILIENCE — 9

Security testing and assurance -Cyber security -Socio technical resilience -Resilient systems design – Version management -Change management-system building-release management.

TOTAL PERIODS 45

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	explain the importance of software security.	Understanding (K2)
CO2	analyze and formulate security requirements.	Analyzing(K4)

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/7/25

CO3	apply secure design principles in software systems.	Analyzing(K4)
CO4	evaluate secure testing strategies across SDLC.	Analyzing(K4)
CO5	recall core security engineering practices.	Analyzing(K4)

TEXT BOOKS

1. “Software Engineering” Ian Sommerville, Pearson Education, edition 2017.
2. Software Engineering- A Practitioner's Approach by Roger S. Pressman, edition 9 ,2023, Mcgrawhill.

REFERENCES

1. "Security Engineering: A Guide to Building Dependable Distributed Systems," Ross Anderson, Wiley, 2020.
2. "Writing Secure Code," Michael Howard and David LeBlanc, Microsoft Press, 2003.
3. "Secure Coding: Principles and Practices," Mark Graff and Kenneth van Wyk, O'Reilly Media, 2003.
4. "Building Secure Software: How to Avoid Security Problems the Right Way," John Viega and Gary McGraw, Addison-Wesley, 2002.

CO-PO MAPPING:

Mapping of Course Outcome (CO’s) with Programme Outcomes (PO’s) and Programme Specific Outcomes PSO’s

(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO’s	PO’s												PSO’s	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	2	2	2	2	2
CO2	2	2	2	2	2	2	-	-	-	2	2	2	2	2
CO3	2	2	2	2	2	2	-	-	-	2	2	2	3	3
CO4	2	2	2	2	2	2	-	-	-	2	2	2	3	3
CO5	2	2	2	2	2	2	-	-	-	2	2	2	3	3

CY23506	ARTIFICIAL INTELLIGENCE LABORATORY	0	0	4	2

COURSE OBJECTIVES

To enable the students to

1.	understand the role of Artificial Intelligence in solving cyber security problems.
2.	apply machine learning and deep learning techniques to real-world security datasets.
3.	implement and test AI algorithms for detection and classification in cyber environments.
4.	analyze and interpret results from AI-driven security solutions.

LIST OF EXPERIMENTS

1. Email Spam Detection using Naive Bayes Classifier.
2. Phishing Website Classification Using Decision Trees.
3. Anomaly Detection in Network Traffic Using Isolation Forest.
4. Password Strength Checker with Machine Learning.
5. Malware Classification using Support Vector Machine (SVM).
6. Social Engineering Detection using Natural Language Processing (NLP).
7. Botnet Detection in Network Traffic using K-Means Clustering and Chatbot for Phishing Awareness Training (Rule-based/NLP).
8. Fake News Detection using Logistic Regression.
9. Intrusion Detection System (IDS) using Random Forest on NSL-KDD Dataset and Ransomware File Behavior Detection Using Autoencoders.
10. Adversarial Attack Simulation on Image Classifiers and Face Anti-Spoofing for Secure Authentication using CNN.
11. Keystroke Dynamics for User Authentication.
12. Network Traffic Classification with Deep Learning (LSTM or CNN).

TOTAL PERIODS **60**

COURSE OUTCOMES

At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	apply basic AI and ML techniques to solve cyber security problems.	Applying (K3)
CO2	implement supervised and unsupervised models for cyber threat detection.	Applying (K3)
CO3	design, execute, and analyze AI experiments for securing (emails, logs, network, images).	Applying (K3)
CO4	build and evaluate AI-driven solutions for advanced cyber-attacks.	Applying (K3)

CO-PO MAPPING :

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	3	3	2	2	2	2	-	-	-	-	2	2	3	3
CO2	3	3	2	2	2	2	-	-	-	-	2	2	3	3
CO3	3	3	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	2	2	2	-	-	-	-	2	2	3	3

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/7/25
★ AUTONOMOUS ★

CY23507	DATA SCIENCE LABORATORY	0	0	2	1

COURSE OBJECTIVES

To enable the students to

1.	understand the python libraries for data science.
2.	understand the basic Statistical and Probability measures for data science.
3.	learn descriptive analytics on the benchmark data sets.
4.	apply correlation and regression analytics on standard data sets.

LIST OF EXPERIMENTS

1. Download, install and explore the features of NumPy, SciPy, Jupyter, Statsmodels and Pandas packages.

2. Working with Numpy arrays

3. Working with Pandas data frames

4. Reading data from text files, Excel and the web and exploring various commands for doing descriptive analytics on the Iris data set.

5. Use the diabetes data set from UCI and Pima Indians Diabetes data set for performing the following:

   a. Univariate analysis: Frequency, Mean, Median, Mode, Variance, Standard Deviation, Skewness and Kurtosis.

   b. Bivariate analysis: Linear and logistic regression modeling

   c. Multiple Regression analysis

   d. Also compare the results of the above analysis for the two data sets.

6. Apply and explore various plotting functions on UCI data sets.

   a. Normal curves

   b. Density and contour plots

   c. Correlation and scatter plots

   d. Histograms

   e. Three dimensional plotting

7. Visualizing Geographic Data with Basemap

	TOTAL PERIODS	30

COURSE OUTCOMES

At the end of this course, the students will be able to		BT MAPPED (Highest Level)
CO1	make use of the python libraries for data science.	Applying (K3)

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/7/25
★ AUTONOMOUS ★

CO2	make use of the basic statistical and probability measures for data science.	Applying (K3)
CO3	perform descriptive analytics on the benchmark data sets.	Applying (K3)
CO4	perform correlation and regression analytics on standard data sets.	Applying (K3)

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and

Programme **Specific Outcomes (PSO's)**

(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

COs	**PO's**												**PSO's**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	-	3	3	3	3
CO2	2	2	2	2	2	2	-	-	-	-	3	3	3	3
CO3	3	3	3	3	3	3	-	-	-	-	3	3	3	3
CO4	3	3	3	3	3	3	-	-	-	-	3	3	3	3

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/7/25
AUTONOMOUS

CY23508	**INDUSTRIAL TRAINING**	**0**	**0**	**2**	**1**

COURSE OBJECTIVES

To enable the students to

1	understand the cyber security threats, cyberattacks, cybercrimes, vulnerabilities and remedies.
2	use advanced tools, techniques and strategies to safeguard information technology systems.
3	analyze the cyber security needs of an organization and participate in cyber security risk assessment.
4	analyze existing legal framework and laws on cyber security.

DESCRIPTION

Industrial Training provides work experience relevant to their field of specialization, before graduation, and it is an essential component for the development of practical and professional skills required for an engineering graduate and supports for prospective employment.

At the end of the industrial training, students should be able to improve their knowledge and skills relevant to their areas of specialization where they have been trained. The students should also be able to relate, apply, and adapt the relevant knowledge, concepts, and theories within an industrial organization, and also to practice the general workplace behavior and interpersonal skills.

The student (either in group or single) should undergo industrial training for a minimum period of two weeks during the summer vacation after the completion of fourth semester as specified in the curriculum in any research organization/university/industry of State/National and International level industry relevant to their branch of specialization, after getting proper approval from the Head of the Institution.

On the completion of the industrial training for the specified period, the student has to submit the industrial training report (at least 25-30 pages) containing the following details, along with the certificate obtained from the industry for the period of training undergone.

1. Introduction of the industry.
2. Industry layout and its various operations with its infrastructure facilities.
3. Formulation of practical problems, data required to formulate the problems and its analysis.
4. Suggestions and recommendations for the above problems

During the period of training, the student has to abide the rules and regulations enforced by the organization and to ensure FULL attendance during the period of industrial training and uphold the discipline and decorum of the institution.

On the completion of the industrial training, the End Semester Examinations shall be conducted by the

Office of the Controller of Examinations at the end of the fifth semester. A three-member committee constituted by the Head of the Institution, consisting of (1) a senior faculty member at the Professor level, (2) senior faculty member at the Associate Professor and (3) faculty member from outside the department, will evaluate the industrial training undergone by the student. The evaluation shall be made based on the report submitted along with the presentation and a Viva voce Examination.

TOTAL PERIODS: 30

COURSE OUTCOMES At the end of the course, the students will be able to		**BT MAPPED** **(Highest level)**
CO1	assess and present risk findings, safety measures that drive leadership action,	Understanding (K2)
CO2	use advanced tools and techniques to reduce the risk of computer attacks.	Applying (K3)
CO3	explain practical defense strategies, analyze security incidents and prepare security audit tasks, reports.	Analyzing (K4)
CO4	explain the challenges in cyber governance, national cyber policies, digital evidence management, legal frameworks and legal procedures.	Analyzing (K4)

CO - PO MAPPING

Mapping of Course Outcomes with Programme Outcomes:

(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium , 1-Weak

COs	**Programme Outcomes (POs)**													
	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO1**	**PSO2**
CO1	2	2	2	2	2	2	-	2	2	1	1	2	2	2
CO2	2	2	2	2	2	2	-	2	2	1	1	2	3	3
CO3	2	2	2	2	2	2	-	2	2	2	2	2	3	3
CO4	2	2	2	2	2	2	-	2	2	2	2	2	2	2

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
05/7/25
AUTONOMOUS

GE23501	**PROFESSIONAL DEVELOPMENT III**	0	0	2	1

COURSE OBJECTIVES	
To enable students to	
1.	enhance their Resume writing skills and improving corporate vocabularies to survive in the corporate world.
2.	evaluate their interview skills and improve their interview presentation.
3.	solve the quantitative aptitude problems and improve their mental ability.
4.	improve critical thinking and reasoning skills.

UNIT I	**RESUME WRITING SKILLS**	6
Updated Resume Building III – Self Introduction III – Dressing Etiquette – JAM V – Corporate Vocabulary.		
UNIT II	**INTERVIEW SKILLS**	6
Interview skills – General guidelines - Work Ethics – Group Discussion III – JAM VI – Presentation Competence – Mock Interview.		
UNIT III	**QUANTITATIVE APTITUDE**	9
Cube Root and Square Root - Time and Work - Ages - Permutation and Combination - Probability – Calendar.		
UNIT IV	**LOGICAL REASONING**	9
Series Completion - Blood Relations - Coding and Decoding - Data Sufficiency - Statements and Assumptions.		
	TOTAL PERIODS:	**30**

COURSE OUTCOMES Upon completion of the course, the students will be able to		**BT MAPPED** (Highest Level)
CO1	excel in drafting Resumes and speaking.	Applying (K3)
CO2	demonstrate the participative skills in group discussions and Interviews.	Applying (K3)
CO3	solve problems based on quantitative aptitude.	Applying (K3)
CO4	enhance their logical and verbal reasoning.	Analyzing (K4)

TEXTBOOKS

1. Aggarwal, R. S. A Modern Approach to Verbal & Non-Verbal Reasoning. Revised ed., 2024–25, S. Chand & Company Ltd., 2024.
2. Aggarwal, R. S. Objective General English: Fully Revised Video Edition. S. Chand & Company Ltd., 2022.

REFERENCES

1. Abhijit Guha, "Quantitative Aptitude ", Tata-Mcgraw Hill.2015.
2. Word Power Made Easy By Norman Lewis, Wr.Goyal Publications.2016.
3. Johnson, D.W. Reaching out — Interpersonal Effectiveness and self- actualisation. Boston: Allyn and Bacon.2019.
4. Infosys Campus Connect Program — students' guide for soft skills.2015.

CO/PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's)
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	Programme Outcomes (PO's)													
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PS01	PS02
CO1	3	2	2	3	3	1	-	-	-	-	-	-	3	2
CO2	-	2	3	-	2	-	2	-	-	-	-	-	3	2
CO3	3	2	2	2	-	-	1	-	-	-	-	-	2	3
CO4	3	2	2	-	-	1	-	-	-	-	2	-	2	3

CY23151	DATA VIRTUALIZATION	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1. learn the basics and types of virtualizations.
2. understand the hypervisors and its types.
3. explore the virtualization solutions.
4. experiment the virtualization platforms.
5. monitor, report, and review about different virtual machines.

UNIT I	INTRODUCTION TO VIRTUALIZATION	9

Virtualization and cloud computing - Need of virtualization – cost, administration, fast deployment, reduce infrastructure cost – limitations- Types of hardware virtualization: Full virtualization - partial virtualization - Paravirtualization-Types of Hypervisors

UNIT II	SERVER AND DESKTOP VIRTUALIZATION	9

Virtual machine basics- Types of virtual machines- Understanding Server Virtualization- types of server virtualization- Business Cases for Server Virtualization – Uses of Virtual Server Consolidation – Selecting Server Virtualization Platform-Desktop Virtualization-Types of Desktop Virtualization.

UNIT III	NETWORK VIRTUALIZATION	9

Introduction to Network Virtualization-Advantages- Functions-Tools for Network Virtualization-VLAN-WAN Architecture-WAN Virtualization.

UNIT IV	STORAGE VIRTUALIZATION	9

Memory Virtualization-Types of Storage Virtualization-Block, File-Address space Remapping-Risks of Storage Virtualization-SAN-NAS-RAID.

UNIT V	VIRTUALIZATION TOOLS	9

VMWare-Amazon AWS-Microsoft HyperV- Oracle VM Virtual Box - IBM PowerVM- Google Virtualization- Case study.

	TOTAL PERIODS	45

COURSE OUTCOMES

	At the end of this course, students will be able to	BT Mapped (Highest Level)
CO1	analyze the virtualization concepts and hypervisor	Understanding (K2)
CO2	apply the virtualization for real-world applications	Applying (K3)
CO3	install & configure the different vm platforms	Applying (K3)
CO4	experiment with the vm with various software	Analyzing (K4)
CO5	explore different virtualization technologies	Analyzing (K4)

TEXTBOOKS

1. Cloud computing a practical approach - Anthony T.Velte , Toby J. Velte Robert Elsenpeter, Tata McGraw- Hill , New Delhi – 2021
2. Cloud Computing (Principles and Paradigms), Edited by Rajkumar Buyya, James Broberg, Andrzej Goscinski, John Wiley & Sons, Inc. 2019

REFERENCES

1. Matthew Portnoy2nd Edition, Sybex, ,A clear, concise introduction to virtualization concepts, types of hypervisors, and use-cases.
2. Nick Marshall, Mike Brown, G. B. Witt Packt Publishing, 2021 ,Deep dive into enterprise-grade server virtualization, clustering, DRS/HA and advanced configuration.
3. Charbel Nemnom 3rd Edition, Packt Publishing, 2019 ,Extensive recipes for planning, deploying and managing Windows Server Hyper-V and its virtual networking/storage features.
4. Storage Virtualization: Techniques and Applications Shyam N. Shenoy, Pavankumar Sahandodia Wiley-IEEE Press, 2016,.

CO-PO MAPPING :

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

	PO's												PSO's	
CO's	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	1	1	1	1	1	2	-	-	-	2	2	2	2	2
CO2	2	2	2	2	2	2	-	-	-	2	2	2	2	2
CO3	2	2	2	2	2	2	-	-	-	2	2	2	2	2
CO4	2	2	2	2	2	2	-	-	-	2	2	2	2	2
CO5	2	2	2	2	2	2	-	-	-	2	2	2	2	2

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
27/12/24
★ AUTONOMOUS ★

CY23152	COGNITIVE SCIENCE AND ANALYTICS	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the nature of Cognitive Science.
2.	identify neural mechanisms of Cognitive Functions
3.	explore how language evolved in humans biologically and cognitively.
4.	apply AI models to validate psychological or cognitive theories.
5.	explore the characteristics of Intelligent Agents.

UNIT I INTRODUCTION TO COGNITIVE SCIENCE 9

Introduction- Cognitive Science- Representation- Computation- The Interdisciplinary Perspective- The Philosophical Approach- The Free Will–Determinism Debate- The Knowledge Acquisition Problem- The Psychological Approach- Structuralism- Functionalism- The Whole Is Greater Than the Sum of Its Parts- Mini-Minds- Mind as a Black Box.

UNIT II COGNITIVE AND NEUROSCIENCE APPROACH 9

Types of Memory- Memory Models- Visual Imagery- Problem Solving- The Neuroscience Perspective- Methodology in Neuroscience- The Big Picture: Brain Anatomy- Visual Object Recognition- The Neuroscience of Attention- The Neuroscience of Memory- Neural Substrates of Working Memory- The Neuroscience of Executive Function and Problem Solving.

UNIT III NETWORK, EVOLUTIONARY, LINGUISTIC APPROACH 9

The Network Perspective-Principles Underlying Artificial Neural Networks-Artificial Neural Network -Evaluating the Connectionist Approach-Semantic Networks-A Hierarchical Semantic Network-The Evolutionary View-Evolution and Cognitive Processes-Evaluating Evolutionary Psychology-Artificial Intelligence and Linguistics-Overall Evaluation of the Linguistic Approach

UNIT IV INTELLIGENCE PERSPECTIVES 9

Introduction- Defining Artificial Intelligence (AI)- Evaluating the Concept of AI-AI Methodologies- The Practical World of Artificial Intelligence-Approaches to the Design of Intelligent Agents- Machine Representation of Knowledge-Machine Reasoning-Logical Reasoning-Inductive Reasoning- Expert Systems-Fuzzy Logic-Artificial Neural Nets (ANNs).

UNIT V INTELLIGENT AGENTS 9

Introduction-Evaluating Robotic Potentials-Biological and Behavioral Foundations of Robotic Paradigms-Foundations of Robotic Paradigms-Robotic Paradigms-Hierarchical Paradigm-The Reactive Paradigm-The Hybrid Deliberative/Reactive Paradigm-Overall Evaluation of Robots as Ultimate Intelligent Agents.

TOTAL PERIODS	**45**

COURSE OUTCOMES		
At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	understand the underlying theory behind cognition.	Understanding (K2)
CO2	connect to the cognition elements computationally.	Analysing (K4)
CO3	recognize concepts like natural selection, evolutionary psychology and modularity of mind.	Understanding (K2)
CO4	apply Intelligence Theories in Real-World Contexts.	Applying (K3)
CO5	analyze how different paradigms influence robot behavior and architecture.	Analysing (K4)

TEXTBOOKS

1. Jay Friedenberg, Gordon Silverman Cognitive Science: An Introduction to the Study of Mind. SAGE Publications,2021.
2. Eric Judith Hurwitz, Marcia Kaufman, Adrian Bowles, Cognitive Computing and Big Data Analytics, Wiley Publications, 2015.

REFERENCES

1. Noah D. Goodman, Andreas Stuhlmuller, "The Design and Implementation of Probabilistic Programming Languages", Electronic version of book , https://dippl.org/.
2. Noah D. Goodman, Joshua B. Tenenbaum, The ProbMods Contributors, "Probabilistic Models of Cognition", Second Edition, 2016, https://probmods.org/.
3. Vijay V Raghavan, Venkat N.Gudivada, VenuGovindaraju, C.R. Rao, Cognitive Computing: Theory and Applications: (Handbook of Statistics 35), Elsevier publications, 2016.
4. Cognitive computing and big data analytics ,Judith Hurwitz,Marcia Kaufman,Adrian Bowles,John Wiley& Sons,2021,3rd edition.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's

(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	1	1	1	1	1	-	-	-	-	-	1	1	2	2
CO2	1	1	1	1	1	-	-	-	-	-	1	1	2	2
CO3	2	2	2	2	2	-	-	-	-	-	2	2	3	3
CO4	2	2	2	2	2	-	-	-	-	-	2	2	3	3
CO5	2	2	2	2	2	-	-	-	-	-	2	2	3	3

CY23153	PRIVACY PRESERVATION IN DATA MINING	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the concepts of data mining and data preprocessing.
2.	analyse about pattern mining and classification.
3.	explore probabilistic anonymity measures.
4.	gain knowledge on utility-based privacy preservation of data.
5.	investigate privacy preserving methods.

UNIT I FUNDAMENTALS OF DATA MINING 9

Introduction to Data Mining, Data Mining functionalities, kinds of patterns , Challenges and Applications of in Data Mining, Data Objects and Attribute Types, Basic Statistical Descriptions of Data, Data Visualization, Data Similarity and Dissimilarity; Introduction to Data Preprocessing, Data Cleaning versus Data Processing, Data Integration, Reduction, Transformation and Discretization.

UNIT II PATTERN MINING AND CLASSIFICATION 9

Mining Frequent Patterns, Associations, and Correlations: Basic Concepts and Methods; Pattern Mining in Multilevel, Multidimensional Space; Constraint-Based Frequent Pattern Mining, Pattern Exploration and Application; Data classification: Decision Tree Induction, Bayes Classification Methods, Rule-Based Classification, Metrics for Evaluating Classifier Performance, k-fold cross-validation, Model Selection Using Statistical Tests of Significance, Techniques to Improve Classification Accuracy.

UNIT III PRIVACY-PRESERVING DATA MINING 9

Introduction to Privacy-Preserving Data Mining Algorithms-The Randomization Method- Group Based Anonymization- Distributed Privacy-Preserving Data Mining; Results of Privacy Preservation of Applications- Applications of Privacy Preserving Datamining; Classification of Microdata Protection Methods- Perturbative Masking Methods- Non-Perturbative Masking Methods-Synthetic Microdata Generation-Trading off Information Loss and Disclosure Risk, Measures of Anonymity.

UNIT IV UTILITY-BASED PRIVACY-PRESERVING DATA 9

k-Anonymous Datamining-Randomization Methods for Privacy-Preserving Datamining; Multiplicative Perturbation for Privacy-Preserving Datamining; Quantification of Privacy preserving Datamining Algorithms; Utility-Based Privacy Preserving Data Transformation Methods, Association Rule Hiding Methods for Privacy.

UNIT V PRIVACY-PRESERVING METHODS 9

Privacy-Preserving Methods across vertically and horizontally Partitioned Data; Privacy-Preserving Data Perturbation Methods; Private Data Analysis via Output Perturbation; Query

Auditing Techniques for Data Privacy; Privacy and the Dimensionality Curse; Personalized Privacy Preservation; Privacy-Preserving DataStream Classification.

TOTAL PERIODS 45

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	outline the concepts of data mining and data preprocessing.	Understanding (K2)
CO2	demonstrate about pattern mining and classification.	Analysing (K4)
CO3	explain probabilistic anonymity measures.	Analysing (K4)
CO4	appraise on utility-based privacy preservation of data.	Analysing (K4)
CO5	formulate, design, and implement the solutions for privacy preservation.	Analysing (K4)

TEXTBOOKS

1. Jiawei Han & Michelin Kamber, Data Mining Concepts & Techniques, 3rd Edition, Elsevier, 2020.
2. Privacy – Preserving Data Mining: Models and Algorithms Edited by Charu C. Aggarwal and S. Yu, Springer,2021.

REFERENCES

1. Charu C. Agarwal, Data Mining: The Textbook, 1st Edition, Springer.2018.
2. K.P. Soman, Shyam Diwakar and V. Aja, ―Insight into Data Mining Theory and Practice‖, Eastern Economy Edition, Prentice Hall of India, 2006.
3. G.K.Gupta, Introduction to Data Mining with Case Studies, EEE, PHI, India, 2006.
4. Privacy preserving, Datamining, Jaideep Vidya,Chris Clifton,Michael Zhu-Springer ,4th edition 2018.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	-	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	-	-	-	-	-	2	2	3	3
CO3	3	3	3	3	3	-	-	2	-	-	2	2	3	3
CO4	3	3	3	3	3	-	-	2	-	-	2	2	3	3
CO5	3	3	3	3	3	-	-	2	-	-	2	2	3	3

CY23154	DIGITAL MARKETING AND SOCIAL MEDIA ANALYTICS	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the fundamental concepts and scope of digital marketing and social media.
2.	explore the scope and components of digital marketing.
3.	identify and collect data from social media outlets.
4.	explore the social analytics process using stream computing.
5.	analyze consumer reactions via internal and external feedback.

UNIT I **FUNDAMENTALS OF DIGITAL MARKETING** **9**

Introduction-Types of Media- Visual Language & Sketch noting- Target Market and Audiences-Customer Personas- Pros and Cons- Customer Journey Mapping- Benefits-Content marketing-Search Engine Optimization (SEO)- Website and Landing Page Optimization.

UNIT II **DIGITAL MARKETING ANALYTICS** **9**

Introduction to Marketing Analytics- Marketing Frameworks- Digital Marketing-Communication Channels- Advantages- Digital Marketing Analytics- Capabilities- Digital RAA Framework- Stages of Digital RAA Framework.

UNIT III **SOCIAL MEDIA ANALYSIS** **9**

Introduction- Identifying data in social media outlets- Four dimensions of Analysis taxonomy-Velocity of data- Validating the hypothesis- Data identification- Data analysis-Iterative methods-Value in real time- Applications.

UNIT IV **STREAM COMPUTING** **9**

Introduction- Stream Computing- Applications- Directed graphs- Streams Example: SSM- Ad-hoc Analysis-Example of Ad-hoc analysis-Data Integrity-Responding to leads identified in Social media- Social analytics process.

UNIT V **ENTERPRISE SOCIAL NETWORK** **9**

Introduction- Social vs Collaboration- Transparency of communication- Enterprise graph-Finding the right data- Customizing and modifying tools-Analyzing consumer reaction-Visualizations- Types.

TOTAL PERIODS **45**

COURSE OUTCOMES

At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	understand key concepts in digital marketing and social media.	Understanding (K2)
CO2	explain the marketing frameworks effectively.	Analyzing (K4)
CO3	identify and extract data from social media platforms.	Understanding (K2)

CO4	explore real-time applications of stream computing.	Applying (K3)
CO5	predict consumer reactions via internal and external feedback.	Analyzing (K4)

TEXTBOOKS

1. A.Karim Feroz,Gohar F.Khan, and Marshall Sponder, "Digital Analytics for Marketing", Second Edition,2024.
2. Rochelle Grayson, "Foundations in Digital Marketing" Building Meaningful Customer Relationships and Engaged Audiences,2023.

REFERENCES

1. Matthew Ganis, Avinash Kohirkar ,"Social Media Analyrics" Techniques and Insights for extracting Business value out of Social media,2016.
2. Bittu Kumar, Social Networking, V & S Publishers, 2013
3. Avinash Kaushik, Web Analytics - An Hour a Day, Wiley Publishing, 2007
4. T. Peterson, Web Analytics Demystified, Celilo Group Media and CafePress, 2004

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	-	2	2	3	3

CY23155	INFORMATION SECURITY MANAGEMENT	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the foundations of governance and risk management.
2.	explore operations security process controls.
3.	analyze common authentication challenges.
4.	identify risks in e-mail systems.
5.	understand the role of social networking in security.

UNIT I	GOVERNANCE AND RISK MANAGEMENT	9

Introduction- Four Types of Policies- Developing and Managing Security Policies- Programme Level Policies- Programme Framework Policies- Issue Specific Policies- System Specific Policies- Developing and Managing Security Policies- Providing Policy Support Documents.

UNIT II	OPERATIONS SECURITY	9

Introduction- Operations Security Principles- Operations Security Process Controls- Operations Security Controls in Action- Configuration and Change Management- Backups -Media Controls- Documentation- Maintenance.

UNIT III	ACCESS CONTROL SYSTEMS AND METHODOLOGY	9

Introduction- Identification- Authentication- Information Owner- Discretionary Access Control- User Provisioning- Mandatory Access Control- Role-Based Access Control- Principles of Authentication- The Problems with Passwords- Multifactor Authentication- Remote User Access and Authentication- Virtual Private Networks.

UNIT IV	NETWORK SECURITY AND RISK MANAGEMENT	9

E-Mail Security- E-mail System at Risk- Securing the E-mail architecture- Organizational Governance- Information Security Executive in the organization- Information Security Organization- Information security Audit- Anatomy of an audit- Establish measures and metrics.

UNIT V	SOCIAL NETWORKING AND SECURITY ANALYSIS	9

Social Networking-Insider threat Defense- Server Virtualization- Benefits of Server Virtualization- Security and Control of Virtual Servers- Security Requirements analysis- System Security Policy- CERT Resilience management model-Operations- Model Relationships- Managing Bluetooth Security.

	TOTAL PERIODS	45

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	apply risk management principles in policy development.	Applying (K3)
CO2	demonstrate operations security controls in practice.	Analyzing (K4)
CO3	explore identification and authentication mechanisms.	Applying (K3)

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
27/12/24

CO4	understand the fundamentals of network security.	Understanding (K2)
CO5	conduct security requirements analysis.	Analyzing (K4)

TEXTBOOKS

1. Mark S. Merkow ,Jim Breithaupt "Information Security: Principles and Practices", Second Edition,2014.
2. Harold F.Tipton CISSP,Micki Krause Nozaki, CISSP,"Information Security Management Handbook", Sixth Edition, Volume 6.

REFERENCES

1. Michel Crouhy, Dan Galai, Robert Mark, "THE ESSENTIALS OF RISK MANAGEMENT, Second Edition, 2014.
2. Mohit Philip, Implementing TLS 1.3: A Developer's Guide, Packt Publishing, 2019
3. Michael W. Lucas, SSH Mastery: OpenSSH, PuTTY, Tunnels and Keys, 2nd Edition, No Starch Press, 2019
4. Chris Sanders & Jason Smith, Applied Network Security Monitoring: Collection, Detection, and Analysis, 2nd Edition, Syngress, 2020

CO-PO MAPPING :

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's

(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	3	2	2	2	2	2	-	2	-	-	2	2	2	2
CO2	2	2	2	2	2	2	-	2	-	-	2	2	2	2
CO3	2	2	2	2	2	2	-	2	-	-	2	2	2	2
CO4	2	2	2	3	3	3	-	2	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	2	-	-	2	2	3	3

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
27/12/24
AUTONOMOUS

CY23156	PREDICTIVE ANALYTICS	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the fundamentals of predictive analytics and multivariate data discovery.
2.	gain proficiency in statistical techniques such as logistic regression and ANOVA.
3.	apply dimension reduction and clustering methods to analyze complex data.
4.	build and evaluate predictive models using visualization tools and algorithms.
5.	utilize R programming for predictive modeling and classification tasks.

UNIT I — DATA DISCOVERY WITH MULTIVARIATE DATA — 9

Introduction-Use Tables to Explore Multivariate Data-PivotTables-Tabulate in JMP-Use Graphs to Explore Multivariate Data-Graph Builder-Scatterplot-Explore a Larger Data Set-Trellis Chart-Bubble Plot-Explore a Real-World Data Set-Use Graph Builder to Examine Results of Analyses.

UNIT II — LOGISTIC REGRESSION AND ANOVA — 9

Introduction-Regression-Perform a Simple Regression and Examine Results-Understand and Perform Multiple Regression-Understand and Perform Regression with Categorical Data-Analysis of Variance-Dependence Technique-The Linear Probability Model-The Logistic Function.

UNIT III — PRINCIPAL COMPONENTS ANALYSIS AND CLUSTER ANALYSIS — 9

Introduction-Basic Steps in JMP-Produce the Correlations and Scatterplot Matrix-Create the Principal Components-Understand Eigenvalue Analysis-Dimension Reduction-Discovery of Structure in the Data-Hierarchical Clustering-K-Means Clustering.

UNIT IV — BUILDING A PREDICTIVE MODEL AND VISUALIZATION — 9

Definition-Data Preparation-Choosing an algorithm-Developing and Testing the Model-Visualization as a Predictive Tool-Evaluating Visualization-Visualizing Model's Analytical Results-Novel Visualization in Predictive Analytics-Big Data Visualization Tools-Tableau-Google Charts-Plotly-Infogram.

UNIT V — PREDICTIVE MODELING WITH R — 9

Introduction-Programming in R-Installing R-Installing RStudio-Getting familiar with the environment-Making Predictions Using R-Predicting using regression-Using classification to predict-Classification by random forest.

TOTAL PERIODS — 45

COURSE OUTCOMES

	At the end of this course, students will be able to	**BT Mapped (Highest Level)**
CO1	understand and explore multivariate data using tables and graphs.	Understanding (K2)
CO2	analyze data using logistic regression and ANOVA techniques.	Analyzing (K4)
CO3	apply principal component and cluster analysis to discover data patterns.	Applying (K3)

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
28/12/24
AUTONOMOUS

CO4	build and visualize predictive models using various algorithms and tools.	Applying (K3)
CO5	evaluate predictive models using r for regression and classification tasks.	Analyzing (K4)

TEXTBOOKS

1. Ron Klimberg, B.D.McCullough, "Fundamentals of Predictive Analytics with JMP", Second Edition, 2017.
2. Anasse Bari, Mohamed Chaouchi, Tommy Jung ,"Predictive Analytics", Second Edition,2017.

REFERENCES

1. Max Kuhn, Kjell Johnson, "Applied Predictive Modeling" Springer- 2013.
2. Eric Siegel ,"Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die",2016.
3. Richard V. McCarthy, Mary M. McCarthy, Wendy Ceccucci, Leila Halawi,"Applying Predictive Analytics: Finding Value in Data",2019.
4. Modeling Techniques in Predictive Analytics with Python and R A Guide to Data Science Thomas W. Miller, Published by Pearson Education,2015.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	-	2	2	3	3

CY23157	CLOUD SERVICES MANAGEMENT	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1. introduce cloud service management terminology, definition & concepts.
2. compare cloud service management with traditional IT services management.
3. identify strategies to reduce risk and eliminate issues associated with adoption of cloud services
4. select appropriate structures for designing, deploying and running cloud-based services.
5. illustrate the benefits and drive the adoption of cloud-based services.

UNIT I CLOUD SERVICE MANAGEMENT FUNDAMENTALS 9

Cloud Ecosystem, The Essential Characteristics, Basics of Information Technology Service Management and Cloud Service Management, Service Perspectives, Cloud Service Models, Cloud Service Deployment Models.

UNIT II CLOUD SERVICES STRATEGY 9

Cloud Strategy Fundamentals, Cloud Strategy Management Framework, Cloud Policy, Key Driver for Adoption, Risk Management, IT Capacity and Utilization, Demand and Capacity matching, Demand Queueing, Change Management, Cloud Service Architecture.

UNIT III CLOUD SERVICE MANAGEMENT 9

Cloud Service Reference Model, Cloud Service LifeCycle, Basics of Cloud Service Design, Dealing with Legacy Systems and Services, Benchmarking of Cloud Services, Cloud Service Capacity Planning, Cloud Service Deployment and Migration, Cloud Marketplace, Cloud Service Operations Management.

UNIT IV CLOUD SERVICE ECONOMICS 9

Pricing models for Cloud Services, Freemium, Pay Per Reservation, pay per User, Subscription based Charging, Procurement of Cloud-based Services, Capex vs Opex Shift, Cloud service Charging, Cloud Cost Models.

UNIT V CLOUD SERVICE GOVERNANCE & VALUE 9

IT Governance Definition, Cloud Governance Definition, Cloud Governance Framework, Cloud Governance Structure, Cloud Governance Considerations, Cloud Service Model Risk Matrix, Understanding Value of Cloud Services, Measuring the value of Cloud Services, Balanced Scorecard, Total Cost of Ownership.

TOTAL PERIODS 45

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	exhibit cloud-design skills to build and automate business solutions.	Understanding (K2)
CO2	explain cloud-based services policies and risk management.	Analyzing (K4)

CO3	describe cloud services and plan cloud service design.	Analyzing (K4)
CO4	analyze the economics of Cloud Adoption.	Analyzing (K4)
CO5	understand the Cloud Service Governance & Value	Analyzing (K4)

TEXTBOOKS

1. Cloud Service Management and Governance: Smart Service Management in Cloud Era by Enamul Haque, Enel Publications 2021
2. Cloud Computing: Concepts, Technology & Architecture by Thomas Erl, Ricardo Puttini, Zaigham Mohammad 2019.

REFERENCES

1. Cloud Computing: Concepts, Technology & Architecture Thomas Erl, Zaigham Mahmood & Ricardo Puttini Prentice Hall, 2nd Edition, 2019.
2. Nick Marshall, Mike Brown, G. B. Witt Packt Publishing, 2021 ISBN 978-1838820350 – Deep dive into enterprise-grade server virtualization, clustering, DRS/HA and advanced configuration.
3. Cloud Strategy: A Decision-based Approach to Successful Cloud Adoption Gregor Hohpe O'Reilly Media, 1st Edition, 2020 ISBN 978-1492051241
4. Cloudonomics: The Business Value of Cloud Computing Joe Weinman Wiley, 1st Edition, 2012 ISBN 978-1118229965

CO-PO MAPPING :

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	1	1	1	1	1	2	-	-	-	-	2	2	2	2
CO2	1	1	1	1	1	2	-	-	-	-	2	2	2	2
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO5	2	2	2	2	2	2	-	-	-	-	2	2	3	3

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
27/12/24
★ AUTONOMOUS ★

CY23251	E-COMMERCE SECURITY	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the fundamentals of cybersecurity and its relevance to e-commerce platforms.
2.	explore threats, vulnerabilities, and risk management in online transactions.
3.	analyze technologies and protocols that ensure secure data transmission and storage.
4.	implement authentication, encryption, and fraud prevention techniques in e-commerce systems.
5.	evaluate legal, ethical, and compliance frameworks related to e-commerce security.

UNIT I FUNDAMNETALS OF E-COMMERCE SECURITY 9

Introduction to E-Commerce Security – Importance, Scope ,Types of E-Commerce – B2B, B2C, C2C, G2C – Cybersecurity Challenges in E-Commerce – Common E –commerce Threats – Vulnerabilities in Web Applications and Online Stores – Security Goals – Confidentiality, Integrity, Availability, Non-repudiation – Security Models – Bell-LaPadula, Clark- Wilson – E-Commerce Infrastructure – Hosting, Payment Gateway, APIs – Role of Cyber security in Customer Trust and Business Continuity.

UNIT II RISK MANAGEMENT AND THREAT ASSESSMENT 9

Risk Assessment and Threat Modeling for E-Commerce – Security Policies, Compliance Requirements – Firewalls ,Intrusion Detection Systems – Access Control Models – DAC, MAC, RBAC – Secure Network Architecture for E-Commerce – Vulnerability Assessment Tools – OWASP ZAP, Nessus – Security Audits –Major Data Breaches – Business Continuity and Incident Response Planning.

UNIT III SECURE COMMUNICATION 9

Cryptography in E-Commerce – Symmetric and Asymmetric Encryption – SSL/TLS Protocols – HTTPS, Digital Certificates – Public Key Infrastructure – Certificate Authorities – Hash Functions and Digital Signatures – Secure Electronic Transaction (SET) Protocol – Email and Document Encryption – PGP, S/MIME – End-to-End Encryption – Data Protection in Transit and at Rest – Key Management and Secure Storage Practices.

UNIT IV AUTHENTICATION AND PRIVACY 9

Authentication Techniques: Passwords, OTPs, Biometrics, Two-Factor and Multi-Factor -Session Management and Timeout Controls – Identity and Access Management (IAM) – User Privacy and Consent Management – Fraud Detection – Rule-Based and AI-Powered Models – Bot Mitigation, Captcha Systems – Transaction Monitoring and Anomaly Detection – Best Practices for Secure Checkout and Payment Processing.

UNIT V FUTURE SECURITY TRENDS 9

Legal and Regulatory Frameworks – IT Act, GDPR, PCI DSS – Data Privacy Laws and Compliance – Cybercrime Investigation,Reporting – IPR ,Digital Rights Management – Ethical Hacking in E-

Commerce – Cyber Forensics for Online Incidents – Cross- Border E-Commerce Security Issues – Third-Party Risk Management and Vendor Security – Future Trends : Blockchain, AI and Quantum-safe Security in E-Commerce.

TOTAL PERIODS **45**

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	understand the fundamentals of e-commerce and security.	Understanding (K2)
CO2	explain risk management in online transactions.	Applying(K3)
CO3	use encryption and secure protocols to safeguard online transactions.	Analyzing (K4)
CO4	analyze authentication and fraud detection mechanisms.	Analyzing (K4)
CO5	identify legal and ethical considerations for cyber security compliance.	Analyzing (K4)

TEXTBOOKS

1. William Stallings, "Effective Cybersecurity: A Guide to Using Best Practices and Standards", Pearson, 2018.
2. Mike Hendrickson, "Cybersecurity for E-commerce", O'Reilly Media, 2017.

REFERENCES

1. Kameshwar C. Wali, "Cyber Security for E-Commerce", Springer, 2019.
2. Yogesh Shetty, "Cybersecurity Handbook for E-commerce", Packt, 2021.
3. Jason Andress, "Foundations of Information Security", No Starch Press, 2020.
4. Kris Hermans, "PCI DSS – A Pocket Guide", Van Haren Publishing, 2019.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	-	-	2	-	-	2	2	2	2
CO2	2	2	2	2	2	-	-	2	-	-	2	2	2	2
CO3	2	2	2	2	2	-	-	2	-	-	2	2	2	2
CO4	3	3	3	3	3	-	-	2	-	-	2	2	3	3
CO5	3	3	3	3	3	-	-	2	-	-	2	2	3	3

CY23252	DATA CENTRE NETWORKING	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the data Centre requirements and architecture.
2.	explain the need of data Centre safety.
3.	outline the design considerations of a data Centre and trouble shooting.
4.	know about system Resource Management.
5.	gain knowledge on network maintenance and Information Security.

UNIT I | **DATA CENTRE ARCHITECTURE** | **9**

Data centre Architecture, Data centre Requirements, Required Physical Area for Equipment and Unoccupied Space, required power to run all the devices, required cooling and HVAC Required weight, Required Network bandwidth Budget Constraints.

UNIT II | **DATA CENTRE SAFETY** | **9**

Selecting a Geographic Location Safety from Natural hazards, Safe from Manmade disaster, Availability of local technical talent, Abundant and Inexpensive Utilities, Selecting an Existing building.

UNIT III | **DATA CENTRE DESIGN** | **9**

Data Centre design, guidelines-Characteristics of an Outstanding Design,Data Centre structures, Raised Floor Design and Deployment, Design and Plan against Vandalism, Data centre design case study, Modular Cabling Design, Points of Distribution, Data center servers, Sever Capacity Planning.

UNIT IV | **DATA CENTRE NETWORK MAINTENANCE** | **9**

ISP Network Infrastructure, ISP WAN Links, Data Centre Maintenance, Network Operations Centre, Network Monitoring, Data centre physical security, Logical security, Consolidation, Reasons for data centre Consolidation, Consolidation opportunity, Server, Storage, Network, Service, Process, Staff , Data Consolidation phases.

UNIT V | **DATA CENTER SECURITY AND ADMINISTRATION** | **9**

Best Practices for System Management , Server Cluster, Data Storage , Network Management, Documentation , Security Guidelines Internet security, Source Security Issues, Best Practices for System Administration and Work Automation, Device Naming, Naming Practices, NIS, DNS, LDAP, Load balancing and types, Terminology, Advantages, Implementing a Network with Load-Balancing Switches.

	TOTAL PERIODS	**45**

COURSE OUTCOMES		
At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	manage Server Systems and Data Centre's Infrastructure Management.	Understanding (K2)
CO2	analyze about the factors of safety of data Centre.	Analyzing(K4)
CO3	monitor the Networks and Resources.	Analyzing(K4)
CO4	plan for Flexible resource allocation.	Applying(K3)
CO5	understand about the best practices in network maintenance.	Analyzing (K4)

TEXTBOOKS

1. Administering Data Centers: Servers, Storage and Voice over IP, Kailash Jayaswal, John Wiley & Sons, Oct 28, 2005.
2. Data center fundamentals, Mauricio Arregoces, Maurizio Portol, Cisco Press, 2003.

REFERENCES

1. Data Center Networking -Network Topologies and Traffic Management in Large-Scale Data Center-Springer Publications, 1st edition 2022.
2. Data Center Handbook: Plan, Design, Build, and Operations of a Smart Data Center,Wiley 1st edition ,2021.
3. Cloud Native Data Center Networkingby Dinesh G. Dutt 2019,Publisher(s): O'Reilly Media.
4. Transmission and Processing for Data Center Networking Le Nguyen Binh Huawei Technologies, European Research Institute, Muenchen, Bayern, Germany, IOP Publishing, Bristol, UK,2020

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	2	-	-	-	-	2	2	2	2
CO2	2	2	2	2	2	2	-	-	-	-	2	2	2	2
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	-	2	2	3	3

CY23253	STORAGE TECHNOLOGIES	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	characterize the functionalities of logical and physical components of storage.
2.	describe various storage networking technologies.
3.	identify different storage virtualization technologies.
4.	discuss the different backup and recovery strategies.
5.	understand common storage management activities and solutions.

UNIT I STORAGE SYSTEMS 9

Introduction to Information Storage: Digital data , Information storage, Key characteristics of data center and Evolution of computing platforms, Information Lifecycle Management, Third Platform Technologies: Cloud computing, essential characteristics, Cloud services and deployment models, big data analytics, Social networking and mobile computing, Characteristics of third platform infrastructure ,transformation - Building blocks of a data center, Computer systems and computer virtualization and Software-defined data center.

UNIT II INTELLIGENT STORAGE SYSTEMS AND RAID 9

Components of an intelligent storage system, Components, addressing, and performance of hard disk drives and solid-state drives, RAID, Types of intelligent storage systems, Scale-up and scale- out storage Architecture.

UNIT III STORAGE NETWORKING TECHNOLOGIES AND VIRTUALIZATION 9

Block-Based Storage System, File-Based Storage System, Object-Based and Unified Storage. Fibre Channel SAN: Software-defined networking, FC SAN components and architecture, topologies, link aggregation, and zoning and Virtualization, Internet Protocol SAN: iSCSI protocol, network components, and connectivity, Link aggregation, switch aggregation, and VLAN, FCIP protocol.

UNIT IV BACKUP, ARCHIVE AND REPLICATION 9

Introduction to Business Continuity, Backup architecture, Backup targets and methods, Data deduplication, Cloud-based and mobile device backup, Data archive, Uses of replication and its characteristics, Compute based, storage-based, and network-based replication, Data migration,

UNIT V SECURING STORAGE INFRASTRUCTURE 9

Information security goals, Storage security domains, Threats to a storage infrastructure, Security controls to protect a storage infrastructure, Governance, risk, and compliance, Storage infrastructure management functions, Storage infrastructure management processes.

	TOTAL PERIODS	45

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
23/12/23
AUTONOMOUS

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	demonstrate the fundamentals of information storage management.	Understanding (K2)
CO2	illustrate the usage of advanced intelligent storage systems.	Applying (K3)
CO3	interpret various storage networking architectures.	Applying (K3)
CO4	examine the disaster recovery and remote replication technologies	Analyzing (K4)
CO5	infer the security measures in information storage management.	Analyzing (K4)

TEXTBOOKS

1. EMC Corporation, Information Storage and Management, Wiley, India 2022.
2. Jon Tate, Pall Beck, Hector Hugo Ibarra, Shanmuganathan Kumaravel and Libor Miklas, Introduction to Storage Area Networks, Ninth Edition, IBM - Redbooks, December 2017.

REFERENCES

1. Storage Networks Explained Ulf Troppens, Rainer Erkens & Wolfgang Muller Wiley, 1st Edition, 2011.
2. SAN Essentials: Storage Area Network Fundamentals Marc Farley AMS Publishing, 2nd Edition, 2007.
3. SAN & NAS: Network Storage Fundamentals Robert SpaldingPearson Education, 1st Edition, 2003.
4. Data Storage Networking, Second Edition Jack Rosenberg & Alan R. EarlsWiley, 2nd Edition, 2010.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO5	2	2	2	2	2	2	-	-	-	-	2	2	3	3

CY23254	**CLOUD COMPUTING**	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1. introduce cloud service management terminology, definition & concepts.
2. compare cloud service management with traditional IT service management.
3. identify strategies to reduce and eliminate risk associated with adoption of cloud services.
4. select appropriate structures for designing, deploying and running cloud-based services.
5. illustrate the benefits of adoption of cloud-based services to solve real world problems.

UNIT I INTRODUCTION TO CLOUD MANAGEMENT 9

The four pillars of cloud computing- Cloud applications and Platforms - Potential customers of cloud technology- Providing the cloud infrastructure- Strategic inflection points in information Technology-Cloud computing and its slogans- User centered solution and cloud computing- Small and Medium Enterprises - Virtual companies - Virtual networked objects.

UNIT II CLOUD STRATEGY AND ARCHITECTURE 9

Moving to a cloud architecture and strategy to achieve business value.- BPM, IS, Porter‘s Value chain model and BPR -SWOT/PEST, Economies of scale, Porter‘s 3 Strategies and 5 Competitive Forces, D‘Aveni‘s hyper competition models- the roles of the strategic IS/IT leaders such as Chief Information Officer(CIO)- The Chief Technology Officer (CTO),- Budgeting-Service level agreements-Outsourcing, Infrastructural interdependencies, the cloud- Human resources at the CIO level.

UNIT III SERVICE PLANNING IN CLOUD 9

IT strategy to deliver on strategic business objectives in the business strategy- IT Project planning in the areas of ITaaS is essential in delivering a successful strategic IT Plan-IT Project planning in the areas of SaaS,PaaS,IaaS in delivering a successful strategic IT Plan-Searching for an open architecture- Infrastructure as a Utility- Cloud System Architecture and its primitives.

UNIT IV CLOUD MANAGEMENT FUNCTIONS 9

Shared services delivered by a Service Oriented Architecture (SOA) in a Private or Public Cloud-Services, Databases and Applications on demand- The effect on Enterprise Architecture and its traditional frameworks such as Zachman- The Open Group Architecture Framework (TOGAF)-Customer Relationship Management-Enterprise Resource Planning-Just-in-Time Inventories-Machine-to-Machine and RFID Communications-Challenges in Organization and Commercial vision.

UNIT V APPLICATIONS OF CLOUDS IN VARIOUS SECTORS 9

Benefit Realization and it Governance-Managing resources (people, process, technology), to realize benefit from Private/Public Cloud IT services-Gartner's 5 pillars of benefit realization-IT governance as a service - High Technology for private banking and Asset Management- Cloud Software for Private Banking-Cloud Software For Asset Management-Cloud Technology can Improve Fund Management-Criteria of Success in Asset Management Technology.

TOTAL PERIODS 45

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
27/12/24

COURSE OUTCOMES		
At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	assess the business value of cloud computing.	Understanding (K2)
CO2	analyze the role of cloud computing in the business process.	Analyzing (K4)
CO3	evaluate how cloud computing can deliver business agility.	Analyzing (K4)
CO4	implement IT governance to cloud IT services.	Analyzing (K4)
CO5	appraise the applications of cloud services.	Analyzing (K4)

TEXTBOOKS

1. Dimitris N. Chorafas: Cloud Computing Strategies, CRC Press, 2021.
2. Arnold J Cummins, —Easiest Ever Guide to Strategic IT Planning,2019.

REFERENCES

1. Cloud Strategy: A Decision-based Approach to Successful Cloud Adoption, Gregor Hohpe , O'Reilly Media, 2020
2. The Cloud Adoption Playbook: Proven Strategies for Transforming Your Organization with the Cloud – Moe Abdula, Ingo Averdunk, Roland Barcia, Kyle Brown & Ndu Emuchay – Wiley, 2018
3. Cloudonomics: The Business Value of Cloud Computing – Joe Weinman – Wiley, 2012
4. Enterprise Cloud Strategy – Eduardo Kassner & Barry Briggs – O'Reilly Media, 2011

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

	PO's												PSO's	
CO's	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO5	2	2	2	2	2	2	-	-	-	-	2	2	3	3

CY23255	SECURITY AND PRIVACY IN CLOUD	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	introduce Cloud Computing terminology, definition & concepts.
2.	understand the security design and architectural considerations for Cloud.
3.	observe the Identity, Access control in Cloud.
4.	follow best practices for Cloud security using various design patterns.
5.	monitor and audit cloud applications for security.

UNIT I **FUNDAMENTALS OF CLOUD SECURITY CONCEPTS** **9**

Overview of cloud security- Security Services - Confidentiality, Integrity, Authentication, Non-repudiation, Access Control - Basic of cryptography - Conventional and public-key cryptography, hash functions, authentication, and digital signatures.

UNIT II **SECURITY DESIGN AND ARCHITECTURE FOR CLOUD** **9**

Security design principles for Cloud Computing - Comprehensive data protection - End-to-end access control - Common attack vectors and threats - Network and Storage - Secure Isolation Strategies - Virtualization strategies - Inter-tenant network segmentation strategies - Data Protection strategies: Data retention, deletion and archiving procedures for tenant data, Encryption, Data Redaction, Tokenization, Obfuscation, PKI and Key

UNIT III **ACCESS CONTROL AND IDENTITY MANAGEMENT** **9**

Access control requirements for Cloud infrastructure - User Identification - Authentication and Authorization - Roles-based Access Control - Multi-factor authentication - Single Sign-on, Identity Federation - Identity providers and service consumers - Storage and network access control options - OS Hardening and minimization - Verified and measured boot - Intruder Detection and prevention.

UNIT IV **CLOUD SECURITY DESIGN PATTERNS** **9**

Introduction to Design Patterns, Cloud bursting, Geo-tagging, Secure Cloud Interfaces, Cloud Resource Access Control, Secure On-Premises Internet Access, Secure External Cloud.

UNIT V **MONITORING, AUDITING AND MANAGEMENT** **9**

Proactive activity monitoring - Incident Response, Monitoring for unauthorized access, malicious traffic, abuse of system privileges - Events and alerts - Auditing – Record generation, Reporting and Management, Tamper-proofing audit logs, Quality of Services, Secure Management, User management, Identity management, Security Information and Event Management.

TOTAL PERIODS **45**

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	understand the cloud concepts and fundamentals.	Understanding (K2)

CO2	explain the security challenges in the cloud.	Applying (K3)
CO3	define cloud policy and Identity and Access Management.	Applying (K3)
CO4	analyze the risks, audit and monitoring mechanisms in the cloud.	Analyzing (K4)
CO5	describe the security aspects in the design of cloud architecture.	Analyzing (K4)

TEXTBOOKS

1. Raj Kumar Buyya , James Broberg, Andrzej Goscinski, —Cloud Computing:‖, Wiley 2021
2. Dave shackleford, —Virtualization Security‖, SYBEX a Wiley Brand 2019.

REFERENCES

1. Cloud Security and Privacy – Tim Mather, Subra Kumaraswamy & Shahed Latif – O'Reilly Media, 2009
2. Cloud Computing Security – Ronald L. Krutz & Russell Dean Vines – Wiley, 2010
3. Security for Cloud Computing – John W. Rittinghouse & James F. Ransome – CRC Press, 2017
4. Practical Cloud Security: A Guide for Secure Design and Deployment – Chris Dotson – Apress, 2016

CO-PO MAPPING :

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	2	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	2	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	2	-	-	2	2	3	3
CO4	3	3	3	3	3	2	-	2	-	-	2	2	3	3
CO5	3	3	3	3	3	2	-	2	-	-	2	2	3	3

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
27/12/24
★ AUTONOMOUS ★

CY23256	STREAM PROCESSING	3	0	0	3

COURSE OBJECTIVES	
To enable the students to	
1.	introduce data processing terminology, definition & concepts.
2.	define different types of data processing.
3.	explain the concepts of real-time data processing.
4.	select appropriate structures for designing and running real-time data services.
5.	illustrate the adoption of real-time data services to solve real world problems

UNIT I	**FOUNDATIONS OF DATA SYSTEMS**	9
Introduction to Data Processing, Stages of Data processing, Data Analytics, Batch Processing, Stream processing, Data Migration, Transactional Data processing, Data Mining, Data Management Strategy, Storage, Processing, Integration, Analytics, Benefits of Data as a Service, Challenges.		
UNIT II	**REAL-TIME DATA PROCESSING**	9
Introduction to Big data, Big data infrastructure, Real-time Analytics, Near real-time solution, Lambda architecture, Kappa Architecture, Stream Processing, Understanding Data Streams, Message Broker, Stream Processor, Batch & Real-time ETL tools, Streaming Data Storage.		
UNIT III	**DATA MODELS AND QUERY LANGUAGES**	9
Relational Model, Document Model, Key-Value Pairs, NoSQL, Object-Relational Mismatch, Many-to-One and Many-to-Many Relationships, Network data models, Schema Flexibility, Structured Query Language, Data Locality for Queries, Declarative Queries, Graph Data models, Cypher Query Language, Graph Queries in SQL, The Semantic Web, CODASYL, SPARQL		
UNIT IV	**EVENT PROCESSING WITH APACHE KAFKA**	9
Apache Kafka, Kafka as Event Streaming platform, Events, Producers, Consumers, Topics, Partitions, Brokers, Kafka APIs, Admin API, Producer API, Consumer API, Kafka Streams API, Kafka Connect API.		
UNIT V	**REAL-TIME PROCESSING USING SPARK STREAMING**	9
Structured Streaming, Basic Concepts, Handling Event-time and Late Data, Fault-tolerant Semantics, Exactly once Semantics, Creating Streaming Datasets, Schema Inference, Partitioning of Streaming datasets, Operations on Streaming Data, Selection, Aggregation, Projection, Watermarking, Window operations, Types of Time windows, Join Operations, Deduplication		
	TOTAL PERIODS	**45**

COURSE OUTCOMES		
At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	understand the utility of different streaming algorithms.	Understanding (K2)
CO2	describe and apply current research trends in data-stream processing.	Applying (K3)

CO3	analyze the use of stream mining algorithms for data stream systems.	Applying (K3)
CO4	program and build stream processing systems, services and applications.	Analyzing (K4)
CO5	solve problems in real-world applications that process data streams.	Analyzing (K4)

TEXTBOOKS

1. Streaming Systems: The What, Where When and How of Large-Scale Data Processing by Tyler Akidau, Slava Chemyak, Reuven Lax, O'Reilly publication
2. Designing Data-Intensive Applications by Martin Kleppmann, O'Reilly Media

REFERENCES

1. Designing Data-Intensive Applications – Martin Kleppmann – O'Reilly Media, 2017
2. Streaming Systems: The What, Where, When, and How of Large-Scale Data Processing – Tyler Akidau, Slava Chernyak, Reuven Lax – O'Reilly Media, 2018
3. Kafka: The Definitive Guide: Real-time Data and Stream Processing at Scale – Neha Narkhede, Gwen Shapira, Todd Palino – O'Reilly Media, 2017
4. Learning Spark: Lightning-Fast Data Analytics – Jules S. Damji, Brooke Wenig, Tathagata Das, Denny Lee – O'Reilly Media, 2020

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	3	2	3	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	2	2	-	-	-	-	2	2	3	3
CO5	3	3	3	3	2	2	-	-	-	-	2	2	3	3

CY23257	PROMPT ENGINEERING	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the fundamentals of prompt engineering.
2.	analyze practical crafting techniques for diversified AI tasks.
3.	apply prompt engineering tools for practical applications.
4.	learn evaluate frameworks, tools, and prompt optimization strategies.
5.	explore analyze ethical, societal, and emerging trends.

UNIT I INTRODUCTION TO PROMPT ENGINEERING 9

Definitions and significance of prompt engineering - Historical evolution and milestones - zero-shot, one-shot, few-shot -Chain-of-thought and role-based prompting - Overview of large language models (LLMs) - Prompt engineering vs. traditional programming. - Role in NLP, NLG, and generative AI.

UNIT II CRAFTING EFFECTIVE PROMPTS 9

Principles of clear and unambiguous prompt writing - Techniques for maximizing model output quality Prompt templates: standard vs. custom - Leveraging context and conditioning in prompts - Parameter tuning: temperature, top-p, max tokens - Prompting for specific tasks: classification, question answering - Controlling style, tone, and verbosity - Failure analysis: common mistakes in prompt crafting - Iterative refinement and testing prompts.

UNIT III PRACTICAL APPLICATIONS AND USE CASES 9

Prompts for text classification - Prompts for summarization - Prompts for translation and language task Prompts for code generation and completion - Reasoning and logic through prompting - Multimodal prompting (text + image, text + code) - Domain-specific prompt tailoring (finance, healthcare, etc.) - Data augmentation ,creation using prompts - Automated data labeling using LLMs.

UNIT IV TOOLS, FRAMEWORKS, AND EVALUATION 9

Overview of prompt engineering platforms and APIs - OpenAI Playground and similar interfaces - Prompt management and versioning tools - Automation for batch prompt testing - Metrics for evaluating prompt effectiveness - A/B testing and experiment design - Human-in-the-loop evaluation methods - Iterative prompt development life cycle - Open-source frameworks and libraries.

UNIT V CHALLENGES, ETHICS, AND FUTURE DIRECTIONS 9

Bias in prompts and model outputs - Robustness ,reliability issues in prompting - Adversarial prompts ,prompt injection attacks–Transparency, explainability in prompt-based systems - Ethical frameworks – Legal,privacy considerations - Automated ,programmatic prompt generation - Deployment of prompt-engineered solutions in production - Emerging next-generation prompt Engineering.

TOTAL PERIODS 45

COURSE OUTCOMES		
At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	describe the fundamentals and key concepts of prompt engineering.	Understanding (K2)
CO2	construct effective prompts for large language model tasks.	Analyzing (K4)
CO3	apply prompt engineering principles to practical AI applications.	Applying (K3)
CO4	evaluate frameworks, tools, and prompt optimization strategies.	Analyzing (K4)
CO5	analyze ethical, societal, and emerging trends in prompt engineering.	Analyzing (K4)

TEXTBOOKS

1. Bruce Hartpence, IPSec Virtual Private Network Fundamentals, Cisco Press, 2nd Edition, 2018.
2. Richard Deal, Practical VPNs: Building and Integrating Virtual Private Networks, 3rd Edition, Addison-Wesley Professional, 2018.

REFERENCES

1. Liu, P. et al. (2023). Pre-train, Prompt, and Predict: A Systematic Survey of Prompting Methods in Natural Language Processing. ACM Computing Surveys.
2. Brown, T. et al. (2020). Language Models are Few-Shot Learners. NeurIPS.
3. Davies, Richard. (Forthcoming, Early Access 2025). Prompt Engineering in Practice. Manning Publications.
4. Focuses on hands-on skills for prompt authoring, prompt design patterns, retriever-augmented generation (RAG), and prompt evaluation.

CO-PO MAPPING :

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	-	2	2	3	3

CY23351	FOUNDATIONS OF VIRTUAL REALITY	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	impart the fundamental aspects and principles of AR/VR technologies.
2.	know the hardware and software components in AR/VR enabled applications.
3.	learn about the graphical processing units and their architectures.
4.	gain knowledge about AR/VR application development.
5.	know the technologies involved in the development of AR/VR based applications.

UNIT I **INTRODUCTION** 9

Introduction to Virtual Reality and Augmented Reality Technologies – Introduction to Trajectories and Hybrid Space-Three I's of Virtual Reality – Virtual Reality Vs 3D Computer Graphics – Benefits of Virtual Reality – Components of VR System – 3D Position Trackers – Types of Trackers – Navigation and Manipulation Interfaces – Gesture Interfaces – Types of Gesture Input Devices – Output Devices – Graphics Display – Human Visual System – Personal Graphics Displays – Large Volume Displays – Sound Displays – Human Auditory System.

UNIT II **VR MODELING** 9

Modeling – Geometric Modeling – Virtual Object Shape – Object Visual Appearance – Kinematics Modeling – Transformation Matrices – Object Position – Transformation Invariants –Object Hierarchies – Viewing the 3D World – Physical Modeling – Collision Detection – Surface Deformation – Force Computation – Force Smoothing and Mapping – Behavior Modeling – Model Management.

UNIT III **VR PROGRAMMING** 9

VR Programming – Toolkits and Scene Graphs – World Toolkit – Java 3D – Comparison of World Toolkit and Java 3D.

UNIT IV **APPLICATIONS** 9

Human Factors in VR – Methodology and Terminology – VR Health and Safety Issues – VR and Society-Applications of VR in Education, Arts, Entertainment, Business, Medical field, Military – Emerging VR Applications – VR Applications in Manufacturing, Robotics, Information Visualization.

UNIT V **AUGMENTED REALITY** 9

Introduction to Augmented Reality-Computer vision for AR-Interaction-Modeling and Annotation-Navigation-Wearable devices.

TOTAL PERIODS 45

COURSE OUTCOMES

At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	understand the basic concepts of AR and VR.	Understanding (K2)
CO2	explain the tools and technologies related to AR/VR.	Applying (K3)

CO3	know the working principle of AR/VR related Sensor devices.	Analyzing (K4)
CO4	analyze the design of various models using modeling techniques.	Analyzing (K4)
CO5	explain AR/VR applications in different domains.	Analyzing (K4)

TEXT BOOKS

1. Charles Palmer, John Williamson, ―Virtual Reality Blueprints: Create compelling VR experiences for mobile, Packt Publisher, 2018.
2. Dieter Schmalstieg, Tobias Hollerer, ―Augmented Reality: Principles & Practice‖, Addison Wesley, 2016.

REFERENCES

1. John Vince, ―Introduction to Virtual Reality‖, Springer-Verlag, 2004.
2. William R. Sherman, Alan B. Craig: Understanding Virtual Reality – Interface, Application, Design‖, Morgan Kaufmann, 2003.
3. Sumit Badotra, Sarvesh Tanwar, Ajay Rana, Nidhi Sindhwani, Ramani Kannan, ―Handbook of Augmented and Virtual Reality‖, De Gruyter, 2023.
4. Srushtika Neelakantam, Tanay Pant, ―Learning Web-based Virtual Reality: Build and Deploy Web-based Virtual Reality Technology Edition 1, Apress, 2017.

CO-PO MAPPING :

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	-	2	2	3	3

CY23352	SECURITY IN EMBEDDED SYSTEMS	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	identify the architecture and features of 8051.
2.	study the design process of an embedded system.
3.	understand the real – time processing in an embedded system.
4.	learn the architecture and design flow of IoT.
5.	build an IoT based system.

UNIT I	8051 MICROCONTROLLERS	9

Microcontrollers for an Embedded System – 8051 – Architecture – Addressing Modes – Instruction Set – Program and Data Memory – Stacks – Interrupts – Timers/Counters – Serial Ports – Programming.

UNIT II	EMBEDDED SYSTEMS	9

Embedded System Design Process – Model Train Controller – ARM Processor – Instruction Set Preliminaries – CPU – Programming Input and Output – Supervisor Mode – Exceptions and Trap – Models for programs – Assembly, Linking and Loading – Compilation Techniques – Program Level Performance Analysis.

UNIT III	PROCESSES AND OPERATING SYSTEMS	9

Structure of a real – time system – Task Assignment and Scheduling – Multiple Tasks and Multiple Processes – Multirate Systems – Pre emptive real – time Operating systems – Priority based scheduling – Interprocess Communication Mechanisms – Distributed Embedded Systems – MPSoCs and Shared Memory Multiprocessors – Design Example – Audio Player, Engine Control Unit and Video Accelerator.

UNIT IV	IOT ARCHITECTURE AND PROTOCOLS	9

Internet of Things – Physical Design, Logical Design – IoT Enabling Technologies – Domain Specific IoTs – IoT and M2M – IoT System Management with NETCONF – YANG – IoT Platform Design – Methodology – IoT Reference Model – Domain Model – Communication Model – IoT Reference Architecture – IoT Protocols - MQTT, XMPP, Modbus, CANBUS and BACNet.

UNIT V	IOT SYSTEM DESIGN	9

Basic building blocks of an IoT device – Raspberry Pi – Board – Linux on Raspberry Pi – Interfaces – Programming with Python – Case Studies: Home Automation, Smart Cities, Environment and Agriculture.

	TOTAL PERIODS	45

COURSE OUTCOMES		
At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	explain the architecture and features of 8051.	Applying (K3)
CO2	describe the model of an embedded system.	Analyzing (K4)
CO3	list the concepts of real time operating systems.	Analyzing (K4)
CO4	understand the architecture and protocols of IoT.	Analyzing (K4)
CO5	Illustrate the design concepts of an IoT based system.	Analyzing (K4)

TEXTBOOKS

1. Marilyn Wolf, Computers as Components – Principles of Embedded Computing System Design, Third Edition, Morgan Kaufmann, 2002.
2. Arshdeep Bahga, Vijay Madisetti, Internet – of- Things – A Hands-on Approach, Universities Press, 2005.

REFERENCES

1. Mohammed Ali Mazidi, Janice Gillispie Mazidi, Rolin D.McKinlay, The 8051 Microcontroller and Embedded Systems Using Assembly and C, Second Edition, Pearson Education, 2008.
2. Mayur Ramgir, Internet – of – Things, Architecture, Implementation and Security, First Edition, Pearson Education, 2020.
3. Lyla B.Das, Embedded Systems: An Integrated Approach, Pearson Education 2003.
4. Jane.W.S .Liu, Real – Time Systems, Pearson Education, 2003.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	-	2	2	3	3

CY23353	QUANTUM CRYTOGRAPHY	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	impart the fundamental aspects and principles of Quantum Cryptography.
2.	know the principles of quantum key distribution protocols.
3.	learn about the quantum communication methods.
4.	gain knowledge about device independent quantum cryptography.
5.	know the technologies involved in quantum cryptography for secure networks.

UNIT I **FUNDAMENTALS OF QUANTUM CRYPTOGRAPHY** 9

Historical Background and Motivation, Basics of Quantum Mechanics for Cryptography, Dirac Notation and Linear Algebra, Qubits and Quantum States, Density Operators and Entanglement, Quantum Operations and Channels, Quantum Information Theory, Entropy Measures: Shannon, von Neumann, Min/Max, Smooth Entropy.

UNIT II **QUANTUM KEY DISTRIBUTION PROTOCOLS** 9

Principles of Quantum and Classical Cryptography, Security in Quantum Communication, The BB84 Protocol, The B92 Protocol, Six-State and Ekert Protocols, Finite-Key Security and Security Proofs, Data Compression and Error Correction in QKD, Practical Implementation of QKD,Experiments.

UNIT III **ADVANCED AND MULTIPARTY QUANTUM COMMUNICATION** 9

Multipartite QKD: Introduction- Quantum Conference Key Agreement (CKA)- Multipartite BB84 Protocol-Security of CKA: Definitions and Proofs-Experimental Realizations of CKA- QKD with Imperfect Devices- Decoy-State Methods- Measurement-Device-Independent QKD- Practical Security of QKD with Real-World Devices.

UNIT IV **DEVICE-INDEPENDENT AND NEXT-GENERATION QUANTUM CRYPTOGRAPHY** 9

Device-Independent Quantum Cryptography (DIQKD) Overview- Bell's Theorem and Bell Inequalities-Quantum, Local, No-Signaling, and Causal Correlations-Security Proofs for DIQKD-Multipartite Device-Independent Protocols-Twin-Field QKD: Principles and Protocols-Twin-Field QKD: Error Rates and Secret Key Rates-Quantum Key Distribution Networks and Quantum Internet-Performance Assessment and Fundamental Limits.

UNIT V **QUANTUM CRYPTOGRAPHY IN CYBER SECURITY & FUTURE APPLICATIONS** 9

Quantum Cryptography vs. Classical Attacks-Post-Quantum Cryptography: Challenges and Threats-Integration with Modern Cyber Security Infrastructure- Quantum Machine Learning Applications in Security- Commercialization and Standardization- Quantum Cryptography for Secure Networks-Future Trends in Quantum Cyber Security- Open Challenges and Research Directions.

	TOTAL PERIODS	45

COURSE OUTCOMES		
At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	understand the basic concepts of Quantum Cryptography.	Understanding (K2)
CO2	explain the principles of quantum key distribution protocols.	Applying (K3)
CO3	know the principles of quantum communication methods.	Analysing (K4)
CO4	analyze about device independent quantum cryptography.	Analysing (K4)
CO5	explain the technologies in quantum cryptography for secure networks.	Analysing (K4)

TEXTBOOKS

1. Quantum Science and Technology, by Raymond Lalamme , Gaby Lenhart Sophia ,Daniel Lidar,1st edition 2021,Springer Publications.
2. Introduction To Quantum Cryptography,Vidick and Wehner,Cambridge University Press,1st edition,2024.

REFERENCES

1. Modern Cryptography Volume 2: Post-Quantum Cryptography Zhiyong Zheng , Kun Tian , Fengxia Liu,Springer; 1st ed. 2023 edition.
2. Introduction to Modern Cryptography, Mihir Bellare and Phillip Rogaway, University of California publishers; eBook (Online Edition).
3. Quantum Computing: An Applied Approach Second Edition 2021, by Jack D.Hidary,Springer.
4. Learn Quantum Computing with Python and IBM Quantum: Write your own practical quantum programs with Python 2nd ed. Edition,by Robert Loredo (Author), Packt Publishing,2025.

CO-PO MAPPING :

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	-	2	2	3	3

CY23354	**ALGORITHIMIC GAME THEORY**	**3**	**0**	**0**	**3**

COURSE OBJECTIVES

To enable the students

1.	understand the core concepts and components involved in game development.
2.	explore game engines, design principles, and development workflows.
3.	implement 2D and 3D game mechanics using scripting and visual tools.
4.	apply animation, audio, UI/UX design and physics for interactive gameplay.
5.	evaluate deployment, monetization, and testing strategies in game production.

UNIT I **INTRODUCTION TO GAME DEVELOPMENT** **9**

Introduction to Game Development – History and Evolution of Games – Game Genres and Platforms – PC, Console, Mobile, Web – Game Development Lifecycle – Pre-production, Production, Post-production – Game Engines – Unity, Unreal, Godot – Game Design Document (GDD) – Elements and Importance – Game Loop Architecture – Update, Render, Physics – Game Assets – 2D/3D Models, Textures, Sprites – Game Development Tools – IDEs, Asset Stores, Repositories –Zero sum and general sum games.

UNIT II **2D AND 3D GAME DEVELOPMENT** **9**

2D Game Development – Coordinate Systems and Object Placement – Sprites and Tile maps -2D,3D Physics and 2D,3D animation- NavMesh and Pathfinding Algorithms Collisions, Rigid Bodies, Gravity – Camera and Viewport Handling – Parallax Effects – Scripting with C# in Unity – Mono Behaviour, Events, Object Pooling Optimization for 2D – UI Development – 2D Audio Integration- Importing and Managing 3D Assets.

UNIT III **ALGORITHIMS IN GAME DEVELOPMENT** **9**

Minmax strategies, Nash equilibrium-Yao's Lemma, Special Classes Games-Potential Games, Local Search Complexity Classes: FNP, TFNP, PPAD Correlated Equilibrium, Coarse Correlated Equilibrium, Multiplicative Weight No Regret Dynamics, No Swap Regret.

UNIT IV **ADVANCED GAME DESIGN THEORY** **9**

Game Audio – Music Design- Advanced UI – Game States – Saving Game Progress – PlayerPrefs, JSON/XML – Multiplayer Basics –Debugging and Profiling in Unity –Game Testing; Bayesian Games, Extensive Form Games, Mechanism Design Gibbard Satterwaite Theorem, Quasi-Linear Environment VCG Mechanism, Knapsack Mechanism Stable Matching, House Allocation.

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
27/12/24
★ AUTONOMOUS ★

UNIT V	GAME DEPLOYMENT ANDS INDUSTRY TRENDS	9

Game Publishing Platforms – Steam, Play Store, App Store – Monetization Models – Ads, In-app Purchases, Subscriptions – Version Control for Games – Git, LFS, Unity Collab – Game Analytics – Player Behavior, Heatmaps – Legal Aspects – Copyright, Licensing, Game Ratings – Marketing and Community Building for Games – Post-Launch Support and Patch Management – Trends in Game Development – AR/VR, Cloud Gaming – Career Paths in the Game Industry – Indie vs AAA.

TOTAL PERIODS 45

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	understand the process and tools used in modern game development.	Understanding (K2)
CO2	apply programming and scripting to build interactive games.	Applying(K3)
CO3	implement animations, audio, UI/UX features, and physics engines.	Applying(K3)
CO4	analyze performance, input, and design considerations in gameplay.	Analyzing (K4)
CO5	evaluate publishing, testing, and monetization strategies for games.	Analyzing (K4)

TEXTBOOKS

1. Nisan, Roughgarden, Tardos, Vazirani,Algorithimic Game Theory, Cambridge University, 2007.
2. Jeremy Gibson Bond, "Introduction to Game Design, Prototyping, and Development", Pearson, 2nd Edition, 2017.

REFERENCES

1. David Nixon, "Learning C# by Developing Games with Unity 2021", Packt Publishing, 2021.
2. Alan Thorn, "Mastering Unity Scripting", Packt Publishing, 2016.
3. William Sherif, "Learning Unity 2D Game Development by Example", Packt Publishing, 2015.
4. Mike Geig, "Unity Game Development Cookbook", O'Reilly Media, 2021.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	3	3	2	2	2	2	-	-	-	-	1	1	2	2
CO2	3	3	2	2	2	2	-	-	-	-	1	1	2	2
CO3	3	3	2	2	2	2	-	-	-	-	2	2	2	2
CO4	3	3	3	2	2	2	-	-	-	-	2	2	2	2
CO5	3	3	3	2	2	2	[illegible]	[illegible]	[illegible]	[illegible]	2	2	2	2

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
7/2/25
AUTONOMOUS

CY23355	INTRODUCTION TO INDUSTRY 4.0 AND IIOT	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1. impart basic idea in Industry 4.0.
2. gain knowledge of designing Industrial 4.0 Systems for various application.
3. learn the design and analysis of Industry 4.0 systems for Energy and smart vehicles.
4. explore customization in Industry 4.0 to enable more customization in manufacturing.
5. know about supply chain management in Industry 4.0 to improve supply chain management.

UNIT I	INTRODUCTION TO INDUSTRY 4.0 AND IIoT	9

Introduction- Historical Context- General framework- Application areas- Dissemination of Industry 4.0 and the disciplines that contribute to its development-Artificial intelligence- The Internet of Things and Industrial Internet of Things-Additive manufacturing- Robotization and automation-Current situation of Industry 4.0,.Industry 4.0 to Industry 5.0 Advances, Industry 4.0: Globalization and Emerging Issues, The Fourth Revolution, LEAN Production Systems, Smart and Connected Business Perspective, Smart Factories.

UNIT II	INDUSTRY 4.0 AND CYBER PHYSICAL SYSTEM	9

Cyber Physical Systems and Next Generation Sensors, Collaborative Platform and Product Lifecycle Management, Augmented Reality and Virtual Reality, Artificial Intelligence, Big Data and Advanced Analysis -Cybersecurity in Industry 4.0, Basics of Industrial IoT: Industrial Processes- Industrial Sensing & Actuation, Industrial Internet Systems.

UNIT III	SMART ENERGY SOURCES	9

IIoT-Introduction, Industrial IoT: Business Model and Reference Architecture: IIoT-Business Models-- IIoT Reference Architecture-Industrial IoT- Layers: IIoT Sensing- IIoT Processing-IIoT Communication-Industrial IoT- Layers: IIoT Communication- IIoT Networking.

UNIT IV	SMART GRID	9

Industrial IoT: Big Data Analytics and Software Defined Networks: IIoT Analytics - Introduction, Machine Learning and Data Science - R and Julia Programming, Data Management with Hadoop-Industrial IoT: Big Data Analytics and Software Defined Networks: SDN in IIoT- Data Center Networks, Industrial IoT: Security and Fog Computing: Cloud Computing in IIoT.

UNIT V	SMART APPLICATIONS	9

Security and Fog Computing - Fog Computing in IIoT, Security in IIoT-Industrial IoT- Application Domains: Factories and Assembly Line, Food Industry- Application Domains: Healthcare, Power

Plants,Inventory Management & Quality Control, Plant Safety and Security (Including AR and VR safety applications), Facility Management- Industrial IoT Application Domains.

	TOTAL PERIODS	45

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	explain the current situation of industry 4.0 and IIoT.	Applying (K3)
CO2	characterize Cyber Physical System in any domain.	Analyzing (K4)
CO3	design software to measure the energy spent and track the electric vehicles.	Analyzing (K4)
CO4	define smart grid on the context of industry 4.0.	Analyzing (K4)
CO5	outline the problems and solutions of self-driving cars.	Analyzing (K4)

TEXTBOOKS

1. Jean-Claude André, —Industry 4.0, Wiley- ISTE, July 2009.
2. Diego Galar Pascual, Pasquale Daponte, Uday Kumar, —Handbook of Industry 4.0 and SMART Systems,Taylor and Francis,2020

REFERENCES

1. Hossam A. Gabbar, —Smart Energy Grid Engineering‖, Academic Press, 2007.
2. Mini S. Thomas, John Douglas McDonald, —Power System SCADA and Smart Grids‖, CRC Press, 2007.
3. Pengwei Du and Ning Lu, —Energy storage for smart grids: planning and operation for renewable and variable energy resources (VERs), Academic Press, 2008.
4. Dr. Amit Mehta, Mr. Jay Bulani, Mr. Vivek Wasalwar, Dr. Naveen Kumar Verma, Introduction to Industry 4.0", Taran Publication, 2024.

CO-PO MAPPING :

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's

(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	3	3	3	3
CO5	3	3	3	3	3	3	-	-	-	-	3	3	3	3

CY23356	DIGITAL TWINS	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1. learn the fundamental concepts of Digital Twins.
2. gain knowledge about digital twin prototypes and the design of use cases.
3. understand the key technologies behind Digital twins.
4. know the emerging technologies and applications in digital twins.
5. observe the Pilot Implementation Scope, Success Metrics behind digital twins.

UNIT I FUNDAMENTALS OF DIGITAL TWINS 9

Origin of Digital Twin -types of digital twins: Discrete, Composite, Product vs Facility, Simulation vs Operational)- key characteristics- Digital Thread vs Digital Twin-Industry use of Digital twins-Features of Digital twins and vision-The value proposition of digital twins- Identifying Opportunities Using Value-at-Stake and Pareto Analysis; Planning Digital Twins: expected business outcomes- Organizational, Technological, and Cultural Factors ; Digital Technologies, Ecosystem, Talent Needs , Visualization, Feedback Loops, and Low-Code/No-Code Approaches, Readiness Evaluation and Prioritization Matrix.

UNIT II DESIGNING AND BUILDING DIGITAL TWIN PROTOTYPES 9

Evaluating and Shortlisting Use Cases- Sector-specific Considerations (Conglomerates, Public Sector, ISVs, etc.)- Defining Roles, Responsibilities, and Agile Interaction Models- Project and Solution Planning Frameworks- Validating Problem Statements and Business Processes- Technology Stack and Infrastructure Setup; Asset Administration Shell and Digital Twin Definition Language (DTDL); Platform Selection: IoT, BPM, Analytics, Application Layers; Microsoft Azure Digital Twins Setup, Configuration, Data Considerations, and Architecture Planning, Prototype Development and Testing, Business Validation.

UNIT III DIGITAL TWIN TECHNOLOGIES 9

Key Technologies of Digital Twins, Generic Deployment Methodology, Automated Inference of Simulators Federated Analytics: Concept and Importance, Federated Analytics: Edge and Cloud Integration, Federated Analytics: Data Aggregation Techniques, Federated Analytics: Privacy and Security Aspects, Blockchain-Based Digital Twin Design, Physics-Based Digital Twins.

UNIT IV APPLICATIONS OF DIGITAL TWINS 9

Applications in Management: Lifecycle and Predictive Maintenance: Applications in Management: AI-Enhanced Knowledge Systems, Applications in Management: Digital Twin Maturity and Barriers, Applications in Management: Business Model Innovation, Applications in Industry: Smart Manufacturing, Applications in Industry: Cognitive Digital Twins, Applications in Industry: Ultraprecision Engineering, Applications in Industry: Logistics and Automation, Applications in Industry: Diagnostics and Control Systems.

UNIT V	DEPLOYMENT, VALUE REALIZATION, AND ENHANCEMENTS	9

Pilot Rollout and Full Deployment, Functional Testing of Infrastructure and Applications, Pilot Implementation Scope, Success Metrics, and Phases, Presenting Results and Scaling to Full Deployment, Case Study: Wind Farm Deployment; Value Tracking and Business Impact Value Proposition Tracking Across Stakeholders Return on Investment (RoI) and Digital Business Models Strategic Business Transformation through Digitalization.

	TOTAL PERIODS	45

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	understand the fundamental concepts of Digital Twins.	Understanding (K2)
CO2	analyze the design of use cases.	Analyzing (K4)
CO3	describe the key technologies behind Digital twins.	Applying (K3)
CO4	explain emerging technologies and applications in digital twins.	Analyzing (K4)
CO5	depict the Pilot Implementation Scope, Success Metrics behind digital twins.	Analyzing (K4)

TEXTBOOKS

1. Toh, C. K., "Ad Hoc Mobile Wireless Networks: Protocols and Systems", Pearson Education, 2016.
2. Jaydip Sen, "Security in Wireless Ad Hoc and Sensor Networks", InTech Open, 2019.

REFERENCES

1. Shanzhi Chen, "Ad Hoc and Sensor Networks: Security and Privacy", World Scientific, 2016.
2. Subir Kumar Sarkar, "Ad Hoc Mobile Wireless Networks: Principles, Protocols and Applications", CRC Press, 2016.
3. Praphul Chandra, "Securing Wireless Ad Hoc Networks", Wiley, 2020.
4. Mohammad S. Obaidat, "Handbook of Green Information and Communication Systems", Academic Press, 2016.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	1	1	2	2	2	2	-	-	-	-	1	1	3	3
CO2	1	1	2	2	2	2	-	-	-	-	1	1	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	[illegible]	[illegible]	[illegible]	-	2	2	3	3

CY23357	MANET AND SENSOR NETWORKS	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1. understand the fundamentals and architecture of Mobile Ad Hoc Networks (MANETs).
2. identify various threats and vulnerabilities specific to MANETs.
3. explore secure routing protocols and intrusion detection mechanisms for MANETs.
4. analyze cryptographic and trust-based security approaches for MANET environments.
5. evaluate MANET security frameworks and research trends.

UNIT I INTRODUCTION TO MANET ARCHITECTURE 9

Introduction to MANET – Characteristics and Applications – MANET Architecture and Communication Models – Routing Challenges – Mobility, Topology Changes – Routing Protocols – Proactive, Reactive, Hybrid – AODV, DSR, OLSR Protocols Comparisons – Limitations of MANET Routing – Energy, Bandwidth, Latency – Routing Metrics – Quality of Service (QoS) in MANETs – Use Cases of MANETs in Tactical and Emergency Networks.

UNIT II SECURITY CHALLENGES IN MANET 9

Security Challenges in MANET – Overview – Types of Attacks – Black Hole, Gray Hole, Wormhole – Rushing, Sybil, and Byzantine Attacks – Security Requirements – Confidentiality, Integrity, Authentication – Vulnerabilities in MANET Routing Protocols – Security Taxonomy for MANET Protocols – Adversarial Models and Attack Surfaces – Simulation Tools for MANET Security Testing – Attacks and Failures.

UNIT III SECURE ROUTING PROTOCOLS 9

Secure Routing Protocols – SAODV, ARAN, SEAD – Trust-based Routing Mechanisms – Key Management in MANET – Challenges and Solutions – Lightweight Cryptography for MANETs – Secure Neighbor Discovery and Link Authentication – Energy-efficient Secure Communication – Privacy Preservation in MANET – Group Key Agreement Protocols – Comparison of Secure Routing Protocols.

UNIT IV INTRUSION DETECTION SYSTEMS (IDS) AND TRUST MODELS 9

Intrusion Detection Systems (IDS) for MANET – Signature-based vs Anomaly-based IDS – IDS Architectures – Distributed, Cooperative, Hierarchical – Watchdog and Pathrater Techniques – Trust and Reputation Models – Misbehavior Detection and Isolation – IDS Challenges in MANET – Mobility, Energy, False Positives – Secure Data Aggregation and Forwarding – Simulation and Evaluation of IDS in MANET.

UNIT V EMERGING TECHNOLOGIES 9

Security Frameworks and Architectures for MANET – Cross-layer Security Approaches – Blockchain Applications in MANET Security – AI/ML for Intrusion Detection and Routing – Game Theory Applications in MANET Defense – Standardization and Protocol Stacks for Secure MANET – Open Research Challenges and Future Trends – Real-time Secure MANET Implementation Scenarios – Comparison of MANET Security Approaches and Models.

	TOTAL PERIODS	45

COURSE OUTCOMES		
At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	understand the architecture of MANETs.	Understanding (K2)
CO2	analyze security threats and vulnerabilities in MANET environments.	Analyzing (K4)
CO3	apply secure routing protocols and trust models for safe communication.	Applying (K3)
CO4	design intrusion detection solutions tailored for MANETs.	Analyzing (K4)
CO5	explain emerging technologies for MANET security.	Analyzing (K4)

TEXTBOOKS

1. Toh, C. K., "Ad Hoc Mobile Wireless Networks: Protocols and Systems", Pearson Education, 2016.
2. Jaydip Sen, "Security in Wireless Ad Hoc and Sensor Networks", InTechOpen, 2019.

REFERENCES

1. Shanzhi Chen, "Ad Hoc and Sensor Networks: Security and Privacy", World Scientific, 2016.
2. Subir Kumar Sarkar, "Ad Hoc Mobile Wireless Networks: Principles, Protocols and Applications", CRC Press, 2016.
3. Praphul Chandra, "Securing Wireless Ad Hoc Networks", Wiley, 2020.
4. Mohammad S. Obaidat, "Handbook of Green Information and Communication Systems", Academic Press, 2016.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	1	1	2	2	2	2	-	-	-	-	1	1	3	3
CO2	1	1	2	2	2	2	-	-	-	-	1	1	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	-	2	2	3	3

CY23451	ADVANCED DISTRIBUTED SYSTEMS	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the computation and communication models of distributed systems.
2.	illustrate the issues of synchronization and collection of information in distributed systems.
3.	describe distributed mutual exclusion and distributed deadlock detection techniques.
4.	elucidate authentication and fault tolerance mechanisms in distributed systems.
5.	indicate the challenges and solutions in securing distributed systems.

UNIT I BASICS OF DISTRIBUTED COMPUTATIONS 9

Introduction: Definition – Relation to Computer System Components – Motivation – Message -Passing Systems versus Shared Memory Systems – Primitives for Distributed Communication – Synchronous versus Asynchronous Executions – Design Issues and Challenges – Applications; A Model of Distributed Computations, Distributed Executions, Communication Networks – Global State of a Distributed System.

UNIT II SYNCHRONIZATION AND MANAGEMENT 9

Logical Time: A Framework for a System of Logical Clocks – Scalar Time – Vector Time – Physical Clock Synchronization: NTP; Message Ordering and Group Communication: Message Ordering Paradigms – Asynchronous Execution with Synchronous Communication – Synchronous Program Order on Asynchronous System – Group Communication – Causal Order – Total Order; Global State and Snapshot Recording Algorithms: Introduction – System Model and Definitions – Snapshot Algorithms for FIFO Channels.

UNIT III DISTRIBUTED MUTEX AND DEADLOCK 9

Distributed Mutual exclusion Algorithms: Introduction – Preliminaries – Lamport's algorithm – Ricart-Agrawala Algorithm — Token-Based Algorithms – Suzuki-Kasami's Broadcast Algorithm; Deadlock Detection in Distributed Systems: Introduction – System Model – Preliminaries – Models of Deadlocks – Chandy-Misra-Haas Algorithm for the AND model and OR Model.

UNIT IV FAULT TOLERANCE AND AUTHENTICATION 9

Unreliable failure detectors – The consensus problem – Atomic broadcast – A solution to atomic broadcast – An implementation of a failure detector – An adaptive failure detection protocol Authentication: Introduction – Background and Definitions – Protocols based on symmetric cryptosystems– Protocols based on asymmetric cryptosystems – Password-based authentication – Authentication protocol failures – Methodologies for designing self-stabilizing systems – Self stabilization as a solution to fault tolerance – Limitations.

UNIT V	SECURITY MANAGEMENT	9
Security in distributed computing and application: Security threats – security mechanism – security policies – Secure Channels – Secure group communication – Access Control – General Issues – Firewalls – Secure mobile code – Denial of Service – Security Management – Case study: Global Security architecture, Ransomware attacks on distributed systems (eg.healthcare systems).		
	TOTAL PERIODS	**45**

COURSE OUTCOMES

At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	explain the architectural models and communication techniques.	Understanding (K2)
CO2	describe synchronization and coordination algorithms.	Applying (K3)
CO3	implement mutual exclusion and deadlock detection algorithms.	Applying (K3)
CO4	demonstrate fault-tolerant systems and authentication protocols.	Applying (K3)
CO5	analyze distributed security mechanisms, threats and policies.	Analyzing (K4)

TEXTBOOKS

1. Kshemkalyani Ajay D, Mukesh Singhal, ―Distributed Computing: Principles, Algorithms and Systems, Cambridge Press, 2020.
2. Andrew S. Tanenbaum & Maarten van Steen, ―Distributed Systems: Principles and Paradigms‖, Third Edition, Prentice Hall, 2017

REFERENCES

1. George Coulouris, Jean Dollimore, Time Kindberg, ―Distributed Systems Concepts and Design‖, Fifth Edition, Pearson Education, 2017.
2. Liu M L, ―Distributed Computing: Principles and Applications‖, Pearson Education, 2019.
3. Wan Fokkink, ―Distributed algorithms: An intuitive approach‖, MIT Press, 2018.
4. Distributed Systems: An Algorithm Approach, Sukumar Ghosh, Second Edition, CRC Press, 2014.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3					2	2	3	3

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/12/25
★ AUTONOMOUS ★

CY23452	MOBILE AND WIRELESS SECURITY	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1. outline the security challenges and solutions in mobile and wireless communication systems.
2. describe security threats and protection mechanisms in cellular networks and MANETs
3. explore security architectures and threat mitigation strategies in wireless sensor networks.
4. learn about security architecture of wireless networks.
5. understand various security issues of IP based mobile networks and ad hoc networks.

UNIT I SECURITY CHALLENGES IN MOBILE COMMUNICATION 9

Mobile Communication History - Security - Wired Vs Wireless - Security Issues - Security Requirements - Security for Mobile Applications - Advantages and Disadvantages of Application level Security - Security of device, network, and server levels - Application Level Security in Wireless Networks - Application of WLANs - Wireless Threats - Vulnerabilities and Attack Methods over WLANs - Security for 1G and 2G Wi-Fi Applications - Recent Security Schemes for Wi-Fi Applications.

UNIT II MANET AND AD HOC SECURITY 9

Generations of Cellular Networks - Security Issues and attacks in cellular networks - GSM, GPRS, UMTS and 3G security for applications - Security and authentication Solutions - MANETs - Applications - Features - Security Challenges; Security Attacks - External Threats and Internal threats for MANET Applications - Security Solutions; Security in Ad Hoc Networks - Security mechanisms - Auto-configuration.

UNIT III WIRELESS SENSOR NETWORK SECURITY 9

Heterogeneous Wireless network architecture - Heterogeneous network application in disaster management - Security problems and solutions in heterogeneous wireless networks - Attacks on wireless sensor networks and counter measures - Prevention mechanisms: authentication and traffic protection - Centralized and passive intruder detection - Decentralized intrusion detection.

UNIT IV WI-FI SECURITY 9

Wi-Fi Security Dedicated Architectures - Hot spot architecture: captive portals - Wireless intrusion detection systems - Wireless honeypots - Attacks on wireless networks - Security in the IEEE 802.11 ,802.1x , 802.11i - Authentication in wireless networks - Layer 3 security mechanisms.

UNIT V IP-BASED MOBILE NETWORKS AND UBIQUITOUS COMPUTING 9

Security in Next Generation Mobile Networks - The SIP - VoIP - IP Multimedia Subsystem - 4G security - Confidentiality - Security of IP-Based Mobile Networks - Security issues related to mobility - Mobility with MIPv6 - Ubiquitous Computing - Need for Novel Security Schemes for UC Security Challenges for UC - Security Attacks on UC networks - Security solutions for UC.

	TOTAL PERIODS	**45**

COURSE OUTCOMES		
At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	demonstrate the need of security in wireless and mobile network.	Understanding (K2)
CO2	analyze threats and security measures for cellular networks and MANETs.	Analyzing (K4)
CO3	illustrate sensor network security threats mitigation techniques.	Applying (K3)
CO4	examine intrusion detection systems and authentication schemes.	Analyzing (K4)
CO5	relate security protocols in IP-based mobile and ubiquitous computing.	Applying (K3)

TEXTBOOKS

1. Pallapa Venkataram, Satish Babu, "Wireless and Mobile Network Security", Ist Edition, TataMcGraw Hill, 2010.
2. Hakima Chaouchi, Maryline Laurent-Maknavicius, —Wireless and Mobile Network Security‖, 1" Edition, Wiley-ISTE, 2010.

REFERENCES

1. Himanshu Dwivedi, Chris Clark, David Thiel, —Mobile Application Security‖, Mcgraw-hill, 2010.
2. Noureddine Boudriga, —Security of Mobile Communications‖, Auerbach Publications, 2009.
3. Jim Doherty, —Wireless and Mobile Device Security‖, Second Edition, Jones and Bartlett Learning, 2021.
4. James Kempf, "Guide to Wireless Network Security, Springer. Wireless Internet Security - Architecture and Protocols", 1st Edition, Cambridge University Press, 2008.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	1	1	1	1	1	1	-	-	-	1	1	1	3	3
CO2	1	1	1	1	1	1	-	-	-	1	1	1	3	3
CO3	2	2	2	2	2	2	-	-	-	2	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	2	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	2	2	2	3	3

CY23453	CELLULAR NETWORK SECURITY	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the architecture, components, and evolution of 5G networks.
2.	identify key threats, vulnerabilities, and risks associated with 5G systems.
3.	analyze and evaluate security mechanisms in 5G network components and protocols.
4.	explore privacy, authentication, and encryption techniques specific to 5G environments.
5.	design secure 5G systems for emerging technologies and regulatory frameworks.

UNIT I INTRODUCTION TO 5G NETWORKS 9

Evolution from 4G to 5G – key differences and motivations – 5G use cases: eMBB, URLLC, mMTC – 5G NR (New Radio) physical and MAC layer overview – 5G Core Architecture (5GC): AMF, SMF, UPF, NRF – Service-Based Architecture (SBA) and Network Functions – Network Slicing and its security implications – Key enabling technologies: SDN, NFV, MEC in 5G – Deployment options: Non-Standalone (NSA) vs Standalone (SA) – Integration of legacy systems with 5G networks.

UNIT II THREATS IN 5G NETWORKS 9

Threat landscape in 5G – overview – Vulnerabilities in 5G RAN and backhaul – Risks due to virtualization and multi-tenancy – Security challenges in network slicing – Supply chain and hardware security threats – Protocol vulnerabilities and attack surfaces – Denial of Service (DoS) and resource exhaustion attacks – IoT-specific threats in 5G networks – Insider threats and trust management challenges.

UNIT III 5G SECURITY ARCHITECTURE 9

5G security architecture and principles – Mutual authentication mechanisms: 5G-AKA – Role of USIM and SEAF in authentication – Subscription Concealed Identifier (SUCI) and privacy – Key hierarchy and key derivation in 5G – Secure key provisioning and lifecycle – Authentication failure handling and fallback – Security context management and updates – Interworking with EPC (LTE) and non-3GPP Access

UNIT IV DEFENSE FRAMEWORK 9

Privacy challenges in highly dense and dynamic 5G environments – IMSI catching, location tracking and identity disclosure – Legal and regulatory frameworks: GDPR and CCPA compliance – Encryption of user and control plane data – Integrity protection and traffic confidentiality – Data anonymization and pseudonymization – Privacy-preserving identity and access management – Lawful interception: technical and ethical concerns – Secure storage and transmission of user data.

UNIT V THREAT DETECTION and MONITORING 9

Security monitoring and threat detection in 5G – AI/ML-based intrusion detection systems – Blockchain integration for decentralized trust – Secure orchestration of SDN and NFV – Zero Trust security models for 5G – post-quantum cryptography readiness in 5G – Honeypots and deception-based defense – Cloud-native 5G security and edge computing – Roadmap to 6G: anticipated security enhancements.

TOTAL PERIODS 45

COURSE OUTCOMES

At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	understand the components and architecture of 5G networks.	Understanding (K2)
CO2	identify and assess security threats and vulnerabilities in 5G systems.	Analyzing (K4)
CO3	apply authentication and key management protocols in 5G infrastructure.	Applying (K3)
CO4	review privacy concerns and data protection techniques in 5G.	Analyzing (K4)
CO5	differentiate between vulnerability assessment and penetration testing methodologies.	Analyzing (K4)

TEXTBOOKS

1. Madhusanka Liyanage, Ahmed Bux, "Security and Privacy in 5G Networks: Challenges and Solutions", Wiley, 2018.
2. Noureddine Boudriga, "Security of Mobile Communications and Wireless Networks", CRC Press, 2016.

REFERENCE BOOKS

1. Anand R. Prasad, "5G Security: Concepts and Challenges", River Publishers, 2020.
2. Jonathan Rodriguez, "Fundamentals of 5G Mobile Networks", Wiley, 2015.
3. Vasileios Mavroeidis, "5G Security: Concepts and Challenges", Springer, 2021.
4. Syed Rameem Zahid, "Security and Privacy in Next Generation Wireless Networks", Springer, 2022.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's

(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	**PO's**												**PSO's**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	[illegible]	[illegible]	[illegible]	[illegible]	2	2	3	3

CY23454	SECURED NETWORK PROTOCOLS	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	outline the architecture and operation of application layer protocols in modern networks.
2.	understand the functions and significance of Internet protocol suite.
3.	illustrate IP network security mechanisms and mobility support in IP-based systems.
4.	discuss the principles associated with wireless and mobile networks.
5.	recognize wireless personal area network technologies and protocols.

UNIT I APPLICATION LAYER PROTOCOLS 9

Network communication architecture and protocols – TCP/IP – HTTP – SHTTP – LDAP – MIME – POP& POP3 – RMON – SNTP – SNMP – Presentation Layer Protocols – Light Weight Presentation Protocol – Session layer protocols – RPC protocols – Transport layer protocols – ITOT – RDP – RUDP – TALI – TCP/UDP – Compressed TCP.

UNIT II NETWORK AND DATALINK LAYER PROTOCOLS 9

Network layer Protocols – Routing protocols – Border gateway protocol – Exterior gateway protocol – Internet protocol IPv4 – IPv6 – Internet message control protocol– IRDP – ARP and InARP – IPCP and IPv6CP – RARP – SLIP – Wide area network protocols – ATM protocols – Broadband access protocols – Point to point protocols.

UNIT III IP NETWORK SECURITY AND MOBILITY SUPPORT 9

Models of traffic demands – Optimal routing with multi-protocol label switching – Link-weight optimization with open shortest path – Extended shortest path-based routing schemes – IP Network Security – Detection of Denial–of–Service attack – IP Traceback – Mobility support for IP – Mobility management approaches – Security threats related to IP mobility – Mobility support in IPv6 – Reactive Versus Proactive mobility support – Relation to multi-homing – Protocols supplementing mobility.

UNIT IV NETWORK ENVIRONMENT AND PROTOCOLS 9

ETHERNET protocols – VLAN protocols – Wireless LAN protocols – Metropolitan area network protocol – Storage area network and SAN Protocols – FDMA, WIFI and WIMAX protocols – Security issues – Mobile IP – Mobile support protocol for IPv4 and IPv6 – Resource reservation protocol – Multi-casting protocol – BGMP – IGMP – MSDP.

UNIT V WIRELESS PERSONAL AREA NETWORK 9

IEEE 802.15 and Bluetooth – WPAN communication protocols – IEEE 802.16 – IEEE 802.16A – WCDMA – Services – WCDMA products – Networks – Device addressing – System addressing – Radio signaling protocol – Multimedia signaling protocol.

TOTAL PERIODS 45

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/7/25
AUTONOMOUS

COURSE OUTCOMES		
At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	distinguish protocols across the application, presentation, session, and transport layers.	Understanding (K2)
CO2	explain the functionalities of network and data link layer protocols.	Understanding (K2)
CO3	analyze IP network security threats and mobility management protocols.	Applying (K3)
CO4	examine modern LAN, WLAN, MAN, and SAN environments.	Analyzing (K3)
CO5	identify WPAN standards and their communication protocols.	Applying (K3)

TEXTBOOKS

1. Jielin Dong, —Networks Protocols Handbook‖, Fourth edition, Javvin Technologies, 2007.
2. Vijay K.Garg, —Wireless Communications and Networking‖, Morgan Kaufmann, 2019

REFERENCES

1. Rolf Oppliger —SSL and TSL: Theory and Practice‖, Arttech House, 2009.
2. Jessica Fridrich, —Steganography in Digital Media: Principles, Algorithms, and Applications‖, Cambridge university press, 2010.
3. Lawrence Harte, —Introduction to CDMA – Network services Technologies and Operations‖, Althos Publishing, 2012.
4. Lawrence Harte, —Introduction to WIMAX‖, Althos Publishing, 2006.

CO–PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3–Strong, 2–Medium, 1–Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	-	2	2	3	3

CY23455	SOFTWARE SECURITY	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1. comprehend the need for Software Security and the threats to software security.
2. realize Secure software architecture design and coding.
3. gain basic knowledge on web security principles.
4. acquire risk management and mitigation of risk in software development.
5. learn testing types and strategies for secure software.

UNIT I THREATS TO SOFTWARE SECURITY 9

Introduction to software Security- Software assurance and software security - Threats to Software security , Insecurity- detecting software security defects early - Managing Secure software development - Risk Management framework - Software security practices in the development lifecycle - Properties of secure software - Building a security assurance case ,Incorporating assurance cases into SDLC -Security Requirements Engineering .

UNIT II SECURE SOFTWARE ARCHITECTURE AND DESIGN 9

Software security practices for architecture and design - Software security knowledge - Software characterization - Threat analysis - Architectural vulnerability assessment - Risk likelihood- Risk Impact Determination - Risk Mitigation Planning - Security principles, guidelines and attack patterns - Secure coding and testing - Code analysis - vulnerabilities - Source code review - Coding practices.

UNIT III CLIENT AND SERVER-SIDE SECURITY 9

Browser Security Principles -Client-side vs. server-side - Exceptions to the same origin policy- Cross-site scripting, defense, request forgery - CSRF defense - Prevent XSS -SQL Injection, effects, Blind SQL Injection - Database Permissions - Stored Procedure Security - Application with Client-side Security, server-side security.

UNIT IV RISK MANAGEMENT 9

Risk Management framework - Five stages of activity- Applying the RMF- business context - Gathering the artifacts, conducting project research, business and technical risk, risk questionnaires, interviewing , Analyzing the research and interview data - technical risks - artifacts - ranking the risk , risk data - business and technical peer review - risk mitigation strategy - Risk Management .

UNIT V SOFTWARE SECURITY TESTING 9

Introduction to Software Security testing - software testing vs software security testing - Functional testing - Risk-based testing - Security testing consideration throughout the SDLC - Unit testing - Testing Libraries, Executable files- Integration testing - System Testing - Security Failures – Errors - Attacker Behaviour and perspectives for Security Analysis -Identity Management and Software development, Case study on Software security Testing.

TOTAL PERIODS 45

COURSE OUTCOMES		
At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	identify security threats and issues in software.	Understanding (K2)
CO2	prepare software by incorporating security principles.	Applying (K3)
CO3	predict the issues in web and database security.	Applying (K3)
CO4	apply risk management strategies and risk mitigation strategies in software development.	Applying (K3)
CO5	use testing strategies for secure software development.	Analyzing (K4)

TEXTBOOKS

1. Gary McGraw, "Software Security–A guide for Project Managers", Addison-Wesley , Professional,2008,ISBN-13:978-0321509178
2. Andrew Homan, "" Web Application Security Exploitation and Countermeasures for Modern Web Applications", O'Reilly Media, Inc, First edition,2020

REFERENCES

1. JamesM.Helfrich, "Security for Software Engineers", CRC Press, Taylor and Francis Group, 2019.
2. "Security Engineering: A Guide to Building Dependable Distributed Systems," Ross Anderson, Wiley, 2020.
3. James Ransome, Anmo lMisra," Core Software Security", CRC Press, Taylor, and Francis Group, 2014
4. "Secure Coding: Principles and Practices," Mark Graff and Kenneth van Wyk, O'Reilly Media, 2003.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	**PO's**												**PSO's**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	-	2	2	3	3

CY23456	INTRUSION DETECTION AND PREVENTION	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	describe the fundamentals of intrusion detection systems and network attacks.
2.	differentiate between signature-based, anomaly-based and hybrid detection techniques.
3.	interpret Data Collection and Theoretical Foundation of Detection and their evasion methods.
4.	examine Alert Management and Correlation techniques for intrusion detection and evaluate their effectiveness.
5.	building and Training intelligent IDS and Ethics, Challenges, and the Future in AI Security

UNIT I **FOUNDATIONS AND INTRODUCTION** 9

Foundations of Intrusion Detection Systems: Types of IDS - IDS Architectures - Deployment Scenarios - IDS Tools and Frameworks - IDS Evaluation Metrics. Network Attacks: Attack Taxonomies, Probes, IPSweep and PortSweep, NMap, MScan, SAINT, Satan, Privilege Escalation Attacks, Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks, Worms Attacks, Routing Attacks

UNIT II **DETECTION APPROACHES** 9

Detection Approaches: Misuse Detection: Pattern Matching, Rule–based Techniques, State–based Techniques, Techniques based on Data Mining. Anomaly Detection: Advanced Statistical Models, Rule based Techniques, Biological Models, Learning Models, Specification–based Detection, and Hybrid Detection.

UNIT III **DATA COLLECTION AND THEORETICAL FOUNDATION** 9

Data Collection, Data Collection for Host–Based IDSs, Audit Logs, System Call Sequences and Data Collection for Network–Based IDSs, Theoretical Foundation of Detection, Taxonomy of Anomaly Detection Systems, Fuzzy Logic, Architecture and Implementation, Centralized, Distributed, Intelligent Agents, Mobile Agents and Cooperative Intrusion Detection

UNIT IV **ALERT MANAGEMENT AND CORRELATION** 9

Alert Management and Correlation, Data Fusion, Alert Correlation, Preprocess, Correlation Techniques, Post process, Alert Correlation Architectures, Validation of Alert Correlation System, Cooperative Intrusion Detection, Basic Principles of Information Sharing and Cooperation Based on Goal–tree Representation of Attack Strategies.

UNIT V **ADVANCED TOPICS AND CASE STUDIES** 9

Building and Training Your Own Intelligent IDS: Gathering and Preparing Data - Model Development Pipeline - Integration and Deployment - Post-Deployment Optimization - Ethics, Challenges, and the Future - Ethical Considerations in AI Security - Challenges and Limitations - Future of AI in Cyber Defense.

	TOTAL PERIODS	45

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	learn fundamentals of IDS , architectures, and types of attacks.	Understanding (K2)
CO2	analyze misuse, anomaly & hybrid detection techniques.	Analyzing(K4)
CO3	apply data collection and theoretical IDS foundations	Applying(K3)
CO4	examine alert management and cooperative IDS strategies	Analyzing(K4)
CO5	analyze an end-to-end IDS deployment plan and assess ethical/legal issues.	Analyzing(K4)

TEXTBOOKS

1. Ali A. Ghorbani, Network Intrusion Detection and prevention concepts and techniques, Springer, 2020.
2. Mr. Amit Banwari Gupta Mr. Mohammad Majharul Islam Jabed, —The AI Shield: Defending Against Zero-Day Threats with Intelligent IDS‖, Quill Tech Publications, May 2025.

REFERENCES

1. R. Scarfone & P. Mell, —Guide to Intrusion Detection and Prevention Systems (IDPS), NIST SP 800-94, 2021.
2. R. Bejtlich, —The Practice of Network Security Monitoring,No Starch Press, 2013.
3. T. Lazarevic et al., —A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection, SIAM, 2003.
4. J. Vallentin et al., —Host-Based Intrusion Detection and Response: Architecture and Implementation,Wiley, 2022.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's

(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO5	2	2	2	2	2	2	-	-	-	-	2	2	3	3

CY23457	VIRTUAL PRIVATE NETWORKS	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand VPN fundamentals, architecture, and types.
2.	analyze and implement secure VPN protocols and tunneling.
3.	apply encryption, authentication, and key management techniques in VPNs.
4.	manage, troubleshoot, and optimize VPN deployments in real environments.
5.	explore advanced VPN technologies and emerging trends.

UNIT I	VPN AND NETWORK SECURITY FUNDAMENTALS	9

Overview of VPNs: Concepts and Use Cases - VPN Types: Remote Access, Site-to-Site, Intranet, Extranet - VPN Architecture and Components - Network Security Basics- Common VPN Threats and Vulnerabilities - VPN vs Traditional Network Security - VPN Policies, Compliance, security models.

UNIT II	VPN PROTOCOLS AND TUNNELLING TECHNIQUES	9

PPTP Protocol: Features and Limitations - L2TP and L2TP/IPSec - IPSec Protocol Suite: Architecture and Modes - SSL/TLS VPNs Concepts and Implementation - GRE and MPLS Tunneling Protocols - Comparison: Layer 2 vs Layer 3 VPNs - VPN Protocol Performance and Scalability - Hands-on: Setting up IPSec VPN with open-source tools - VPN Protocol Security Analysis.

UNIT III	VPN SECURITY MECHANISMS	9

Symmetric vs Asymmetric Encryption - Digital Signatures and Certificates - Authentication Methods: Pre-shared Keys, Digital Certificates, EAP - IKEv1 and IKEv2 Key Exchange Protocols - Perfect Forward Secrecy - VPN Traffic Filtering and Access Controls - Anti-Replay and Integrity Checks - VPN Logging and Audit Trails.

UNIT IV	VPN DEPLOYMENT AND MANAGEMENT	9

Designing VPN Architectures for Enterprises -Client and Server Configurations - Integration with Firewalls and IDS/IPS - Performance Tuning and Optimization - Troubleshooting - VPN Traffic and Bandwidth, Failover and Redundancy Techniques - VPN Scalability Challenges .

UNIT V	FUTURE TRENDS AND IMPROVEMENTS	9

Cloud VPNs and VPN-as-a-Service (VPNaaS) - Software-Defined VPNs (SD-VPN) - VPNs for IoT and Mobile Environments - Onion Routing and Tor vs VPN - Quantum-safe, Post-Quantum VPN Technologies - Privacy Enhancements and Anonymity Networks – Legal and Ethical Considerations.

	TOTAL PERIODS	45

COURSE OUTCOMES		
At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	describe VPN fundamentals, architecture, and types.	Understanding (K2)
CO2	analyze and configure VPN protocols and tunneling techniques.	Analyzing (K4)
CO3	apply encryption, authentication, and key management in VPN security.	Applying (K3)
CO4	troubleshoot and optimize VPN deployments effectively.	Analyzing (K4)
CO5	investigate emerging VPN technologies and trends.	Analyzing (K4)

TEXTBOOKS

1. Bruce Hartpence, IPSec Virtual Private Network Fundamentals, Cisco Press, 2nd Edition, 2018.
2. Richard Deal, Practical VPNs: Building and Integrating Virtual Private Networks, 3rd Edition, Addison-Wesley Professional, 2018.

REFERENCES

1. William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson, 2016.
2. Eric Maiwald, Securing Cisco IP Telephony Networks, Cisco Press, 2017.
3. Joseph Steinberg, VPNs Illustrated: Tunnels, VPNs, and IPsec, Addison-Wesley, 2015.
4. Gregory B. White, VPN Security, Packt Publishing, 2019.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	-	2	2	2	2
CO2	2	2	2	2	2	2	-	-	-	-	2	2	2	2
CO3	2	3	3	3	3	3	-	-	-	-	3	3	2	2
CO4	2	3	3	3	3	3	-	-	-	-	3	3	3	3
CO5	2	3	3	3	3	3	-	-	-	-	3	3	3	3

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/8/25
★ AUTONOMOUS ★

CY23551	WEB TECHNOLOGIES	3	0	0	3
COURSE OBJECTIVES					
To enable the students to					
1.	understand different internet technologies.				
2.	learn java-specific web services architecture.				
3.	model web applications using frameworks.				
4.	examine server-side programs using servlets and jsp.				
5.	build web applications.				
UNIT I	**WEBSITE BASICS, HTML 5, CSS 3, WEB 2.0**				9
Web Essentials: Clients, Servers and Communication – The Internet – Web browsers ,servers, URL's, HTTP,FTP,SMTP,TELNET – Web Clients – Web Servers – HTML5 – Tables – Lists – Image – HTML5 control elements – Drag and Drop – Audio – Video controls - CSS3 – Inline, embedded and external style sheets – Rule cascading – Inheritance – Backgrounds – Border Images – Colors – Shadows – Text – Transformations – Transitions – Animations. Bootstrap Framework					
UNIT II	**CLIENT-SIDE PROGRAMMING**				9
Introduction to JavaScript – Core Language Constructs: control structures, functions, scope – JavaScript DOM Model – Event Handlin– Exception Handling & Validation – Built-in Objects & Browser APIs – DHTML with JavaScript (dynamic styling, animations, responsive updates) – JSON Introduction & Syntax (JSON. Parse/stringify, AJAX integration) – Modularization & Function Files – ES6+ Features & Tooling.					
UNIT III	**SERVER-SIDE PROGRAMMING**				9
Java Servlet Architecture: web containers, servlet engines – Servlet Life Cycle– Request & Response Objects – Form GET & POST Actions (parameter retrieval, file upload) – Session Management – Understanding Cookies (creation, security flags) – Filters & Listeners – Database Connectivity - JDBC – Connection Pooling & Data Sources – Error Handling & Security.					
UNIT IV	**PHP and XML**				9
Introduction to PHP – Variables & Data Types – Program Control– Built-in Functions – Form Validation & Security – Basic XML– Document Type Definition & XML Schema – XML Parsers & Validation – XSL & XSLT – PHP-XML Integration – Web Services Basics					

UNIT V	INTRODUCTION TO ANGULAR and WEB APPLICATIONS FRAMEWORKS	9

Introduction to AngularJS, MVC Architecture, understanding attributes, Expressions and data binding, Conditional Directives, Style Directives, Controllers, Filters, Forms, Routers, Modules, Services; Web Applications Frameworks and Tools – Firebase- Docker- Node JS- React- Django- UI & UX.

	TOTAL PERIODS	45

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	construct a basic website using html and cascading style sheets	Understanding (K2)
CO2	build dynamic web page with validation using java script objects.	Applying (K3)
CO3	develop server-side programs using servlets and jsp.	Applying (K3)
CO4	construct simple web pages in php and represent data in xml format.	Analyzing (K4)
CO5	develop interactive web applications.	Analyzing (K4)

TEXTBOOKS

1. Deitel and Deitel and Nieto, Internet and World Wide Web - How to Program, Prentice Hall, 5th Edition, 2021.
2. Jeffrey C and Jackson, Web Technologies A Computer Science Perspective, Pearson Education, 2019.

REFERENCES

1. Stephen Wynkoop and John Burke —Running a Perfect Websitell, QUE, 2nd Edition, 2020.
2. Chris Bates, Web Programming – Building Intranet Applications, 3rd Edition, Wiley Publications, 2012.
3. Gopalan N.P. and Akilandeswari J., —Web Technologyll, Prentice Hall of India, 2011.
4. UttamK.Roy, —Web Technologiesll, Oxford University Press, 2011.

CO-PO MAPPING :

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3				-	2	2	3	3

CY23552	MOBILE APP DEVELOPMENT	3	0	0	3
COURSE OBJECTIVES					
To enable the students to					
1.	learn development of native applications with basic gui components				
2.	build cross-platform applications with event handling				
3.	construct applications with location and data storage capabilities				
4.	infer web applications with database access				
5.	take part in building web applications with cloud database access.				
UNIT I	**FUNDAMENTALS OF MOBILE & WEB APPLICATION DEVELOPMENT**				9
Web & Mobile App Development: Fundamentals of Web vs. Mobile apps (architecture, platforms) – Native Apps (platform-specific SDKs, performance, UX) – Hybrid Apps (WebView containers, frameworks like Ionic) – Cross-Platform Apps (React Native, Flutter; code sharing, performance trade-offs) – Progressive Web Apps (service workers, offline support, installability) – Responsive Web Design (fluid grids, media queries, mobile-first approach)					
UNIT II	**NATIVE APP DEVELOPMENT USING JAVA**				9
Native Web App, Benefits of Native App, Scenarios to create Native App, Tools for creating Native App, Cons of Native App, Popular Native App Development Frameworks, Java & Kotlin for Android, Swift & Objective-C for iOS, Basics of React Native, Native Components, JSX, State, Props					
UNIT III	**HYBRID APP DEVELOPMENT**				9
Hybrid Web App, Benefits of Hybrid App, Criteria for creating Native App, Tools for creating Hybrid App, Cons of Hybrid App, Popular Hybrid App Development Frameworks, Ionic, Apache Cordova					
UNIT IV	**CROSS-PLATFORM APP DEVELOPMENT USING REACT-NATIVE**				9
What is Cross-platform App, Benefits of Cross-platform App, Criteria for creating Cross-platform App, Tools for creating Cross-platform App, Cons of Cross-platform App, Popular Cross- platform App Development Frameworks, Flutter, Xamarin, React-Native, Basics of React Native, Native Components, JSX, State, Props					
UNIT V	**NON-FUNCTIONAL CHARACTERISTICS OF APP FRAMEWORKS**				9
Native SDKs (Xcode/Android Studio) offer top-tier runtime performance, full-featured debugging, and polished UI/UX but incur longer time-to-market and parallel maintenance; cross-platform frameworks (Flutter, React Native) provide fast hot-reload builds, near-native speeds, solid debugging, balanced time-to-market, high code reusability, and strong UI parity; hybrid solutions (Ionic, Cordova) enable rapid web-tech development, quickest MVP delivery, easy debugging via browser tools, and maximum code reuse but deliver moderate performance and less native-like UX.					
	TOTAL PERIODS				45

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	develop native applications with gui components.	Understanding (K2)
CO2	develop hybrid applications with basic event handling.	Applying (K3)
CO3	implement cross-platform applications with location and data storage .	Applying (K3)
CO4	implement cross platform applications with basic gui and event handling.	Analyzing (K4)
CO5	develop web applications with cloud database access.	Analyzing (K4)

TEXTBOOKS

1. Lauren Darcey and Shane Conder, —Android Wireless Application Developmentǁ, Pearson Education, 2nd ed. 2022.
2. Barry Burd, John Paul Mueller, —Android Application Development All in one for Dummies",Wiley Publications, 2020.

REFERENCES

1. Reto Meier, —Professional Android 2 Application Developmentǁ, Wiley India Pvt Ltd, 2020
2. Mark L Murphy, —Beginning Androidǁ, Wiley India Pvt Ltd, 2019
3. Android Application Development All in one for Dummies by Barry Burd, Edition: I, 2018
4. UttamK.Roy, —Web Technologiesǁ, Oxford University Press, 2011.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	2			-	-	2	2	3	3
CO5	3	3	3	3	3	2	-	-	-	-	2	2	3	3

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
7/25
★ AUTONOMOUS ★

CY23553	MICROSERVICES	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the architectural principles of microservices.
2.	explore inter-service communication, service discovery, and API gateway patterns.
3.	implement microservices using containers, orchestration, and DevOps tools.
4.	apply security, logging, and monitoring techniques in microservices-based systems.
5.	evaluate deployment, scalability, and fault tolerance in distributed microservices architectures.

UNIT I	ARCHITECTURE AND DESIGN PRINCIPLES	9

Introduction to Microservices-Microservices architecture, Characteristics, Benefits, challenges and design principles ;Domain-driven design basics – Service decomposition strategies – RESTful service design – Service granularity – API-first design – Event Sourcing – Idempotency – Stateless services – Service registry and discovery – Service communication – Synchronous vs Asynchronous – REST, and RPC, Message Queues – Orchestration vs Choreography - Edge services – API Gateway functions – Security at the gateway – Cloud-native microservices – 12-factor app principles.

UNIT II	INTER SERFVICE COMMUNICATION	9

Inter-service communication – REST vs Messaging – JSON, Protocol Buffers – Service registry – Eureka, Client-side vs Server-side discovery – Service mesh – Envoy proxy – Resilience patterns – Retry, Timeout, Rate limiting and throttling – API Gateway: Kong, Ambassador, NGINX – Authentication and Authorization –web tokens– Securing microservices – Secrets management – AWS Secrets Manager – Zero Trust model – Network policies and secure communication.

UNIT III	DOCKER AND CONTAINERIZATION	9

Containerization with Docker – Docker Compose for multi- container apps – Best practices – Kubernetes architecture – Pods, Services, Deployments, Replica Sets – Kubernetes – Helm charts – Namespaces – Rolling updates and rollbacks – Horizontal Pod Autoscaling – Service discovery in Kubernetes – Ingress controllers and load balancing – Logging and monitoring – Prometheus and Grafana tools— Distributed tracing platforms-Jaeger, Zipkin -CI/CD pipelines.

UNIT IV	TYPES OF MICROSERVICES	9

Event-driven microservices – Event brokers – Apache Kafka, RabbitMQ – Message formats and schemas – Avro, JSON Schema – Publisher-subscriber pattern – Message queues vs streams – Event streaming platforms – Kafka architecture – Stream processing frameworks – Apache Flink, Spark Streaming – Handling event failures – Dead Letter Queues – Replay strategies – Schema evolution – Contract testing – Pact – Idempotency and event duplication – Transactional outbox – Command and Query Responsibility Segregation (CQRS).

UNIT V	APPLICATIONS AND FUTURE TRENDS	9

Observability in microservices – Metrics, Logs, Traces – Service monitoring – Health checks, Uptime monitoring – Centralized logging, Performance tuning, Load testing, Fault tolerance – Hystrix, Resilience4j – Blue/Green and Canary deployments – Chaos engineering – Tools and practices – Scalability strategies – Cost optimization and FinOps for microservices deployments.

TOTAL PERIODS 45

COURSE OUTCOMES

	At the end of this course, students will be able to	**BT Mapped (Highest Level)**
CO1	understand the principles and components of microservices architecture.	Understanding (K2)
CO2	apply inter-service communication and security techniques.	Applying (K3)
CO3	deploy microservices using container orchestration tools.	Applying (K3)
CO4	analyze event-driven architecture and asynchronous communication.	Analyzing (K4)
CO5	explain the observability and fault-tolerance of microservices.	Analyzing (K4)

TEXTBOOKS

1. Sam Newman, "Building Microservices: Designing Fine-Grained Systems", 2nd Edition, O'Reilly Media, 2021.
2. Susan J. Fowler, "Production-Ready Microservices", O'Reilly Media, 2016.

REFERENCES

1. Christian Posta, "Istio in Action", Manning Publications, 2022.
2. Kasun Indrasiri, Prabath Siriwardena, "Microservices Security in Action", Manning Publications, 2020.
3. Bilgin Ibryam and Roland Hub, "Kubernetes Patterns", O'Reilly Media, 2019.
4. Mark Richards, "Fundamentals of Software Architecture", O'Reilly Media, 2020.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	2	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	2	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	2	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	2	2	2	3	3
CO5	3	3	3	3	3	3	-	[illegible]	[illegible]	2	2	2	3	3

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/7/25
★ AUTONOMOUS ★

CY23554	DEVSECOPS	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the fundamentals devops terminologies
2.	summarize the different version control tools like git, mercurial
3.	relate the concepts of continuous integration / continuous testing / continuous deployment)
4.	experiment with configuration management using ansible
5.	illustrate the benefits and drive the adoption of cloud-based devops tools.

UNIT I **INTRODUCTION TO DEVOPS** 9

DevOps Essentials: CI/CD principles, Infrastructure, containerization with Docker & Kubernetes, automated testing, monitoring & logging, collaboration– AWS-Compute Engine, Cloud Storage, Cloud Functions and Deployment Manager – Azure :Virtual Machines, Blob Storage, Azure Functions, ARM templates, Azure DevOps– Version Control: Git & GitHub distributed workflows, branching strategies, pull requests, GitHub Actions, code review and collaboration.

UNIT II **COMPILE AND BUILD USING MAVEN & GRADLE** 9

Introduction, Installation of Maven, POM files, Maven Build lifecycle, build phases, Maven Profiles, Maven repositories, Maven plugins, Maven create and build Artifacts, dependency management, Installation of Gradle, understand build using Gradle.

UNIT III **CONTINUOUS INTEGRATION USING JENKINS** 9

Jenkins Architecture Overview, creating a Jenkins Job, configuring a Jenkins job, Introduction to Plugins, Adding Plugins to Jenkins, commonly used plugins (Git Plugin, Parameter Plugin, HTML Publisher, Copy Artifact and Extended choice parameters). Configuring Jenkins to work with java, Git and Maven, creating a Jenkins Build and Jenkins workspace.

UNIT IV **CONFIGURATION MANAGEMENT USING ANSIBLE** 9

Introduction to Ansible architecture, use cases – Installation & Setup (pip/OS packages, configuration) – Master/Slave Configuration– YAML Basics – Ansible Modules – Inventory Files – Playbooks– Roles – Ad-hoc Commands (syntax, patterns, common operations).

UNIT V **BUILDING DEVOPS PIPELINES USING AZURE** 9

GitHub & Azure DevOps Workflow: GitHub Account Creation – Repository Setup– Azure DevOps Organization Creation– Pipeline Creation– Building Sample Code -azure-pipelines, yml Modification.

TOTAL PERIODS 45

COURSE OUTCOMES

At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	understand different actions performed through Version control tools.	Understanding (K2)
CO2	perform Continuous Integration and automate test cases.	Applying (K3)

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/7/25
AUTONOMOUS

CO3	implement Automated Continuous Deployment.	Applying (K3)
CO4	explain configuration management using Ansible.	Analyzing (K4)
CO5	understand to leverage Cloud-based DevOps tools using Azure DevOps.	Analyzing (K4)

TEXTBOOKS

1. Roberto Vormittag, —A Practical Guide to Git and GitHub for Windows Users: From Beginner to Expert in Easy Step-By-Step Exercises‖, Second Edition, Kindle Edition, 2020.
2. Jason Cannon, —Linux for Beginners: An Introduction to the Linux Operating System and Command Line‖, Kindle Edition, 2014

REFERENCES

1. Hands-On Azure Devops: Cicd Implementation for Mobile, Hybrid, And Web Applications Using Azure Devops and Microsoft Azure: CICD Implementation of DevOps and Microsoft Azure (English Edition), 2020 by Mitesh Soni
2. Kim, Gene, Jez Humble, Patrick Debois & John Willis, The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations, IT Revolution Press, 2016.
2. Jeff Geerling, —Ansible for DevOps: Server and configuration management for humans‖, First Edition, 2015.
3. David Johnson, —Ansible for DevOps: Everything You Need to Know to Use Ansible for DevOps, Second Edition, 2016.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's

(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	3	3	3	3	3	3	-	-	-	-	3	3	3	3
CO4	3	3	3	3	3	3	-	-	-	-	3	3	3	3
CO5	3	3	3	3	3	3	-	-	-	-	3	3	3	3

CY23555	FULL STACK DEVELOPMENT	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the principles of modern frontend and backend development frameworks.
2.	explore the features and capabilities of popular frontend frameworks like React and Angular.
3.	analyze backend development using Node.js, Express, and database integration.
4.	build full-stack applications and component-based architecture.
5.	implement RESTful APIs, middleware, authentication, and state management.

UNIT I — MODERN WEBARCHITECTURE AND FRONTEND PRINCIPLES — 9

Web Architecture – Monolithic vs SPA vs Micro-Frontend – HTML5, CSS3, and Modern JavaScript ES6+ Features – Introduction to NPM, Webpack, Babel – Transpiling, Bundling – UI Design Principles – Responsive and Adaptive Design – Frontend Development Lifecycle – Tooling and Automation – DOM Manipulation, Virtual DOM Concepts – Stateful vs Stateless Components – Reusability Patterns – Accessibility, Internationalization – Frontend Testing: Unit Testing, E2E Testing Tools .

UNIT II — REACT FRAMEWORK AND COMPONENT BASED DEVELOPMENT — 9

ReactJS – JSX, Components, Props and State – Functional vs Class Components – React Hooks – Component Lifecycle – Effect Hook, Memoization – Routing in React – React Router DOM,Forms – Controlled and Uncontrolled – Styled Components, CSS Modules – State Management – Context API, Redux Basics – Testing React Components – Jest, React Testing Library – Optimization in React.

UNIT III — ANGULAR FRAMEWORK AND STATE MANAGEMENT — 9

Angular Fundamentals – Modules, Components, Services – Templates, Data Binding, Directives and Pipes – Dependency Injection, Providers in Angular – Routing .Navigation – Lazy Loading Modules – Reactive Forms,Form Validation – RxJS , Observables in Angular – HTTP Client Module – Interceptors and Error Handling – State Management with NgRx– Testing Angular Applications – Jasmine and Karma.

UNIT IV — BACK-END DEVELOPMENT — 9

Node.js Overview – Event Loop and Async Programming – File System, Buffers, Streams – Creating Web Servers using HTTP Module, Express.js – Routing, Middleware, Templating Engines – RESTful APIs – CRUD Operations with Express – Authentication with JWT – Session vs Token – Database Integration – MongoDB with Mongoose – API Validation, Security – Testing Backend APIs – Postman, Mocha, Chai.

UNIT V	FULLSTACK INTEGRATIONAND DEPLOYMENT	9

Full Stack Development Workflow – Frontend-Backend Integration – Authentication, Authorization – Role-based Access Control – Environment Variables, Configuration Management – Deployment Strategies – CI/CD Overview – Web Sockets and Real-Time Communication – GraphQL vs REST – Basic Implementation – Performance Optimization – Caching, Compression – Monitoring, Logging – PM2, Winston, Morgan – Error Handling ,Graceful Shutdown Practices.

	TOTAL PERIODS	45

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	understand the purpose of modern frontend and backend frameworks.	Understanding (K2)
CO2	implement component-based architecture using React and Angular.	Applying (K3)
CO3	develop RESTful APIs and integrate backend logic using Node.js,Express.	Applying (K3)
CO4	analyze frontend-backend integration workflows and state management techniques.	Analyzing (K4)
CO5	test and debug full-stack applications with attention to performance and security.	Analyzing (K4)

TEXTBOOKS

1. Eric Elliott, "Programming JavaScript Applications", 2nd Edition, O'Reilly Media, 2019.
2. Adam Freeman, "Pro Angular", Apress, 5th Edition, 2022.

REFERENCES

1. Cássio de Sousa Antonio, "React Design Patterns and Best Practices", Packt Publishing, 2018.
2. Valeri Karpov, "Professional Node.js: Building Javascript Based Scalable Software", Apress, 2016.
3. Basarat Syed, "TypeScript Deep Dive", Self-published, 2020.
4. Kyle Simpson, "You Don't Know JS Yet", 2nd Edition, 2020.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's

(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	3	3	-	-	-	-	3	3	3	3
CO2	2	2	2	2	3	3	-	-	-	-	3	3	3	3
CO3	2	2	2	2	3	3	-	-	-	-	3	3	3	3
CO4	3	3	3	3	3	3	-	-	-	-	3	3	3	3
CO5	3	3	3	3	3	3	[illegible]	[illegible]	[illegible]	[illegible]	3	3	3	3

CY23556	GIT AND GITHUB	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1. understand the principles of version control systems and Git architecture.
2. learn basic and advanced Git operations for effective source code management.
3. explore branching strategies, conflict resolution, and collaboration techniques.
4. utilize GitHub for remote repository management and project collaboration.
5. apply workflow for issue tracking, CI/CD integration, and code review processes.

UNIT I **VERSION CONTROL SYSTEMS AND GIT FUNDAMENTALS** **9**

Introduction – Local vs Centralized vs Distributed – Git Features, Installation – Git Commands – git init, clone, status, add, commit – Git Repositories – Staging Area , Commit History –git Directory ,Object Model – Git Configuration ,Help System ,Viewing Logs ,File Differences ,git log, diff, show – Git ,Global Ignore Files.

UNIT II **BRANCHING, MERGING AND COLLABORATION** **9**

Branching Concepts – git branch, checkout, switch – Merging Strategies – Fast-forward, Three-way Merge – Resolving Merge Conflicts – Tools and Commands – Rebasing and Cherry-picking– Tagging Commits – Lightweight vs Annotated Tags – Undoing Changes — Stashing, Cleaning Workspace – RefLogs and Recovering Lost Commits

UNIT III **GITHUB PLATFORM AND REMOTE COLLABORATION** **9**

Introduction to GitHub – Features and Use Cases – Creating and Cloning GitHub Repositories – Pushing and Pulling – git push, pull, fetch –Forks and Pull Requests – GitHub Issues, Labels, and Milestones – Managing Collaborators and Permissions – Using GitHub Projects and Wikis – Enabling Branch Protection Rules.

UNIT IV **WORKFLOWS, INTEGRATION AND AUTOMATION** **9**

Git Workflow Models – Centralized, Feature Branch, Git Flow – GitHub Actions – CI/CD Overview –Basic GitHub Action Workflow – Automating Testing ,Deployment – Webhooks ,API Integrations – Managing Secrets, Environment Variables – Third-party Tools – Codecov, SonarCloud, Travis CI – Continuous Integration vs Continuous Deployment .

UNIT V **SECURITY, BEST PRACTICES AND TROUBLESHOOTING** **9**

Repository Security – Private vs Public, Access Control – Commit Signing, Verification – Managing Large Repositories, Git LFS – Best Practices – Commit Messages, Branch Naming, .gitignore – Debugging issues– Rewriting History– git rebase, filter-branch, BFG – Backup and Disaster Recovery in Git– Using Git in Professional Teams.

TOTAL PERIODS **45**

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/7/25
AUTONOMOUS

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	understand the fundamentals of Git and version control systems.	Understanding (K2)
CO2	apply Git commands and workflows.	Applying (K3)
CO3	use GitHub for collaborative software development.	Applying (K3)
CO4	analyze branching, merging strategies and CI/CD integration with GitHub.	Analyzing (K4)
CO5	apply security, optimization, and troubleshooting techniques in Git-based projects.	Applying (K3)

TEXTBOOKS

1. Mariot Tsitoara, "Git for Programmers", Apress, 2021.
2. Scott Chacon and Ben Straub, "Pro Git", 2nd Edition, A CRC press, 2014.

REFERENCES

1. Ramon Van Meer, "Mastering GitHub Actions", Packt Publishing, 2022.
2. Kyle Banker, "GitHub Essentials", Packt Publishing, 2018.
3. Rick Umali, "Learn Git in a Month of Lunches", Manning, 2015.
4. Jon Loeliger and Matthew McCullough, "Version Control with Git", O'Reilly Media, 2nd Edition, 2012.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's

(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	-	2	2	3	3

CY23557	RESPONSIBLE AND SAFE AI SYSTEMS	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the principles of safe AI systems.
2.	identify the AI risks for Gen models.
3.	analyze different transparency techniques.
4.	develop domain skills to analyze the metrics for responsible AI.
5.	explore applications of AI in different domains.

UNIT I PRINCIPLES OF SAFE AI SYSTEMS 9

AI Capabilities in recent years-Imminent risks from AI Models: Toxicity, bias, goal misspecification, adversarial examples-Long-term risks: Misuse, Mis-generalization, Rogue AGI-Principles of RAI - Transparency; Accountability; Safety, Robustness and Reliability; Privacy and security; Fairness, non-discrimination; Human-Centered Values; Inclusive and Sustainable development, Interpretability.

UNIT II AI RISKS FOR GEN MODELS 9

Deep Learning Techniques: basic principles of transformers, autoencoders, generative adversarial networks, reinforcement learning and self-supervised learning; Language/Vision Models -AI Risks for Gen models: misinformation and deepfakes, privacy violation, bias and harmful discrimination-Adversarial cybercrime and Attacks – Vision, NLP, Superhuman Go agents.

UNIT III TRANSPARENCY TECHNIQUES 9

ML Poisoning Attacks -Implications for current and future AI safety-Explainability-Imminent and Long-term potential for transparency techniques-Mechanistic Interpretability-Representation Engineering, model editing, probing-Critiques of Transparency for AI Safety-visualization, audit trails and Post hoc analysis.

UNIT IV METRICS FOR RESPONSIBLE AI 9

Privacy, Fairness in AI-Metrics -Tools for RAI: fairness, bias, explainability , privacy , transparency and monitoring tools; adversarial testing, explanations (Lime/SHAP/GradCam), audit mechanisms - Regulation landscape - DPDP act (India), GDPR (EU), EU AI act, US presidential declaration, Ethical approvals, informed consent, participatory design, future of work, Indian context-Artificial general intelligence-Instrumental Convergence: Power Seeking, Deception.

UNIT V	RESPONSIBLE AI DOMAINS	9

RAI in Legal domain: document analysis, contract management, e-discovery, legal chatbots—applications of RAI in Health care domain-RAI in Education domain: personalized learning and virtualized teaching assistant -Key applications of RAI in cyber security-Policy issues in RAI.

	TOTAL PERIODS	45

COURSE OUTCOMES

	At the end of this course, students will be able to	BT Mapped (Highest Level)
CO1	explain the principles of safe AI systems.	Understanding (K2)
CO2	explore the AI risks for Gen models.	Applying (K3)
CO3	relate the objectives different transparency techniques.	Analyzing (K4)
CO4	describe the metrics for responsible AI.	Applying (K3)
CO5	recognize the applications of AI in different domains.	Analyzing(K4)

TEXTBOOKS

1. Responsible Artificial intelligence, Virgia Dignukm, Springer,2019.
2. Jason Brownlee, Generative Deep Learning: Teaching Machines to Paint, Write, Compose, and Play, 2nd Edition, 2020.

REFERENCES

1. Human centered AI: An illustrated Scientific Quest, Panagiotis Germanakos,Springer Nature,1st edition,2025.
2. Francois Chollet, Deep Learning with Python, Manning Publications, 2018.
3. Josh Patterson, Michael Bowles, Hands-On Generative Adversarial Networks with Keras, Packt Publishing, 2019.
4. Artificial Intelligence and its societal Implications, Lawal O Yesufu Puteri Nor Ellyza Nohuddin, Springer,1st edition,2025.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's

(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	-	2	2	3	3

CY23651	EXPLORATORY DATA ANALYTICS	3	0	0	3

COURSE OBJECTIVES	
To enable the students to	
1.	understand the principles and workflow of exploratory data analysis (EDA).
2.	preprocess and clean real-world datasets for analysis.
3.	apply univariate and bivariate statistical techniques to uncover insights.
4.	perform multivariate exploratory techniques, including dimensionality reduction.
5.	use interactive visualization tools to communicate analytical findings.

UNIT I	FUNDAMENTALS OF EXPLORATORY DATA ANALYSIS	9

The role of EDA in the data science lifecycle -Types of data: numerical, categorical, time-series, text Overview of EDA tools (Python pandas, R dplyr) - Data import/export and basic data structures (DataFrame, tibble) - Missing values, outliers, and data integrity checks.

UNIT II	DATA PREPROCESSING AND CLEANING	9

Handling missing data: deletion, imputation techniques - Outlier detection and treatment - Data transformation: normalization, scaling, encoding categorical variables - Feature engineering basics - Data sampling and partitioning.

UNIT III	UNIVARIATE AND BIVARIATE ANALYSIS	9

Descriptive statistics: measures of central tendency and dispersion - Frequency distributions and histograms - Boxplots, density plots and violin plots - Scatter plots, correlation coefficients - Cross-tabulation and contingency tables.

UNIT IV	MULTIVARIATE ANALYSIS AND DIMENSIONALITY REDUCTION	9

Correlation matrix and heatmaps - Principal Component Analysis (PCA) for feature reduction, Cluster analysis overview: k-means, hierarchical clustering - t-SNE and UMAP for high-dimensional visualization - Exploratory factor analysis basics.

UNIT V	INTERACTIVE VISUALIZATION AND REPORTING	9

Introduction to interactive dashboards (Plotly, Dash, Shiny) - Geospatial exploratory plots - Time-series EDA techniques - Text data exploration: word clouds, frequency analysis - best practices for EDA reporting and storytelling.

	TOTAL PERIODS	45

COURSE OUTCOMES		
At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	outline the steps and principles of exploratory data analysis.	Applying (K3)
CO2	preprocess and clean datasets for exploratory purposes.	Analyzing (K4)

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/7/25
AUTONOMOUS

CO3	compute and interpret univariate and bivariate statistics and plots.	Analyzing (K4)
CO4	implement multivariate EDA techniques, including PCA and clustering.	Analyzing (K4)
CO5	develop interactive visualizations and reports.	Analyzing (K4)

TEXTBOOKS

1. John W. Tukey, ―Exploratory Data Analysis‖, First Edition, Addison-Wesley, 2022.
2. Wes McKinney, ―Python for Data Analysis: Data Wrangling with Pandas, NumPy, and IPython, Second Edition, O'Reilly Media, 2017.

REFERENCES

1. Hadley Wickham & Garrett Grolemund, ―R for Data Science: Import, Tidy, Transform, Visualize, and Model Data‖, First Edition, O'Reilly Media, 2016.
2. Peter Bruce & Andrew Bruce, ―Practical Statistics for Data Scientists: 50+ Essential Concepts Using R and Python‖, First Edition, O'Reilly Media, 2017.
3. Jake VanderPlas, ―Python Data Science Handbook: Essential Tools for Working with Data‖, First Edition, O'Reilly Media, 2016.
4. Claus O. Wilke, ―Fundamentals of Data Visualization‖, First Edition, O'Reilly Media, 2019.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	3	3	2	2	2	2	-	-	-	-	2	2	3	3
CO2	3	3	2	2	2	2	-	-	-	-	2	2	3	3
CO3	3	3	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	-	2	2	3	3

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/12/25
★ AUTONOMOUS ★

CY23652	DATA PREPROCESSING AND WRANGLING	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	recognize common data quality issues and their impact on analysis
2.	perform data profiling and auditing to assess dataset health
3.	apply techniques for handling missing inconsistent, and erroneous data
4.	standardize and transform data formats for downstream processing
5.	automate data cleaning workflows using modern tools and libraries

UNIT I INTRODUCTION TO DATA QUALITY AND CLEANING 9

Definition and dimensions of data quality, Importance of data quality in analytics, Types of data issues: completeness, consistency, accuracy, integrity, Causes and consequences of poor data quality, Data cleaning lifecycle: steps and activities, Overview of manual vs. automated cleaning, Error types: syntax, semantic, duplication, outliers, Introduction to data validation and verification techniques, Role of data governance in ensuring quality.

UNIT II DATA PROFILING AND AUDITING 9

Overview of data profiling and its role in data quality, Descriptive statistics for quality assessment, Pattern discovery techniques (regex, value distribution), Anomaly detection using statistical methods, Understanding and defining data quality rules, Constraint checking: domain, range, and referential integrity, Profiling categorical, numerical, and text data, Tools and libraries for profiling (pandas-profiling, R‘s Data Explorer), Auditing data pipelines for compliance and accuracy.

UNIT III HANDLING MISSING AND ERRONEOUS DATA 9

Classification of missing data: MCAR, MAR, MNAR, Detection methods for missing values, Deletion strategies: listwise, pairwise, and their limitations, Imputation techniques: mean, median, mode, Advanced imputation: k-NN, regression-based, MICE, Identifying and handling inconsistent values, Detecting and resolving duplicate records, Outlier detection: z-score, IQR, Mahalanobis distance, Impact of erroneous data on model performance.

UNIT IV STANDARDIZATION AND TRANSFORMATION 9

Data type parsing: date/time, string, categorical conversion, Standardization and formatting best practices, Normalization methods: Min-Max, Z-score, Scaling techniques: StandardScaler, RobustScaler, Feature generation and enrichment, Introduction to text cleaning and preprocessing, Tokenization and stop-word removal, Stemming vs. Lemmatization, Deduplication and record, linkage approaches.

UNIT V AUTOMATED DATA CLEANING WORKFLOWS 9

Overview of automation in data cleaning, Introduction to pyjanitor and cleaning functions in pandas, building reusable cleaning pipelines, Integration with ETL tools (Airflow, Talend, Luigi), Logging and versioning cleaned datasets, Data cleaning in real-time vs batch workflows, Case studies: cleaning messy datasets (e.g., open data, survey data), Documentation and reproducibility in cleaning projects, best practices for scalable and maintainable data cleaning.

	TOTAL PERIODS	45

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	identify and classify data quality issues in diverse datasets.	Understanding (K2)
CO2	perform comprehensive data profiling and quality auditing.	Applying (K3)
CO3	implement methods to handle missing, inconsistent and erroneous data.	Applying (K3)
CO4	apply standardization and transformation techniques to prepare data.	Analyzing (K4)
CO5	develop automated, reproducible data cleaning workflows .	Analyzing (K4)

TEXTBOOKS

1. Jacqueline Kazil & Katharine Jarmul, —Data Wrangling with Python: Tips and Tools to Make Your Life Easier‖, First Edition, O'Reilly Media, 2016
2. Tirthankar Dasu & Theodore Johnson, —Exploratory Data Mining and Data Cleaning‖, First Edition, John Wiley & Sons, 2003

REFERENCES

1. Carlo Batini & Monica Scannapieco, —Data Quality: Concepts, Methodologies and Techniques‖, First Edition, Springer, 2006
2. Rupak Chakraborty, —Python Data Cleaning Cookbook‖, First Edition, Packt Publishing, 2019
3. Jacqueline Kazil, —pyjanitor: Clean your Data with Python‖, O'Reilly Media, 2020
4. Ian H. Witten, Eibe Frank & Mark A. Hall, —Data Mining: Practical Machine Learning Tools and Techniques‖, Fourth Edition, Morgan Kaufmann, 2016

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	-	2	2	3	3

CY23653	**BIOMETRIC SECURITY**	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the fundamental principles of biometric systems and their applications in security.
2.	explore various physiological and behavioral biometric modalities and technologies.
3.	analyze the performance, reliability, and vulnerabilities of biometric systems.
4.	implement biometric systems with secure design, storage, and matching techniques.
5.	evaluate privacy, ethical, and legal considerations in deploying biometric systems.

UNIT I	**INTRODUCTION TO BIOMETRIC SYSTEM**	**9**

Introduction to Biometrics – Definition and Scope – History of Biometric Systems – Types of Biometric Systems – Physiological vs Behavioral – Biometric System Components – Sensors, Feature Extraction, Matching – Performance Metrics – FAR, FRR, EER, ROC Curves – Identity Verification vs Identification – Open-set vs Closed-set – Template Creation and Storage – Data Capture Techniques – Biometric System Architecture – Enrollment and Authentication – Challenges in Biometric Systems – Universality, Uniqueness, Permanence – Applications of Biometrics – Civil, Forensic, Commercial.

UNIT II	**PHYSIOLOGICAL BIOMETRIC MODALITIES**	**9**

Fingerprint Recognition – Acquisition, Minutiae Extraction – Matching Algorithms – Pattern Matching, Ridge Flow, Core Detection – Sensor Technologies – Optical, Capacitive, Ultrasonic – Spoof Detection and Liveness Techniques – Face Recognition – Geometry-based and Appearance-based Techniques – 3D Face Recognition – Depth Sensing and IR Cameras – Facial Landmark Detection and Alignment – Challenges – Illumination, Pose, Expression, Aging – Performance Enhancement Techniques.

UNIT III	**BIOMETRIC RECOGNITION**	**9**

Iris Recognition – Structure of the Iris – Image Acquisition – Iris Segmentation and Normalization – Feature Extraction – Matching Algorithms – Hamming Distance, Gabor Filters – Voice Biometrics – Feature Extraction (MFCC, LPC) – Speaker Identification and Verification – Signature and Keystroke Dynamics – Features and Matching – Hand Geometry and Palmprint Recognition – Multimodal Biometrics – Fusion Techniques – Evaluation of Multibiometric Systems.

UNIT IV	**BIOMETRIC SECURITY AND PROTECTION**	**9**

Template Security – Biometric Cryptosystems – Cancelable Biometrics – Watermarking and Steganography in Biometrics – Biometric Standards – ISO/IEC 19794, ANSI/NIST ITL – Data Protection and Storage Guidelines – System Design and Integration – API and SDKs – Security Attacks – Replay, Spoofing, Hill Climbing – Template Protection Techniques – Fuzzy Vault, Fuzzy Commitment – Revocability and Renewability of Templates – Anti-spoofing Mechanisms and Evaluation.

UNIT V	**FUTURE OF BIOMETRICS**	**9**

Privacy Issues in Biometrics – Surveillance and Consent – Ethical Concerns – Bias, Inclusion, and Fairness – Legal Frameworks – GDPR, UIDAI, IT Act Provisions – Cross-matching and Database Linking Risks –

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
AUTONOMOUS
5/7/25

Accountability and Audit Mechanisms – Usability and User Acceptance Factors – Biometric Deployment Case Studies – Aadhaar, e-Passport – Trends in Biometric Authentication – Mobile and Wearables – Future of Biometrics – Deep Learning and AI Integration.

	TOTAL PERIODS	**45**

COURSE OUTCOMES

At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	understand the core principles and applications of biometric systems.	Understanding (K2)
CO2	analyze biometric modalities such as fingerprint, face, and iris recognition.	Analyzing (K4)
CO3	apply biometric system design and feature extraction methods.	Applying (K3)
CO4	evaluate performance metrics and security of biometric systems.	Analyzing (K4)
CO5	discuss legal, privacy, and ethical implications of biometrics.	Analyzing (K4)

TEXTBOOKS

1. Anil K. Jain, Arun Ross, Karthik Nandakumar, "Introduction to Biometrics", Springer, 2016.
2. Ratha, Nalini K., and Ruud Bolle, "Automatic Fingerprint Recognition Systems", Springer, 2nd Edition, 2016.

REFERENCES

1. John D. Woodward, Jr., Nicholas M. Orlans, and Peter T. Higgins, "Biometrics: Identity Assurance in the Information Age", McGraw-Hill, 2016.
2. Julian Ashbourn, "Biometrics: Advanced Identity Verification", Springer, 2018.
3. Arun A. Ross and M. Govindarajan, "Handbook of Multibiometrics", Springer, 2017.
4. Nalini K. Ratha and Venu Govindaraju, "Advances in Biometrics: Sensors, Algorithms and Systems", Springer, 2019.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	**PO's**												**PSO's**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	3	3	2	2	2	2	-	-	-	-	2	2	3	3
CO2	3	3	3	2	2	2	-	-	-	-	2	2	3	3
CO3	3	3	3	3	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	3	3	3	3
CO5	3	3	3	3	3	3	[illegible]	[illegible]	[illegible]	-	3	3	3	3

CY23654	SECURITY METRICS	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the key concepts and challenges of security metrics.
2.	develop the ability to collect, analyze, and manage security data.
3.	evaluate security operations and compliance through practical projects.
4.	analyze and measure the cost, value, and cultural impact of security within organizations.
5.	implement security measurement programs and adapt metrics in an organization.

UNIT I **SECURITY METRICS** 9

Security Metrics- Introduction- Metric and Measurement, Security Metrics Today, The Dissatisfying State of Security Metrics, Reassessing Our Ideas About Security Metrics. Designing Effective Security Metrics: Choosing Good Metrics, GQM for Better Security Metrics, Uses for GQM.

UNIT II **DATA REALITY** 9

Data Sources for Security Metrics; The Security Process Management Framework: Managing Security as a Business Process, the SPM Framework. Analyzing Security Metrics Data: The Most Important Step, Analysis Tools, and Techniques. Designing the Security Measurement Project: Before the Project Begins, Phase One: Build a Project Plan and Assemble the Team, Phase two: Gather the Metrics Data, phase Three: Analyze the Metrics Data and Build Conclusions, phase Four: Present Results, Phase Five: Reuse the Results, Project Management Tools.

UNIT III **OPERATIONAL METRICS** 9

Measurements Security Operations: Sample Metrics for Security Operations, Sample Measurement Project for Security Operations, Summary. Measuring Compliance and Conformance: The Challenges of Measuring Compliance, Sample Measurement Projects for Compliance and Conformance.

UNIT IV **COST VALUE METRICS** 9

Measuring Security Cost and Value: Sample Measurement Projects for Compliance and Conformance, The Importance of Data to Measuring Cost and Value, Summary. Measuring People, Organizations and Culture: Sample Measurement Projects for People, Organizations, and Culture.

UNIT V **FUTURE TRENDS AND IMPROVEMENTS** 9

The Security Improvement Program: Moving from Projects to Programs, Managing Security Measurement with a Security Improvement Program, Requirements for a SIP, Measuring the SIP. Summary. Learning Security: Different Contexts for Security Process Management: Organizational Learning, Three Learning Styles for IT Security Metrics.

	TOTAL PERIODS	45

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	acquire a complete understanding on all the security metrics.	Understanding (K2)
CO2	develop methods to design effective security metrics.	Applying (K3)
CO3	perform security operations and compliance through practical projects.	Analyzing (K4)
CO4	summarize the security operations, Compliance and Conformance.	Applying (K3)
CO5	identify the parameters for measuring the security cost and value.	Analyzing (K4)

TEXTBOOKS

1. IT Security Metrics, Lance Hayden, Tata McGraw-Hill,2021
2. Security Metrics, Caroline Wong, Tata McGraw-Hill,2021

REFERENCES

1. Measuring and Managing Information Risk: A FAIR Approach,2021
2. Jack Freund and Jack Jones, Butterworth-Heinemann, 2014.
3. Information Security Metrics: A Definitive Guide to Effective Security Monitoring and Measurement,2022
4. Security Risk Management: Building an Information Security Risk Management Program from the Ground Up,2022

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO5	2	2	2	2	2	2	-	-	-	-	2	2	3	3

CY23655	BIG DATA COMPUTING	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand big data concepts.
2.	implement Hadoop related tools for Big Data Analytics.
3.	learn and use NoSQL big data management.
4.	apply MapReduce analytics using Hadoop and related tools.
5.	explore Machine Learning Concepts.

UNIT I	BIG DATA	9

Introduction to big data – Traditional Analytics and Big Data Analytics-The Need for Big Data Analytics in Cybersecurity -Applying Big Data Analytics in Cybersecurity-Challenges to Big Data Analytics for Cybersecurity -Introduction to Network Forensics-Network Forensics Process -Applying Big Data Analysis for Network Forensics -Big Data Software Tools.

UNIT II	BASICS OF HADOOP	9

Introduction-Hadoop and its Eco system-Hadoop Core Components-Features of Hadoop-Hadoop Distributed File System-MapReduce framework and programming model-Hadoop YARN- Hadoop 2 Execution Model- Hadoop Ecosystem Tools-Ambari—Features-Hadoop Administration- Hbase- Hive -Pig-Mahout

UNIT III	NOSQL DATA MANAGEMENT	9

Introduction to NoSQL – aggregate data models – key-value and document data models– relationships – graph databases – schema less databases – materialized views – distribution models- master-slave replication – consistency - Cassandra – Cassandra data model – Cassandra examples – Cassandra clients.

UNIT IV	MAPREDUCE, HIVE AND PIG	9

Introduction-MapReduce Task and MapReduce Reduction: Map-Tasks, Key-Value Pair, grouping by key, Partitioning, Combiners, Reduce Tasks, MapReduce Processing Steps, Node Failures -Hive: Architecture, Installation, Data Types and File Formats, Built-in Functions-Pig: Apache Pig, Installing Pig, Pig Latin Scripts.

UNIT V	MACHINE LEARNING ALGORITHMS FOR BIG DATA ANALYTICS	9

Introduction-Regression Analysis Simple Linear Regression, Least Square Estimation, Multiple Regressions, Modelling Possibilities using Regression, Prediction using Regression Analysis, K-Nearest-Neighbour Regression Analysis, Clustering Analysis: Overview of Clustering, K Means, Hierarchical Clustering.

	TOTAL PERIODS	45

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/2/25
★ AUTONOMOUS ★

COURSE OUTCOMES		
At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	describe big data and use cases from selected business domains.	Applying (K3)
CO2	use Hadoop-related tools such as HBase, Cassandra, Pig, and Hive for big data analytics.	Applying (k3)
CO3	explain NoSQL big data management.	Analyzing (K4)
CO4	perform map-reduce analytics using Hadoop.	Analyzing (K4)
CO5	demonstrate understanding of machine learning principles	Understanding (K2)

TEXTBOOKS

1. Onur Savas, Julia Deng, Big Data Analytics in Cyber Securityl,2022.
2. Raj Kamal; Preeti Saxena, —BIG DATA ANALYTICS: Introduction to Hadoop, Spark, and Machine-Learningl,2021.

REFERENCES

1. Anany E. Capriolo, D. Wampler, and J. Rutherglen, "Programming Hive", O'Reilley, 2012.
2. Lars George, "HBase: The Definitive Guide", O'Reilley, 2011.
3. Eben Hewitt, Cassandra: The Definitive Guide", O'Reilley, 2010.
4. Alan Gates, "Programming Pig", O'Reilley, 2011.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	-	2	2	3	3

CY23656	SOCIAL NETWORKS	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	describe the fundamental concepts, classification and explore social media opportunities.
2.	explain trust management principles in online social networks.
3.	identify potential risks and their impact in the organizations.
4.	recognize policies, legal frameworks, and privacy concerns governing social media usage.
5.	illustrate security challenges and privacy concerns in with decentralized systems.

UNIT I **OPPORTUNITIES OF SOCIAL MEDIA AND NETWORKS** **9**

Introduction to social media and networks – Understanding social media – Different types and classifications – The value of social media – Cutting edge Versus bleeding edge –The problem with social media – Possibility of security issue – Opportunities of social media – Building social authority – Engaging customers – Sharing information – Employment and social media – Considerations for setting up social media.

UNIT II **IDENTITY MANAGEMENT** **9**

Trust management in online social networks –handling real world network datasets, strength of weak ties, strong and weak relationships, positive, negative relationships- Trust – credibility and reputations in social systems – Online social media and Policing – Information privacy disclosure – Revelation – Phishing in OSM – Identifying fraudulent entities in online social networks – Controlled information sharing – Identity management – Open Security Issues in online social networks.

UNIT III **RISK MANAGEMENT** **9**

Risks of social media – Public embarrassment – False information – Information leakage – Retention and archiving content – Backing up social media – Loss of data and equipment – Cybercrime – Scams – Cyberstalking – Cyberbullying – Predators – Social Engineering- Link analysis-cascading behaviour in networks- – Hacked accounts – Laws and Regulations – Forensics – Malware, viruses and exploit distribution.

UNIT IV **POLICIES AND PRIVACY** **9**

Policies and Privacy – Blocking users – Controlling app privacy – Location awareness – Security – Fake accounts –Passwords – Privacy and information sharing – Content security – Accountability – Governance – Clear and understandable roles – Crisis management – Continuity planning – Monitor social media – Review social media. – Privacy and security issues associated with various social media-power laws and rich-get-richer phenomena.

UNIT V **PEER TO PEER NETWORKS** **9**

Data privacy in P2P systems – Privacy in distributed data storage systems – Privacy in massive data sharing systems – Evaluation – Privacy policy model – Data model –Strength of social relationships – small world phenomenon-pseudo core (how to go viral on web) Privacy preserving reputation systems –

Security and privacy issues in mobile social networks – Privacy issues in context–aware MSNs – Security and privacy support in MSNs Middleware.

	TOTAL PERIODS	45

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	illustrate the various types of social media.	Understanding (K2)
CO2	identify fraudulent and malicious entities in online social networks.	Applying (K3)
CO3	demonstrate threats associated with social media platforms.	Applying (K3)
CO4	apply privacy by design principles in social media platforms.	Applying (K3)
CO5	analyze security vulnerabilities and design limitations in P2P systems.	Analyzing (K4)

TEXTBOOKS

1. Michael Cross, —Social Media Security: Leveraging Social Networking While Mitigating Risk‖, Syngress, 2014.
2. Barbara Carminati, Elena Ferrari, Marco Viviani, —Security and Trust in Online Social Networks‖, Springer, 2022.

REFERENCES

1. Networks, crowds and markets by David Easley and Jon Kleinberg, Cambridge University Press,2010.
2. C P Kumar. —Social Media Security: Protecting Your Digital Life‖, C. P. Kumar Publisher, 2023.
3. Social and Economic Networks by Matthew O. Jackson, Princeton University Press,2010.
4. Richard Chbeir, Bechara Al Bouna, —Security and Privacy Preserving in Social Networks‖, Spinger, 2013.

CO–PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's

(1/2/3 indicates strength of correlation) 3–Strong, 2–Medium, 1–Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	2	-	-	3	3	3	3
CO2	2	2	2	2	2	2	-	2	-	-	3	3	3	3
CO3	2	2	2	2	2	2	-	2	-	-	3	3	3	3
CO4	3	3	3	3	3	3	-	2	-	-	3	3	3	3
CO5	3	3	3	3	3	3	-	2	-	-	3	3	3	3

CY23657	SECURITY AUDIT AND RISK ASSESSMENT	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the security audit planning strategies.
2.	gain knowledge about information risk.
3.	discover knowledge in collecting data about organization.
4.	acquire knowledge in various analysis on Information Risk Assessment.
5.	introduce the System Risk analysis.

UNIT I — SECURITY AUDIT PLANNING — 9

Need for Audit Planning - Steps in Audit Planning- Audit Risk Assessment- Performing Audit- Internal Controls- Audit Evidence- Audit Testing- Follow up activities- Security Monitoring and Auditing- Assurance and Trust- Need for Assurance- Role of Requirements in Assurance- Audit Assurance in Software Development Phases- Building Secure and Trusted Systems- Designing an Auditing System- Auditing to detect Violations of a Security Policy- Auditing Mechanisms- Audit Browsing.

UNIT II — INFORMATION RISK — 9

What is Risk- Going Deeper with Risk- Components of Risk- Putting it Altogether- Information Security Risk- Information Security Risk Assessment Overview- Assess Information Security Risk- Risk assessment and security Program- Information Security Management in a Nutshell- Drivers, Laws and Regulations- Federal Information Security Management- Gramm-Leach-Blile (GLBA)- Health Insurance Portability and Accountability Act(HIPAA)- State Governments- ISO 27001- Drivers, Laws and Regulations- Risk Assessment Framework- Practical Approach.

UNIT III — DATA COLLECTION AND RISK SCHEDULING — 9

Data Collection-Introduction- The Sponsor- The Project Team- The size and Breadth of the Risk Assessment- Scheduling and Deadlines- Assessor and Organization Experience- Work load- Data Collection Mechanisms- Collectors- Containers- Executive Interview- Document Requests- IT Asset Inventories- Asset Scoping- Business Impact Analysis and Other Assessments Critical Success Factor Analysis- Profile & Control Survey- Consolidation.

UNIT IV — INFORMATION RISK ASSESSMENT — 9

Compiling Observations from Organizational- Risk Documents- Preparation of Threat and Vulnerability Catalogs- Threat Catalog- Vulnerability Catalogs- Threat Vulnerability Pairs- Overview of the System Risk Computation- Designing the Impact Analysis Scheme- Confidentiality, Integrity- Availability- Preparing the Impact Score- Designing the Control analysis Scheme- Designing the Likelihood Analysis Scheme- Exposure- Frequency- Controls- Likelihood- Final Risk Score.

UNIT V — SYSTEM RISK ANALYSIS — 9

System Risk Analysis- Risk Classification- Risk Rankings- Risk Prioritization and Treatment- Review of Audit Findings- Review of Security Incidents- Review of Security Exceptions- System Specific Risk

Treatment- information Security Risk Assessment Reporting- Risk Analysis Executive Summary- Methodology- Organizational- System Specific- Results- Organizational Analysis- System Specific- Risk Register- Post Mortem.

TOTAL PERIODS	**45**

COURSE OUTCOMES

At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	acquire the knowledge on various secure auditing techniques.	Understanding (K2)
CO2	analyze about components of information risk.	Analyzing (K4)
CO3	understand the basic ideas about data collection workload.	Analyzing (K4)
CO4	appreciate the concepts of vulnerability catalogs and impact analysis scheme.	Analyzing (K4)
CO5	identify the knowledge in risk classification technique.	Analyzing (K4)

TEXTBOOKS

1. Mark Talabis, ―Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis‖, Syngress; 1st Edition, Nov 2012.
2. David L. Cannon, ―CISA Certified Information Systems Auditor Study Guide‖, SYBEX Publication.

REFERENCES

1. Thomas R.Peltier, Information Security Risk Analysis‖, CRC Press, 20012. Schank Roger C.,
2. Martin Weiss, Michael G.Solomon, Auditing IT Infrastructures for Compliance,2nd edition,2016,Jones and Barlett Learning.
3. The Security Risk Handbook ,by Charles Swanson ,Taylor and Francis 1st edition 2023.
4. The Security Risk Assessment Handbook, A Complete Guide for Performing Security Risk Assessments Douglas J. Landoll by CRC Press ,2021 ,3rd Edition

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's

(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO5	2	2	2	2	2	2	-	-	-	-	2	2	3	3

CY23851	CYBER SECURITY ESSENTIALS	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	interpret types of cybercrimes, cybercriminals, and cyber offenses.
2.	analyze the various type of cyber-attacks.
3.	discover the various security issues related to mobile and wireless devices.
4.	understand the various perspectives of cyber act.
5.	infer the intellectual property rights and ethical dimensions of cybercrimes.

UNIT I	INTRODUCTION TO CYBERCRIMES	9

Introduction–Cyber Crime definition and origins– Cybercrime and information Security–Cyber criminals– Classification of Cybercrimes, Cyber-offenses: categories of cybercrime, Attack plan: active, passive attacks, reconnaissance, social engineering and classification, cyberstalking, and types, cybercafe and cybercrimes, botnets the fuel for cybercrime, attack vector, cloud computing and cybercrime.

UNIT II	CYBERATTACKS	9

Password cracking: password cracking techniques and tools, prevention measures of password cracking; Malwares: types of keylogger, spywares, viruses, worms, worms, trojans and backdoors, detection and prevention of trojans and backdoors, steganography, DoS, DDoS attacks, SQL injection and prevention measures, buffer overflow and prevention, Phishing and Identity theft: techniques ,types and preventions, attacks on wireless networks and securing techniques.

UNIT III	MOBILE AND WIRELESS DEVICES	9

Introduction – Proliferation of Mobile and Wireless devices, 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: mobile phone theft, mobile viruses, Mishing, vishing, smishing, hacking Bluetooth; Security Implications for Organizations, Organization Measures for handling Mobile Devices, Related Security Issues and Polices.

UNIT IV	The INDIAN IT ACT and LEGAL PERSPECTIVES	9

The Need of Cyber laws, The Indian IT Act, Amendments, Consequences of Not Addressing the Weakness in Information Technology Act, Cybercrime and Punishment, Challenges to Indian Law and Cybercrime Scenario in India, e-commerce, Contract aspects in cyber law, the Indian contract act, Intellectual property rights and the Indian evidence act, security aspects of cyber law, digital signatures, Criminal aspects in cyber law.

UNIT V	CYBER ETHICS	9

Cyber security : Organizational implications-Insider attack, cost of cybercrime and IPR issues, perils of web threats in an organization, social media marketing: the security risks and perils, associated challenges, protecting people's privacy: guidelines and computer usage policy, incident handling forensics in an organization, media and asset protection, endpoint security; Intellectual property in the cyberspace: Copyright, patent, trademarks, the ethical dimensions-Mindset and Skills Cybercriminals – Sociology of Cybercriminals – Information Warfare: Perception vs eminent reality.

	TOTAL PERIODS	**45**

COURSE OUTCOMES

At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	classify the types of cybercrimes, cybercriminals, and cyber offenses.	Analyzing (K4)
CO2	explore the impacts of various cyber-attacks.	Analyzing (K4)
CO3	detect the various types of attacks on mobile and wireless devices.	Analyzing (K4)
CO4	explain the consequences of cybercrime and its punishment.	Analyzing (K4)
CO5	describe the intellectual property rights and cyber ethics.	Analyzing (K4)

TEXTBOOKS

1. Sunit Belapure and Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India Pvt. Ltd, 2021.
2. Jonathan Rosenoer, "Cyber Law: The law of the Internet", Springer–Verla.2019.

REFERENCES

1. Mark F Grady, Fransesco Parisi, "The Law and Economics of Cyber Security",Cambridge University Press, 2012.
2. Dr. Farooq Ahmad, Cyber Law in India, Allahbad Law Agency– Faridabad.2018.
3. Charles J. Brooks Christopher Grow Philip Craig Donald Short, Cybersecurity Essentials, 2021, by John Wiley & Sons,
4. James Graham Richard Howard,ryan Olson,Cyber security essentials ,Taylor & Francis Group,CRC Press,2021

CO-PO MAPPING :

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	3	3	3	3	3	3	-	3	-	-	2	2	3	3
CO2	3	3	3	3	3	3	-	3	-	-	2	2	3	3
CO3	3	3	3	3	3	3	-	3	-	-	2	2	3	3
CO4	2	2	2	2	2	2	-	3	-	-	2	2	3	3
CO5	2	2	2	2	2	2	-	3	-	-	2	2	3	3

CY23852	FUNDAMENTALS OF COMPUTER FORENSICS	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	know the history and evolution of digital and computer forensics.
2.	discover the principles of investigating computer crimes.
3.	learn about anti-forensic techniques.
4.	understand the need for mobile forensics.
5.	explore web attack forensics and email forensics.

UNIT I **INTRODUCTION** 9

Introduction -Evolution of Computer Forensics - Stages of Computer Forensic Process - Benefits of Computer Forensics - Digital Forensics- Uses of Digital Forensics- Role of Forensics Investigator - Forensics Readiness - Goals of Forensic Readiness, Benefits and Planning of Forensic Readiness. Introduction to Computer Crime Investigation process: Assess the Situation, Acquire the Data, Analyze the Data, Report the Investigation.

UNIT II **COMPUTER FORENSICS** 9

Introduction: Forensic Science- Locard's Exchange Principle, Scientific Method, Organizations of Note, Role of the Forensic Examiner in the Judicial System, key technical concepts on File Extensions and File Signatures: Storage and Memory Computing Environments, Data Types, File Systems. Labs and tools: Forensic Laboratories, Policies and Procedures Quality Assurance, Digital Forensic Tools, Accreditation. Collection of evidence and issues: Collection and documenting, chaining of custody, cloning, live vs dead system, introduction to hashing algorithms, overview of window system artefacts.

UNIT III **ANTI-FORENSICS** 9

Anti-forensics: Hiding the data, password attacks, steganography, data destruction; Legal aspects: Fourth Amendment, criminal, searches without a warrant and search with a warrant, electronic discovery, expert testimony, Technical Issues, Legal Issues, Administrative Issues; Forensics with respect to internet: Web browser, Email, social networking site.

UNIT IV **NETWORK AMD MOBILE DEVICE FORENSICS** 9

Network forensics: Introduction to Social Engineering, Network Security Tools, Network Attacks, Incident Response, Network Evidence, and Investigations; Mobile Device Forensics: Introduction to cellular networks, operating systems, Cell Phone Evidence, cell phone forensic tools, Global Positioning Systems (GPS); Challenges and Concerns: Standards and Controls, Cloud Forensics:(Finding/ Identifying Potential Evidence Stored in the Cloud, Cloud, Forensics and Legal Concerns, Data storage in Solid State Drives.

UNIT V **WEB ATTACK AND EMAIL FORENSICS** 9

Introduction to web attacks, web attack forensics, web services forensics, web application forensics, website traffic analysis, web attack forensic tools. Email structure and services, email attack and crimes, privacy in email, email forensics, email forensics tools;Legal Aspects of Computing Against Individual, property and an organization with respect to Indian IT Act.

TOTAL PERIODS 45

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	classify of digital and computer forensics.	Understanding (K2)
CO2	identify the procedure and principles of investigating computer crimes.	Applying (K3)
CO3	explain about anti-forensic techniques.	Analysis (K4)
CO4	describe the challenges and concepts behind mobile and network forensics.	Analysis (K4)
CO5	outline about web attack forensics and email forensics	Analysis (K4)

TEXT BOOKS

1. The Basics of Digital Forensics the Primer for Getting Started in Digital Forensics, Syngress imprint of Elsevier,2012.
2. Dr. Ajay Prasad, Dr. Jeetendra Pande, "Digital Forensics", Uttarakhand Open University, Haldwani, Mumbai, 2016.

REFERENCES

1. Computer Evidence Collection &Presentation by Chrostopher L.T. Brown,Firewall Media. 2017.
2. Linda Volonino, Reynaldo Anzaldua; Computer Forensics For Dummies, Wiley, Publishing, Inc.2016.
3. Real Digital Forensics by Keith j.Jones, Richard Bejitlich,Curtis W.Rose ,Addison - Wesley Pearson Education. 2015
4. Computer Forensics, Computer Crime Investigation by John R,Vacca, Firewall Media, New Delhi. 2012.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's

(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	Programme Outcomes PO's												PSO's	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2	2	2	2	2	2	-	3	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	3	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	3	-	-	2	2	3	3
CO4	2	2	2	2	2	2	-	3	-	-	2	2	3	3
CO5	2	2	2	2	2	2	-	3	-	-	2	2	3	3

CY23853	PRIVACY AND SECURITY IN ONLINE SOCIAL MEDIA	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	describe the fundamental concepts, classification and explore social media opportunities.
2.	identify potential risks and their impact in the organizations.
3.	illustrate security challenges and privacy associated with social media
4.	recognize the taxonomy of various security solutions.
5.	explain trust management principles in online social networks.

UNIT I SOCIAL MEDIA AND OPPORTUNITIES 9

Introduction to different types of social media-Content communities -The value of social media - history of social networking - problems with social media; Opportunities of Social Media: New methods of marketing to customers-Building social authority-Engaging customers-Sharing information-Getting the word out- advantage of collective intelligence; social media to find employees, employment-Limiting personal information- social media in the workplace.

UNIT II SOCIAL MEDIA SET UP AND RISKS 9

The place of social media in organization: Identifying audience-Internet versus intranet-Making the right decision-Identifying the representation on the Internet-Approved representatives and privacy; social media campaigns and hoaxes-The human factor -content management, promotion ; Public embarrassment, False information, Information leakage, Retention and archiving content, Backing up social media, Loss of data/equipment; Cybercrime, Social engineering and Hacked accounts.

UNIT III RISK MANAGEMENT AND SECURITY 9

Risk management: Laws and regulations, Forensics, Police use of social media, Malware, viruses, and exploit distribution; Policies, Privacy, blocking users, Controlling app privacy, Location awareness, Security: reviews and strategies, Fake accounts, Passwords, Privacy and information sharing, Content security, the pitch, the promise, and the reality behind lack of control in social media, monitoring social media, keeping it fresh and taking control.

UNIT IV TAXONOMY OF VARIOUS SOLUTIONS 9

Taxonomy Of Various Solutions: In built security solutions, third party software solutions, Machine learning based, deep learning based Artificial Intelligence based security solutions for Detecting various attacks-Case study-eg. Fake account detection, Characteristic analysis of X network accounts; Preventive Measures: Tips to protect account and information, Open issues and challenges in existing security solutions, Guiding principles to protect the user account in social platform.

UNIT V ONLINE PRIVACY 9

Privacy in online social networks: Privacy and threat defenses; Access control reputation and policies:

user managed access control, flexible user privacy policy, social semantic network-based access control; Security and Privacy in P2P systems: support of data privacy, privacy preserving reputation management, security and privacy issues in mobile social networks.

TOTAL PERIODS **45**

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	illustrate the various types of social media and the problems.	Understanding (K2)
CO2	explain potential risks and their impact in the organizations.	Analyzing (K4)
CO3	demonstrate the importance of risk management, security and privacy.	Applying (K3)
CO4	apply various security measures in online social media.	Applying (K3)
CO5	analyze security vulnerabilities and design limitations in P2P systems.	Analyzing (K4)

TEXTBOOKS

1. Michael Cross, "Social Media Security: Leveraging Social Networking While Mitigating Risk", Syngress, 2014.
2. Brij B. Gupta, Somya Ranjan Sahoo, "Online Social Networks Security, Principles, Algorithm, Applications and Perspectives", Taylor and Francis, CRC Press, 2021.

REFERENCES

1. Richard Chbeir, Bechara Al Bouna, "Security and Privacy Preserving in Social Networks", Spinger, 2013.
2. Barbara Carminati, Elena Ferrari, Marco Viviani, "Security and Trust in Online Social Networks", Springer, 2022.
3. C P Kumar. "Social Media Security: Protecting Your Digital Life", C. P. Kumar Publisher, 2023.
4. Yaniv Altshuler, Yuval Elovici, Armin B. Cremers, Nadav Aharony, Alex Pentland, "Security and Privacy in Social Networks", Springer, 2013.

CO–PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3–Strong, 2–Medium, 1–Weak

CO's	PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	2	-	3	-	-	3	3	3	3
CO2	2	2	2	2	2	2	-	3	-	-	3	3	3	3
CO3	2	2	2	2	2	2	-	3	-	-	3	3	3	3
CO4	3	3	3	3	3	3	-	3	-	-	3	3	3	3
CO5	3	3	3	3	3	3	-	3	-	-	3	3	3	3

CY23854	INTRODUCTION TO SENSOR TECHNOLOGIES	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1. acquire knowledge about the principles and analysis of sensors.
2. identify the characteristics and response of micro sensors.
3. acquire adequate knowledge of different transducers and Actuators.
4. learn about the Micro sensors and Micro actuators.
5. know the selection of sensor materials for fabrication for different applications.

UNIT I FUNDAMENTALS AND TEMPERATURE SENSORS 9

Difference between sensor, transducer and Actuators- Classification of sensors: Proprioceptive and Exteroceptive – Active and Passive– Contact and Non-contact, selection and characteristics: Range; resolution, Sensitivity, error, repeatability, linearity and accuracy, Primary sensing elements. Temperature sensors: Principle of operation, construction details, characteristics and applications of Bimetallic thermometer, Resistance thermometer, Thermistor, Thermocouples and Total radiation Pyrometers.

UNIT II STRAIN, FORCE, TORQUE AND PRESSURE SENSORS 9

Strain gauges, strain gauge beam force sensor, piezoelectric force sensor, load cell, torque sensor, Piezoresistive and capacitive pressure sensor, Manometer, vacuum sensors, Pirani gauge and the applications.

UNIT III DISPLACEMENT, LEVEL AND FLOW SENSORS 9

Displacement Sensors: LVDT, RVDT, eddy current, transverse inductive, Hall Effect, magneto resistive, magneto-strictive sensors. Liquid level sensor: Fabry Perot sensor, ultrasonic sensor, capacitive liquid level sensor. Flow sensors: pressure gradient technique, ultrasonic, electromagnetic sensors and Hot wire anemometer. Micro flow sensor, Coriolis mass flow and drag flow sensor.

UNIT IV MICRO MACHINING TECHNOLOGIES 9

Overview of silicon processes techniques, Photolithography, Ion Implantation, and Diffusion, Chemical Vapor Deposition, Physical vapor Deposition, Epitaxy, Etching, Bulk micromachining, Surface Micromachining, LIGA and other techniques.

UNIT V ACTUATORS 9

Definition, types and selection of Actuators; linear; rotary; Logical and Continuous Actuators, Pneumatic actuator, Hydraulic actuator - Control valves and cylinders Electrical actuating systems: Solenoids, Electric Motors- D.C motors - AC motors - Three Phase Induction Motor, Stepper motors -Piezoelectric Actuator.

	TOTAL PERIODS	45

COURSE OUTCOMES

At the end of this course, students will be able to		BT Mapped (Highest Level)
CO1	analyze the basics and design the resistive sensors.	Understanding (K2)
CO2	identify the materials used for the design of inductive and Capacitive Sensors.	Applying (K3)
CO3	explain the operations of various types of Actuators.	Applying (K3)
CO4	design Micro sensors and Micro Actuators for various applications.	Understanding (K2)
CO5	describe fabrication process and compare various Micro machining processes.	Analyzing (K4)

TEXT BOOKS

1. Sergej Fatikow and Ulrich Rembold, " Microsystem Technology and Microbotics" First edition, Springer –Verlag NEwyork, Inc, 1997
2. Jacob Fraden, "Hand Book of Modern Sensors: Physics, Designs and Application" Fourth edition, Springer, 2010.

REFERENCES

1. Robert H Bishop, "The Mechatronics Hand Book", CRC Press, 2002.
2. Thomas. G. Bekwith and Lewis Buck.N, "Mechanical Measurements", Oxford and IBH publishing Co. Pvt. Ltd.
3. Massood Tabib and Azar, "Microactuators Electrical, Magnetic, thermal, optical, mechanical, chemical and smart structures", First edition, Kluwer academic publishers, Springer, 1999.
4. Manfred Kohl, Shape Memory Actuators, first edition, Springer.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	Programme Outcomes PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	-	2	2	3	3

CY23855	IOT AND ITS APPLICATIONS	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	understand the fundamentals about IoT.
2.	study about IoT Access technologies.
3.	explain the different IoT hardware platforms and building blocks.
4.	know about IoT Data Analytics and supporting services.
5.	analyze about various IoT case studies and industrial applications.

UNIT I **FUNDAMENTALS OF IoT** 9

Evolution of Internet of Things, Enabling Technologies, M2M Communication, IoT World Forum (IoTWF) standardized architecture, Simplified IoT Architecture, Core IoT Functional Stack, Fog, Edge and Cloud in IoT, Functional blocks of an IoT ecosystem, Sensors, Actuators, Smart Objects and Connecting Smart Objects.

UNIT II **IoT PROTOCOLS** 9

IoT Access Technologies: Physical and MAC layers, topology and Security of IEEE 802.15.4, 802.11ah and Lora WAN, Network Layer: IP versions, Constrained Nodes and Constrained Networks,6LoWPAN, Application Transport Methods: SCADA, Application Layer Protocols: CoAP and MQTT.

UNIT III **DESIGN AND DEVELOPMENT** 9

Design Methodology, Embedded computing logic, Microcontroller, System on Chips, IoT system building blocks IoT Platform overview: Overview of IoT supported Hardware platforms such as: Raspberry pi, Arduino Board details.

UNIT IV **DATA ANALYTICS AND SUPPORTING SERVICES** 9

Data Analytics: Introduction, Structured Versus Unstructured Data, Data in Motion versus Data at Rest, IoT Data Analytics Challenges, Data Acquiring, Organizing in IoT/M2M, Supporting Services: Computing Using a Cloud Platform for IoT/M2M Applications/Services, Everything as a service and Cloud Service Models.

UNIT V **INDUSTRIAL APPLICATIONS** 9

IoT applications in home, infrastructures, buildings, security, Industries, Home appliances, other IoT electronic equipments, Industry 4.0 concepts.

TOTAL PERIODS 45

COURSE OUTCOMES

At the end of this course, students will be able to		**BT Mapped (Highest Level)**
CO1	understand the basics of IoT.	Understanding (K2)
CO2	implement the state of the Architecture of an IoT.	Analyzing (K4)

CO3	identify the design methodology and hardware platforms involved in IoT.	Understanding (K2)
CO4	explain the analysis and organization of data.	Understanding (K2)
CO5	compare IOT Applications in Industrial & real world.	Applying (K3)

TEXT BOOKS

1. IoT Fundamentals: Networking Technologies, Protocols and Use Cases for Internet of Things, David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton and Jerome Henry, Cisco Press, 2017.
2. Internet of Things – A hands-on approach, Arshdeep Bahga, Vijay Madisetti, Universities Press, 2015.

REFERENCES

1. The Internet of Things – Key applications and Protocols, Olivier Hersent, David Boswarthick, Omar Elloumi and Wiley, 2012.
2. "From Machine-to-Machine to the Internet of Things – Introduction to a New Age of Intelligence", Jan Ho¨ ller, Vlasios Tsiatsis, Catherine Mulligan, Stamatis, Karnouskos, Stefan Avesand. David Boyle and Elsevier, 2014.
3. Architecting the Internet of Things, Dieter Uckelmann, Mark Harrison, Michahelles and Florian (Eds), Springer,2011.
4. Recipes to Begin, Expand, and Enhance Your Projects, 2nd Edition, Michael Margolis, Arduino Cookbook and O"Reilly Media,2011.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's
(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	Programme Outcomes PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO4	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO5	2	2	2	2	2	2	-	-	-	-	2	2	3	3

CY23856	INDUSTRIAL IOT	3	0	0	3

COURSE OBJECTIVES

To enable the students to

1.	learn IOT fundamental computations and evolutions of industry 4.0.
2.	know the perspective of industrial IOT process.
3.	study about IIOT reference architectures and offsite technologies.
4.	find the available on-site reality and communication technologies.
5.	acquire the knowledge of industrial data acquisition and its applications.

UNIT I	**OVERVIEW OF INDUSTRIAL IOT**	**9**
IOT architecture, application based IOT protocol, cloud computing, fog computing, sensor cloud, big data; industry 4.0 – industrial revolution, Evolution of industry 4.0, environmental impacts, industrial internet, applications – IIoT – Basics of CPS, CPS and IIoT.		
UNIT II	**INDUSTRY 4.0 BASICS**	**9**
Design requirements, drivers of industry 4.0, sustainability assessment of industry, smart business perspective, cyberseurity, impacts of industry 4.0 – Industrial IoT – Industrial internet systems, industrial sensing, industrial process.		
UNIT III	**IIOT REFERENCE ARCHITECTURE**	**9**
Business models – definition, business for IoT and IIoT, reference architecture of IoT and IIoT, IIRA; Offsite Technologies – cloud computing and fog computing for IIoT.		
UNIT IV	**ON SITE TECHNOLOGIES**	**9**
Need for industry 4.0 - Augmented reality - virtual reality - big data and advanced analytics - smart factories – lean manufacturing system; industrial data transmission – foundation field bus, profibus, HART, inter bus, bit bus, CC-link, mod bus, Digital STROM, CAN, Lonworks, ISA 100.11a, wireless HART, LoRa, LoRaWAN.		
UNIT V	**CASE STUDIES OF IIOT SYSTEMS**	**9**
Industrial data acquisition – DCS, PLC, SCADA – IIOT analytics – Machine learning and data science in industries – plant safety and security; case studies – manufacturing industry - automotive industry - mining industry.		
	TOTAL PERIODS	**45**

COURSE OUTCOMES

	At the end of this course, students will be able to	**BT Mapped (Highest Level)**
CO1	understand the revolution in industrial data processing techniques.	Understanding (K2)
CO2	explain the design requirements, security and internet system for IIOT.	Applying (K3)
CO3	recognize architectural and computing strategies of IIOT.	Analyzing (K4)

PAAVAI ENGINEERING COLLEGE, NAMAKKAL
Approved
BOARD OF STUDIES
CYBER SECURITY
5/7/24
AUTONOMOUS

CO4	identify the state of art technologies for industrial data communication.	Applying (K3)
CO5	realize the industrial data acquisition methods with real time examples.	Analyzing (K4)

TEXT BOOKS

1. Sudip Misra, chandana Roy, Anandarup Mukharjee, "Introduction to Industrial Internet of Tings and Industry 4.0", CRC Press, Taylor & Francis Group, 2021.
2. Ismail Butun, "Industrial IoT: Challenges, Design Principles, Applications, and Security", Springer Nature, 2020.

REFERENCES

1. Jiafu Wan, Iztok Humar, Daqiang Zhang, "Industrial IoT Technologies and Applications", Springer, 2016.
2. R.Anandan, Suseendran Gopalakrishnan,Souvik Pal, Noor Zaman Subhas Chandra Mukhopadhyay, Gourab Sen Gupta, "Industrial Internet of Things (IIoT): Intelligent Analytics for Predictive Maintenance", John Wiley & Sons, 2022.
3. Anand Sharma, Sunil Kumar Jangir, Manish Kumar, Dilip Kumar Choubey, Tarun Shrivastava, S.Balamurugan, "Industrial Internet of Things Technologies and Research Directions", CRC Press, 2020.
4. Sudan Jha, Usman Tariq, Gyanendra Prasad Joshi, Vijender Kumar Solanki, "Industrial Internet of Things Technologies, Design, and Applications", CRC Press, 2022.

CO-PO MAPPING:

Mapping of Course Outcome (CO's) with Programme Outcomes (PO's) and Programme Specific Outcomes PSO's

(1/2/3 indicates strength of correlation) 3-Strong, 2-Medium, 1-Weak

CO's	Programme Outcomes PO's												PSO's	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO2	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO3	2	2	2	2	2	2	-	-	-	-	2	2	3	3
CO4	3	3	3	3	3	3	-	-	-	-	2	2	3	3
CO5	3	3	3	3	3	3	-	-	-	-	2	2	3	3