KUMARAGURU COLLEGE OF TECHNOLOGY,

An autonomous Institution affiliated to Anna University, Chennai

COIMBATORE – 641 049.

M.E. COMPUTER SCIENCE AND ENGINEERING
(CYBER SECURITY)

REGULATION 2024

I to IV Semesters

Department of Computer Science and Engineering

VISION

To evolve as a School of Computer Science with centers of excellence having international reputation to serve the changing needs of Indian industry and society.

MISSION

- Computer Science and Engineering department is committed to bring out career-oriented graduates who are industry ready through innovative practices of teaching-learning process.
- To cultivate professional approach, strong ethical values and team spirit along with leadership qualities among the graduates by organizing workshops, seminars and conferences periodically. Association with professional bodies and invitation to external experts should help this.
- To contribute towards techno-economic and social development of the nation through quality human resources and encouraging entrepreneurship among the young graduates.

PROGRAM EDUCATIONAL OBJECTIVES (PEOs)

The Program Educational Objectives of Postgraduate Program are

PEO1: Graduates will pursue successful careers in industry, government, or entrepreneurial ventures.

PEO2: Graduates will apply core knowledge and specialized skills to solve complex problems in the field of computer science and engineering with a focus on cyber security.

PEO3: Graduates will apply ethical practices and cyber security expertise to address societal challenges and ensure the safe use of digital technologies.

PROGRAM OUTCOMES (POs)

Graduates of the Computer Science and Engineering Postgraduate Program should have the ability to:

PO1 An ability to independently carry out research /investigation and development work to solve practical problems

PO2 An ability to write and present a substantial technical report/document

PO3 Students should be able to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

PO4 Students will be able to analyse, design, and develop secure computing solutions by applying advanced knowledge in computer science, cryptography, network security, ethical hacking, and related areas to protect systems against cyber threats.

PO5 Demonstrate the ability to develop the capabilities appropriate for the industry trends by engaging in independent and life-long learning including industry goal oriented online courses and mini-projects.

KUMARAGURU COLLEGE OF TECHNOLOGY

COMPUTER SCIENCE AND ENGIEERING
REGULATION 2024
M.E. Computer Science and Engineering (Cyber Security)- Curriculum

Semester I

S. No	Course Code	Course Title	Course Mode	Course Category	L	T	P	J	C
1.	24MAT501	Mathematical Foundations for Cyber Security	Theory	BS	3	0	0	0	3
2.	24CBI502	Advanced Data Structures and Algorithms	Embedded	PC	3	0	2	0	4
3.	24CBI503	Operating System Security	Embedded	PC	3	0	2	0	4
4.	24CBI504	Cryptography and Network Security	Embedded	PC	3	0	2	0	4
5.	24CBI505	Database Management System and Security	Embedded	PC	3	0	2	0	4
6.	24CBI506	Research Methodology and Ethics	Embedded	ES	3	0	2	0	4
7.	24__O__	Open Elective I	Theory	OE	3	0	0	0	3
Total Credits									**26**
Total Contact Hours / Week									**31**

Semester II

S. No	Course code	Course Title	Course Mode	Course Category	L	T	P	J	C
1.	24CBI507	Digital Forensics	Embedded	PC	3	0	2	0	4
2.	24CBI508	Web Application Security	Embedded	PC	3	0	2	0	4
3.	24CBT509	Artificial Intelligence for Cyber Security	Theory	PC	3	0	0	0	3
4.	24CB____	Program Elective I	Embedded/ Theory	PE	*	0	*	0	3
5.	24CB____	Program Elective II	Embedded/ Theory	PE	*	0	*	0	3
6.	24CB____	Program Elective III	Embedded/ Theory	PE	*	0	*	0	3
7.	24__O___	Open Elective II	Theory	OE	3	0	0	0	3
Total Credits									**23**
Total Contact Hours / Week									**28** *****

SEMESTER-III

S. No	Course code	Course Title	Course Mode	Course Category	L	T	P	J	C
1.	24CB____	Program Elective IV	Embedded/ Theory	PE	*	0	*	0	3

2.	24CBJ601	Internship #	Project	PRJ	0	0	0	*	2
3.	24CBJ602	Project Phase I	Project	PRJ	0	0	0	20	10
								Total Credits	**15**
								Total Contact Hours / Week	**23 ***
SEMESTER-IV									
S. No	**Course code**	**Course Title**	**Course Mode**	**Course Category**	**L**	**T**	**P**	**J**	**C**
1.	24CBJ603	Project Phase II	Project	PRJ	0	0	0	40	20
								Total Credits	**20**
								Total Contact Hours / Week	**40**
Total Credits :84									

Internship (2C) to be undergone during I yr summer vacation - Evaluated and credits listed in III semester

List of Program Electives

S. No	Course code	Course Title	Course Mode	Course Category	L	T	P	J	C
1.	24CBC001	Blockchain Technology and Security	Embedded	PE	2	0	2	0	3
2.	24CBC002	Cloud Security	Embedded	PE	2	0	2	0	3
3.	24CBC003	Secure Software Development	Embedded	PE	2	0	2	0	3
4.	24CBE004	Cyber Physical Systems and Security	Theory	PE	3	0	0	0	3
5.	24CBE005	Cyber Ethics and Laws	Theory	PE	3	0	0	0	3
6.	24CBC006	Cyber Security audit and compliances	Embedded	PE	2	0	2	0	3
7.	24CBC007	Malware Analysis and System Security	Embedded	PE	2	0	2	0	3
8.	24CBC008	Incident Response Management	Embedded	PE	2	0	2	0	3
9.	24CBE009	Cyber Threat Hunting and Intelligence	Theory	PE	3	0	0	0	3
10.	24CBC010	Mobile Device Forensics	Embedded	PE	2	0	2	0	3
11.	24CBC011	Intrusion Detection and Prevention System	Embedded	PE	2	0	2	0	3
12.	24CBC012	Mobile Application Security	Embedded	PE	2	0	2	0	3

List of Open Electives									
S. No	Course code	Course Title	Course Mode	Course Category	L	T	P	J	C
1.	24MEO001	Sustainable Innovations and Practices	Theory	OE	3	0	0	0	3
2.	24MEO002	Electric and Autonomous Mobility	Theory	OE	3	0	0	0	3
3.	24IEO074	Modern Financial Strategies and Innovations	Theory	OE	3	0	0	0	3
4.	24IEO075	Sports Analytics and Emerging Technologies	Theory	OE	3	0	0	0	3
5.	24IEO076	Healthcare Innovation and Technology	Theory	OE	3	0	0	0	3
6.	24IEO077	Corporate Strategy and Innovation	Theory	OE	3	0	0	0	3
7.	24IEO078	Gamification and Gaming	Theory	OE	3	0	0	0	3
8.	24IEO079	Environmental Innovations and Management	Theory	OE	3	0	0	0	3

Semester-wise Credits	
Semester – I	26
Semester – II	23
Semester – III	15
Semester – IV	20
Total Credits	**84**

SYLLABUS

24MAT501	**Mathematical Foundations for Cyber Security Systems**	**L**	**T**	**P**	**J**	**C**
		3	**0**	**0**	**0**	**3**
BS		**SDG**	**4,9**			

Pre-requisite courses	**Nil**	**Data Book / Codes / Standards (If any)**	Nil

Course Objectives:	**The purpose of taking this course is to:**
1	Apply modular arithmetic to cryptographic algorithms.
2	Understand prime numbers, primality testing and their role in encryption.
3	Use combinatorics to assess password strength and brute-force attack feasibility.
4	Apply graph theory to analyse network topology vulnerabilities.

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Bloom's Taxonomy Level (BTL)**
CO 1	Understand the concept of equivalence relations and their role in partitioning sets for classification of objects and data.	U
CO 2	Apply the characteristic of a ring and compute the quotient field of an integral domain for computational systems.	Ap
CO 3	Utilize the Fundamental Theorem of Arithmetic for unique prime factorization and its role in cryptographic systems.	Ap
CO 4	Analyse advanced primality testing algorithms to evaluate large integers for use in cryptographic key generation.	An
CO 5	Construct the design and functioning of pseudorandom number generators based on block ciphers and distinguish them from stream cipher-based generators.	An

Course Outcomes (CO)	**Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)**				
	1	**2**	**3**	**4**	**5**
1	2			3	3
2		2		3	3
3	3	1		3	3
4	3			3	3
5		2		3	3

Course Content	
GROUP THEORY Introduction to Set Theory, Binary Operations on Sets, Equivalence Relations, Introduction to Groups, Subgroups, Cyclic Groups, dihedral groups , Permutation Groups, cosets, Lagrange's theorem, Normal Subgroups, Quotient Groups, Isomorphisms, Homomorphisms	**9 Hours**
RINGS AND FIELDS Definition and basic concepts in rings, examples and basic properties, zero divisors, integral domains, fields, characteristics of a ring, quotient field of an integral domain, subrings, ideals, maximal ideal,	**9 Hours**

prime ideal, quotient rings. Euclidean domains, Polynomials, prime, irreducible elements and their properties. Eisensteins irreducibility criterion and Gauss's lemma.	
ELEMENTARY NUMBER THEORY The division algorithm, Divisibility and the Euclidean algorithm, The fundamental theorem of arithmetic, Modular arithmetic and basic properties of congruences; Principles of mathematical induction and well ordering principle. Primality Testing algorithms, Chinese Remainder Theorem, Quadratic Congruence	**9 Hours**
ADVANCED NUMBER THEORY Advanced Number Theory – Primality Testing algorithms, Chinese Remainder Theorem, Quadratic Congruence, Discrete Logarithm, Factorization Methods, Side Channel Attacks, Shannon Theory, Perfect Secrecy, Semantic Security.	**9 Hours**
PSEUDORANDOM NUMBER GENERATION AND PROBABILITY THEORY Principles of Pseudorandom Number Generation, Principles of Pseudorandom Number Generation using a Block Cipher, Stream Ciphers, RC4 , True Random Number Generators. Introduction – Concepts of Probability - Conditional Probability - Baye's Theorem - Random Variables – discrete and continuous- central Limit Theorem-Stochastic Process- Markov Chain.	**9 Hours**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**0**	**Project Hours:**	**0**	**Total Hours:**	**45**

Learning Resources

Textbooks

1. D.S. Dummit and R.M. Foote, "Abstract Algebra", Wiley Publisher, 2011
2. Michael Artin, "Algebra", Pearson Education,2011.
3. J.A. Gallian, "Contemporary Abstract Algebra", Narosa Publishing House,2008.

Reference books/ Web Links

1. I. N. Herstein, "Topics in Algebra", Wiley,2006.
2. N. Jacobson, "Basic Algebra I", Hindustan Publishing Company,2009.
3. William Stallings, "Cryptography and Network Security Principles and Practice", Pearson Education, 2017.

Online Resources

1. https://www.youtube.com/playlist?list=PLzkMouYverAI7bP0--gDY0286QD-Mwd2r.
2. https://www.coursera.org/learn/mathematical-foundations-cryptography.
3. https://www.classcentral.com/course/youtube-wimsa-math-in-cyber-security-181677

Assessment

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)

Course Curated by

Expert(s) from Industry	**Expert(s) from Higher Education Institution**	**Internal Expert**	
-	-	Dr A.Roshini, AP III / CSE	
Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

		L	T	P	J	C
24CBI502	**Advanced Data Structures and Algorithms**	3	0	2	0	4
PC		SDG	4,9			

Pre-requisite courses	**Nil**	**Data Book / Codes / Standards (If any)**	Nil

Course Objectives:	**The purpose of taking this course is to:**
1	To understand the usage of algorithms in computing
2	To learn and use hierarchical data structures and its operations
3	To learn the usage of graphs and its applications
4	To select and design data structures and algorithms that is appropriate for problems
5	To study about NP Completeness of problems

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Bloom's Taxonomy Level (BTL)**
CO 1	Analyze and compare various algorithms for efficiency	An
CO 2	Implement and analyze hierarchical data structures	Ap
CO 3	Design algorithms using graph structure and various string-matching algorithms to solve real-life problems	Ap
CO 4	Design solutions using dynamic programming & greedy techniques	Ap
CO 5	Classify NP-hard/NP-complete problems	An

Course Outcomes (CO)	**Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)**				
	1	**2**	**3**	**4**	**5**
1	3		3		
2	2		2	3	
3	3	1	3	2	1
4	3		3	2	
5	3				

Course Content

ROLE OF ALGORITHMS IN COMPUTING & COMPLEXITY ANALYSIS Algorithms – Algorithms as a Technology -Time and Space complexity of algorithms- Asymptotic analysis-Average and worst-case analysis-Asymptotic notation-Importance of efficient algorithms- Program performance measurement - Recurrences: The Substitution Method – The Recursion-Tree Method- Data structures and algorithms.	**9 Hours**

Practical Component Implementation of recursive function for tree traversal and Fibonacci - Implementation of iteration function for tree traversal and Fibonacci - Implementation of Merge Sort and Quick Sort - Implementation of a Binary Search Tree	**8 Hours**
HIERARCHICAL DATA STRUCTURES Binary Search Trees: Basics – Querying a Binary search tree – Insertion and Deletion- Red Black trees: Properties of Red-Black Trees – Rotations – Insertion – Deletion -B-Trees: Definition of B -trees – Basic operations on B-Trees – Deleting a key from a B-Tree- Heap – Heap Implementation – Disjoint Sets - Fibonacci Heaps: structure – Mergeable-heap operations- Decreasing a key and deleting a node-Bounding the maximum degree **Practical Component** Red-Black Tree Implementation - Heap Implementation - Fibonacci Heap Implementation	**9 Hours** **8 Hours**
GRAPHS Elementary Graph Algorithms: Representations of Graphs – Breadth-First Search – Depth-First Search – Topological Sort – Strongly Connected Components- Minimum Spanning Trees: Growing a Minimum Spanning Tree – Kruskal and Prim- Single-Source Shortest Paths: The Bellman-Ford algorithm – Single-Source Shortest paths in Directed Acyclic Graphs – Dijkstra‘s Algorithm; Dynamic Programming - All-Pairs Shortest Paths: Shortest Paths and Matrix Multiplication – The Floyd-Warshall Algorithm **Practical Component** Graph Traversals - Spanning Tree Implementation - Shortest Path Algorithms (Dijkstra's algorithm, Bellman Ford Algorithm)	**9 Hours** **8 Hours**
ALGORITHM DESIGN TECHNIQUES Dynamic Programming: Matrix-Chain Multiplication – Elements of Dynamic Programming – Longest Common Subsequence- Greedy Algorithms: – Elements of the Greedy Strategy- An Activity-Selection Problem - Huffman Coding. **Practical Component** Implementation of Matrix Chain Multiplication - Activity Selection and Huffman Coding Implementation	**9 Hours** **6 Hours**
NP COMPLETE AND NP HARD NP-Completeness: Polynomial Time – Polynomial-Time Verification – NP- Completeness and Reducibility – NP-Completeness Proofs – NP-Complete Problems.	**9 Hours**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**30**	**Project Hours:**	**0**	**Total Hours:**	**75**

Learning Resources
Textbooks
-
Reference books/ Web Links
1. S.Sridhar,” Design and Analysis of Algorithms”, Oxford University Press, 1st Edition, 2014. 2. Adam Drozdex, “Data Structures and algorithms in C++”, Cengage Learning, 4th Edition, 2013. 3. T.H. Cormen, C.E.Leiserson, R.L. Rivest and C.Stein, "Introduction to Algorithms", Prentice Hall of India, 3rd Edition, 2012. 4. Mark Allen Weiss, “Data Structures and Algorithms in C++”, Pearson Education, 3rd Edition, 2009.

5. E. Horowitz, S. Sahni and S. Rajasekaran, “Fundamentals of Computer Algorithms”, University Press, 2nd Edition, 2008.
6. Alfred V. Aho, John E. Hopcroft, Jeffrey D. Ullman, “Data Structures and Algorithms”, Pearson Education, Reprint 2006.

Online Resources

1. https://ocw.mit.edu/courses/6-851-advanced-data-structures-spring-2012/
2. https://www.classcentral.com/course/edx-advanced-data-structures-21429
3. https://www.coursera.org/learn/advanced-data-structures
4. https://web.stanford.edu/class/cs166/index.html

Assessment (Embedded course)

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)
Lab Workbook, Experimental Cycle tests, viva-voce.

Course Curated by

Expert(s) from Industry	Expert(s) from Higher Education Institution	Internal Expert	
-	-	Dr V.Vanitha, P/CSE	
Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

		L	T	P	J	C
24CBI503	**Operating System Security**	**3**	**0**	**2**	**0**	**4**
PC		**SDG**	**4,9**			

Pre-requisite courses	**Nil**	**Data Book / Codes / Standards (If any)**	Nil

Course Objectives:	**The purpose of taking this course is to:**
1	To understand the operating system concepts like process, memory, file system, and scheduling.
2	To explore protection models, threats, and mechanisms including access control and secure system design.
3	To analyze and mitigate security threats such as malware, buffer overflows, and cryptographic attacks.
4	To understand and configure secure Linux networking environments using tools and protocols like SSH, firewalls, and LAMP stack.
5	To gain hands-on experience with system administration tasks including user management, auditing, and recovery

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Bloom's Taxonomy Level (BTL)**
CO 1	Explain the structure and operations of operating systems and perform basic process and memory management operations	U
CO 2	Demonstrate knowledge of protection mechanisms in operating systems and implement basic access control techniques	Ap
CO 3	Identify and mitigate common operating system security threats such as malware and buffer overflow, and implement secure coding practices	Ap
CO 4	Perform system administration tasks including user management, system monitoring, and scheduling in a secure Linux environment.	Ap
CO 5	Apply secure Linux-based network services and analyze case studies on OS protection and co-existence	Ap

Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)					
Course Outcomes (CO)	**1**	**2**	**3**	**4**	**5**
1	2		3	3	
2	2		3	3	
3	2		3	3	
4	2		3	3	
5	2	1	3	3	

Course Content	
INTRODUCTION Introduction, Computer system organization and architecture, Operating system structure and operations, Process Management, Memory Management, file systems management Protection and security, Scheduling Algorithms, Interprocess Communication **Practical Component:** Process Creation & Management: Use fork(), exec(), wait() to create and manage processes in Linux - CPU Scheduling Simulation: Implement FCFS, SJF, or Round Robin in C - Memory Allocation Techniques: Simulate First Fit, Best Fit, and Worst Fit algorithms.	**9 Hours** **6 Hours**
OPERATING SYSTEMS PROTECTION Protection Goals, Protection Threats, Access Control Matrix, Access Control Lists(ACL's), Capability Lists(C-lists), Protection systems, Lampson's access matrix, mandatory protection systems, Reference monitor, Secure operating system definition **Practical Component:** Access Control Matrix: Implement a basic access control matrix in C - File Permissions: Demonstrate file-level access control using chmod, umask, and ls -l - Access Control List (ACL): Configure ACLs in Linux using setfacl and getfacl.	**9 Hours** **6 Hours**
OPERATING SYSTEM SECURITY Security Goals, Security Threats, Security Attacks- Trojan Horses, Viruses and Worms, Buffer Overflow attacks and Techniques, Formal Aspects of Security, Encryption- Attacks on Cryptographic Systems, Encryption Techniques, Authentication and Password Security, Intrusion detection, malware defenses, UNIX and Windows Security **Practical Component:** Buffer Overflow Simulation: Demonstrate a buffer overflow and use basic protection - Password Hashing: Write a secure login system using password hashing (e.g., SHA-256) - Basic Intrusion Detection: Use tools like chkrootkit or fail2ban to detect unauthorized access.	**9 Hours** **6 Hours**
SYSTEM ADMINISTRATION Security Basics, Securing the Server Itself, Maintenance and Recovery, Monitoring and Audit, Introduction to Linux Systems, Configuration Management, Log Auditing and Vulnerability Assessment. **Practical Component:** User & Group Management: Use useradd, passwd, groupadd, usermod for admin tasks - Scheduled Tasks: Create automated jobs using cron - System Monitoring: Use top, vmstat, dmesg for performance and error monitoring	**9 Hours** **6 Hours**
LINUX NETWORKING Networking Technologies: DHCP, DNS, NFS/ISCSI, SMTP, SNMP, LAMP, Firewall/IDS/SSH, Securing Linux. Case Studies: Security and Protection- MULTICS, UNIX, LINUX ad Windows, Windows and Linux Coexisting **Practical Component:** SSH Configuration**:** Secure a system using SSH and key-based authentication - Firewall Setup: Use ufw or iptables to configure basic firewall rules - LAMP Stack Installation: Set up Apache, MySQL, and PHP on Linux (Ubuntu/CentOS).	**9 Hours** **6 Hours**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**30**	**Project Hours:**	**0**	**Total Hours:**	**75**

Learning Resources

Textbooks

Reference books/ Web Links

1. Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, “Operating System Concepts”, 10th Edition, Wiley Publication, 2018 (Unit 1)
2. Dhananjay M. Dhamdhere, “Operating Systems: A Concept-Based Approach”, 3rd Edition, McGraw-Hill, 2015 (Unit 2, 3)
3. Jordan Krause, “Windows Server 2016 Security, Certificates, and Remote Access Cookbook: Recipe-based guide for security, networking and PKI in Windows Server 2016”, Pckt Publishing, 2018.
4. Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley, Dan Mackin,“Linux Administration Handbook”, Fifth Edition, Addison-Wesley, 2017 (Unit 5)
5. Promod Chandra P Bhat,, “An Introduction to Operating Systems: Concepts and practice”, 5th Edition, Prentice Hall of India, 2019.
6. William Stalling, “Operating System: Internals and Design Principles”, 9th Edition, Pearson, 2017.
7. Tom Adelstein and Bill Lubanovic, “Linux System Administration”, 1st Edition, Shroff., 2012.

Online Resources

1. nptel.ac.in/courses/106106144
2. Linux Server Management and Security | Coursera
3. Operating Systems and You: Becoming a Power User | Coursera

Assessment (Embedded course)

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)
Lab Workbook, Experimental Cycle tests, viva-voce.

Course Curated by

Expert(s) from Industry	Expert(s) from Higher Education Institution	Internal Expert
-	-	Dr V.Vanitha, P/CSE

Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

24CBI504	Cryptography and Network Security	L	T	P	J	C
		3	0	2	0	4
PC		SDG	4,9			

Pre-requisite courses	Nil	Data Book / Codes / Standards (If any)	Nil

Course Objectives:	The purpose of taking this course is to:
1	To understand fundamental principles of cryptography and network security mechanisms.
2	To explore symmetric and asymmetric encryption algorithms and their applications in secure communications.
3	To analyze and implement cryptographic techniques including digital signatures, key management, and message authentication.
4	To investigate common network vulnerabilities, threats, and countermeasures using real-world tools and techniques.
5	To develop practical skills in ethical hacking, reconnaissance, and system exploitation in controlled environments.

Course Outcomes:	After successful completion of this course, the students shall be able to	Bloom's Taxonomy Level (BTL)
CO 1	Explain security services, mechanisms, and vulnerabilities in wired and wireless networks, for secure communication.	U
CO 2	Apply classical, modern cryptographic techniques and demonstrate the ability to manage keys and implement cryptographic hash functions for data integrity, confidentiality.	Ap
CO 3	Use network analysis and penetration testing tools to identify, simulate, and assess vulnerabilities	Ap
CO 4	Apply ethical hacking methodologies to analyse threats, vulnerabilities, and explo	Ap
CO 5	Apply systematic reconnaissance, footprinting, port scanning, and OS enumerati using relevant tools and scripting methods to assess security vulnerabilities.	Ap

Course Outcomes (CO)	Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)				
	1	2	3	4	5
1	2			3	
2			2	3	
3	2			3	
4				3	3
5	1		1	3	3

Course Content	
INTRODUCTION TO NETWORK SECURITY Security Mechanisms and Services, Classical Encryption Techniques – Block Ciphers, DES, Finite Fields and AES, Block Cipher Operation, Stream Cipher - Uses of Modes of operation **Practical Component** Implementation of DES and AES modules	**9 Hours** **4 Hours**
ASYMMETRIC CIPHERS and MESSAGE AUTHENTICATION Modern Asymmetric block ciphers – RSA - Discrete Log problem - Diffie Hellman Key Exchange - Elliptic curve cryptography - MAC – Cryptographic Hash Functions- Digital Signatures – NIST Digital Signature Algorithm - Key management system- Key Distribution & Key Agreements **Practical Component** Implementation of RSA, Diffie Hellman key exchange algorithm - Implementation of Hash algorithm	**9 Hours** **10 Hours**
SECURITY ISSUES IN INTERNET PROTOCOL Reconnaissance-Wireshark- TCPDump - Netdiscover - Shodan ,NESSUS,Hping3 NSE Scripts: Introduction - How to write and read NSE script - TCP session Hijacking - UDP session Hijacking -HTTP Session – Hijacking - Spoofing basics - IP, DNS and ARP Spoofing **Practical Component** Reconnaissance and Network Scanning using Wireshark, TCPDump, Netdiscover, and shodan - Vulnerability Scanning using NESSUS - Writing and Executing NSE Scripts using Nmap	**9 Hours** **6 Hours**
ETHICAL HACKING Concept of ethical hacking - Phases involved in hacking - Footprinting - Introduction to foot printing, Understanding the information gathering methodology of the hackers, tools used for the reconnaissance phase. Port Scanning - Introduction, using port scanning tools, ping sweeps, Scripting enumeration-Introduction, enumerating windows OS & Linux OS **Practical Component** Install Kali or Backtrack Linux - Practice the basics of reconnaissance - Passive Footprinting Using OSINT Tools - Active Footprinting and Network Mapping - Enumeration of Windows and Linux Systems	**9 Hours** **4 Hours**
SYSTEM HACKING Aspect of remote password guessing, Role of eavesdropping, Various methods of password cracking, Keystroke Loggers, Understanding Sniffers, Comprehending Active and Passive Sniffing, ARP Spoofing and Redirection, DNS and IP Sniffing, HTTPS Sniffing **Practical Component** Demonstrate software keyloggers – Usage of Wireshark, tcpdump, and Ettercap to monitor network traffic – Demonstration of MITM via ARP spoofing.	**9 Hours** **6 Hours**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**30**	**Project Hours:**	**0**	**Total Hours:**	**75**

Learning Resources

Textbooks

1. William Stallings, “Network Security Essentials: Applications and Standards”, Pearson Education India; 6th edition (2018)
2. Ric Messier, CEH v11: Certified Ethical Hacker Study Guide, Wiley (2021).

Reference books/ Web Links

1. Ric Messier, CEH v11: Certified Ethical Hacker Study Guide, Wiley (2021).
2. William Stallings, “Cryptography and Network Security – Principles and Practices”, Pearson Education; Seventh edition, 2017
3. AtulKahate, “Cryptography and Network Security”, 2nd Edition, Tata McGraw Hill, 2008
4. Bruce Schneier, “Applied Cryptography”, JohnWiley& Sons Inc, 2001.
5. Charles P fleeger and Shari Lawrence P fleeger, “Security in Computing”, Fourth edition, PearsonEducation,2015.
6. Rajat Khare, "Network Seuciryt and Ethical Hacking", Luniver Press, 2006

Online Resources

1. https://onlinecourses.nptel.ac.in/noc22_cs90/preview
2. https://www.coursera.org/learn/crypto
3. https://cursa.app/en/free-course/cryptography-and-network-security-ebgc
4. https://www.coursera.org/specializations/certified-ethical-hacking-v12-cehv12-exam-prep-course-

Assessment (Embedded course)

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)
Lab Workbook, Experimental Cycle tests, viva-voce.

Course Curated by

Expert(s) from Industry	Expert(s) from Higher Education Institution	Internal Expert
-	-	Dr N.Suganthi, P/CSE

Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

24CBI505	**Database Management Systems and Security**	**L**	**T**	**P**	**J**	**C**
		3	**0**	**2**	**0**	**4**
PC		**SDG**	**4,9**			

Pre-requisite courses	**Nil**	**Data Book / Codes / Standards (If any)**	Nil

Course Objectives:	**The purpose of taking this course is to:**
1	Learn the fundamentals of data models, conceptualize and depict a database system using Entity Relationship diagram
2	Study the principles to be followed to create an effective relational database and write SQL queries to store/retrieve data to/from database systems.
3	Know the fundamental concepts of transaction processing, concurrency control techniques and recovery procedure.
4	Understand the need of security in Database Management systems
5	Learn how to secure Database Management systems

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Bloom's Taxonomy Level (BTL)**
CO 1	Describe common database security threats and analyze traditional and advanced security models such as Access Matrix, Take-Grant, and PN models.	U
CO 2	Apply classical security models to simulate secure access control policies using Linux or UNIX-based environments.	Ap
CO 3	Design secure database architectures by integrating intrusion detection strategies and statistical protection models using tools.	Ap
CO 4	Demonstrate role-based and method-level access control in object-oriented database systems using models.	An
CO 5	Apply object-level protection and fine-grained access control in active databases using models.	Ap

Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)					
Course Outcomes (CO)	**1**	**2**	**3**	**4**	**5**
1	2		3		3
2	2		3	2	3
3	2		3		3
4	3		3	2	
5	3	2	1		3

Course Content	
INTRODUCTION TO DATABASE SECURITY Introduction to Databases Security Problems in Databases Security Controls Conclusions Security Models - Introduction Access Matrix Model Take-Grant Model Acten Model PN Model Hartson and Hsiao's Model Fernandez's Model Bussolati and Martella's Model for Distributed databases **Practical Component** SQL Injection Attack Simulation and Prevention - Implementing Role-Based Access Control	**9 Hours** **6 Hours**
SECURITY MODELS Security Models - Bell and LaPadula's Model Biba's Model Dion's Model Sea View Model Jajodia and Sandhu's Model The Lattice Model for the Flow Control conclusion Security Mechanisms Introduction User Identification/Authentication Memory Protection Resource Protection Control Flow Mechanisms Isolation Security Functionalities in Some Operating Systems Trusted Computer System Evaluation Criteria **Practical Component** Simulate Bell-LaPadula and Biba Models Using Linux User Permissions - Implement Role-Based Access Control (RBAC) with sudo and Groups	**9 Hours** **6 Hours**
DATABASE DESIGN WITH INTRUSION DETECTION STRATEGIES Security Software Design Introduction A Methodological Approach to Security Software Design Secure Operating System Design Secure DBMS Design Security Packages Database Security Design Statistical Database Protection & Intrusion Detection Systems Introduction Statistics Concepts and Definitions Types of Attacks Inference Controls evaluation Criteria for Control Comparison. Introduction IDES System RETISS System ASES System Discovery **Practical Component** Apply column-level access controls on a MySQL/PostgreSQL database - Deploy a Basic Intrusion Detection System using snort/ Suricata	**9 Hours** **5 Hours**
SECURITY MODELS FOR OBJECT ORIENTED DATABASES Models For The Protection Of New Generation Database Systems -1 Introduction A Model for the Protection of Frame Based Systems A Model for the Protection of Object Oriented Systems SORION Model for the Protection of Object-Oriented Databases **Practical Component** Simulate Object-Oriented DBMS Access Control - Simulate method-level access restrictions based on roles.	**9 Hours** **6 Hours**
SECURITY MODELS FOR ACTIVE DATABASE SYSTEMS Models For The Protection Of New Generation Database Systems -2 A Model for the Protection of New Generation Database Systems: the Orion Model Jajodia and Kogan's Model A Model for the Protection of Active Databases Conclusions **Practical Component** Implement object-level protection with class hierarchies and access rights - Implement Jajodia and Kogan’s Fine-Grained Access Control	**9 Hours** **7 Hours**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**30**	**Project Hours:**	**0**	**Total Hours:**	**75**

Learning Resources

Textbooks

1. Database Security and Auditing, Hassan A. Afyouni, India Edition, CENGAGE Learning, 2013.
2. William Stallings, Lawrie Brown, “Computer Security: Principles and Practice”, Fourth Edition, Pearson(2021).
3. Elmasri, R., & Navathe, S. B. ,Fundamentals of database systems (7th ed.). Pearson(2017).
4. Database Security, Castano, Second edition, Pearson Education. 1995

Reference books/ Web Links

1. Pfleeger, C. P., Pfleeger, S. L., & Margulies, J., Security in computing , Pearson 2015
2. Anderson, R. J., Security engineering: A guide to building dependable distributed systems , Wiley,2020.
3. Alfred, Basta, and Zgola Melissa. "Database Security. 2011.

Online Resources

1. https://learn.eccouncil.org/course/sql-injection-attacks
2. https://www.coursera.org/learn/packt-security-architecture-and-engineering-f4vdz

Assessment (Embedded course)

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)
Lab Workbook, Experimental Cycle tests, viva-voce.

Course Curated by

Expert(s) from Industry	Expert(s) from Higher Education Institution		Internal Expert
-	-		Dr N.Rajathi, P/IT
Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

24CBI506	Research Methodology and Ethics	L	T	P	J	C
		3	0	2	0	4
ES		SDG	4			

Pre-requisite courses	Nil	Data Book / Codes / Standards (If any)	Nil

Course Objectives:	The purpose of taking this course is to:
1	To understand the philosophy of science and ethics.
2	To understand the research integrity and publication ethics.
3	To prepare article and submit to the journal.

Course Outcomes:	After successful completion of this course, the students shall be able to	Bloom's Taxonomy Level (BTL)
CO 1	Understand the concepts of research and formulate a research problem.	U
CO 2	Design and plan the research, collect data, interpret data and organize data.	Ap
CO 3	Demonstrate skill in writing research papers and prepare effective presentation.	Ap
CO 4	Understand the philosophy of science and ethics, research integrity and publication ethics.	U
CO 5	Understand the indexing and citation databases.	U
CO 6	Familiarize the types of open access publications and research metrics.	U

Course Outcomes (CO)	Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)				
	1	2	3	4	5
1	3	3			3
2	2	3			3
3	2	3			3
4	2	3		1	3
5	2	3			3
6	2	3		1	3

Course Content	
INTRODUCTION TO RESEARCH METHODS Definition and Objectives of Research - Scientific Methods, Various Steps in Scientific Research, Research planning - Selection of a Problem for Research, Formulation of the Selected Problems -Purpose of the Research, Formulation of research objectives - Formulation of research questions - Hypotheses Generation and Evaluation -Literature search, and review, Research abstract. **Practical Component** Problem formulation - Formulate research questions for domain specific Problems.	**9 Hours** **8 Hours**

RESEARCH DESIGN/PLAN Types and Methods of Research - Classification of Research - Sampling Techniques, Methods of Collecting Primary Data, Use of Secondary Data, Experimentation - Design of Experiments, Survey Research and Construction of Questionnaires - Pilot Studies and Pre-tests - Data Collection methods, Processing of Data, Editing, Classification and Coding, Transcription, Tabulation, Validity and Reliability.	**9 Hours**
RESEARCH REPORTS/THESIS Structure and Components of Research Report/thesis, Types of Report, Planning of Report/thesis Writing, Research Report Format, Layout of Research Report, Presentation of data and Data Analysis Reporting, Mechanism of writing a research report, Principles of Writing, Writing of Report-Writing of thesis-Differences between thesis and research paper writing.	**9 Hours**
Practical Component Software tool to identify predatory publications - Journal finder / journal suggestion tools viz. JANE, Elsevier Journal Finder, Springer, Journal Suggester, etc.	**8 Hours**
PHILOSOPHY AND ETHICS Introduction to philosophy: definition, nature and scope, concept, branches - Ethics: definition, moral philosophy, nature of moral judgements and reactions. Ethics with respect to science and research - Intellectual honesty and research integrity - Scientific misconducts: Falsification, Fabrication and Plagiarism (FFP) - Redundant Publications: duplicate and overlapping publications, salami slicing - Selective reporting and misrepresentation of data.	**9 Hours**
Practical Component Indexing database – Citation databases Scopus and Web of science - Plagiarism software – Use of plagiarism checking software like Turnitin, Urkund and other open-source software tools.	**8 Hours**
PUBLICATION ETHICS AND OPEN ACCESS PUBLISHING Publication ethics: definition, introduction and importance -Publication misconduct: definition, concept, problems that lead to unethical behaviour and vice versa, types - Violation of publication ethics, authorship and contributor ship - Identification of publication misconduct, complaints and appeals.	**9 Hours**
Practical Component Research Metrics: Impact Factor of journal as per Journal Citations Report, SNIP, SJR, IPP, Cite Score - Metrics: h-index, g index, i10 Index - Open access publications and initiatives - Upload manuscript to a journal through editorial manager.	**6 Hours**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**30**	**Project Hours:**	**0**	**Total Hours:**	**75**

Learning Resources

Textbooks

1. C.R. Kothari, Research Methodology Methods and Techniques, Fourth edition, New Age International Publishers, (2019).
2. Ranjit Kumar, Research Methodology, A Step-by-Step Guide for Beginners, 4th Edition, Sage Publishing, (2023).
3. R. Pannerselvam, Research Methodology, 2nd edition, Prentice Hall India, (2019).
4. C. Neal Stewart Jr., Research Ethics for Scientists: A Companion for Students, Wiley Publishing,(2011).

Reference books/ Web Links

1. Paul Oliver, The student's guide to research ethics, Open University Press, McGraw-Hill Education, McGraw-Hill House, second edition, (2010).

Assessment (Embedded course)

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)
Lab Workbook, Experimental Cycle tests, viva-voce.

Course Curated by

Expert(s) from Industry	Expert(s) from Higher Education Institution	Internal Expert	
-	-	Dr. V. Manivel Muralidaran, P/Mechanical	
Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

24CBI507	**Digital Forensics**	**L**	**T**	**P**	**J**	**C**
		3	**0**	**2**	**0**	**4**
PC		**SDG**	**4,9**			

Pre-requisite courses	**Cryptography and Network Security**	**Data Book / Codes / Standards (If any)**	Nil

Course Objectives:	**The purpose of taking this course is to:**
1	Understand the Fundamentals of Digital Forensics
2	Apply Legal and Ethical Principles in Investigations
3	Acquire and Analyse Digital Evidence from Various Sources
4	Perform Malware Analysis and Incident Response
5	Utilize Forensic Tools for Investigation and Reporting

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Bloom's Taxonomy Level (BTL)**
CO 1	Apply the role of digital forensics and adhere to legal and ethical standards in handling digital evidence.	Ap
CO 2	Apply forensic techniques for evidence acquisition and imaging from various digital devices using industry-standard tools.	Ap
CO 3	Analyze file systems to recover deleted files and carve data from unallocated space, demonstrating proficiency in data recovery practices.	An
CO 4	Investigate digital evidence from computers, networks, and mobile devices, including memory, applications, and cloud environments, to identify security incidents.	An
CO 5	Analyze malware using static and dynamic analysis techniques and utilize automated forensic toolkits to support incident response and legal proceedings.	An

Course Outcomes (CO)	**Program Outcomes (PO)** **(Strong-3, Medium – 2, Weak-1)**				
	1	**2**	**3**	**4**	**5**
1		3			
2					3
3	1			3	
4					3
5	1	3	1		

Course Content

OVERVIEW OF DIGITAL FORENSICS	**9 Hours**
Understanding the role of digital forensics in investigations. Legal and Ethical Considerations: Adhering to legal and ethical standards in digital investigations. Digital Forensics Process: Introduction to the forensic investigation process. Digital Evidence Acquisition**:** Types of Digital Evidence: Identifying and classifying digital evidence. Evidence Acquisition Tools: Using tools for acquiring data from different devices. Forensic Imaging: Creating forensic images of storage media	

Practical Component Identification and classification of the digital evidence with Autopsy tools – Creation a forensic image of a USB drive using tools like FTK Imager or dd.	**6 Hours**
FILE SYSTEMS AND DATA RECOVERY File System Analysis: Understanding file systems and their structures. Deleted File Recovery: Techniques for recovering deleted files. File Carving: Extracting files from unallocated space. **Practical Component** Demonstration of the data recovery techniques – Analysing FAT/NTFS file systems to extract metadata and directory structure using Autopsy	**9 Hours** **6 Hours**
COMPUTER, NETWORK AND MOBILE DEVICE FORENSICS Computer Forensics: Investigating computers for evidence- Network Forensics: Analysing network traffic and logs- Memory Forensics: Examining volatile memory for evidence. Mobile Device Investigation: Extracting evidence from smartphones and tablets. App and Cloud Forensics: Investigating applications and cloud-based services. Challenges in Mobile Forensics: Addressing unique challenges in mobile investigations. **Practical Component** Demonstration the process of analysing the network traffic and logs - Extract data from an Android or iOS device.	**9 Hours** **6 Hours**
MALWARE ANALYSIS Introduction to Malware - Understanding different types of malware- Static and Dynamic Analysis: Analysing malware behaviour and code. Responding to malware incidents- Incident Response and Forensic Tools- Incident Response Planning: Preparing for and responding to security incidents. **Practical Component** Analysing the malware behaviour and its code - Capturing and analysing a memory dump to identify running processes and possible malware.	**9 Hours** **6 Hours**
FORENSIC TOOLKITS Introduction to popular forensic tools- Automated Forensics: Leveraging automation for efficient investigations-Automated Forensics: Leveraging automation for efficient investigations. Legal Aspects of Digital Forensics: Expert Witness Role: Preparing for and testifying in court- Digital Forensics Laws and Regulations: Understanding legal frameworks - Case Studies: Analysing legal cases involving digital forensics. **Practical Component** End-to-end forensic investigation using Autopsy - Prepare an expert witness report for a simulated forensic case.	**9 Hours** **6 Hours**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**30**	**Project Hours:**	**0**	**Total Hours:**	**75**

Learning Resources

Reference books/ Web Links

1. André Årnes by "Digital Forensics", Publisher(s): Wiley, Released July 2017, ISBN: 9781119262381.
2. Digital forensics and cybercrime: 10th International EAI Conference, ICDF2C 2018, New Orleans, LA, USA, September 10-12, 2018, Proceedings.

3. Adam M. Bossler, Kathryn C. Seigfried-Spellar, Thomas J. Holt., "Cybercrime and Digital Forensics: An cybercrime And Digital Forensics: An Introduction", Routledge publication, 3rd Edition May 2022.

Online Resources

1. https://www.coursera.org/learn/digital-forensics-concepts
2. https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-0?active-tab=content-tab
3. https://www.edx.org/learn/computer-forensics/rochester-institute-of-technology-computer-forensics

Assessment (Embedded course)

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)
Lab Workbook, Experimental Cycle tests, viva-voce.

Course Curated by

Expert(s) from Industry	Expert(s) from Higher Education Institution	Internal Expert
-	-	Dr.G.Kanagaraj AP II / CSE

Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

24CBI508	**Web Application Security**	**L**	**T**	**P**	**J**	**C**
		3	**0**	**2**	**0**	**4**
PC		**SDG**	**4,9**			

Pre-requisite courses	**Nil**	**Data Book / Codes / Standards (If any)**	Nil

Course Objectives:	**The purpose of taking this course is to:**
1	Understand the Evolution and Fundamentals of Web Application Security
2	Implement Secure Authentication, Authorization, and Session Management
3	Apply Secure Development Practices and Security Frameworks
4	Analyse and Secure APIs Against Modern Threats
5	Conduct Vulnerability Assessment and Penetration Testing Using Standard Tools

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Bloom's Taxonomy Level (BTL)**
CO 1	Explain the evolution of software security and identify common web application threats with examples	U
CO 2	Demonstrate secure coding practices by applying input validation, authentication, and session management techniques in web applications	Ap
CO 3	Implement security models and frameworks such as SDL, CLASP, and SAMM to plan and evaluate secure software development and deployment practices.	Ap
CO 4	Analyze and secure RESTful and microservice APIs using techniques using token-based authentication, OAuth2, and service mesh	An
CO 5	Conduct vulnerability assessment and penetration testing using Burp Suite, OpenVAS, and Nikto to identify and mitigate web application security flaws	Ap

Course Outcomes (CO)	**Program Outcomes (PO)** **(Strong-3, Medium – 2, Weak-1)**				
	1	**2**	**3**	**4**	**5**
1	1	3			
2		1			3
3				3	
4				1	3
5		3			

Course Content

FUNDAMENTALS OF WEB APPLICATION SECURITY The history of Software Security-Recognizing Web Application Security Threats, Web Application Security, Authentication and Authorization, Secure Socket layer, Transport layer Security, Session Management-Input Validation **Practical Component**	**9 Hours** **6 Hours**

Installation of wireshark and explore the various protocols – Analysing the difference between HTTP vs HTTPS - Analysing the various security mechanisms embedded with different protocols	
SECURE DEVELOPMENT AND DEPLOYMENT Web Applications Security - Security Testing, Security Incident Response Planning, The Microsoft Security Development Lifecycle (SDL), OWASP Comprehensive Lightweight Application Security Process (CLASP), The Software Assurance Maturity Model (SAMM) **Practical Component** Identification the vulnerabilities using OWASP ZAP tool - Implementation and test secure login mechanisms.	**9 Hours** **6 Hours**
SECURE API DEVELOPMENT API Security- Session Cookies, Token Based Authentication, Securing Natter APIs: Addressing threats with Security Controls, Rate Limiting for Availability, Encryption, Audit logging, Securing service-to-service APIs: API Keys, OAuth2, Securing Microservice APIs: Service Mesh, Locking Down Network Connections, Securing Incoming Requests. **Practical Component** Creation of simple REST API using python for following operation 1. GET 2. PUSH 3. POST 4. DELETE - Setting up of HTTPS on a local web server	**9 Hours** **6 Hours**
VULNERABILITY ASSESSMENT AND PENETRATION TESTING Vulnerability Assessment Lifecycle, Vulnerability Assessment Tools: Cloud-based vulnerability scanners, Host-based vulnerability scanners, Network-based vulnerability scanners, Database based vulnerability scanners, Types of Penetration Tests: External Testing, Web Application Testing, Internal Penetration Testing, SSID or Wireless Testing, Mobile Application Testing. **Practical Component** Installation of Burp Suite to do following vulnerabilities: 1. SQL injection 2. cross-site scripting (XSS) – Analysing and secure a simple web application using secure coding principles.	**9 Hours** **6 Hours**
HACKING TECHNIQUES AND TOOLS Social Engineering, Injection, Cross-Site Scripting(XSS), Broken Authentication and Session Management, Cross-Site Request Forgery, Security Misconfiguration, Insecure Cryptographic Storage, Failure to Restrict URL Access, Tools: Comodo, OpenVAS, Nexpose, Nikto, Burp Suite, etc. **Practical Component** Attacking the website using Social Engineering method - Setting up DVWA or bWAPP in a local environment (XAMPP or Docker)	**9 Hours** **6 Hours**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**30**	**Project Hours:**	**0**	**Total Hours:**	**75**

Learning Resources
Reference books/ Web Links

1. Andrew Hoffman, "Web Application Security: Exploitation and Countermeasures for Modern Web Applications", O'Reilly Media publication, 2020.
2. Bryan Sullivan, Vincent Liu, "Web Application Security: A Beginners Guide", The McGraw-Hill Companies Publication, 2012.
3. Neil Madden, "API Security in Action", Manning Publications Co., 2020.
4. Michael Cross, "Developer's Guide to Web Application Security", Syngress Publishing, 2007.
5. Ravi Das and Greg Johnson, "Testing and Securing Web Applications", Taylor & Francis Group, LLC Publication, 2021, .
6. Prabath Siriwardena, "Advanced API Security", Apress Media LLC Publication, 2020.
7. Malcom McDonald, Web Security for Developers,No Starch Press Inc publication, 2020.
8. Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, and Terron Williams, "Grey Hat Hacking: The Ethical Hacker's Handbook", The McGraw-Hill Companies publication, Third Edition, 2011.

Online Resources

1. https://www.offsec.com/cyberversity/web-application-security/
2. https://www.csk.gov.in/documents/Application_Security_Guidelines.pdf
3. https://www.brightsec.com/blog/api-security/
4. https://www.coursera.org/learn/ibm-penetration-testing-threat-hunting-cryptography
5. https://www.coursera.org/learn/certified-ethical-hacking-v12-ethical-hacking-fundamentals

Assessment (Embedded course)

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)
Lab Workbook, Experimental Cycle tests, viva-voce.

Course Curated by

Expert(s) from Industry	Expert(s) from Higher Education Institution	Internal Expert	
-	-	Dr.G.Kanagaraj AP II / CSE	
Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	Date	26-06-25

24CBT509	**Artificial Intelligence for Cyber Security**	**L**	**T**	**P**	**J**	**C**
		3	**0**	**0**	**0**	**3**
PC		**SDG**	**4,8**			

Pre-requisite courses	**Nil**	**Data Book / Codes / Standards (If any)**	Nil

Course Objectives:	**The purpose of taking this course is to:**
1	Introduce the fundamentals of Artificial Intelligence and its application in the cyber security domain.
2	Explore the use of machine learning, deep learning, and natural language processing for threat detection and analysis.
3	Examine ethical considerations, challenges and adversarial risks in deploying AI systems for cyber defense.
4	Promote analytical thinking through case studies, practical implementations, and research-based learning.

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Bloom's Taxonomy Level (BTL)**
CO 1	Outline the role and significance of AI in cyber security by examining real-world use cases and applications.	U
CO 2	Apply feature engineering techniques to prepare cyber security datasets for machine learning models.	Ap
CO 3	Identify AI techniques to automate and enhance threat detection and analysis in cyber security systems.	Ap
CO 4	Leverage AI models to examine network traffic and detect harmful behaviours and trends.	Ap
CO 5	Analyse real-world case studies to understand practical applications, benefits, and limitations of AI in cyber security.	An

Course Outcomes (CO)	**Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)**				
	1	**2**	**3**	**4**	**5**
1	3			2	3
2	3			2	1
3	2		3		
4	3			2	
5		3		2	

Course Content

INTRODUCTION TO CYBER SECURITY AND AI Introduction to Cyber Security- Understanding the Cyber security Landscape- Threats and Attack Vectors Introduction to Artificial Intelligence - Basics of Machine Learning and Deep Learning- AI in Cyber security Overview- Use cases and Applications- Challenges and Opportunities	**9 Hours**

FUNDAMENTALS OF MACHINE LEARNING FOR CYBER SECURITY Machine Learning Basics: Supervised and Unsupervised Learning- Feature Engineering-Machine Learning Algorithms for Cyber security : Decision Trees, Random Forests- Support Vector Machines-Neural Networks for Anomaly Detection	**9 Hours**
CYBER THREAT INTELLIGENCE WITH AI Threat Intelligence - Types of Threats- Indicators of Compromise (IoCs)- AI for Threat Detection and Analysis- Behavioral Analysis -Signature-based Detection –Threat Hunting with AI	**9 Hours**
AI IN NETWORK SECURITY Network Security Overview -Firewalls, IDS, IPS-Intrusion Detection and Prevention Systems-AI for Network Anomaly Detection-Network Traffic Analysis-Deep Packet Inspection	**9 Hours**
SECURITY AUTOMATION AND ORCHESTRATION Security Orchestration, Automation, and Response (SOAR)-Workflow Automation-Incident Response with AI-5.2 Security Tools Integration-Integrating AI into Security Operations- Ethical Issues in AI and Cyber security- Legal Aspects of AI in Cyber security-case studies - Real-world Application of AI in Cyber security.	**9 Hours**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**0**	**Project Hours:**	**0**	**Total Hours:**	**45**

Learning Resources

Textbooks

1. Emmanuel Ameisen, Building Machine Learning Powered Applications: Going from Idea to Product,2020.
2. Qing Li ,Security Intelligence: A Practitioner's Guide to Solving Enterprise Security- Challenges,2015.
3. Christian Espinosa, Threat Intelligence: A Practitioner's Guide, 2023.

Reference books/ Web Links

1. Carl Doersch , Applied Machine Learning for Cyber Security 2021.
2. Chiheb Chebbi , Mastering Machine Learning for Penetration Testing,2018
3. Stuart J. Russell and Peter Norvig, Artificial Intelligence A Modern Approach, 2010

Online Resources

1. https://www.coursera.org/specializations/ai-for-cybersecurity?
2. https://www.eccouncil.org/cybersecurity-exchange/cyber-novice/free-cybersecurity-courses-beginners/.
3. https://www5.open.ac.uk/click-start/.
4. https://alison.com/course/ai-powered-cybersecurity-fundamentals

Assessment
CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)

Course Curated by			
Expert(s) from Industry	**Expert(s) from Higher Education Institution**	**Internal Expert**	
-	-	Dr.A.Roshini, AP III / CSE	
Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

PROGRAM ELECTIVES

24CBC001	**BLOCKCHAIN TECHNOLOGY AND SECURITY**	**L**	**T**	**P**	**J**	**C**
		2	**0**	**2**	**0**	**3**
PE		**SDG**	**9, 11**			

Pre-requisite courses	Cryptography & Network Security	**Data Book / Codes / Standards (If any)**	Nil

Course Objectives:	**The purpose of taking this course is to:**
1	Understand the popular blockchain platforms and ecosystems like Bitcoin, Ethereum, Hyperledger
2	Apply blockchain solutions to real-world use cases including digital identity, supply chain tracking, and secure transactions.
3	Demonstrate critical thinking in evaluating blockchain architectures and their suitability for specific applications.

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Bloom's Taxonomy Level (BTL)**
CO 1	Apply foundational knowledge of blockchain technology to identify its core components and evaluate its benefits in creating decentralized ecosystems	Ap
CO 2	Apply the principles of Bitcoin to explain its key components and payment mechanisms within the Bitcoin network	Ap
CO 3	Apply the concepts of alternative coins and smart contracts to demonstrate the use of decentralized platforms for real-world applications	Ap
CO 4	Analyze the architecture of Ethereum ecosystem for smart contract development	An
CO 5	Analyze enterprise blockchain platform such as Hyperledger Fabric by evaluating their protocols comparing them with alternative blockchain solutions	An

Course Outcomes (CO)	**Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)**				
	1	**2**	**3**	**4**	**5**
1	3				2
2	3		2		2
3	3		2		2
4	3			2	2
5	3			2	2

Course Content

BLOCKCHAIN FUNDAMENTALS Blockchain – definition, elements of blockchain, benefits and limitations, types of blockchain. Consensus – definition, types, consensus in blockchain, Decentralization – decentralization using blockchain, Methods of decentralization, Routes to decentralization, Blockchain and full ecosystem decentralization	**6 Hours**

Practical Component: Set up and explore basic blockchain development environments (e.g., Ethereum, Ganache, Truffle, or Remix IDE). - Implement a basic blockchain structure with blocks, hashes, and linking mechanisms. - Demonstrate the creation of a block, hashing its contents, and linking it to a previous block using cryptographic functions.	**6 Hours**
BITCOIN NETWORK AND PAYMENTS Bitcoin – Definition, Digital keys – Private keys, public keys, addresses. Transactions – Lifecycle, types, transaction verification, Blockchain – genesis block, Mining – Tasks of miners, mining rewards, mining algorithm, hash rate, Minig systems, Bitcoin network, Wallets and its types, Bitcoin payments. **Practical Component:** Generate public and private key pairs and create wallet addresses using tools like Bitcoin Core or online wallet generators - Simulate or visualize the flow of a Bitcoin transaction from creation, broadcast, confirmation, and final inclusion in a block.- Use tools or simple Python code to simulate mining by finding a valid nonce for a given hash difficulty.	**6 Hours** **8 Hours**
SMART CONTRACTS Alternative coins- theoretical foundations, Bitcoin limitations, Smart Contracts – Definition, Smart contract templates, Oracles, Deploying smart contracts, Decentralized Organizations, Platforms for Decentralization. **Practical Component:** Use Remix IDE to examine and modify basic smart contract templates (e.g., voting system, escrow, simple storage)	**6 Hours** **2 Hours**
ETHEREUM NETWORK Ethereum – The Ethereum network, Components of the Ethereum ecosystem, Keys and addresses, Accounts, Transactions and messages, Ether cryptocurrency, Ethereum Virtual Machine, Ethereum blocks and blockchain, Fee schedule, supporting protocols, Solidity language **Practical Component:** Use tools like Etherscan to explore live Ethereum data blocks, transactions, addresses, and contracts.- Use Solidity to write a basic smart contract, deploy it, and interact with it on Remix IDE using the JavaScript VM or testnet.	**8 Hours** **6 Hours**
HYPERLEDGER Hyperledger Projects, Protocol, Reference architecture, Hyperledger Fabric, Corda, Alternative blockchains **Practical Component:** Launch the Fabric test network using Docker and execute basic chaincode interactions.- Write a simple Go or JavaScript chaincode (e.g., asset transfer) and deploy it on the Fabric test network	**4 Hours** **8 Hours**

Theory Hours:	**30**	**Tutorial Hours:0**		**Practical Hours:**	**30**	**Project Hours:0**		**Total Hours:**	**60**

Learning Resources

Textbooks

1. Imran Bashir, “Mastering Blockchain: Distributed Ledger technology, Decentralization, and Smart Contracts Explained”, Second Edition, Packet Publishing, Birmingham, UK (2018)

Reference books/ Web Links

1. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, “ Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction” Princeton University Press, 2016.
2. Alex Leverington, “Ethereum Programming” Packt Publishing Limited, 2017.
3. Andreas Antonopoulos, Satoshi Nakamoto, “Mastering Bitcoin”, O’Reilly Publishing, 2014.

4. Roger Wattenhofer, “The Science of the Blockchain” Create Space Independent Publishing Platform, 2016.
5. Arshdeep Bahga and Vijay Madisetti, “Blockchain Applications: A Hands-On Approach”, 2017.
6. Ritesh Modi, Solidity Programming Essentials: A beginner's guide to build smart contracts for Ethereum and blockchain, Packt Publishing, First edition, 2018.
7. Kumar Saurabh, Ashutosh Saxena, Blockchain Technology: Concepts and Applications, First Edition, Wiley Publications, First edition, 2020.
8. Chandramouli Subramanian, Asha A George, et al, Blockchain Technology, Universities Press (India) Pvt. Ltd, First edition, August 2020.

Online Resources

1. https://www.edx.org/learn/blockchain
2. https://www.coursera.org/specializations/blockchain
3. https://www.cybrary.it/blog/blockchain-technology-in-information-security

Assessment (Embedded course)

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)
Lab Workbook, Experimental Cycle tests, viva-voce.

Course Curated by

Expert(s) from Industry	Expert(s) from Higher Education Institution		Internal Expert
-	-		Dr.L Latha P / CSE
Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

24CBC002	**Cloud Security**	**L**	**T**	**P**	**J**	**C**
		2	**0**	**2**	**0**	**3**
PE		**SDG**	**4,9**			

Pre-requisite courses	Cryptography and Network Security	**Data Book / Codes / Standards (If any)**	Nil

Course Objectives:	**The purpose of taking this course is to:**
1	To Introduce Cloud Computing terminology, definition & concepts
2	To understand the security design and architectural considerations for Cloud
3	To understand the Identity, Access control in Cloud
4	To follow best practices for Cloud security using various design patterns

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Bloom's Taxonomy Level (BTL)**
CO 1	Explain the core cloud security services including confidentiality, integrity, authentication, access control, and the application of cryptographic techniques.	U
CO 2	Apply cloud security design principles and recommend architecture-level strategies to mitigate threats in storage, network, and virtualization layers.	Ap
CO 3	Implement identity and access control mechanisms such as role-based access control, multi-factor authentication, and identity federation in a cloud environment.	Ap
CO 4	Analyze and use cloud security design patterns such as secure interfaces, cloud bursting, and access control to enforce secure cloud deployment models.	An
CO 5	Design and implement monitoring and auditing mechanisms to detect, log, and respond to unauthorized activities in cloud environments using SIEM and incident response strategies.	Ap

Course Outcomes (CO)	**Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)**				
	1	**2**	**3**	**4**	**5**
1		2		2	
2		3		2	
3	3			2	
4	3			2	
5	3			2	

Course Content	
FUNDAMENTALS OF CLOUD SECURITY CONCEPTS Overview of cloud security- Security Services - Confidentiality, Integrity, Authentication, Nonrepudiation, Access Control - Basic of cryptography - Conventional and public-key cryptography, hash functions, authentication, and digital signatures. **Practical Component**	**6 Hours**

Simulation of a cloud scenario using Cloud Sim and run a scheduling algorithm – Simulation of resource management using cloud sim	**6 Hours**
SECURITY DESIGN AND ARCHITECTURE FOR CLOUD 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 **Practical Component** Simulation of log forensics using cloud sim – Simulation of a secure file sharing using a cloud sim	**6 Hours** **6 Hours**
ACCESS CONTROL AND IDENTITY MANAGEMENT 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. **Practical Component** Implementation of data anonymization techniques over the simple dataset (masking, k-anonymization, etc) – Implementation of any encryption algorithm to protect the images	**6 Hours** **6 Hours**
CLOUD SECURITY DESIGN PATTERNS Introduction to Design Patterns, Cloud bursting, Geo-tagging, Secure Cloud Interfaces, Cloud Resource Access Control, Secure On-Premise Internet Access, Secure External Cloud **Practical Component** Implementation of any image obfuscation mechanism – Implementation of a role-based access control mechanism in a specific scenario	**6 Hours** **6 Hours**
MONITORING, AUDITING AND MANAGEMENT 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 **Practical Component** Implementation of an attribute-based access control mechanism based on a particular scenario – Development of a log monitoring system with incident management in the cloud	**6 Hours** **6 Hours**

Theory Hours:	**30**	**Tutorial Hours:**		**Practical Hours:**	**30**	**Project Hours:**		**Total Hours:**	**60**

Learning Resources
Textbooks
1. Raj Kumar Buyya , James Broberg, Andrzej Goscinski, “Cloud Computing:”, Wiley 2013 2. Dave shackleford, “Virtualization Security”, SYBEX a wiley Brand 2013. 3. Mather, Kumaraswamy and Latif, “Cloud Security and Privacy”, OREILLY 2011
Reference books/ Web Links

1. Mark C. Chu-Carroll ―Code in the Cloud‖,CRC Press, 2011
2. Mastering Cloud Computing Foundations and Applications Programming Rajkumar Buyya, Christian Vechhiola, S. ThamaraiSelvi.

Online Resources

1. https://www.coursera.org/learn/cloud-security-basics
2. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/
3. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security-architecture/

Assessment (Embedded course)

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)
Lab Workbook, Experimental Cycle tests, viva-voce.

Course Curated by

Expert(s) from Industry	Expert(s) from Higher Education Institution	Internal Expert
-	-	Dr.G.Kanagaraj AP II / CSE

Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

24CBC003	Secure Software Development	L	T	P	J	C
		2	0	2	0	3
PE		SDG	4,9			

Pre-requisite courses	Nil	Data Book / Codes / Standards (If any)	Nil

Course Objectives:	The purpose of taking this course is to:
1	To learn the development principles and process models of secure software engineering
2	To study the requirements, modelling, design testing and validation procedures that ensure security.
3	To apply secure software engineering principles across cross-disciplines.

Course Outcomes:	After successful completion of this course, the students shall be able to	Bloom's Taxonomy Level (BTL)
CO 1	Explain the fundamental principles used in secured software development and life cycle process.	U
CO 2	Compare various approaches to building secure and safe systems for critical applications.	U
CO 3	Perform security requirements analysis, construct threat models, and design secure software architectures using security patterns and best practices.	Ap
CO 4	Apply secure coding principles, identify common vulnerabilities, and validate software security using testing tools and remediation practices	Ap
CO 5	Implement web application security mechanisms and analyze software systems using safety and security metrics to assess trustworthiness and risk.	Ap

Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)					
Course Outcomes (CO)	1	2	3	4	5
1	2		3	2	
2	2		3	2	
3	2		3	2	
4	2		3	2	2
5	2		3	2	2

Course Content	
INTRODUCTION System engineering-Systems engineering and the systems-System engineering processes-Understanding Software systems engineering-The software system engineering processes-Steps	**6 Hours**

in the software development processes-Functional and non-functional requirements Verification and validation. **Practical Component:** Functional vs. Non-Functional Requirements Analysis-Model the Software Development Process Lifecycle-Requirement Traceability Matrix (RTM)	**6 Hours**
ENGINEERING SECURE AND SAFE SYSTEMS Introduction-The approach-security versus safety-Four approaches to develop critical systems-The dependability approach-The safety engineering approach-The secure systems approach- The real-time systems approach Security-critical and safety-critical systems. **Practical Component:** Safety and Security Requirement Elicitation - Dependability Modeling using Fault Tree Analysis (FTA)- Risk Assessment Matrix Creation.	**6 Hours** **6 Hours**
ARCHITECTING SECURE SOFTWARE SYSTEMS Security Requirements Analysis, Threat Modelling, Security Design Patterns Anti-Patterns, Attack Patterns, Security Design Patterns, Authentication, Authorization -Security Coding Security Algorithm, Security Protocol, Key Generation. **Practical Component:** Threat Modeling with STRIDE-Implement Role-Based Access Control (RBAC)- Authentication & Authorization Simulation	**6 Hours** **6 Hours**
VALIDATING SECURITY AND SECURE CODING PRINCIPLES Generating the Executable, Security Testing vulnerability assessment, code coverage tools - Secured Deployment, Security Remediation, Security Documentation, Security Response Planning, Safety-Critical Systems Coding in C String manipulation, vulnerabilities and exploits, Pointers based vulnerabilities. Coding C++ and JAVA - Memory management, common errors, Integer Security, Double free Vulnerabilities **Practical Component:** Vulnerability Scanning using Static Analysis Tools -Secure String Handling in C-Double Free and Integer Overflow in C++/Java- Security Testing using Code Coverage Tools	**6 Hours** **6 Hours**
SECURITY IN WEB-FACING APPLICATIONS Overview of web security, Identity Management, public key infrastructure, Code injection, Parameter tampering, secured web programming, application vulnerability description language. Security and safety metrics: Defining metrics-differentiating measures and metrics Software Metrics-Measuring and re-porting metrics Metrics for meeting requirements-Risk metrics-Security metrics for software systems-safety metrics for software systems **Practical Component:** Demonstrate SQL Injection & its Prevention - Implement Secure Identity Management-Web Application Vulnerability Scanning -Develop a dashboard showing risk and vulnerability metrics from scan results.	**6 Hours** **6 Hours**

Theory Hours:	**30**	**Tutorial Hours:**	**0**	**Practical Hours:**	**30**	**Project Hours:**	**0**	**Total Hours:**	**60**

Learning Resources

Textbooks

Reference books/ Web Links

1. Asoke K. Talukder, Manish Chaitanya, Architecting Secure Software Systems, Auerbach Publications, 2008.
2. John Musa D, Software Reliability Engineering, 2nd Edition, Tata McGraw-Hill, 2014
3. Mano Paul ,7 Qualities of Highly secure Software Taylor and Francis, CRC Press (2012)
4. Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw and Nancy Mead Software Security Engineering: A Guide for Project Managers by. Addison-Wesley, (2008).
5. Gary McGraw, Software Security: Building Security, Addison-Wesley (2006).

Online Resources

1. https://www.coursera.org/specializations/secure-software-design
2. https://www.edx.org/certificates/professional-certificate/linuxfoundationx-secure-software-development-fundamentals

Assessment (Embedded course)

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)
Lab Workbook, Experimental Cycle tests, viva-voce.

Course Curated by

Expert(s) from Industry	Expert(s) from Higher Education Institution	Internal Expert
-	-	Dr V.Vanitha, P/CSE

Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

24CBE004	**Cyber Physical Systems and Security**	**L**	**T**	**P**	**J**	**C**
		3	**0**	**0**	**0**	**3**
PE		**SDG**	**4,9**			

Pre-requisite courses	**Nil**	**Data Book / Codes / Standards (If any)**	Nil

Course Objectives:	**The purpose of taking this course is to:**
1	To provide foundational knowledge on the architecture, characteristics, and real-world applications of Cyber Physical Systems (CPS)
2	To enable students to understand and design CPS components, with a focus on feedback mechanisms and distributed system synchronization
3	To familiarize students with the hardware and communication platforms used in CPS, and guide them in analyzing and modeling dynamic, hybrid systems using appropriate wireless technologies.
4	To equip students with the ability to develop secure IoT-based CPS applications and assess privacy, security, and ethical challenges across various CPS infrastructures, including Industry 4.0 environments.

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Bloom's Taxonomy Level (BTL)**
CO 1	Explain the architecture, characteristics, and real-world applications of Cyber Physical Systems (CPS)	U
CO 2	Design and simulate control mechanisms in CPS using embedded processors, sensors, actuators, and feedback control systems.	Ap
CO 3	Analyse the suitability of hardware and communication platforms for dynamic, hybrid CPS models.	An
CO 4	Demonstrate IoT-based CPS applications using platforms such as Accessors, CapeCode, and TerraSwarm tools.	Ap
CO 5	Assess and recommend security and privacy mechanisms for CPS across local, networked, and cloud-connected infrastructures	Ap

Course Outcomes (CO)	**Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)**				
	1	**2**	**3**	**4**	**5**
1	3				
2	3		3		
3	3			2	
4	3				3
5	3				2

Course Content	
CPS APPLICATIONS ARCHITECTURE AND CHALLENGES Cyber Physical System Introduction. Applications and Advantages. CPS characteristics. 5C Architecture. Technology Platforms in CPS. Abstraction Layers in Computing. Static Vs. Dynamic Systems. Homogenous Vs. Heterogeneous systems. Possibilities and Challenges. Role of Architecture Description Languages. Cyber Physical Systems in Real world, Basic Principle of Cyber Physical Systems, CPS system requirements, Cyber Physical System Application	**9 Hours**
COMPONENTS OF CPS Physical Space - Sensors and Actuators - Embedded Processors, Input and Output Interfaces- ADC and DAC. Control Systems - Feedback Control systems open and closed loop. Human in the loop predictive model based control systems - Concurrency and Synchronization of components in distributed CPS.	**9 Hours**
CYBER PHYSICAL SYSTEM PLATFORMS AND MODELS Hardware platforms for Cyber Physical Systems (Sensors/Actuators, Microprocessor/ Microcontrollers), Wireless Technologies for Cyber Physical Systems-Continuous Dynamics, Discrete dynamics, Hybrid Systems	**9 Hours**
INTEGRATING CYBER AND PHYSICAL SPACE Highly dynamic networked systems. Designing Communication stack in node operating system for CPS. Comparison with Industry 4.0, the Industrial Internet, Machine-to-Machine (M2M) technologies. Issues integrating the heterogeneous physical systems with existing cyberspace. Building IoT Applications with Accessors - CapeCode - Terra Swarms- Swarm Sensors, Swarm OS and Swarmlets Design	**9 Hours**
SECURITY AND PRIVACY IN CYBER PHYSICAL SYSTEMS Security and Privacy Issues in CPSs, Local Network Security for CPSs, Internet-Wide Secure Communication, Security and Privacy for Cloud-Interconnected CPSs, Case Study: Cyber security in Digital Manufacturing/Industry 4.0 - Contemporary issues	**9 Hours**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**0**	**Project Hours:**	**0**	**Total Hours:**	**45**

Learning Resources*

Textbooks

1. Rajeev Alur, “Principles of Cyber Physical Systems”, MIT Press, 2023
2. E. A. Lee, Sanjit Seshia , "Introduction to Embedded Systems – A Cyber–Physical Systems Approach", Second Edition, MIT Press, 2017, ISBN: 978-0-262-53381-2

Reference books/ Web Links

1. Houbing song, Danda B Rawat, Sabina Jeschke, Christian Brecher, “Cyber Physical Systems Foundations, Principles and Applications”, Elsevier, 2017
2. Houbing Song, Glenn A.Fink, Sabina Jesche, “Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Solutions”, IEEE Press.
3. Raj Rakumar “Cyber Physical Systems”, Addison-Wesley, 2017
4. Yunchuan Sun, “Secure and Trustworthy Transportation Cyber Physical Systems”, Springer, 2017

Online Resources

1. https://www.coursera.org/learn/cyber-physical-systems-1?utm_source=chatgpt.com
2. https://www.udacity.com/course/cyber-physical-systems-design-analysis--ud9876?utm_source=chatgpt.com

Assessment
CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE), Quiz

Course Curated by

Expert(s) from Industry	Expert(s) from Higher Education Institution	Internal Expert	
-	-	Dr N.Suganthi, P/CSE	
Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

24CBE005	**Cyber Ethics and Laws**	**L**	**T**	**P**	**J**	**C**
		3	**0**	**0**	**0**	**3**
PE		**SDG**	**8, 16**			

Pre-requisite courses	**Nil**	**Data Book / Codes / Standards (If any)**	Nil

Course Objectives:	**The purpose of taking this course is to:**
1	Provide a comprehensive understanding of cyber law frameworks, Information Technology Act, data protection regulations and international legal norms governing digital activities.
2	Equip students with the ability to apply ethical reasoning to real-world digital dilemmas, and evaluate legal documents, privacy policies and terms of service.
3	Develop the competency to make informed decisions in technology-driven environments and contribute effectively to governance and cyber security.

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Bloom's Taxonomy Level (BTL)**
CO 1	Apply ethical principles and relevant cyber laws to real-world scenarios in cyberspace	Ap
CO 2	Apply legal regulations and ethical frameworks to evaluate emerging technologies in compliance with cyber laws	Ap
CO 3	Apply international conventions to assess contemporary issues in cyberspace	Ap
CO 4	Analyze the legal frameworks governing intellectual property rights in the cyberspace	An
CO 5	Analyze the role of critical thinking in addressing the issues in cyber ethics.	An

Course Outcomes (CO)	**Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)**				
	1	**2**	**3**	**4**	**5**
1	3				2
2	3		2		2
3	3		2		2
4	3			2	2
5	3			2	2

Course Content

OVERVIEW OF ETHICS IN CYBERSPACE Importance of Cyber Law, need for Cyber regulation based on cyber ethics, Ethics in information security-the nine P's, AI ethics, Blockchain ethics	**9 Hours**
CYBER LAW, CYBER HEALTH AND ETHICS Blockchain legal regulations, humanistic approach to ethics, digital health- meeting ethical and policy changes, Law, cyber ethics and technology	**9 Hours**
CYBER GOVERNANCE AND ETHICS International convention for cyber space and ethical frameworks, republican net neutrality, ethics and autonomous weapon systems	**9 Hours**

CYBER LAW AND RELATED LEGISLATION Patent Law, Trademark Law, Copyright, Domain Names and Copyright disputes, Electronic Database and its Protection, IT Act and Civil Procedure Code, Relevant Sections of Indian Evidence Act, Law relating to Employees and Internet, Alternative Dispute Resolution, Online Dispute Resolution	**9 Hours**
CYBER EDUCATION AND ETHICS Ethics and intelligence, secret services, critical thinking of citizens, cyber bullying, limiting access of technology.	**9 Hours**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**0**	**Project Hours:**	**0**	**Total Hours:**	**45**

Learning Resources

Textbooks

1. Christoph Stuckelberger, Pavan Duggal, “Cyber Ethics 4.0- serving humanity with values”, Globethics.net, (2018)
2. Kumar K, “Cyber Laws: Intellectual property & E Commerce Security”, Dominant Publisher, (2011)

Reference books/ Web Links

1. NIIT, “Information Security policy & Implementation Issues”, PHI, (2003)
2. Verma S, K, Mittal Raman, “Legal Dimensions of Cyber Space”, Indian Law Institute, New Delhi, (2004)
3. Jonthan Rosenoer, “Cyber Law: The Law of the Internet”, Springer, New York,(1997).
4. OUP Sudhir Naib, “The Information Technology Act, 2005: A Handbook”, New York, (2011)
5. S. R. Bhansali, “Information Technology Act, 2000”, University Book House Pvt. Ltd. Jaipur(2003).
6. Vasu Deva, “Cyber Crimes and Law Enforcement”, Commonwealth Publishers, New Delhi, (2003).

Online Resources

1. https://alison.com/course/introduction-to-cyber-law
2. https://www.futurelearn.com/courses/introduction-to-cyber-security
3. https://cyberlaw.ccdcoe.org/wiki/Main_Page

Assessment

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE), Quiz

Course Curated by

Expert(s) from Industry	Expert(s) from Higher Education Institution	Internal Expert	
-	-	Dr.L Latha P / CSE	
Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

24CBC006	**Cyber Security Audit and Compliances**	**L**	**T**	**P**	**J**	**C**
		2	**0**	**2**	**0**	**3**
PE		**SDG**	**9,16**			

Pre-requisite courses	**Nil**	**Data Book / Codes / Standards (If any)**	Nil

Course Objectives:	**The purpose of taking this course is to:**
1	Develop knowledge of IT audit frameworks, standards, and essential compliance protocols.
2	Equip students with practical skills to audit critical IT infrastructure components including networks, operating systems, and mobile devices.
3	Build competency in auditing modern technologies such as cloud platforms, virtual environments, and applications.
4	Enable students to evaluate audit findings and suggest risk mitigation and compliance improvements.
5	Foster understanding of regulatory frameworks like ISO 27001, COBIT, SOX, PCI-DSS, and HIPAA.

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Bloom's Taxonomy Level (BTL)**
CO 1	Identify audit components and processes related to IT infrastructure, applications, and standards.	U
CO 2	Conduct vulnerability assessment and audits using tools on systems and network devices.	Ap
CO 3	Identify risks in cloud, mobile, and wireless platforms.	Ap
CO 4	Perform application-level audits with the help of checklists and compliance reports.	An
CO 5	Apply appropriate standards and frameworks (ISO, COBIT, ITIL, SOX) in audit practices.	Ap

Course Outcomes (CO)	**Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)**				
	1	**2**	**3**	**4**	**5**
1	3		2		
2	2		3		3
3	2		2		3
4	2		2		3
5	2		2		

Course Content

INTRODUCTION TO AUDITING AND TECHNIQUES Audit Overview: Building an Effective Internal IT Audit Function- The Audit Process - Auditing Techniques: Auditing Entity-Level Controls: Test Steps for Auditing Entity-Level Controls- Knowledge Base - Master Checklist. Auditing Data Centers and Disaster Recovery: Data Center Auditing Essentials - Test Steps for Auditing Data Centers. Auditing Routers, Switches, and Firewalls: Network Auditing Essentials - Auditing Switches, Routers, and Firewalls - Tools and Technology. **Practical Component:**	**7 Hours** **6 hours**

Auditing Network Devices: Routers & Switches - Simulate router/switch setup, run a basic security configuration checklist (Cisco Packet Tracer / GNS3) - Firewall Audit and Network Traffic Analysis - Use nmap to scan for open ports, Wireshark to capture traffic, analyze logs (Nmap, Wireshark, Kali Linux)	
AUDITING OPERATING SYSTEMS Auditing Windows Operating Systems: Windows Auditing Essentials - Test Steps for Auditing Windows - How to Perform a Simplified Audit of a Windows Client - Tools and Technology. Auditing Unix and Linux Operating Systems: Unix and Linux Auditing Essentials - Test Steps for Auditing Unix and Linux. Tools and Technology. **Practical Component:** Windows OS Audit – User and Group Policies. Review and audit local users, groups, password policies, account lockout policies. (Windows VM, PowerShell, Local Security Policy (secpol.msc)). Windows OS Audit – Logs and Event Analysis - Analyze event logs for signs of policy violations or attacks- (Windows Event Viewer, PowerShell scripts). Linux OS Audit – User and File Permissions - identify insecure permissions and unnecessary services - Linux terminal, chmod, ps, chkconfig, systemctl - Linux OS Audit – Using Tools (Lynis, AuditD)	**6 Hours** **6 hours**
AUDITING WEB SERVER AND DATABASES Auditing Web Servers and Web Applications: Web Auditing Essentials - Test Steps for Auditing the Host Operating System - : Test Steps for Auditing Web Servers - Test Steps for Auditing Web Applications. Auditing Databases: Database Auditing Essentials - Test Steps for Auditing Databases - Tools and Technology. Auditing Storage: Storage Auditing Essentials - Test Steps for Auditing Storage. Auditing Virtualized Environments: Virtualization Auditing Essentials - Test Steps for Auditing Virtualization. **Practical Component:** Audit of Web Server and Host OS - Inspect Apache/Nginx configurations, check for outdated software and unnecessary services (Ubuntu VM, Apache2, Nmap, Nikto, CIS Benchmarks) - Audit of Web Applications Perform vulnerability assessment on DVWA/Mutillidae using OWASP ZAP/Burp Suite - Audit of Database Systems - Check MySQL user privileges, audit logs, unused accounts, weak passwords - Audit of Storage and Virtualization Environments - Audit shared drives (NFS/Samba), check virtual NICs and snapshots, analyze logs	**6 Hours** **6 Hours**
IT SYSTEMS AUDITING: WLANS, MOBILE DEVICES, APPLICATIONS, CLOUD & PROJECTS Auditing WLAN and Mobile Devices: WLAN and Mobile Device Auditing Essentials - Test Steps for Auditing Wireless LANs - Test Steps for Auditing Mobile Devices. Auditing Applications - Application Auditing Essentials - Test Steps for Auditing Applications - Master Checklists. Auditing Cloud Computing and Outsourced Operations: Test Steps for Auditing Cloud Computing and Outsourced Operations. Auditing Company Projects: Project Auditing Essentials - Test Steps for Auditing Company Projects. **Practical Component** Auditing Wireless LAN (WLAN) - Auditing Mobile Devices - Auditing Cloud Environments and Projects - Review IAM policies, encryption settings, service usage logs, audit against compliance checklist	**5 Hours** **6 Hours**
FRAMEWORKS, STANDARDS, AND REGULATIONS & RISK MANAGEMENT Frameworks, Standards, and Regulations: COSO – COBIT – ITIL - ISO 27001 - NSA INFOSEC Assessment Methodology. Regulations: An Introduction to Legislation Related to Internal Controls - The Sarbanes-Oxley Act of 2002 - Gramm-Leach-Bliley Act - Privacy Regulations - Health Insurance Portability and Accountability Act of 1996 - EU Commission and Basel II - Payment Card Industry (PCI) Data Security Standard. Risk Management: Benefits of Risk Management- Risk Management from an Executive Perspective - Quantitative Risk Analysis - Qualitative Risk Analysis - IT Risk Management Life Cycle	**6 Hours**

Practical Component Compliance Checklist Preparation and Gap Analysis (HIPAA, SOX, PCI-DSS Checklists)- IT Risk Management Lifecycle Implementation - IT Risk Management Lifecycle Implementation - NIST RMF Steps Diagram, Risk Life Cycle Template	**6 Hours**

Theory Hours:	**30**	**Tutorial Hours:**	**0**	**Practical Hours:**	**30**	**Project Hours:**	**0**	**Total Hours:**	**60**

Learning Resources

Textbooks

1. Chris Davis, Mike Schiller, and Kevin Wheeler, “IT Auditing: Using Controls to Protect Information Assets”., McGraw-Hill Companies United States (2011).
2. Reed, Mark S., “IT Auditing and Application Controls for Small and Mid-Sized Enterprises”, Wiley, New York (2013).

Reference books/ Web Links

1. Calder, Alan, “Introduction to Information Security”, Information Security Risk Management for ISO 27001/ISO 27002, Kogan Page, London (2019): pp. 1–28.
2. Cowan, Crispin, “Security Auditing in Linux Systems”, PhD Thesis., Oregon Graduate Institute of Science and Technology, Portland, Oregon (2000). DOI: 10.5555/559634
3. Bruce, Schneier, “The Impact of Cyber Risk on Business Continuity”, Technical Report No. IS-1042, Harvard Kennedy School, Cambridge, MA, USA (2018). DOI: 10.1007/s10207-018-0402-y
4. Stallings, William, “Auditing the Cloud: Security Issues”, International Journal of Information Security, Vol. 20 No. 3 (2021): pp. 123–132. DOI: 10.1007/s10207-021-00501-6, https://link.springer.com/article/10.1007/s10207-021-00501-6
5. Sharma, Ankit, “Audit-Driven Compliance in Hybrid IT Environments”, Proceedings of the IEEE International Conference on Cloud Engineering, Paper #CLOUD2022: pp. 451–458, Bangalore, India, March 16–18, 2022. DOI: 10.1109/IC2E53580.2022.00078, Abstract URL

Online Resources

1. https://www.coursera.org/learn/it-security
2. https://app.cybrary.it/browse/course/cybersecurity-audit-overview/
3. https://onlinecourses.nptel.ac.in/noc25_cs116/preview

Assessment (Embedded course)

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)
Lab Workbook, Experimental Cycle tests, viva-voce.

Course Curated by

Expert(s) from Industry	**Expert(s) from Higher Education Institution**		**Internal Expert**
-	-		Dr C.Rajankrupa, AP III / MCA
Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

24CBC007	Malware Analysis and System Security	L	T	P	J	C
		2	0	2	0	3
PE		SDG	4,9			

Pre-requisite courses	Nil	Data Book / Codes / Standards (If any)	Nil

Course Objectives:	The purpose of taking this course is to:
1	To introduce the fundamental concepts of malware types, behaviour and propagation techniques.
2	To equip students with practical skills for analyzing and reverse-engineering malware using both static and dynamic analysis techniques.
3	To develop the ability to identify, detect, and mitigate malware threats in real-world systems through manual and automated tools.
4	To expose students to malware evasion techniques and the corresponding countermeasures used in defensive security.

Course Outcomes:	After successful completion of this course, the students shall be able to	Bloom's Taxonomy Level (BTL)
CO 1	Articulate the purpose and limitations of malware analysis, including legal, ethical and technical constraints.	U
CO 2	Identify how software vulnerabilities are exploited as infection vectors and understand the relationship between vulnerabilities and malware propagation.	Ap
CO 3	Apply forensic skills to extract and isolate suspicious files from infected systems for further analysis and reverse engineering.	Ap
CO 4	Utilize antivirus detection tools to identify known threats and understand their limitations in detecting obfuscated or novel malware.	Ap
CO 5	Analyze network behaviour of suspected malware, including DNS queries, outbound connections and command-and-control communications.	An

Course Outcomes (CO)	Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)				
	1	2	3	4	5
1	3			3	
2	2			3	
3				3	2
4	3			3	
5	3				3

Course Content	
MALWARE ANALYSIS Malware Analysis and Reverse Engineering, Types of Malware Analysis, Purpose of Malware Analysis Limitations of Malware Analysis, The Malware Analysis Process, Malware Classes Infectors, Network Worms, Trojan Horse Backdoors, Remote-Access Trojan, Information Stealers	**6 Hours**

Practical Component Implementation of static malware analysis - Implementation of static malware analysis.	**4 Hours**
MALWARE DEPLOYMENT Malware Infection Vectors, Speed, Stealth, Coverage, Shelf Life, Types of Malware Infection Vectors, Physical Media, E-mails. Instant Messaging and Chat, Social Networking, URL Links, File Shares, Software Vulnerabilities- Protective Mechanisms- The Two States of Malware, Static Malware, Dynamic Malware, Protective Mechanisms, Static Malware Protective Mechanisms, Dynamic Malware Protective Mechanisms	**6 Hours**
Practical Component Implementation of malware samples using tools like PEiD, Exeinfo PE, Strings, and Resource Hacker - Demonstration of Volatility or Rekall to detect rootkits, injected processes, and hidden malware - Demonstration on custom YARA rules to detect malware families.	**8 Hours**
MALWARE DEPENDENCIES Dependency Types, Environment Dependencies, Program Dependencies, Timing Dependencies, Event Dependencies, Malware Collection- Your Own Backyard, Scan for Malicious Files, Look for Active Rootkits, Inspect Startup Programs, Inspect Running Processes, Extract Suspicious Files, The Portable Executable File-The Windows Portable Executable File, The PE File Format, Relative Virtual Address, PE Import Functions.	**6 Hours**
Practical Component Deployment of ransomware samples in a VM and analysing the file encryption routines - Implementation of Angler/Nuclear exploit kits in a controlled environment.	**6 Hours**
THE PROPER WAY TO HANDLE FILES The Proper Way to Handle Files- File's Analysis Life Cycle, Transfer, Analysis, Storage, Inspecting Static Malware- Static Analysis Techniques, File Type Identification, Antivirus Detection, Protective Mechanisms Identification, PE Structure Verification.	**6 Hours**
Practical Component Demonstration of RAT sample to analyse the malware behaviour - Analysing different samples and classify them into categories: infectors, worms, trojans, backdoors using Cukoo Sandbox.	**6 Hours**
STATIC MALWARE Inspecting Static Malware-Static Analysis Techniques, ID Assignment-File Type Identification, Antivirus Detection, Protective Mechanisms Identification, PE Structure Verification, Dynamic Analysis-Analyzing Host Behavior, Analyzing Network Behavior.	**6 Hours**
Demonstration of PE header and sections to identify anomalies in the executable file - Demonstration on packet capture and analysis of network traffic generated by malware during execution.	**6 Hours**

Theory Hours:	**30**	**Tutorial Hours:**	**0**	**Practical Hours:**	**30**	**Project Hours:**	**0**	**Total Hours:**	**60**

Learning Resources

Textbooks

1. Christopher C. Elisan "Advance Malware Analysis", Mc Craw Hill Education, 2020.
2. Michael Sikorski, Andrew Honig , "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software", Starch Press,2012.

Reference books/ Web Links

1. Cameron H. Malin, Eoghan Casey, James M. Aquilina and Curtis W. Rose, “Malware Forensics Field Guide for Windows Systems”, Syngress, Elsevier, 2014
2. Ken Dunham, Saeed Abu-Nimeh, Michael Becher and Seth Fogie, “ Mobile Malware Attacks and Defense”, Syngress, Elsevier, 2009
3. Alexey Kleymenov, Amr Thabet , “Mastering Malware Analysis: A Malware Analyst's Practical Guide to Combating Malicious Software, APT, Cybercrime, and IoT Attacks” (2nd Edition),Packet Publishing, 2022

Online Resources

1. https://www.udemy.com/course/malware-analysis-fundamentals/?couponCode=LEARNNOWPLANS
2. https://www.udemy.com/course/reverse_engineering/?couponCode=LEARNNOWPLANS\
3. https://www.edx.org/learn/computer-programming/ibm-malware-analysis-and-assembly-language-introduction

Assessment (Embedded course)

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)
Lab Workbook, Experimental Cycle tests, viva-voce.

Course Curated by

Expert(s) from Industry	Expert(s) from Higher Education Institution		Internal Expert
-	-		Dr.A.Roshini, AP III / CSE
Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

24CBC008	**Incident Response Management**	**L**	**T**	**P**	**J**	**C**
		2	**0**	**2**	**0**	**3**
PE		**SDG**	**4,9**			

Pre-requisite courses	**Nil**	**Data Book / Codes / Standards (If any)**	Nil

Course Objectives:	**The purpose of taking this course is to:**
1	To introduce the concepts of incident response, including its significance, goals, lifecycle phases, and organizational readiness strategies.
2	To equip students with the skills to detect, investigate, and characterize cyber security incidents through data collection and analysis techniques.
3	To develop proficiency in digital forensics, including live data acquisition, forensic duplication, and network evidence analysis across different platforms.
4	To enable learners to perform malware triage, document incident findings through professional reports, and implement effective remediation strategies.

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Bloom's Taxonomy Level (BTL)**
CO 1	Explain the phases of the incident response lifecycle and identify roles, goals, and preparation steps essential for organizational readiness.	U
CO 2	Apply incident indicators using investigative techniques, build timelines, and determine the scope of the attack.	Ap
CO 3	Demonstrate data acquisition techniques such as live response, forensic duplication, and network evidence collection across platforms.	U
CO 4	Apply forensic analysis on Windows systems and applications using structured methodologies to extract actionable intelligence.	Ap
CO 5	Explain malware triage, write incident reports adhering to professional standards, and apply remediation techniques in real-world scenarios.	U

Course Outcomes (CO)	**Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)**				
	1	**2**	**3**	**4**	**5**
1		3		3	
2		3		3	
3	3			2	
4	3			2	
5	3			3	

Course Content	
PREPARING FOR THE INEVITABLE INCIDENT Real-World Incidents: Constitutes an Incident - Incident Response - Care About Incident Response. IR Management: Computer Security Incident - Goals of Incident Response – People Involved in the IR Process - The Incident Response Process. Pre-Incident Preparation: Preparing the Organization for Incident Response - Preparing the IR Team - Preparing the Infrastructure for Incident Response. **Practical Component** Creation of an Incident Response (IR) plan document including roles, escalation paths, and communication protocols - Define an IR team and simulate an organization's IR preparation with role-play scenarios.	**6 Hours** **6 Hours**
INCIDENT DETECTION AND CHARACTERIZATION Getting the Investigation Started: Collecting Initial Facts Building an Attack Timeline - Understanding Investigative Priorities. Initial Development of Leads Defining Leads of Value - Turning Leads into Indicators - Resolving Internal and External Leads Discovering the Scope of the Incident: Examining Initial Data - Customer Data Loss Scenario - ACH Fraud Scenario. **Practical Component** Analysing sample logs to reconstruct an incident timeline – Usage of IOC (Indicators of Compromise) to detect potential threats.	**6 Hours** **6 Hours**
DATA COLLECTION **Live Data Collection:** When to Perform a Live Response - Selecting a Live Response Tool - What to Collect - Live Data Collection on Windows and Unix-Based Systems **Forensic Duplication:** Forensic Image Formats - Traditional Duplication - Live System Duplication - Duplication of Enterprise Assets **Network Evidence:** The Case for Network Monitoring - Setting Up a Network Monitoring System -Network Data Analysis - Collect Logs Generated from Network Events. **Practical Component** Usage of tools to collect volatile data from live systems - Creation and verify a forensic disk image	**6 Hours** **6 Hours**
DATA ANALYSIS **Analysis Methodology:** Define Objectives – Know, Access, Analyze user Data - Evaluate Results. **Investigating Windows Systems**: NTFS and File System Analysis - Prefetch, Event Logs, Scheduled Tasks - The Windows Registry - Memory Forensics, Alternative Persistence Mechanisms **Investigating Applications:** Application Data - Where Is Application Data Stored? General Investigation Methods - Web Browsers, E-Mail Clients, Instant Message Clients. **Practical Component** Setting up of a network monitoring system and capture evidence – Analysing NTFS structure, event logs, prefetch, and registry entries.	**6 Hours** **6 Hours**
REMEDIATION Malware Triage: Malware Handling - Triage Environment -Static and Dynamic Analysis. Report Writing and its importance- Reporting Standards- Report Style and Formatting - Quality Assurance Remediation: Remediation Introduction - Basic Concepts - Remediation Pre-Checks - Form the Remediation Team. **Practical Component**	**6 Hours**

Extraction and analysing data from browsers, emails, and IM clients - Static/dynamic analysis of malware and preparation of a formal incident report.	**6 Hours**

Theory Hours:	**30**	**Tutorial Hours:**	**0**	**Practical Hours:**	**30**	**Project Hours:**	**0**	**Total Hours:**	**60**

Learning Resources

Reference books/ Web Links

1. Jason T. Luttgens, Matthew Pepe, and Kevin Mandia,"Incident Response & Computer Forensics", McGraw Hill publication, 2023.
2. Richard Bejtlich, "The Practice of Network Security Monitoring",No Starch Press publication,2013.
3. Vinny Troia, "Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques", Wiley publication, 2020.
4. Gerard Johansen, "Digital Forensics and Incident Response: An intelligent way to respond to attacks", Packt publication, 2017.
5. Harlan Carvey, "Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 7", Syngress Media,U.S, 2012.
6. Don Murdoch GSE, "Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder", CreateSpace Independent Publishing Platform Publication, 2014.
7. Dafydd Stuttard and Marcus Pinto, "The Web Application Hacker's Handbook", Wiley Publication, 2011.
8. Sherri Davidoff and Jonathan Ham, "Network Forensics: Tracking Hackers through Cyberspace", Pearson Prentice Hall Publication, 2012.

Online Resources

1. https://www.coursera.org/specializations/cyber-incident-response
2. https://www.coursera.org/learn/packt-incident-response-and-risk-management-ce9ny
3. https://www.coursera.org/learn/stages-of-incident-response

Assessment (Embedded course)

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)
Lab Workbook, Experimental Cycle tests, viva-voce.

Course Curated by

Expert(s) from Industry	Expert(s) from Higher Education Institution	Internal Expert	
-	-	Dr.G.Kanagaraj AP II / CSE	
Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

24CBE009	**Cyber Threat Hunting and Intelligence**	**L**	**T**	**P**	**J**	**C**
		3	**0**	**0**	**0**	**3**
PE		**SDG**	**4,9,16**			

Pre-requisite courses	**Nil**	**Data Book / Codes / Standards (If any)**	Nil

Course Objectives:	**The purpose of taking this course is to:**
1	Understand the principles and processes of Cyber Threat Intelligence (CTI), including its strategic, operational, and tactical levels.
2	Learn and apply systematic threat hunting techniques using models like the Cyber Kill Chain and Threat Hunting Maturity Model.
3	Analyze adversary behavior using frameworks such as MITRE ATT&CK and simulate threat actor actions through emulation tools.
4	Set up and operate a cyber security research environment for data collection, analysis, and threat detection using industry-standard tools.
5	Evaluate and communicate threat hunting outcomes effectively through documentation, automation, and collaboration with incident response teams.

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Bloom's Taxonomy Level (BTL)**
CO 1	Explain the fundamentals of Cyber Threat Intelligence (CTI), including intelligence levels, the Intelligence Cycle, and the collection process, to lay the groundwork for effective incident response.	U
CO 2	Apply threat hunting techniques using frameworks like the Cyber Kill Chain and Threat Hunting Maturity Model, by building hypotheses and conducting structured hunts based on technical data.	Ap
CO 3	Analyze adversarial behaviors and tactics using the MITRE ATT&CK Framework, data dictionaries, and open-source tools, to map adversary actions and simulate emulation plans.	An
CO 4	Apply and configure ELK/HELK, Mordor, Caldera, and Atomic Red Team to build and manage a cyber research environment for implementing automated threat detection.	Ap
CO 5	Apply threat hunting methodologies and tools like MaGMa to measure and analyze results and use the outcomes to inform and support the Incident Response Team with actionable insights.	Ap

Course Outcomes (CO)	**Program Outcomes (PO)** **(Strong-3, Medium – 2, Weak-1)**				
	1	**2**	**3**	**4**	**5**
1	3	2		3	
2	3	3		3	
3	3	2		2	
4	3	2		2	
5	3	2		3	

Course Content

CYBER THREAT INTELLIGENCE Cyber Threat Intelligence: Strategic, Operational, Tactical Levels. The Intelligence Cycle: Planning and Targeting - Preparation and Collection - Processing and Exploitation - Analysis and Production - Dissemination and Integration - Evaluation and Feedback. Defining your Incident Response (IR). The Collection Process: Indicators of Compromise - Understanding Malware - OSINT and Honeypots.	**7 Hours**
THREAD HUNTING Processing and Exploitation: Cyber Kill Chain - Bias and Analysis - Threat Hunting : Technical Requirements - Types of Threat Hunts - Threat Hunter Skill Set - Pyramid of Pain - The Threat Hunting Maturity Model: Threat Hunting Process - Data-Driven Methodology - TaHiTI – Targeted Hunting Integrating Threat Intelligence - Building a Hypothesis - Technical Requirements: Understanding the Data - Operating Systems and Networking Basics - Windows-native Tools - Data Sources (Endpoint, Network, Security).	**8 Hours**
UNDERSTANDING THE ADVERSARY Mapping the Adversary: Technical Requirements - The ATT&CK Framework: Tactics, Techniques, Sub-techniques, and Procedures - ATT&CK Matrix and Navigator. Mapping with ATT&CK: Testing Yourself Working with Data: Technical Requirements - Using Data Dictionaries- Open-Source Security Events Metadata - MITRE CAR and Sigma - Emulating the Adversary: Creating an Adversary Emulation Plan Adversary Emulation Tools: MITRE ATT&CK Emulation Plan - Atomic Red Team, Mordor, Caldera.	**12 Hours**
WORKING WITH A RESEARCH ENVIRONMENT Creating a Research Environment: Technical Requirements - Setting Up a Research Environment VMware ESXI, Windows Server, ELK, HELK - Bonus – Adding Mordor Datasets to ELK. How to Query the Data: Technical Requirements - Atomic Hunting with Atomic Red Team - Testing Cycles - Quasar RAT. Hunting for the Adversary : Technical Requirements - MITRE Evaluations and Sigma Rules - Using MITRE Caldera - Importance of Documenting and Automating the Process - The Importance of Documentation - Threat Hunter Playbook, Jupyter Notebook - The Importance of Automation.	**12 Hours**
COMMUNICATING TO SUCCEED Assessing Data Quality: Technical Requirements - Distinguishing Data Quality - OSSEM Power-up, DeTT&CT, Sysmon-Modular - Understanding the Output - Understanding Hunt Results. Defining Good Metrics to Track Success : Technical Requirements - Defining Good Metrics - Using MaGMa for Threat Hunting - Engaging the Response Team and Communicating Results - Getting the Incident Response Team Involved - Impact of Communication on Success.	**6 Hours**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**0**	**Project Hours:**	**0**	**Total Hours:**	**45**

Learning Resources

Textbooks

1. Costa-Gazcón, Valentina. Practical Threat Intelligence and Data-Driven Threat Hunting. Packt Publishing, February 2021.
2. Kaplan, C. Aaron, and Leuprecht, Christian. Cyber Intelligence Tradecraft: What It Is, How to Do It. Rowman & Littlefield, 2017.
3.

Reference books/ Web Links

1. Singer, P.W., and Friedman, Allan. Cyber security and Cyberwar: What Everyone Needs to Know. 2014.
2. Troia, Vinny. "Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques.". 2018: pp. 15-30.
3. Recorded Future. Guide for Security Teams to Unlocking the Power of Intelligence. 2015.
4. Cajigas, Carlos. "Adversary Simulation and Red Team Tactics." Technical Report No. 1234. XYZ Institute, City, Country, 2018.
5. Anderson, Ross J. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed., 2020.

Online Resources

1. https://www.coursera.org/learn/ibm-penetration-testing-threat-hunting-cryptography -- Penetration Testing, Threat Hunting, and Cryptography
2. https://www.coursera.org/learn/introduction-threat-intelligence-lifecycle -- Introduction to the Threat Intelligence Lifecycle
3. https://www.coursera.org/specializations/certified-in-cybersecurity#courses -- ISC2 Certified in Cybersecurity Specialization

.

Assessment

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)

Course Curated by

Expert(s) from Industry	Expert(s) from Higher Education Institution	Internal Expert	
-	-	Dr. C. Rajan Krupa AP III / MCA	
Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

24CBC010	**Mobile Device Forensics**	**L**	**T**	**P**	**J**	**C**
		2	**0**	**2**	**0**	**3**
PE		**SDG**	**4,9**			

Pre-requisite courses	**Digital Forensics**	**Data Book / Codes / Standards (If any)**	Nil

Course Objectives:	**The purpose of taking this course is to:**
1	To introduce the principles and phases of digital forensics, including the identification, collection, examination, analysis, and presentation of digital evidence.
2	To provide an understanding of digital crimes, related legal frameworks, and investigative techniques used in the collection and analysis of digital evidence.
3	To familiarize students with digital forensic readiness concepts, standards, and frameworks in both law enforcement and enterprise environments.
4	To develop hands-on skills in performing forensic analysis of iOS and Android devices using specialized tools and techniques.

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Bloom's Taxonomy Level (BTL)**
CO 1	Explain the phases of the digital forensic process, including identification, collection, examination, analysis, and presentation of digital evidence.	U
CO 2	Describe various types of digital crimes and analyze investigation methods and legal considerations used in evidence collection.	U
CO 3	Apply digital forensic readiness strategies in enterprise and law enforcement contexts, including frameworks and industry standards.	Ap
CO 4	Apply forensic tools and procedures to acquire and analyze data from iOS devices, including jailbroken environments and iCloud sources.	Ap
CO 5	Use forensic acquisition and analysis of Android devices using ADB, rooting techniques, and app decompilation tools.	Ap

Course Outcomes (CO)	**Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)**				
	1	**2**	**3**	**4**	**5**
1		2		2	
2		3		2	
3	2			2	
4	3			3	
5	2			3	

Course Content	
INTRODUCTION TO DIGITAL FORENSICS Forensic Science – Digital Forensics – Digital Evidence – The Digital Forensics Process - Introduction – The Identification Phase – The Collection Phase – The Examination Phase – The Analysis Phase – The Presentation Phase	**6 Hours**
Practical Component Collecting Digital Evidence from mobile devices - Identify potential sources of digital evidence and apply basic preservation techniques.	**6 Hours**
DIGITAL CRIME AND INVESTIGATION Digital Crime – Substantive Criminal Law – General Conditions – Offenses – Investigation Methods for Collecting Digital Evidence – International Cooperation to Collect Digital Evidence.	**6 Hours**
Practical Component Identifying the challenges in mobile device forensics – Usage of investigation methods (interviews, system imaging) to collect mock evidence.	**6 Hours**
DIGITAL FORENSIC READINESS Introduction – Law Enforcement versus Enterprise Digital Forensic Readiness – Rationale for Digital Forensic Readiness – Frameworks, Standards and Methodologies – Enterprise Digital Forensic Readiness – Challenges in Digital Forensics.	**6 Hours**
Practical Component Comparion existing forensic readiness frameworks (e.g., NIST, ISO) for applicability – Designing of a forensic readiness plan for an enterprise or law enforcement agency.	**6 Hours**
iOS FORENSICS Mobile Hardware and Operating Systems – iOS Fundamentals – Jailbreaking – File System - Hardware – iPhone Security – iOS Forensics – Procedures and Processes – Tools – Oxygen Forensics – MobilEdit – iCloud.	**6 Hours**
Practical Component Demonstrating the jailbreak concept - Jailbreak a simulated iOS device and acquire data using forensic tools.	**6 Hours**
ANDROID FORENSICS Android basics – Key Codes – ADB – Rooting Android – Boot Process – File Systems – Security -Tools – Android Forensics – Forensic Procedures – ADB – Android Only Tools – Dual Use Tools -Oxygen Forensics – MobilEdit – Android App Decompiling.	**6 Hours**
Practical Component Demonstration of Rooting the android mobile device – Demonstration of the ADB tool with an example use case.	**6 Hours**

Theory Hours:	**30**	**Tutorial Hours:**	**0**	**Practical Hours:**	**30**	**Project Hours:**	**0**	**Total Hours:**	**60**

Learning Resources

Reference books/ Web Links

1. Andre Arnes, “Digital Forensics”, Wiley, 2018.
2. Chuck Easttom, “An In-depth Guide to Mobile Device Forensics”, First Edition, CRC Press, 2022.

3. Vacca, J, Computer Forensics, Computer Crime Scene Investigation, 2nd Ed, Charles River Media, 2005, ISBN: 1-58450-389
Online Resources
1. https://www.coursera.org/learn/digital-forensics-concepts 2. https://www.classcentral.com/course/study-com-computer-science-335-mobile-forensics-112962 3. https://www.classcentral.com/classroom/youtube-mobile-app-analysis-with-santoku-linux-andrew-hoog-228034

Assessment (Embedded course)
CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE) Lab Workbook, Experimental Cycle tests, viva-voce.

Course Curated by			
Expert(s) from Industry	**Expert(s) from Higher Education Institution**	**Internal Expert**	
-	-	Dr.G.Kanagaraj AP II / CSE	
Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

24CBC011	Intrusion Detection and Prevention System	L	T	P	J	C
		2	0	2	0	3
PE		SDG	4,9			

Pre-requisite courses	Nil	Data Book / Codes / Standards (If any)	Nil

Course Objectives:	The purpose of taking this course is to:
1	Gain foundational knowledge of intrusion detection and prevention principles, goals, and relevance in cyber security.
2	Analyze various types of IDPS, their architectural components, and deployment strategies in diverse network environments.
3	Assess the strengths, limitations, and performance challenges of intrusion detection and prevention systems.
4	Develop the skills to design, configure, and implement basic IDPS solutions for monitoring and threat mitigation.

Course Outcomes:	After successful completion of this course, the students shall be able to	Bloom's Taxonomy Level (BTL)
CO 1	Summarize the historical development of intrusion detection systems and the evolution of auditing techniques.	U
CO 2	Apply endpoint and system-level approaches to enhance security posture in host-based and network-based systems.	Ap
CO 3	Utilize sniffing and spoofing tools in a controlled environment to simulate and analyze network attacks.	Ap
CO 4	Evaluate data collection techniques for IDS/IPS, to access the strengths and weakness of host systems.	An
CO 5	Examine the Snort configuration file to identify key parameters for customization.	An

Course Outcomes (CO)	Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)				
	1	2	3	4	5
1	3				
2	2			3	
3	3				
4	2			3	
5	2			3	

Course Content	
HISTORY AND COMPONENTS OF IDS History of Intrusion detection, Audit, Concept and definition, Internal and external threats to data, attacks, Need and types of IDS, Information source Host based information sources, Network based information sources, Components of IDS, Host and Network based IDS, Implementing and Evaluating IDS, Intrusion Detection Vs Intrusion Prevention, CVE standards.	**6 Hours**
Practical Component Anomaly-based Intrusion Detection - Misuse Detection with Signature-based IDS	**6 Hours**
IDS INFRASTRUCTURE IDS Architecture, IDS/IPS Management and Architecture Issues with regard to deploying IDS/IPS systems, end point approach to security, system approach to security, IDS Interoperability models: CIDF (Common Intrusion Detection Framework), IDMEF (Intrusion Detection Message Exchange Format), IODEF (Incident Object Description Exchange Format), CVE (Common Vulnerabilities and Exposures), OVAL (Open Vulnerability and Assessment Language)	**6 Hours**
Practical Component Custom Rule Creation in Snort - Deploying OSSEC (HIDS) vs. Snort (NIDS)	**6 Hours**
DATA COLLECTION MECHANISM Data Sampling, Packet Sampling, Flow Sampling, techniques for visualizing network data, Packet Sampling tools, Tcpdump windump, Wireshark tool, Writing Tcpdump/Windump Filters, libcap/winpcap libraries, pcap file, sniffing and spoofing tools, data and methodologies of computer intrusion detection, statistical & machine approaches to detection of attacks on computers.	**6 Hours**
Practical Component Implementation of Inline blocking - Metric calculation for accessing IDS performance	**6 Hours**
HOST-BASED INTRUSION DETECTION SYSTEM Host-based intrusion detection system (IDS)/Intrusion prevention system (IPS), network based IDS/IPS. Data collection for IDS/IPS.Intrusion detection techniques, misuse detection: pattern matching, rule-based and state-based; anomaly detection : statistical based, machine learning based, cloud based, hybrid detection.	**6 Hours**
Practical Component Deploying a network-based IDS/IPS and monitoring traffic for attacks on a simulated network.	**4 Hours**
PACKET ANALYSIS USING SNORT Introduction to SNORT, SNORT installation, scenarios, Running SNORT on Multiple Network Interfaces, Command line interfaces, Snort files, Snort Modes and Snort Alert Modes, Working with Snort Rules, Rule Headers, Rule Options, The Snort Configuration File etc. Plugins, Preprocessors and Output Modules, Using Snort with MySQL.	**6 Hours**
Practical Component Integration of Snort or another IDS with a MySQL database to store alerts for further analysis - Implementation of Wireshark for packet analysis alongside Snort to detect and respond to network intrusions - Switching Snort from IDS mode to IPS mode and evaluation of its ability to block real-time attacks.	**8 Hours**

Theory Hours:	**30**	**Tutorial Hours:**	**0**	**Practical Hours:**	**30**	**Project Hours:**	**0**	**Total Hours:**	**60**

Learning Resources

Textbooks

1. Ali A. Ghorbani, Wei Lu, “Network Intrusion Detection and Prevention: Concepts and Techniques”, Springer, 2010.
2. Rafeeq Rehman : “ Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID,” 1st Edition, Prentice Hall , 2003.

Reference books/ Web Links

3. Christopher Kruegel,Fredrik Valeur, Giovanni Vigna: “Intrusion Detection and Correlation Challenges and Solutions”, 1st Edition, Springer, 2005.
4. Carl Endorf, Eugene Schultz and Jim Mellander “ Intrusion Detection & Prevention”, 1st Edition, Tata McGraw-Hill, 2004.
5. Stephen Northcutt, Judy Novak, “Network Intrusion Detection”, 3rd Edition, New Riders Publishing, 2002.
6. T. Fahringer, R. Prodan, “A Text book on Grid Application Development and Computing Environment”. 6th Edition, KhannaPublihsers, 2012.

Online Resources

1. https://www.coursera.org/learn/introduction-to-intrusion-detection-systems-ids.
2. https://www.classcentral.com/subject/intrusion-detection-systems
3. https://www.open.edu/openlearn/mod/oucontent/view.php?id=48325&section=3

Assessment (Embedded course)

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)
Lab Workbook, Experimental Cycle tests, viva-voce.

Course Curated by

<table>
<tr><th>Expert(s) from Industry</th><th colspan="2">Expert(s) from Higher Education Institution</th><th colspan="2">Internal Expert</th></tr>
<tr><td>-</td><td colspan="2">-</td><td colspan="2">Dr. A.Roshini AP III / CSE</td></tr>
<tr><td>Recommended by BoS on</td><td colspan="4">09.05.2025</td></tr>
<tr><td>Academic Council Approval</td><td>No: 28</td><td colspan="2">Date</td><td>26-06-25</td></tr>
</table>

24CBC012	Mobile Application Security	L	T	P	J	C
		2	0	2	0	3
PE		SDG	11			

Pre-requisite courses	Cryptography & Network Security	Data Book / Codes / Standards (If any)	Nil

Course Objectives:	The purpose of taking this course is to:
1	Learn about the security models of mobile operating systems, and security protocols used in mobile app communication and data storage.
2	Acquire practical skills in performing security audits on mobile applications using industry-standard tools like OWASP ZAP, Burp Suite and Drozer.
3	Develop the competency to build and deploy secure mobile applications that protect user data and comply with privacy regulations.

Course Outcomes:	After successful completion of this course, the students shall be able to	Bloom's Taxonomy Level (BTL)
CO 1	Apply best practices in mobile browser security to secure mobile applications from common vulnerabilities	Ap
CO 2	Apply secure development practices to WAP and Mobile HTML applications to mitigate SQL injection and phishing attacks	Ap
CO 3	Apply security mechanisms and evaluate threats across different Bluetooth versions.	Ap
CO 4	Analyze application-specific vulnerabilities in SMS and MMS communication across mobile platforms.	An
CO 5	Analyze the security features and implementations across various mobile operating systems and security policy enforcement mechanisms.	An

Course Outcomes (CO)	Program Outcomes (PO) (Strong-3, Medium – 2, Weak-1)				
	1	2	3	4	5
1	3				3
2	3		2		3
3	3		2		3
4	3			2	3
5	3			2	3

Course Content	
TOP MOBILE ISSUES AND DEVELOPMENT STRATEGIES Top Issues Facing Mobile Devices, Physical Security , Secure Data Storage (on Disk), Strong Authentication with Poor Keyboards , Multiple-User Support with Security, Safe Browsing Environment , Secure Operating Systems, Application Isolation, Information Disclosure, Virus, Worms, Trojans, Spyware, and Malware , Difficult Patching/Update Process, Strict Use and Enforcement of SSL, Phishing , Cross-Site Request Forgery (CSRF), Location Privacy/Security, Insecure Device Drivers, Multi Factor Authentication, Tips for Secure Mobile Application Development.	**6 Hours**
Practical Component:	**6 Hours**

Implement login with multiple roles and secure session handling- Perform penetration testing on a mobile app using Frida or Drozer.	
WAP AND MOBILE HTML SECURITY WAP and Mobile HTML Security WAP and Mobile HTML Basics, Authentication on WAP/Mobile HTML Sites, Encryption, Application Attacks on Mobile HTML Sites, Cross-Site Scripting, SQL Injection, Cross-Site Request Forgery, HTTP Redirects, Phishing, Session Fixation, Non-SSL Login, WAP and Mobile Browser Weaknesses, Lack of HTTP Only Flag Support, Lack of SECURE Flag Support, Handling Browser Cache, WAP Limitations. **Practical Component:** Simulate SQL injection on login forms and apply parameterized query defenses.- Inject and test XSS vulnerabilities on a mobile web app, and apply input validation.	**6 Hours** **6 Hours**
BLUETOOTH SECURITY Bluetooth Security Overview of the Technology , History and Standards , Common Uses , Alternatives, Future, Bluetooth Technical Architecture , Radio Operation and Frequency, Bluetooth Network Topology , Device Identification , Modes of Operation , Bluetooth Stack ,Bluetooth Profiles, Bluetooth Security Features , Pairing , Traditional Security Services in Bluetooth, Security “Non-Features” , Threats to Bluetooth Devices and Networks, Bluetooth Vulnerabilities, Bluetooth Versions Prior to v1.2, Bluetooth Versions Prior to v2.1. **Practical Component:** Capture and analyze Bluetooth traffic during a secure session.- - Use tools to intercept Bluetooth communication between devices.	**6 Hours** **6 Hours**
SMS SECURITY SMS Security Overview of Short Message Service, Overview of Multimedia Messaging Service, Wireless Application Protocol (WAP), Protocol Attacks, Abusing Legitimate Functionality, Attacking Protocol Implementations, Application Attacks, iPhone Safari, Windows Mobile MMS, Motorola RAZR JPG Overflow, Walkthroughs, Sending PDUs, Converting XML to WBXML. **Practical Component:** Demonstrate spoofing or DoS via malformed SMS.- -Use command-line tool to convert XML into WBXML and decode WBXML back.	**6 Hours** **6 Hours**
ENTERPRISE SECURITY Enterprise Security on the Mobile OS Device Security Options, PIN, Remote, 346 Secure Local Storage, Apple iPhone and Keychain, Security Policy Enforcement, Encryption, Full Disk Encryption, E-mail Encryption, File Encryption, Application Sandboxing, Signing, and Permissions, Application Sandboxing, Application Signing, Permissions, Buffer Overflow Protection, Windows Mobile, iPhone, Android, BlackBerry, Security Feature Summary. **Practical Component:** Request, monitor, and revoke app permissions using developer tools - Simulate an app crash due to buffer overflow and test platform protection.	**6 Hours** **6 Hours**

Theory Hours:	**30**	**Tutorial Hours:**	**0**	**Practical Hours:**	**30**	**Project Hours:**	**0**	**Total Hours:**	**60**

Learning Resources
Textbooks
Himanshu Dwivedi, Chris Clark, David Thiel, “Mobile Application Security”, TATA McGraw Hill Publication, 1st edition, 2010.
Reference books/ Web Links

1. Kami S. Makki, et al, “Mobile and Wireless Network Security and Privacy”, Springer Publication, First Edition, 2007.
2. Abhishek Dubey, “Android Security Attacks Defenses”, CRC Press Publication, First Edition, 2013.

Online Resources

1. https://developer.android.com/quality/privacy-and-security
2. https://www.udemy.com/course/mobile-application-security-and-penetration-testing-e/?srsltid=AfmBOopTINuyccNTeMAe1OLfCKeGi4SskR7atqqV34epqmyDiDhsTdnl&couponCode=LEARNNOWPLANS

Assessment (Embedded course)

CAT, Activity and Learning Task(s), Assignments, End Semester Examination (ESE)
Lab Workbook, Experimental Cycle tests, viva-voce.

Course Curated by

Expert(s) from Industry	Expert(s) from Higher Education Institution	Internal Expert
-	-	Dr.G.Kanagaraj AP II / CSE

Recommended by BoS on	09.05.2025		
Academic Council Approval	No: 28	**Date**	26-06-25

OPEN ELECTIVES

24MEO001	**SUSTAINABLE INNOVATIONS AND PRACTICES**	**L**	**T**	**P**	**J**	**C**
		3	**0**	**0**	**0**	**3**
OE		**SDG**	**3**			

Pre-requisite: Nil

	Faculty Name:	**Mr. M. Sathish**
	Designation:	**Assistant Professor-II**
	Concern/industry/Institution:	**KCT**
	LinkedIn profile	**https://www.linkedin.com/in/sathish-mathiyazhagan-2a63b65b/**

Course Objectives:	**The purpose of taking this course is to:**
1	Gain a deep understanding of sustainability principles.
2	Learn how to design and implement sustainable solutions.
3	Enhance knowledge of sustainable business practices.

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Revised Bloom's Taxonomy Level (RBT)**
CO 1	Understand the fundamental principles of sustainability and sustainable development.	U
CO 2	Analyse the impact of human activities on the environment and society.	An
CO 3	Assess and design sustainable solutions for various sectors.	An
CO 4	Evaluate the role of policy, technology, and global cooperation in achieving sustainability goals.	E

MODULE	**Hours**
INTRODUCTION TO SUSTAINABILITY Introduction- Definition and history of sustainability-The three pillars: environmental, social, and economic sustainability-The Anthropocene: Human impact on the Earth-Sustainable Development Goals (SDGs) overview-Systems Thinking and Global Challenges-Systems thinking in sustainability-Global environmental challenges: Climate change, deforestation, pollution-Introduction to ecological footprints and planetary boundaries.	**9**
ENVIRONMENTAL SUSTAINABILITY Climate Change and Energy-Science of climate change and global warming-Renewable energy: Solar, wind, and other alternatives-Transitioning to a low-carbon economy-Biodiversity and Ecosystems-The importance of biodiversity and ecosystems-Threats to biodiversity: Habitat loss, pollution, and overexploitation-Conservation strategies and sustainable resource management.	**8**
SOCIAL SUSTAINABILITY Poverty, Inequality, and Development-The relationship between poverty, inequality, and sustainability-Sustainable development in low-income countries-Social justice and equity in the context of sustainable development-Sustainable Cities and Communities-Urbanization and its impact	**8**

on sustainability-Designing sustainable cities: Smart cities, green infrastructure-Case studies of sustainable urban planning.	
ECONOMIC SUSTAINABILITY The Economics of Sustainability-Economic growth and sustainability: The concept of decoupling-The circular economy and sustainable business models-Sustainable finance and green investing-Corporate Responsibility and Policy-The role of businesses in sustainability-Corporate social responsibility (CSR) and ethical practices-Government policies and international agreements-Paris Agreement.	**10**
GLOBAL COOPERATION AND FUTURE DIRECTIONS Global Cooperation for Sustainable Development-The role of international organizations -UN, World Bank in sustainability-Global partnerships and collaborative efforts to achieve the SDGs-Case studies of successful global sustainability initiatives-Innovations and Future Trends-Technological innovations driving sustainability clean tech, AI-Future scenarios and challenges in sustainability. Case Study: Developing a comprehensive sustainability plan for a real-world challenge.	**10**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**0**	**Project Hours:**	**0**	**Total Hours:**	**45**

Learning Resources

Reference books/ Web Links

1. Tom Theis and Jonathan Tomkin, *Sustainability: A Comprehensive Foundation*, OpenStax CNX (2018).
2. Ken Webster, The Circular Economy: A Wealth of Flows, 2nd Edition Ellen MacArthur Foundation Publishing, Cowes, UK, (2017).
3. Jeffrey D. Sachs, The Age of Sustainable Development, Columbia University Press (2015).
4. Mark Maslin, Climate Change: A Very Short Introduction, Oxford University Press (2014).

Online Resources

1. “Introduction to Sustainability " https://www.coursera.org/learn/sustainability
2. “The Age of Sustainable Development" https://www.coursera.org/learn/sustainable-development

Assessment	
Formative	Continuous
Assignments, Quiz, Case Studies	CAT-I,CAT-II and End Semester Examination

Course Curated By

Expert(s) from Industry	**Expert(s) from Higher Education Institutions**	**Internal Expert(s)**
		Mr. M. Sathish, AP-II, CSE

24MEO002	Electric and Autonomous Mobility	L	T	P	J	C
		3	0	0	0	3
OE		SDG	3			

Pre-requisite: Nil

	Faculty Name:	**Mr. V. Senthilkumar**
	Designation:	**Assistant Professor-II**
	Concern/industry/Institution:	**KCT**
	LinkedIn profile	**https://www.linkedin.com/in/senthil-kumar-v-5498aa60/**

Course Objectives:	**The purpose of taking this course is to:**
1	Understand the design and evolution of electric vehicles and their market trends.
2	Analyse electric mobility ecosystems and emerging business models.
3	Apply deep learning techniques to enhance computer vision and sensor fusion in autonomous vehicles.
4	Implement object detection and tracking methods using advanced computer vision and sensor fusion techniques.

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Revised Bloom's Taxonomy Level (RBT)**
CO1	Understand the design and evolution of electric vehicles and their market trends.	U
CO2	Evaluate EV components, charging technologies, and infrastructure challenges.	U
CO3	Analyse electric mobility ecosystems and emerging business models.	An
CO4	Apply deep learning techniques to enhance computer vision and sensor fusion in autonomous vehicles.	Ap
CO5	Implement object detection and tracking methods using advanced computer vision and sensor fusion techniques.	E

MODULE	**Hours**
INTRODUCTION TO ELECTRIC VEHICLES (EVS) Overview of Electric Vehicles: Historical development and evolution of EVs, Components and Architecture of EVs: Key components of EVs: Electric motors, batteries, power electronics, and control systems. EV Market and Trends: Current global and regional market trends, Government policies, incentives, and regulations supporting EV adoption.	**6**
EV CHARGING INFRASTRUCTURE AND TECHNOLOGY EV Charging Basics: Types of EV charging (AC, DC, wireless), levels of charging (Level 1, Level 2, Level 3) and their differences. Charging Infrastructure Deployment: Planning and implementation of public and private charging stations., Role of smart grids and Vehicle-to-Grid (V2G) technology. Challenges and Solutions in Charging Infrastructure: Addressing range anxiety and charging time issues, Infrastructure challenges in urban and rural areas.	**9**
ELECTRIC MOBILITY ECOSYSTEM AND BUSINESS MODELS Electric Mobility and Urban Planning: Impact of EVs on urban transportation systems, Role of EVs in reducing urban pollution and congestion, Integration of EVs with public transportation and shared mobility services. Business Models for Electric Mobility: Emerging business models: Mobility-as-a-Service (MaaS), Car-as-a-Service (CaaS),EV fleet management for businesses and public transportation, Economic and environmental benefits of electric mobility.Case Studies in Electric Mobility: Successful case studies of electric mobility implementations in different regions.	**10**

ADVANCED DEEP LEARNING TECHNIQUES FOR AUTONOMOUS VEHICLES Advanced Computer Vision Techniques: Convolutional Neural Networks (CNNs): Used for detecting and classifying objects. Semantic Segmentation, Instance Segmentation: Identifies and distinguishes objects in complex environments. Deep Learning for Sensor Fusion: Sensor Integration, Ulti-Modal Learning, Data Handling, Reinforcement Learning for Autonomous Driving: Basics of Reinforcement Learning, Application in Driving, Simulations Safety and Reliability in Deep Learning Systems: Ensuring Safety, Testing and Validation.	**10**
ADVANCED COMPUTER VISION TECHNIQUES FOR AUTONOMOUS VEHICLES Object Detection and Tracking: YOLO (You Only Look Once),SSD (Single Shot MultiBox Detector),Kalman Filters, Semantic and Instance Segmentation: Semantic Segmentation, Instance Segmentation Sensor Fusion for Enhanced Perception: Integration of Camera and LiDAR Data, Multi-Modal Fusion Techniques, Noise Reduction and Data Synchronization.	**10**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**0**	**Project Hours:**	**0**	**Total Hours:**	**45**

Learning Resources

Reference books/ Web Links

1. Tom Denton, Electric and Hybrid Vehicles, Routledge, (2020).
2. Shai Shalev-Shwartz and Shaked Shammah, Deep Learning for Autonomous Vehicles, Springer, (2021).
3. James Larminie and John Lowry, Electric Vehicle Technology Explained, Wiley, (2012).

Online Resources

1. https://www.coursera.org/learn/electric-vehicles-mobility
2. https://www.coursera.org/learn/introduction-deep-learning-computer-vision?specialization=deep-learning-computer-vision
3. https://www.coursera.org/programs/coursera-for-campus-faculty-ovg1y/learn/advanced-deep-learning-techniques-computer-vision?specialization=deep-learning-computer-vision

Assessment	
Formative	Continuous
Assignments, Quiz, Case Studies	CAT-I,CAT-II and End Semester Examination

Course Curated By

Expert(s) from Industry	**Expert(s) from Higher Education Institutions**	**Internal Expert(s)**
		Mr. V. Senthilkumar, CSE

24IEO074	**Modern Financial Strategies and Innovations**	**L**	**T**	**P**	**J**	**C**
		3	**0**	**0**	**0**	**3**
OE		**SDG**	**4, 9**			

Pre-requisite: Nil

	Faculty Name:	**Mayuri P T**
	Designation:	**Assistant Professor 1**
	Concern/industry/Institution:	**KCT**
	LinkedIn profile	**https://www.linkedin.com/in/mayuri-palanisamy**

Course Objectives:	**The purpose of taking this course is to:**
1	This course covers essential financial principles and concepts useful for both personal and corporate finance.
2	This course provides an in-depth introduction to the ideas, methods, and institutions that help manage risks and foster enterprise in financial markets.

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Revised Bloom's Taxonomy Level (RBT)**
CO 1	Understanding the financial principles and concept of Finance	U
CO 2	Equip learners with the financial decision-making skills.	Ap
CO 3	Evaluate company performance using profitability, efficiency, leverage, and other ratios.	E
CO 4	Assess the working capital needs of the business.	An
CO 5	Manage risks and foster enterprise in financial markets.	Ap

MODULE:	**Hours**
FINANCIAL STATEMENTS AND CASHFLOWS Introduction to Finance- Balance sheet - Assets, Liabilities, and Stockholders & Equity-Income Statement- Profit & loss- Cash flows -Sources and use of cashflows- Liquidity Leverage Ratios-Turnover Ratios- Profitability Ratios-Financial Ratios: Market Value Ratios- Financial Forecasting.	**9**
TIME VALUE OF MONEY Introduction to Time Value of Money-Present Value (PV) and Future Value (FV)- difference between the quoted interest rate and effective annual rate- Annual Percentage Rate (APR) -Effective Annual Interest Rate (EAR)-Annuity and perpetuity- Applications of time value of money.	**9**
VALUATION AND CAPITAL BUDGETING Basic terms of bonds-Interest Rates-Zero Coupon bonds- Types of Bonds- Bond Ratings- structure of bond market- Basic Concepts of Stock- Parameter Estimation- Growth Opportunities- P/E ratio-Stock Markets- Tax salvage value - Opportunity Costs- Sunk Costs- Side Effects- Capital Budgeting with Example.	**9**

RISK AND RETURN Historical record of return and risk- Trade-off between risk and return-Calculate return and risk-Systematic risk and unsystematic risk- Beta Coefficient- Valuation & Risk Estimation- The Capital Asset Pricing Model.	**9**
FINANCIAL MARKETS Financial Markets Introduction- Distribution and Outliers- Insurance Fundamentals-Forecasting--Introduction to Behavioural Finance- Prospect Theory- Leverage- Shares and Dividends- Investment Banks Introduction- Importance of Financial Theory.	**9**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**0**	**Project Hours:**	**0**	**Total Hours:**	**45**

Learning Resources

Reference books/ Web Links

1. Introduction to Finance by Lawrence J. Gitman, Jeff Madura
2. The Financial Times Guide to Investing: The definitive companion to investment and the financial markets by Glen Arnold

Online Resources

4. https://www.coursera.org/learn/introduction-to-finance-the-basics
5. https://www.coursera.org/learn/financial-markets-global
6. https://www.coursera.org/learn/introduction-to-finance-the-role-of-financial-markets

Assessment

Formative	Continuous
Assignments, Presentations, Quiz	CAT- I, CAT – II and End Semester Examination

Course Curated By

Expert(s) from Industry	Expert(s) from Higher Education Institutions	Internal Expert(s)
		Ms. Mayuri P T, MBA-IEV

24IEO075	Sports Analytics and Emerging Technologies	L	T	P	J	C
		3	0	0	0	3
OE		SDG	4, 8			

Pre-requisite: Nil

	Faculty Name:	Asmitha Shree R
	Designation:	Assistant Professor 1
	Concern/industry/Institution:	KCT
	LinkedIn profile	https://www.linkedin.com/in/asmitha-shree

Course Objectives:	The purpose of taking this course is to:
1	To provide a foundational understanding on the relation between sports and society.
2	To enable students to apply core marketing principles in the context of sports.
3	To develop analytical skills for comparing sports marketing with other sectors.
4	To foster an understanding of the influence of data-driven decision-making in sports.
5	To develop critical thinking and problem-solving skills in sports management.

Course Outcomes:	After successful completion of this course, the students shall be able to	Revised Bloom's Taxonomy Level (RBT)
CO 1	Understand the social dynamics, cultural identity, and globalization's impacts on the sports world.	U
CO 2	Understand the Evolution and Commercialization of Sports.	U
CO 3	Apply Marketing Principles to Sports.	Ap
CO 4	Analyse and differentiate between sports marketing and other marketing industries.	An
CO 5	Understanding Machine Learning Workflow in sports analytics.	U
CO 6	Apply regression analysis and machine learning models to predict sports outcomes.	Ap

MODULE	Hours
THE SOCIAL DYNAMICS OF SPORTS Exploring the concepts of games, play, and sports - Analyzing the impact of globalization, nationalism, and politics in sports - Understanding race, cultural identity, and their influence on the sports world.	**8**
THE EVOLUTION AND COMMERCIALIZATION OF SPORTS Examining the rise of women's sports, gender, and sexuality - Investigating why sports captivate global audiences - Understanding the mega business of sports- outdoor sports-extreme sports, and the search for adventure.	**8**
INTRODUCTION TO THE SPORTS MARKETING Introduction to the Sports Marketing- Sports Marketing Challenges- Marketing Basics Applied to Sports Marketing- The Traditional 4 P's: A Meaningful Update for Sports- Fan Marketing- Influence Marketing: Sports- Service vs. Product Marketing in Sports- Sports Marketing versus other Marketing Industries- Event Marketing & Management.	**9**
ENTERTAINMENT MARKETING Entertainment Marketing -Business Marketing- Creating Creative Content-Virtual Reality and Over the Top TV, Entertainment Branding (Placement) -Digital Viral Marketing- Dangers of Viral Marketing- Personal Entertainment Experience- Virtual Reality.	**10**

PREDICTION MODELS WITH SPORTS Machine Learning-The Machine Learning Workflow- Model: NHL Game Outcomes-Introduction to Regression Analysis -Building the Logistic Regression Model-Interpreting Regression Results - Considerations in Deploying The Model-Case Study: Regression Analysis - Batsman's performance and salary , Regression Analysis - Batsman's performance and salary ,Regression Analysis with Cricket Data.	**10**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**0**	**Project Hours:**	**0**	**Total Hours:**	**45**

Learning Resources

Textbooks

1. Grant Jarvie., Sport, Culture and Society: An Introduction., Taylor & Francis, (4th Edition, 2021).
2. Matthew D. Shank and Mark R. Lyberger., Sports Marketing: A Strategic Perspective., Routledge ,(6th Edition, 2021).
3. Thomas W. Miller Machine Learning and Data Mining for Sports Analytics, Pearson Education, Inc,(2017).

Reference books/ Web Links

1. Richard Giulianotti ,The Globalization of Sport: The Politics, Economics, and Culture of Sports", (2005)
2. Manfred Bruhn, Peter Rohlmann , "Sports Marketing: Fundamentals - Strategies – ,Springer, Instruments", (2022).

Online Resources

1. https://www.coursera.org/learn/international-entertainment-sports-marketing
2. https://www.coursera.org/learn/sports-marketing
3. https://www.coursera.org/learn/prediction-models-sports-data#modules
4. https://www.coursera.org/learn/machine-learning-sports-analytics
5. https://www.coursera.org/learn/foundations-sports-analytics#modules

Assessment	
Formative	Continuous
Assignments / Mini project, Quiz	CAT-I,CAT-II and End Semester Examination

Course Curated By

Expert(s) from Industry	**Expert(s) from Higher Education Institutions**	**Internal Expert(s)**
		Ms. Asmitha Shree, CSE

24IEO076	Healthcare Innovation and Technology	L	T	P	J	C
		3	0	0	0	3
OE		SDG	3			

Pre-requisite: Nil

	Faculty Name:	**G. Shobana**
	Designation:	**Assistant Professor-II**
	Concern/industry/Institution:	**KCT**
	LinkedIn profile	**www.linkedin.com/in/shobana-g-0425b348/**

Course Objectives:	**The purpose of taking this course is to:**
1	Understand Healthcare Systems and their Challenges.
2	Explore Ethical and AI-driven Approaches in Healthcare.
3	Investigation of Healthcare Marketplace Dynamics.

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Revised Bloom's Taxonomy Level (RBT)**
CO 1	Understand the structure and functions of healthcare systems, along with the associated ethical and technological frameworks.	U
CO 2	Understand the implementation and challenges of electronic health records (EHR) and eHealth models.	U
CO 3	Analyse Healthcare Market Dynamics over time.	An
CO 4	Examine Insurance and Medical Technology Markets and the impact of technological advancements on healthcare delivery and policy.	An
CO 5	Understand the global medical innovations, their impact, and the trends shaping the healthcare industry.	U

MODULE	**Hours**
INTRODUCTION TO HEALTHCARE SYSTEMS Overview of healthcare systems-Issue in healthcare – patients-Intermediaries -providers-challenges in healthcare access and delivery- Characteristics of Physician Practices -healthcare organizations and functions- Procedure Codes and Diagnosis Codes- Payment Systems- EMRs, EHRs, and PHRs-Stereotypical Plan Design- Public and Private Plans- Ethical frameworks - AI in health care delivery and payment structure.	**6**
EHR MANAGEMENT SYSTEM eHealth -model -challenges- Future scope- Collecting the data- Clinical use of personal health data-Mobile apps -social media apps -design of eHealth solutions-Evaluating health apps- Data and digital health records- Anatomy-Predictive and precision medicine- Privacy and security- performance-Interacting with healthcare professional – Advantages -Telehealth- personalize healthcare-EHR applications- patient journey -Features- Login, Authentication, Credentialing- Clinical Decision Support-types- CDS Committees-Introduction to Databases-Components of a SQL Server-EHR Interfaces- Training- Communications- Change Management.	**12**
HEALTHCARE MARKETPLACE Marketplace Overview, Healthcare Spending Drivers, Quality Trends, Market Evolution-Health Cost Growth- Issues -Effects of Health Behaviours.	**10**

Physician and hospital Service Market: Provider Market Overview-Price Discrimination- Physician Market Evolution-Physician Sites of Care- Physician-Hospital Market Evolution: Hospital Features-Scale and Scope, Hospital Issues, Quality and Safety- Hospital Future Trends, Policy Impact on Hospitals.	
INSURANCE AND MEDICAL TECHNOLOGY MARKET Risky Business, Utility of Wealth- working of Insurance model- Moral Hazard and Adverse Selection-Early Public Health Insurance- Healthcare Laws and Regulations (HIPAA, FDA, etc.) Quality and Safety Standards in Healthcare-Role of Policy -Future Health Reform. **Medical Technology Market**: Device- Drug-Medical Device Evolution-Medical Devices -Vision -New Technology Make Money-Measuring Medical Technology Value -FDA Approval for Pharmaceuticals- FDA Approval for Medical Devices- Drive Towards Cost-Effectiveness-preparing a Global Health Technology -Pharma & Device Convergence-Medical Technology Market.	**10**
GLOBAL MEDICAL INNOVATION Globalization of the Medical Industry, Medical Tourism Evolution & Growth, Medical Tourism in India, Key Issues, Health Bads and Their Consequences-Goals of Health Information Technology-Value of Health Information Technology- Insurer Information Technology- Provider Information Technology-Integrated Health Care Delivery-Key Questions for an Innovation Valuation-Technology-Secure- Return Investment on Technology.	**7**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**0**	**Project Hours:**	**0**	**Total Hours:**	**45**

Learning Resources

Reference books/ Web Links

1. Robert E. Hoyt, Ann K. Yoshihashi, Health Informatics: Practical Guide for Healthcare and Information Technology Professionals, Lulu.com (2019).
2. Peter M. Ginter, Linda E. Swayne, and Robert J. Duncan, Healthcare Systems: An Introduction, Health Administration Press (2018).
3. Sharon B. Buchbinder, Nancy H. Shanks, Introduction to Healthcare Management, Jones & Bartlett Learning (2017).
4. Richard Gartee, Electronic Health Records: Understanding and Using Computerized Medical Records, Pearson (2014).
5. Peter R. Kongstvedt, Healthcare Economics and Policy, Jones & Bartlett Learning (2013).

Online Resources

1. https://www.coursera.org/learn/intro-to-healthcare
2. https://www.coursera.org/learn/health-it-fundamentals
3. https://www.coursera.org/learn/ehealth
4. https://www.coursera.org/specializations/healthcare-marketplace

Assessment

Formative	Continuous
Assignments, Quiz, Case Studies	CAT-I,CAT-II and End Semester Examination

Course Curated By

Expert(s) from Industry	Expert(s) from Higher Education Institutions	Internal Expert(s)
		Ms. G. Shobana, AP-II, IT

24IEO077	**Corporate Strategy and Innovation**	**L**	**T**	**P**	**J**	**C**
		3	**0**	**0**	**0**	**3**
OE		**SDG**	**4, 9**			

Pre-requisite: Nil

	Faculty Name:	**Ms. P. T Mayuri**
	Designation:	**Assistant Professor 1**
	Concern/industry/Institution:	**KCT**
	LinkedIn profile	**https://www.linkedin.com/in/mayuri-palanisamy**

Course Objectives:	**The purpose of taking this course is to:**
1	This course is designed to help learners develop structured approaches to making sound strategic decisions in multi-business firms.
2	This focuses on modern practices in product management, especially for digital products.
3	It covers essential skills for product managers, emphasizing the need to understand customer needs, use actionable analytics, and apply agile methodologies.

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Revised Bloom's Taxonomy Level (RBT)**
CO 1	Develop structured, decision-based frameworks for making key corporate strategy decisions.	Ap
CO 2	Understand how to make informed decisions about business diversification and entering new markets or industries.	U
CO 3	Learn how to design corporate headquarters that add value across business units.	Ap
CO 4	Develop the ability to leverage actionable analytics and user data to drive product decisions.	E
CO 5	Understand how to iterate and enhance digital products continuously, using feedback and analytics.	An

MODULE	**Hours**
CORPORATE ADVANTAGE Introduction to Corporate strategy- Understanding Differences: Number of Businesses, Corporate Advantage, Competition- Sum-of-the-parts Analysis- Corporate Strategy Decisions- value multi-business firms.	**9**
DIVERSIFICATION AND DIVESTITURE Understanding the Basic Modes of Diversification- Diversification Test -Five-step Approach- Understanding the Basic Modes of Divestiture- Divestiture Test- Three-step Approach to the Divestiture Decision.	**9**
CORPORATE HEADQUARTERS Example of Corporate Headquarters- Controls of Corporate Headquarters- HQ Influence Models- Financial Perspective- Uncertainty Perspective- Synergy Perspective- Social Perspective- Synergistic Portfolio Framework.	**9**

FOCUS AND PRODUCT INNOVATING METHODS Introduction to Product Management Journey- Creating, Testing and Facilitating- Product Owner-Team Collaboration- Qualitative Analytics- Quantitative Analytics- Managing Habits- Customer Collaboration- Funnel Focus- Managing Product.	**9**
EXPLORING AND AMPLIFYING PRODUCTS Introduction to Exploring a new Product Idea- Building for learning- Horizons of growth- Corporate Innovation Pipeline- Business Model Design- Introduction to Amplifying an existing products-Business model types- Actionable analytics- Data science- Chanel - Modality- Roadmap.	**9**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**0**	**Project Hours:**	**0**	**Total Hours:**	**45**

Learning Resources

Reference books/ Web Links

1. Competitive Strategy: Techniques for Analyzing Industries and Competitors, Michael E. Porter
2. User Experience Is Brand Experience: The Psychology Behind Successful Digital Products and Services by Felix Van De Sand, Anna-Katharina Frison, Pamela Zotz
3. Corporate Strategy and Product Innovation by Robert R. Rothberg

Online Resources

1. https://www.coursera.org/learn/corporatestrategy
2. https://www.coursera.org/learn/uva-darden-digital-product-management

Assessment	
Formative	Continuous
Assignments/ Presentations, Quiz	CAT- I, CAT – II and End Semester Examination

Course Curated By

Expert(s) from Industry	**Expert(s) from Higher Education Institutions**	**Internal Expert(s)**
		Ms. Mayuri P T, MBA-IEV

<table>
<tr><td><b>24IEO078</b></td><td rowspan="2"><b>Gamification and Gaming</b></td><td><b>L</b></td><td><b>T</b></td><td><b>P</b></td><td><b>J</b></td><td><b>C</b></td></tr>
<tr><td rowspan="2"><b>OE</b></td><td><b>3</b></td><td><b>0</b></td><td><b>0</b></td><td><b>0</b></td><td><b>3</b></td></tr>
<tr><td></td><td><b>SDG</b></td><td colspan="4"><b>3, 4, 9</b></td></tr>
</table>

Pre-requisite: Nil

	Faculty Name:	**Dr. K. Saranya**
	Designation:	**Assistant Professor-II**
	Concern/industry/Institution:	**Kumaraguru college of Technology**
	LinkedIn profile	**https://www.linkedin.com/in/dr-saranya-k-b3a93313a/**

Course Objectives:	**The purpose of taking this course is to:**
1	Understand the core differences between Gamification and Games.
2	Explore how gamification drives innovation in business.
3	Analyse the effectiveness of gamification in Advocacy, Media, Politics, and Education.
4	Identify the risks and future trends in gamification.

Course Outcomes:	**After successful completion of this course, the students shall be able to**	**Revised Bloom's Taxonomy Level (RBT)**
CO 1	Acquire in-depth knowledge of gamification principles and identify specific applications across various contexts.	U
CO 2	Develop a comprehensive conceptual framework for gamification tailored to different sectors.	C
CO 3	Critically analyse and evaluate the benefits and risks associated with gamification.	E
CO 4	Analyse the role of motivation in gamification and how it drives innovation in the game market.	An

MODULE	**Hours**
GAMIFICATION Core concepts, distinctions between gamification and games, Motivation in Gamification, Gamification drive Innovation, Game Market.	**9**
GAMIFICATION IN BUSINESS Business sector adopts gamification techniques -Case studies, features of gamification in business, marketing strategies.	**8**
GAMIFICATION FOR ADVOCACY AND MEDIA Applications in civil society, differences from business gamification, effectiveness in raising awareness, media outlets adopt gamification techniques, features of gamification in media, journalism and communication benefiting from gamification.	**10**
GAMIFICATION IN POLITICS AND EDUCATION Political gamification, effectiveness for political campaigns, differences from other sectors, gamification effective for policymaking. Educational applications, effectiveness in teaching and learning.	**10**

RISKS AND FUTURE IN GAMIFICATION Gamification desirability, Social and mental sickness, features of gamification in social networks, need of gamers-Future with games.	**8**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**0**	**Project Hours:**	**0**	**Total Hours:**	**45**

Learning Resources

Reference books/ Web Links

1. Yu-Kai Chou,” Actionable Gamification: Beyond Points, Badges, and Leaderboards”, Fremont (CA), 2014.
2. B. Burke, “Gamify: How Gamification Motivates People to Do Extraordinary Things”, Bibliomotion, 2014.
3. J. Lerner, “Making Democracy Fun: How Game Design Can Empower Citizens and Transform Politics”, Boston (MA), 2014.

Online Resources

1. https://www.coursera.org/specializations/esports
2. https://www.coursera.org/learn/gamification

Assessment	
Formative	Continuous
Assignments / Mini project, Quiz, Case Studies	CAT-I,CAT-II and End Semester Examination

Course Curated By

Expert(s) from Industry	**Expert(s) from Higher Education Institutions**	**Internal Expert(s)**
		Dr. K. Saranya, CSE

24IEO079	Environmental Innovations and Management	L	T	P	J	C
		3	0	0	0	3
OE		SDG	6, 15			

Pre-requisite: Nil

	Faculty Name:	**Dr. N. Rajathi**
	Designation:	**Professor**
	Concern/industry/Institution:	**KCT**
	LinkedIn profile	**https://www.linkedin.com/in/dr-rajathi-natarajan-7748758b/**

Course Objectives:	The purpose of taking this course is to:
1	Explore urbanization, climate change, sustainability, and circular economy principles in managing environmental challenges.
2	Understand integrated water resource management and pollution control in relation to environmental hazards and public health.
3	Investigate population dynamics, agriculture's impact on the environment, and ethical approaches to solving complex environmental issues.

Course Outcomes:	After successful completion of this course, the students shall be able to	Revised Bloom's Taxonomy Level (RBT)
CO 1	Analyse and address the environmental challenges associated with global trends.	An
CO 2	Evaluate and apply integrated water resource management principles to address complex water-related challenges,	Ap
CO 3	Explain the impact of environmental hazards.	U
CO 4	Explain the relationship between global population dynamics, agriculture, and soil resources.	U
CO 5	Identify and apply environmental ethics and management principles to complex issues.	Ap

MODULE	Hours
GLOBAL TRENDS AND ENVIRONMENT MANAGEMENT Sustainability and the SDGs-Demographic Trends-Global urbanization-Environment Management -Cities and the rising sea level-Climate Change and Water-Circular Thinking in Waste Management-Plastic as Part of the Circular Economy-Stakeholder and Social Sustainability Analysis-–Utility Management -Environmental Management in Rural Areas-Phases in Solid Waste Management -Regulation -Outdoor and Indoor air pollution –Technologies for the environment built .	**9**
WATER RESOURCE MANAGEMENT AND POLICY The rules of resource, uses and their circumvention- Integrated water resource management to water-food-energy –Integrated Water shed management –water as source of conflict and cooperation.	**9**
ENVIRONMENTAL HAZARDS AND GLOBAL PUBLIC HEALTH	**9**

Air and water pollution –key concepts – controlling air pollution –key concepts in water pollution-controlling water pollution –physical hazards and soil waste - Solid Waste Disposal Methods-Hazardous Waste Disposal Methods-Population pressure –Build environment.	
POPULATION, FOOD, AND SOIL Population the world- population changes-Global population – Global population dynamics - Agriculture and Environment – Agriculture and Human Nutrition- Modern Agriculture Effects and Alternatives -Soil and Environment –Soil resource and Profile.	**9**
ENVIRONMENTAL MANAGEMENT & ETHICS Introduction – Environmental Ethics- Environmental management of tame and wicked problems-Decision support tools-Environmental regulation and principles.	**9**

Theory Hours:	**45**	**Tutorial Hours:**	**0**	**Practical Hours:**	**0**	**Project Hours:**	**0**	**Total Hours:**	**45**

Learning Resources

Reference books/ Web Links

1. Circular Economy for the Management of Operations. United States, CRC Press, (2020).
2. Pangare, Vasudha. Global Perspectives on Integrated Water Resources Management. India, Academic Foundation, (2006).
3. Hutchinson, Emma, and Kovats, Sari. Environment, Health and Sustainable Development. United Kingdom, McGraw-Hill Education, (2017).
4. Wild, Alan. Soils, Land and Food: Managing the Land during the Twenty-First Century. United Kingdom, Cambridge University Press, (2003).
5. Krishnamoorthy, Bala. Environmental Management: Text and Cases. India, Prentice Hall India Pvt., Limited, (2017).
6. Politics and Policies for Water Resources Management in India. United Kingdom, Taylor & Francis,(2020).

Online Resources

1. https://onlinecourses.nptel.ac.in/noc23_hs155/preview
2. https://www.coursera.org/learn/global-environmental-management
3. https://www.coursera.org/learn/water-management
4. https://www.coursera.org/learn/environmental-hazards-and-global-public-health
5. https://www.coursera.org/learn/population-food-and-soil
6. https://www.coursera.org/learn/environmental-management-ethics

Assessment

Formative	Continuous
Assignments, Case Study , Quiz	CAT-I,CAT-II and End Semester Examination

Course Curated By

Expert(s) from Industry	**Expert(s) from Higher Education Institutions**	**Internal Expert(s)**
		Dr. N. Rajathi, IT