



NANDHA ENGINEERING COLLEGE

(AUTONOMOUS)

(Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai)

ERODE – 638052 TAMIL NADU

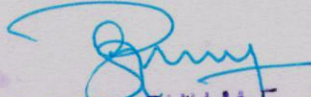
Email: principal@nandhaengg.org Mobile: 73737 12234

1.1.2 Details of Courses where syllabus revision was carried out

B.E.- CSE (CYBER SECURITY)

R-22 Curriculum

Course Code	Course Name	% of Change
22CCC14	Ethical Hacking	100%
22CCC15	Web Security	100%
22CCP09	Ethical Hacking Laboratory	100%
22CCP10	Web Security Laboratory	100%
22CCC16	Cyber Forensics	100%
22CCC17	Blockchain Technology	100%
22CCP11	Cyber Forensics Laboratory	100%
22CCX01	Cyber laws	100%
22CCX02	Social Network Security	100%
22CCX03	Biometric Security	100%
22CCX04	Cloud Security	100%
22CCX05	E-commerce Security	100%
22CCX06	Data Privacy and Protection	100%
22CCX07	Cyber Physical System	100%
22CCX08	Intrusion Detection System	100%
22CCX11	Mobile Device Security	100%
22CCX12	Malware Analysis	100%
22CCX13	Digital Forensics	100%
22CCX14	Data Analytics for Cyber Security	100%
22CCX15	Vulnerability Assessment and Penetration Testing	100%


Dr. S. PRABHU M.E., Ph.D.,
Associate Professor & Head



NANDHA ENGINEERING COLLEGE

(AUTONOMOUS)

(Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai)

ERODE – 638052 TAMIL NADU

Email: principal@nandhaengg.org Mobile: 73737 12234

Course Code	Course Name	% of Change
22CCX16	Information Security Management	100%
22CCX17	Cyber Security Governance, Risk and Compliance	100%
22CCX18	Hardware Security	100%
Average		100%

Dr.S.PRABHU M.E., Ph.D.,
Associate Professor & Head
Department of Computer Science and Engineering
(Cyber Security)
Nandha Engineering College (Autonomous)
Erode - 638 052.

SEMESTER: V									
S.No.	COURSE CODE	COURSE TITLE	CATEGORY	PRE-REQUISITE	CONTACT PERIODS	L	T	P	C
THEORY & EMBEDDED COURSES									
1	22CCC13	Automata Theory and Compiler Design	PCC	-	4	3	1	0	4
2	22CCC14	Ethical Hacking	PCC	22CCC05	3	3	0	0	3
3	22CCC15	Web Security	PCC	22CCC11, 22CCC12	3	3	0	0	3
4	E1	Elective (PEC)	PEC	-	3	3	0	0	3
5	E2	Elective (PEC)	PEC	-	3	3	0	0	3
6	E3	Elective (PEC / OEC)	PEC / OEC	-	3	3	0	0	3
PRACTICALS									
7	22CCP09	Ethical Hacking Laboratory	PCC	22CCP04	4	0	0	4	2
8	22CCP10	Web Security Laboratory	PCC	22CCP06, 22CCP08	4	0	0	4	2
MANDATORY NON-CREDIT COURSES									
9	22MAN08R	Soft/Analytical Skills – IV **	MC	-	3	1	0	2	0
TOTAL					30	19	1	10	23

** Ratified by Twelfth Academic Council

SEMESTER: VI									
S.No.	COURSE CODE	COURSE TITLE	CATEGORY	PRE-REQUISITE	CONTACT PERIODS	L	T	P	C
THEORY & EMBEDDED COURSES									
1	22CCCI16	Cyber Forensics	PCC	-	3	3	0	0	3
2	22CCCI17	BlockchainTechnology	PCC	-	3	3	0	0	3
3	E4	Elective (PEC)	PEC	-	3	3	0	0	3
4	E5	Elective (PEC)	PEC	-	3	3	0	0	3
5	E6	Elective (PEC / OEC)	PEC / OEC		3	3	0	0	3
6	E7	Elective (OEC)	OEC	-	3	3	0	0	3
PRACTICALS									
7	22CCPI1	Cyber Forensics Laboratory	PCC	-	4	0	0	4	2
TOTAL					22	18	0	4	20

(C) Programme Elective Courses (PEC)**Vertical 1: Web Application & Decentralized Cloud Security**

S.NO	COURSE CODE	COURSE TITLE	CATEGORY	PRE-REQUISITE	CONTACT PERIODS	L	T	P	C
1.	22CCX01	Cyber laws	PEC	-	3	3	0	0	3
2.	22CCX02	Social Network Security	PEC	-	3	3	0	0	3
3.	22CCX03	Biometric Security	PEC	-	3	3	0	0	3
4.	22CCX04	Cloud Security	PEC	-	3	3	0	0	3
5.	22CCX05	E-commerce Security	PEC	-	3	3	0	0	3
6.	22CCX06	Data Privacy and Protection	PEC	-	3	3	0	0	3
7.	22CCX07	Cyber Physical System	PEC	-	3	3	0	0	3
8.	22CCX08	Intrusion Detection System	PEC	-	3	3	0	0	3

Vertical 2: Digital Forensics & Infosec Auditing

S.NO	COURSE CODE	COURSE TITLE	CATEGORY	PRE-REQUISITE	CONTACT PERIODS	L	T	P	C
1.	22CCX11	Mobile Device Security	PEC	-	3	3	0	0	3
2.	22CCX12	Malware Analysis	PEC	-	3	3	0	0	3
3.	22CCX13	Digital Forensics	PEC	-	3	3	0	0	3
4.	22CCX14	Data Analytics for Cyber Security	PEC	-	3	3	0	0	3
5.	22CCX15	Vulnerability Assessment and Penetration Test	PEC	-	3	3	0	0	3
6.	22CCX16	Information Security Management	PEC	-	3	3	0	0	3
7.	22CCX17	Cyber Security Governance, Risk and Compliance	PEC	-	3	3	0	0	3
8.	22CCX18	Hardware Security	PEC	-	3	3	0	0	3

Vertical 3: Machine Intelligence

S.NO	COURSE CODE	COURSE TITLE	CATEGORY	PRE-REQUISITE	CONTACT PERIODS	L	T	P	C
1.	22CCX21	Knowledge Engineering	PEC	-	3	3	0	0	3
2.	22CCX22	Optimization Techniques	PEC	-	3	3	0	0	3
3.	22CCX23	Computer vision	PEC	-	3	3	0	0	3
4.	22CCX24	Pattern Recognition	PEC	-	3	3	0	0	3
5.	22CCX25	Big Data Analytics	PEC	-	3	3	0	0	3
6.	22CCX26	Health care Analytics	PEC	-	3	3	0	0	3
7.	22CCX27	Image and Video Analytics	PEC	-	3	3	0	0	3
8.	22CCX28	Business Intelligence	PEC	-	3	3	0	0	3

22CCCI4 – ETHICAL HACKING*(Common to 22CSX22, 22ITX22, 22CIX32)*

L	T	P	C
3	0	0	3

PRE-REQUISITE: Linux**Course Objective:**

- To provide a comprehensive understanding of computer-based vulnerabilities, including various kinds of malware and attacks, and to explore tools and techniques for foot printing, social engineering, port scanning, and ping sweeping. The course aims to equip students with practical skills in ethical hacking to identify and expose system vulnerabilities.

Course Outcomes

The student will be able to

Cognitive Level**Weightage of COs in End Semester Examination**

CO1	Analyze and gain knowledge on the basics of computer-based vulnerabilities	Ap	20%
CO2	Demonstrate and analyze the network and vulnerability attacks in system.	An	20%
CO3	Investigation about foot printing, reconnaissance and scanning methods using tools	Ap	20%
CO4	Analyze the basics of scanning methodologies and exploitation techniques using modern tools	An	20%
CO5	Perform in a team to identify the options for network protection and firewall protection in ethical hacking.	Ap	20%

UNIT I-INTRODUCTION

Ethical Hacking Overview - Role of Security and Penetration Testers - Penetration-Testing Methodologies- Laws of the Land - Overview of TCP/IP- The Application Layer - The Transport Layer- The Internet Layer - IP Address in

UNIT II-NETWORK AND COMPUTER ATTACKS

Network and Computer Attacks - Malware - Protecting Against Malware Attacks. - Intruder Attacks -Denial-of-Service Attacks- Distributed Denial-of-Service Attacks-- Buffer Overflow Attacks- Ping of Death Attacks - Session Hijacking-Addressing Physical Security- Keyloggers

UNIT III-FOOTPRINTING AND SOCIAL ENGINEERING

Web tools for Footprinting , Competitive Intelligence - Analyzing a Company's Web Site-Using Other Footprinting Tools-Using E- mail Addresses-Using HTTP Basics-Other Methods of Gathering Information-Using Domain Name System Zone Transfers .- Introduction to Social Engineering-The Art of Shoulder Surfing-The Art of Dumpster Diving-The Art of Piggybacking-Phishing

UNIT IV-PORT SCANNING

Introduction to Port Scanning- Types of Port Scans - Port-Scanning Tools – Nmap- Unicorns can — Nessus and OpenVAS-Ping Sweeps - Fping - Hping-Crafting IP Packets

UNITY-DESKTOPANDSERVEROSVULNERABILITIES**(9)**

Windows OS Vulnerabilities-Windows File Systems-Remote Procedure Call—NetBIOS-Server Message Block-Common Internet File System-Null Sessions-Web Services-SQL Server-Buffer Overflows-Passwords and Authentication-Tools for Identifying Vulnerabilities in Windows-Best Practices for Hardening Windows Systems

TOTAL(L:45):45PERIODS**TEXTBOOKS:**

1. Michael T. Simpson, Kent Backman, and James E. Corley, Hands-On Ethical Hacking and Network Defense, Course Technology, Delmar Cengage Learning, 2010.

REFERENCES:

1. Dr. John Smith, Dr. Emily Johnson, Dr. Mohammad Khan, A Survey of Ethical Hacking Techniques and Tools for Penetration Testing, 2020
2. The Basics of Hacking and Penetration Testing - Patrick Engebretson, SYNGRESS, Elsevier, 2013.

Mapping of Cos with Pos /PSOs

Cos	Pos												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	3	3											3	3
2		3		3									3	3
3				3	3								3	3
4		3			3								3	3
5		2						3	3				3	3
CO (W.A)	0. 6	2.2	0	2	2	0	0	0.6	0.6	0	0	0	3	3



22CCCI5 – WEB SECURITY

L	T	P	C
3	0	0	3

PREREQUISITE: NIL

Course Objective:

- This course focuses on wide spectrum of topics from legal and ethical issue, risk management, and implementation in the context of Web security.

Course Outcomes

The student will be able to

Cognitive Level

**Weight age of COs
In End Semester Examination**

CO1	Analyze the concept of web applicationits needs.	An	20%
CO2	Acquainted with the process for secure development and deployment of web applications	An	20%
CO3	Acquire the skill to design and develop Secure Web Applications that use Secure APIs	Ap	20%
CO4	Ability to get the importance of carrying out vulnerability assessment and penetration testing	An	20%
CO5	Apply knowledge of hacking to build a strong defense against hacking in ethicalway.	Ap	20%

UNITI – FUNDAMENTALS OF WEB APPLICATION SECURITY

(9)

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

UNITII–SECURE DEVELOPMENT AND DEPLOYMENT

(9)

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)

UNITIII–WEB SECURE API

(9)

API Security- Session Cookies, Token Based Authentication, Securing Natter APIs: Addressing threatswith Security Controls, Rate Limiting for Availability, Encryption, Audit logging, securing service-to- service APIs: API Keys, OAuth2, Securing Microservice APIs: Service Mesh, Locking Down NetworkConnections, Securing Incoming Requests.

UNITIV – VULNERABILITY ASSESSMENT AND PENETRATION TESTING	(9)
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.	
UNITY– HACKING TECHNIQUES AND TOOLS	(9)
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, Niko, Burp Suite, etc.	
TOTAL(L:45):45PERIODS	

TEXTBOOKS:

1. Andrew Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications, First Edition, 2020, O’Reilly Media, Inc.
2. Bryan Sullivan, Vincent Liu, Web Application Security: A Beginners Guide, 2012, The McGraw-Hill Companies.
3. Neil Madden, API Security in Action, 2020, Manning Publications Co., NY, USA.

REFERENCES:

1. Michael Cross, Developer’s Guide to Web Application Security, 2007, Syngress Publishing, Inc.
2. Ravi Das and Greg Johnson, Testing and Securing Web Applications, 2021, Taylor & Francis Group, LLC.
3. Prabath Siriwardena, Advanced API Security, 2020, Apress Media LLC, USA.
4. Malcolm McDonald, Web Security for Developers, 2020, No Starch Press, Inc.

Mapping of Cos with Pos / PSOs														
COs	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1														3
2					3									
3		3	3		3							3		
4	3	3	3											
5														3
CO (W.A)	3	3	3		3							3		3

22CCP09 – ETHICAL HACKING LABORATORY

L	T	P	C
0	0	4	2

PREREQUISITE: Linux

Course Objective:

- Understand the fundamental concepts and principles of ethical hacking, develop practical skills in identifying system vulnerabilities, and learn methodologies and tools used by ethical hackers. Gain hands-on experience in penetration testing, vulnerability assessment, and explore the legal and ethical considerations of ethical hacking practices.

Course Outcomes

The student will be able to

Cognitive Level

	Course Outcomes	Cognitive Level
CO1	Demonstrate proficiency in using various ethical hacking tools and techniques to identify and exploit vulnerabilities.	Ap
CO2	Apply ethical hacking methodologies to assess the security posture of computer systems and networks.	Ap
CO3	Analyze and interpret the results of ethical hacking tests to prioritize and remediate security risks.	An
CO4	Develop strategies to enhance the security of information systems based on ethical hacking findings.	An
CO5	Evaluate the legal and ethical implications of ethical hacking practices and adhere to professional standards and guidelines.	Ap

LIST OF EXPERIMENTS:

1. Linux Commands (Basic & Advanced)
2. Information Gathering
3. Vulnerability Analysis
4. Web Application Analysis
5. Database Assessment
6. Password Attacks
7. Wireless Attacks
8. Reverse Engineering
9. Exploitation tools
10. Sniffing & Spoofing

TOTAL (P:60) = 60 PERIODS

Mapping of Cos with Pos / PSOs

COs	Pos												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1		3			3								3	3
2	3												3	3
3		3											3	3
4			3										3	3
5		3		3				3					3	3
CO (W.A)	0.6	1.8	0.6	0.6	0.6	0	0	0.6	0	0	0	0	3	3

22CCPI0 – WEB SECURITY LABORATORY

L	T	P	C
0	0	4	2

PREREQUISITE:

Course Objective:

- To focus on hands-on, practical experience in understanding and implementing web security practices

Course Outcomes

The student will be able to

Cognitive Level

CO1	Apply the concept of web applications and analyses its needs.	Ap
CO2	Analyses the process for secure development and deployment of web applications	An
CO3	Acquire the skill to design and develop Secure Web Applications that use Secure APIs	Ap
CO4	Ability to get the importance of carrying out vulnerability assessment and penetration testing	An
CO5	Acquire the skill to think like a hacker and to use hackers tool sets	C

List of Exercises

(9)

1. Install Wireshark and explore the various protocols
 - a. Analyses the difference between HTTP vs HTTPS
 - b. Analyses the various security mechanisms embedded with different protocols.
2. Identify the vulnerabilities using OWASP ZAP tool
3. Create simple REST API using python for following operation
 - a. GET
 - b. PUSH
 - c. POST
 - d. DELETE
4. Install Burp Suite to do following vulnerabilities:
 - a. SQL injection
 - b. Cross-site scripting (XSS)
5. Attack the web site using Social Engineering method.
6. Study of different types of vulnerabilities for hacking a websites / Web Applications.
7. Study of the features of firewall in providing network security and to set Firewall Security in windows.
8. Analysis the Security Vulnerabilities of E-commerce services.
9. Analysis the security vulnerabilities of E-Mail Application
10. Case -Study

TOTAL:60PERIODS

Mapping of Cos with POs/PSOs														
COs	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	3												3	
2	3	3											3	
3		3	3											3
4				3									3	
5							3							
CO (W.A)	3	3	3				3						3	3

22CCCI6 - CYBER FORENSICS (Common to 22CIX33)					
		L	T	P	C
		3	0	0	3
PREREQUISITE: NIL					
Course Objective:	<ul style="list-style-type: none"> Aware of fundamentals on cyber forensics and usage of cyber forensics tools and enhance the knowledge on database, email and threats in crypto currency. systems. 				
Course Outcomes The Student will be able to		Cognitive Level	Weightage of COsin End Semester Examination		
CO1	Explain the basic of Forensics investigation process.	Ap	20%		
CO2	Explain Linux forensics and file systems and the challenges various devices.	An	20%		
CO3	Develop expertise network forensics, mastering techniques to investigate and analyze network activitiesfor identifying security breaches and Threats effectively.	Ap	20%		
CO4	Explain forensic investigations in cloud environments,focusing on data retrieval, analysis.	Ap	20%		
CO5	Analyze the specialized skills in Bit coin forensics, Enabling the mtotrace transactions, investigate illicit activities.	An	20%		

UNIT I - INTRODUCTION TO COMPUTER FORENSICS	(9)
Introduction to Cyber forensics: Forensics investigation process –Forensics protocol– Digital forensics standards–Digital evidence – Types of cybercrime – Notable data breaches– Case study- Challenges in Cyber security – Cyberforensics tools. WWindows forensics: Digital Evidence – File systems – Time analysis—Challenges-Case Study.	
UNIT II – LINUX FORENSICS AND FILE SYSTEM	(9)
Linux forensics: Popular Linux— File systems —Process —Artifacts —Linux distribution used for forensics analysis –Challenges –Case study. Mac OS forensics: File systems– Process – Artifacts – Information to collect Macbook forensics investigation – Case study. Anti-forensics: Data wiping and shredding – Trial obfuscation–Encryption– Datahiding–Anti-forensicsdetectiontechnique	
UNIT III – NETWORK FORENSICS	(9)
Network forensics: OSI Model – Artifacts – ICPM Attack – Analysis tools. Mobile forensics: Android operating system – Mutual Extraction – Physical acquisition – Chip – off – Micro – read – Challenges – iOS operating system.	
UNIT IV – CLOUD FORENSICS DATA	(9)
loud forensics: Cloud computing model – Server – side forensics – Client – side forensics – Challenges –Artifacts – use – Forensics as a Service. Malware forensics: Types – Analysis –Tools – Challenges –Malware as a Service. Web attack forensics: Web attack test – Intrusion forensics – Database forensics – Log Forensics – Content analysis – File metadata forensics	

UNIT V - BITCOIN FORENSICS	(9)
Email sand email criminals: Protocols – Email criminals – Email forensics. Solid State device forensics: Components – Data wiping – Analysis. Bit coin forensics: Crypto currency – Block chain – Artifacts – Challenges.	
TOTAL (L:45) = 45 PERIODS	

TEXT BOOKS:

1. Niranjan Reddy , Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations, Apress, First Edition, 2019
2. CEH official Certified Ethical Hacking Review Guide, Wiley India Edition, 2015.

REFERENCES:

1. John Vacca, — Computer Forensics, Cengage Learning, 2005
2. Marjie Tabriz, — Computer Forensics and Cyber Crime: An Introduction, 3rd Edition, Prentice Hall, 2013.
3. Ankit Fadia — Ethical Hacking, Second Edition, Mac millan India Ltd, 2006
4. Kenneth C. Brancik— Insider Computer Fraud, Auerbach Publications Taylor & Francis Group — 2008.

Mapping of COs with POs / PSOs														
COs	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1								3					3	3
2	3										3		3	3
3											3		3	3
4			3								3		3	3
5			3								3	3	3	3
CO (W.A)	3		3					3			3	3	3	3

22CCC17 - BLOCKCHAIN AND TECHNOLOGY					
		L	T	P	C
		3	0	0	3
PREREQUISITE: NIL					
Course Objective:		<ul style="list-style-type: none"> To provide students with a comprehensive understanding of blockchain technology, its underlying principles, and its practical applications 			
Course Outcomes The student will be able to		Cognitive Level	Weightage of COs in End Semester Examination		
CO1	Analyze how blockchain technology might impact various sectors, including finance, healthcare, and governance.	An	20%		
CO2	Create and manage cryptocurrency wallets, execute trades, and interact with blockchain-based applications.	C	20%		
CO3	Evaluate various scalability solutions and enhancements, such as the Lightning Network and Segregated Witness (SegWit), and their impact on Bitcoin's performance and usability.	E	20%		
CO4	Develop, deploy, and manage chain code (smart contracts) on the Hyperledger Fabric platform using Go or JavaScript.	C	20%		
CO5	Analyze various use cases of blockchain technology in industries such as finance (e.g., cryptocurrencies, decentralized finance), supply chain (e.g., traceability, logistics), healthcare (e.g., patient records, clinical trials), and more.	An	20%		

UNIT I - INTRODUCTION TO BLOCKCHAIN	(9)
Blockchain- Public Ledgers, Blockchain as Public Ledgers - Block in a Blockchain, Transactions The Chain and the Longest Chain - Permissioned Model of Blockchain, Cryptographic -Hash Function, Properties of a hash function-Hash pointer and Merkle tree	
UNIT II - BITCOIN AND CRYPTOCURRENCY	(9)
A basic crypto currency, Creation of coins, Payments and double spending, FORK – the precursor for Bitcoin scripting, Bitcoin Scripts, Bitcoin P2P Network, Transaction in Bitcoin Network, Block Mining, Block propagation and block relay	
UNIT III - BITCOIN CONSENSUS	(9)
Bitcoin Consensus, Proof of Work (PoW)- Hashcash PoW , Bitcoin PoW, Attacks on PoW ,monopoly problem- Proof of Stake- Proof of Burn - Proof of Elapsed Time - Bitcoin Miner, Mining Difficulty, Mining Pool-Permissioned model and use cases.	
UNIT IV - HYPERLEDGER FABRIC & ETHEREUM	(9)

Architecture of Hyperledger fabric v1.1- chain code- Ethereum: Ethereum network, EVM, Transaction fee,Mist Browser, Ether, Gas, Solidity.

UNIT V - BLOCKCHAIN APPLICATIONS

(9)

Smart contracts, Truffle Design and issue- DApps- NFT. Blockchain Applications in Supply Chain Management, Logistics, Smart Cities, Finance and Banking, Insurance,etc- Case Study.

TOTAL (L:45) : 45 PERIODS

TEXT BOOKS:

1. Bashir and Imran, Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular Blockchain frameworks, 2017.
2. Andreas Antonopoulos, "Mastering Bitcoin: Unlocking Digital Cryptocurrencies", O'Reilly, 2014

REFERENCES:

1. Daniel Drescher, "Blockchain Basics", First Edition, Apress, 2017.
2. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press, 2016.
5. Melanie Swan, "Blockchain: Blueprint for a New Economy", O'Reilly, 2015

Mapping of COs with POs / PSOs

COs	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1		3			3									
2				3									3	
3		3												3
4	3		3	3									3	
5		3												
CO (W.A)	3	3	3	3	3								3	3.

22CCPI I - CYBER FORENSICS LABORATORY

	L	T	P	C
	3	0	0	3

PREREQUISITE:

Course Objective:	<ul style="list-style-type: none"> To equip students with the critical skills and knowledge needed to excel in the field of cyber forensics, preparing them for careers in law enforcement, corporate security, and digital investigations.
--------------------------	--

Course Outcomes The student will be able to		Cognitive Level
CO1	Apply important variety of forensic tools for effective digital investigations.	Ap
CO2	Analyze the data and determine the number of successfully recover deleted files in digital investigation.	An
CO3	Design of forensics images of hard drives and restoring evidence images using EnCase Forensics.	Ap
CO4	Demonstrate knowledge about the enhancing their forensic investigations skills.	An
CO5	Identify the last connected USB devices and conducting live forensic investigations with autopsy advancing their USB forensics and real-time analysis skills.	C

LIST OF EXPERIMENTS:

1. Study of Computer Forensics and different tools used for forensic investigation
2. How to Recover Deleted Files using Forensics Tools
3. Study the steps for hiding and extract any text file behind an image file/ Audio file using Command Prompt
4. How to Extract Exchangeable image file format (EXIF) Data from Image Files using Exifreader Software
5. How to make the forensic image of the hard drive using EnCase Forensics
6. How to Restoring the Evidence Image using EnCase Forensics
7. How to Extracting Browser Artifacts
8. How to view Last Activity of your PC.
9. Find Last Connected USB on your system (USB Forensics)
10. Live Forensics Case Investigation using Autopsy

TOTAL (P:60) = 60 PERIODS

Mapping of COs with POs / PSOs

COs	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	3												3	
2	3	3											3	
3		3	3											3
4				3									3	
5							3							
CO (W.A)	3	3	3	3			3						3	3

22CCX01 – CYBER LAWS						
			L	T	P	C
			3	0	0	3
PREREQUISITE: NIL						
Course Objective:		<ul style="list-style-type: none"> To equip students with a thorough understanding of the legal and regulatory landscape related to cyberspace and digital activities 				
Course Outcomes		Cognitive Level	Weightage of COs in End Semester Examination			
The Student will be able to						
CO1	Analyze potential new legal issues and the need for evolving legal frameworks to address technological advancements.	An	20%			
CO2	Analyze the rights of individuals regarding their personal data, such as the right to access, correction, and erasure of information.	An	20%			
CO3	Analyze the rights of individuals regarding their digital information and the obligations of organizations to safeguard data privacy.	An	20%			
CO4	Apply forensic methods to detect and investigate network intrusions, data exfiltration, and other cloud-based incidents.	Ap	20%			
CO5	Apply critical thinking to analyze and solve problems related to cybercrime, including developing investigative strategies and response plans.	Ap	20%			

UNIT I – INTRODUCTION	(9)
Introduction - Credit Card Frauds in Mobile and Wireless Computing Era - Security Challenges in Mobile and Computer- Security Challenges Posed by Mobile Devices - Registry Setting for Mobile Devices – Authentication Service Security - Attacks on Mobile / Cell Phones–Mobile Devices: Security Implications for Organizations– Organizational Measures for Handling Mobiles Devices – Related Security Issues – Organizational Security Policies and Measures in Mobile Computing Era – Laptop.	
UNIT II – INFORMATION ACT	(9)
Phishing –Identity Theft (ID Theft)- Password Cracking –Keyloggers and spywares - Virus and Worms - Trojan Horses and Backdoors - Steganography - DoS and DDoS Attacks –SQL Injection – Buffer Overflow – Attacks on Wireless Networks.	
UNIT III – CYBER ACT	(9)
Cybercrimes and the Legal Landscape around the world – Why Do We Need Cyberlaws - The Indian IT Act – Challenges to Indian Law and Cybercrime Scenario in India –Consequences of Not Addressing the Weakness in Information Technology Act - Digital Signatures and The Indian IT Act- Amendments to the Indian IT Act – Cybercrime and Punishment - Cyberlaws, Technology and Students: Indian Scenario – Intellectual Property in the Cyberspace.	

UNIT IV – CYBER FORENSICS	(9)
Historical Background of Cyber forensics – Cyber forensics and Digital Evidence – Forensics Analysis of E-Mail – Networks Forensics – Approaching a Computer Forensics Investigation – Computer Forensics and Steganography – OSI 7 Layer Model to Computer Forensics – Computer Forensics from Compliance Perspective – Challenges in Computer Forensics – Special Tools and Techniques – Forensics Auditing	
UNIT V– CYBER CRIME	
Introduction - Definition and Origins of the Word - Cybercrime and Information security - Classifications of Cybercrimes - The Legal Perspectives - An India Perspectives - Cybercrime and the Indian ITA 2000 - A Global Perspective on Cybercrimes – Cybercrime Era – Criminals Plan the Attacks – Social Engineering – Cyberstalking – Cyberstalking – cybercafe and Cybercrime – The Fuel for Cybercrime – CloudComputing.	

TEXT BOOKS:
I. Sunit Belapure and Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India Pvt. Ltd, 2011.
REFERENCES:
<ol style="list-style-type: none"> 1. Verma S, K, Mittal Raman, Legal Dimensions of Cyber Space, Indian Law Institute, New Delhi, (2004) 2. S. R. Bhansali, Information Technology Act, 2000, University Book House Pvt. Ltd., Jaipur (2003). 3. Blockchain, Blueprint for a new Economy, Melanie Swan, 2017 – O'Reilly 4. Sudhir Naib, The Information Technology Act, 2005: A Handbook, OUP, New York, (2011) 5. Upadhyaya and A. Upadhyaya, Material Science and Engineering, Anshan Publications, 2007

Mapping of COs with POs / PSOs														
Cos	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	-	3	-	3	-	-	-	3	-	-	-	-	-	3
2	-	-	-	-	-	-	-	3	-	-	-	-	-	-
3	-	-	-	-	-	-	-	3	-	-	-	-	-	-
4	3	-	-	-	-	-	--	3	-	-	-	-	-	3
5	-	-	-	3	-	-	3	3	-	-	-	-	-	3
CO (W.A)	3	3	-	3	-	-	3	3	-	-	-	-	-	3

22CCX02 - SOCIAL NETWORK SECURITY						
(Common to 22CSX25,22ITX25, 22AIX21, 22CIX34)						
			L	T	P	C
			3	0	0	3
PREREQUISITE: NIL						
Course Objective:		<ul style="list-style-type: none"> To focuses on understanding and addressing security issues related to social networking platforms, including protecting user privacy, preventing cyber threats, and managing data security. 				
Course Outcomes The student will be able to		Cognitive Level	Weightage of COs in End Semester Examination			
CO1	Apply network analysis and explore its applications.	Ap	20%			
CO2	Comprehend the role of ontologies in the Semantic Web, ontology-based knowledge representation,	An	20%			
CO3	Develop skills to extract the evolution of web communities	C	20%			
CO4	Predict human behavior in social communities through reality mining	An	20%			
CO5	Visualizing social network on various technologies	An	20%			

UNIT I - INTRODUCTION	(9)
Introduction to Semantic Web: Limitations of current Web - Development of Semantic Web – Emergence of the Social Web - Social Network analysis: Development of Social Network Analysis - Key concepts and measures in network analysis - Electronic sources for network analysis: Electronic discussion networks, Blogs and online communities - Web-based networks - Applications of Social Network Analysis.	
UNIT II - MODELLING, AGGREGATING AND KNOWLEDGE REPRESENTATION	(9)
Ontology and their role in the Semantic Web: Ontology-based knowledge Representation – Ontology languages for the Semantic Web: Resource Description Framework - Web Ontology Language - Modelling and aggregating social network data: State-of-the-art in network data representation - Ontological representation of social individuals - Ontological representation of social relationships - Aggregating and reasoning with social network data - Advanced representations.	
UNIT III - EXTRACTION AND MINING COMMUNITIES IN WEB SOCIAL NETWORKS	(9)
Extracting evolution of Web Community from a Series of Web Archive - Detecting communities in social networks - Definition of community - Evaluating communities - Methods for community detection and mining - Applications of community mining algorithms - Tools for detecting community's social network infrastructures and communities - Decentralized online social networks - multi-relational characterization of dynamic social network communities.	

UNIT IV - PREDICTING HUMAN BEHAVIOUR AND PRIVACY ISSUES

Understanding and predicting human behaviour for social communities - User data management – Inference and Distribution – Enabling new human experiences-Reality Mining-Context- Awareness - Privacy in online social networks - Trust in online environment - Trust models based on subjective logic - Trust network analysis - Trust transitivity analysis - Combining trust and reputation - Trust derivation based on trust comparisons - Attack spectrum and countermeasures.

UNIT - V VISUALIZATION AND APPLICATIONS OF SOCIAL NETWORKS (9)

Graph theory - Centrality - Clustering - Node-Edge Diagrams - Matrix representation – Visualizing online social networks, Visualizing social networks with matrix-based representations - Matrix and Node-Link Diagrams - Hybrid representations - Applications - Cover Networks-Community welfare - Collaboration networks - Co- Citation networks.

TOTAL(L:45):45PERIODS**TEXTBOOKS:**

1. Peter Mika, —Social Networks and the Semantic Web, First Edition, Springer 2007.
2. Borko Furht, —Handbook of Social Network Technologies and Applications, 1st Edition, Springer, 2010.

REFERENCES:

1. Guandong Xu, Yanchun Zhang and Lin Li, —Web Mining and Social Networking –Techniques and applications, First Edition, Springer, 2011.
2. Dion Goh and Schubert Foo, —Social information Retrieval Systems: Emerging Technologies and Applications for Searching the Web Effectively, IGI Global Snippet, 2008.
3. Max Chevalier, Christine Julien and Chantal Soulé-Dupuy, —Collaborative and Social Information Retrieval and Access: Techniques for Improved user Modelling, IGI Global Snippet, 2009.

Mapping of Cos with POs/PSOs

Cos	Pos												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1		3	3										3	3
2		3	3			3							3	3
3				3									3	3
4		3					3						3	3
5		3		3									3	3
CO (W.A)	0	3	3	3	0	3	3	0	0	0	0	0	3	3

22CCX03- BIOMETRIC SECURITY (Common to 22CSX28,22ITX28, 22AIX22, 22CIX35)				
	L	T	P	C
	3	0	0	3
PREREQUISITE: NIL				
Course Objective:	<ul style="list-style-type: none"> To provide students with a comprehensive understanding of biometric security systems, covering their design, implementation, evaluation, and applications in various security contexts. 			
Course Outcomes The Student will be able to		Cognitive Level	Weightage of COs in End Semester Examination	
CO1	Analyze the biometric systems, their functionalities, and the underlying principles and their practical Applications in real-world scenarios.	An	20%	
CO2	Apply the face recognition and face detection methods.	Ap	20%	
CO3	Evaluate encoding and matching algorithms used to extract distinctive features from there is for Verification purposes.	E	20%	
CO4	Illustrate the architecture and components involved in capturing data from multiple biometric sources.	An	20%	
CO5	Research types of attacks that can occur at the user interface level.	An	20%	

UNIT I - INTRODUCTION TO BIOMETRICS	(9)
Biometric functionalities – Biometric system errors – The design cycle of biometric systems – Applications of biometric systems – Security and privacy issues – Fingerprint recognition – Fingerprint acquisition – Feature extraction – Fingerprint indexing – Palmprint.	
UNIT II - FACE RECOGNITION	(9)
Introduction to face recognition – Image acquisition–Face detection–Feature extraction and matching.	
UNIT III – IRIS RECOGNITION	(9)
Introduction to iris recognition – Design of an iris recognition system – Iris segmentation – Iris normalization - Iris encoding and matching–Iris quality–Biometric traits–Hand geometry–Soft biometrics.	
UNIT IV - MULTI-BIOMETRICS	(9)
Multi-biometrics – Sources of multiple evidence – Acquisition and processing architecture – Fusion levels.	
UNIT V – SECURITY OF BIOMETRIC SYSTEMS	(9)
Adversary attack – Attacks at the user interface – Attacks on the biometric processing – Attacks on the template database.	
TOTAL:45PERIOD	

TEXTBOOKS:

1. Anil K Jain, Arun A Ross and Karthik Nandakumar, Introduction to Biometrics, Springer, First Edition, 2011.
2. Rachid Guerraoui and Franck Petit, Stabilization, Safety, and Security of Distributed Systems, Springer, FirstEdition,2010.

REFERENCES:

1. Marcus Smith, Monique Mann and Gregor Urbas, Biometrics, Crime and Security, Taylor and Francis, FirstEdition, 2018.
2. Ravindra Das, The Science of Biometrics SecurityTechnologyfor Identity Verification, Taylor andFrancis, FirstEdition, 2018.

Mapping of Cos with POs/PSOs

Cos	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	3	3	3	3	3	-	-	-	-	-	-	-	3	
2	3	-	-	3	3	-	-	-	-	-	-	-	3	2
3	3	-	-	3	3	-	-	-	-	-	-	-	-	-
4	3	3	3	3	3	-	-	-	-	-	-	-	-	-
5	3	3	-	3	3	3	-	-	-	-	-	-	3	-
CO (W.A)	3	1.8	1.2	3	3	0.6	-	-	-	-	-	-	1.8	0.4

22CCX04 - CLOUD SECURITY
(Common to 22CSX23,22ITX23, 22AIX23)

L	T	P	C
3	0	0	3

PREREQUISITE: NIL

Course Objective:

- To introduce the fundamental concepts and architecture of cloud computing.
- To understand and address security concerns, risks, and legal aspects.
- To explore data security strategies and best practices for securing data in the cloud
- To evaluate security criteria for building and managing private clouds and selecting external cloud service providers.
- To assess and evaluate cloud security through comprehensive frameworks

Course Outcomes The student will be able to		Cognitive Level	Weightage of COs in End Semester Examination
CO1	Analyze various the concepts of cloud computing, policy and compliance in cloud environment.	An	20%
CO2	Develop and implement secure cloud architectures, security patterns, and strategies for secure cloud operations.	Ap	20%
CO3	Apply key strategies and best practices for managing cloud data security risks and monitoring security controls	Ap	20%
CO4	Apply the fundamental concepts in infrastructure security facilities in cloud computing.	Ap	20%
CO5	Implement security operations activities and architectures for efficient and secure cloud management	Ap	20%

UNIT I - INTRODUCTION	(9)
Introduction to Cloud computing and security: Understanding cloud computing – The IT foundation for Cloud. An historical view: Roots of Cloud computing – A brief primer on architecture. Security architecture: Cloud computing architecture – Cloud reference architecture – Control over security in the cloud model – Making sense of cloud deployment – Making sense of services models – Real- world cloud usage scenarios.	
UNIT II - SECURING THE CLOUD	(9)
Security concerns – Risk issues and legal aspects – Security concerns –Assessing risk tolerance in Cloud Computing–Legal and regulatory issues–Securing the Cloud: Architecture–Security patterns and architectural element – Cloud security architecture –Planning key strategies for secure operation.	
UNIT III - CLOUD DATA SECURITY	(9)
Securing the cloud: Data security – Overview of data security in Cloud Computing. Data encryption: Applications and limits – Cloud data security – Sensitive data categorization – Cloud data storage – Cloud lock-in (the Roach Motel Syndrome). Securing the cloud: Key strategies and Best practices–Overall strategy– Effectively managing risk –Overview of security controls –The limits of security controls – Best practices – Security monitoring.	

UNIT IV - SECURITY CRITERIA	(9)
Security criteria: Building an internal cloud – Private clouds – Motivation and overview – Security criteria for ensuring a private cloud – Security criteria – Selecting an external cloud provider – Selecting a CSP – Overview of assurance – Selecting a CSP – Overview of risks – Selecting a CSP	
UNIT V – EVALUATING CLOUD SECURITY	(9)
Security criteria – Evaluating cloud security – An information security framework – Evaluating cloud security – Checklists for evaluating cloud security – Metrics for the checklists – Operating a cloud – Architecture to efficient and secure operations – Security operations activities.	
TOTAL(L:45): 45 PERIODS	

TEXTBOOKS:
<ol style="list-style-type: none"> Raghuram Yeluri and Enrique Castro-Leon, Building the Infrastructure for Cloud Security: A Solutions View, A press, First Edition, 2014 Ronald L Krutz and Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley, First Edition, 2010
REFERENCES:
<ol style="list-style-type: none"> Chris Dotson, Practical Cloud Security A Guide for Secure Design and Deployment, O'Reilly Media, First Edition, 2019 Raymond Choo and Ryan Ko, The Cloud Security Ecosystem Technical, Legal, Business and Management Issues, Elsevier Science, First Edition, 2015

Mapping of Cos with POs/PSOs														
COs	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1		3											3	3
2			3										3	3
3	3			3			3						3	3
4	3												3	3
5				3		3							3	3
CO (W.A)	1.2	0.6	0.6	1.2	0	0.6	0.6	0	0	0	0	0	3	3

22CCX05 - E-COMMERCE SECURITY (Common to 22CSX27,22ITX27)					
		L	T	P	C
		3	0	0	3
PREREQUISITE: NIL					
Course Objective:		<ul style="list-style-type: none"> To focuses on understanding and implementing security measures to protect online transactions and digital business operations. 			
Course Outcomes The student will be able to		Cognitive Level	Weightage of COsin End Semester Examination		
CO1	Analysis the historical context, benefits, drawbacks, and societal implications.	An	20%		
CO2	Acquire knowledge of key e-commerce technologies such as symmetric and asymmetric encryption, SSL	Ap	20%		
CO3	Conduct investigation about the diverse security threats inherent in e - commerce	Ap	20%		
CO4	Design and develop - commerce security policies, including privacy protection, security infrastructure implementation	An	20%		
CO5	Gain insight into the various threats faced by e-business	An	20%		

UNIT I - INTRODUCTION	(9)
Introduction to e-Commerce -The Background of e-Commerce-Delimitation-Advantages and Disadvantages of e-Commerce-Advantages of e-Commerce-enetsto Consumers-Benetsto Society- e-Commerce Disadvantages	
UNIT II - E-COMMERCE TECHNOLOGIES	(9)
Symmetric Encryption – Asymmetric Encryption- Secure Socket Layer – Digital Signature- Electronic Certificates -Wise Cards-Electronic Money – Characteristics of e-Commerce Technologies	
UNIT III - SECURITY THREATS TO E-COMMERCE	(9)
Client Dangers-Communication Channel Perils-Server Risks-Security Necessities and Security Approach- Authentication--Privacy-Approval- Integrity	
UNIT IV - SECURITY POLICY	(9)
Privacy-Security Infrastructure-Solution for Trust-Four Trusting Convictions-Seven Basic Factors at Influence Trust -Secure Trading for Electronic Businesses Makes Trust-Solutions for Security -Testing E-Commerce Security	

UNIT V - E-BUSINESS THREATS AND SOLUTIONS	(9)
E-Business Threats- Authentication Attacks-Respect ability Attacks- Secrecy Attacks-Infection-Trojan Horse-Worms-e-Business Solutions	
TOTAL (L:45) = 45 PERIODS	

TEXTBOOKS:
1. Tavares, Joao Manuel R.S, Handbook of e-business security, LCCN 2018013131 ISBN 9781138571303,2019.
REFERENCES:
1. Mehdi Khosrowpour, E-commerce Security: Advice from Experts, Idea Group Inc(IGI),2004 2. Ronggang Zhang , Lijuan Fang , Xiaoping He , Chuan Wei, The Whole Process of E-commerce Security Management System, February 2023

Mapping of COs with POs / PSOs														
COs	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1		3											3	3
2	3												3	3
3				3									3	3
4			3										3	3
5						3							3	3
CO (W.A)	3	3	3			3							3	3

22CCX06 – DATA PRIVACY AND PROTECTION*(Common to 22CSX026,22ITX26, 22AIX24)*

L	T	P	C
3	0	0	3

PREREQUISITE: Nil**Course Objective:**

- To provide students with a comprehensive understanding of how to safeguard personal and sensitive data from unauthorized access, breaches, and misuse. .

Course Outcomes

The Student will be able to

Cognitive Level**Weightage of COs in End Semester Examination**

CO1	Apply knowledge on fundamental principles of Data privacy.	Ap	20%
CO2	To design and development of data preservation by using datamining.	An	20%
CO3	Ability to assess privacy risks associated with Privacy regulations.	Ap	20%
CO4	Analyses various approaches in data security by using tools.	An	20%
CO5	Apply security on storage and database.	Ap	20%

UNIT I – INTRODUCTION TO DATA PRIVACY**(9)**

Data Privacy and its Importance - Need for Sharing Data - Methods of Protecting Data - Importance of Balancing Data Privacy and Utility – Introduction to Anonymization Design Principles - Nature of Data in the Enterprise Static Data Anonymization on Multidimensional Data: Introduction - 36 Classification of Privacy Preserving Methods - Classification of Data in a Multidimensional Data Set - Group-Based Anonymization.

UNIT II – PRIVACY PRESERVING DATAMINING**(9)**

Introduction - Privacy Preserving Graph Data - Privacy Preserving Time Series Data - Privacy Preservation of Longitudinal Data - Privacy Preservation of Transaction Data - Static Data Anonymization: Threats to Anonymized Data-Threats to Data Structures-Threats by Anonymization Techniques.

UNIT III – PRIVACY REGULATIONS**(9)**

Introduction - UK Data Protection Act 1998. - Federal Act of Data Protection of Switzerland 1992 - Payment Card Industry Data Security Standard (PCI DSS) - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) : Effects of Protection - Anonymization Considerations - Anonymization Design for HIPAA - Explicit Identifiers - Quasi-Identifiers - Sensitive Data. – Anonymization Design Checklist.

UNIT IV – DATA SECURITY**(9)**

Securing Unstructured Data : Structured Data vs. Unstructured Data – At Rest ,in Transit and in Use - Approaches to secure Unstructured Data – Newer Approaches to Secure Unstructured Data. Information Rights Management : Overview – IRM Technology Details – Getting Started with IRM. Encryption: History of Encryption – Symmetric Key Cryptography – Public Key Cryptography.

UNITY-CONTEMPORARYISSUES**(9)**

Storage Security: Evolution – Modern Storage Security – Risk Remediation – Best Practices. Database Security: General Concepts – Database Security Layers – Database-Level Security – Database Backup and Recovery – Database Auditing and Monitoring.

TOTAL(L:45):45PERIODS**TEXTBOOKS:**

1. Venkataraman, Nataraj, and Ashwin Shiram. Data Privacy: Principles and Practice. CRC Press, 2017

REFERENCES:

1. Rhodes-Ousley, Mark. Information Security: The Complete Reference, Second Edition, And Information Security Management: Concepts and Practice. New York, McGraw-Hill, 2013.
2. David Salomon, Data Privacy and Security, Springer, 2003
3. Andrew Vladimirov Michajlows ki, Konstantin, Andrew A. Vladimirov, and Konstantin V. Gavrilenko. Assessing Information Security: Strategies, Tactics, Logic and Framework. IT Governance Ltd, 2010.

Mapping of Cos with Pos / PSOs

Cos	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	3	-	-	-	-	-	-	-	-	-	-	-	-	-
2	-	3	-	-	-	-	-	-	-	-	-	-	-	-
3	-	3	-	3	-	-	-	-	-	-	-	-	3	2
4	-	3	-	-	3	-	-	-	-	-	-	-	-	-
5	3	-	3	-	-	-	-	-	-	-	-	-	3	2
CO (W.A)	1.2	1.8	0.6	0.6	0.6	-	-	-	-	-	-	-	1.2	0.8

22CCX07 - CYBER PHYSICAL SYSTEMS				
<i>(Common to 22AIX25, 22CIX36)</i>				
		L	T	P
		3	0	0
PREREQUISITE: Nil				
Course Objective:	<ul style="list-style-type: none"> To focus on the integration of computer-based algorithms with physical processes, aiming to teach students about the design, analysis, and implementation of systems where physical and cyber components interact. 			
Course Outcomes The Student will be able to		Cognitive Level	Weightage of COs in End Semester Examination	
CO1	Gain a foundational understanding of CPS, including demarcating specific systems,	An	20%	
CO2	Able to analysis information and its symbolic realities	Ap	20%	
CO3	Design and development of various decision-making techniques applicable to cyber-physical Systems	E	20%	
CO4	Develop skills in employing data networks and wireless communications within the framework of CPS, and grasp the practical applications of artificial intelligence and machine learning.	An	20%	
CO5	Gain insight into upcoming technologies and their potential applications across different sectors along with ethics.	An	20%	

UNIT I - INTRODUCTION TO CYBER PHYSICAL SYSTEMS	(9)
Introduction to Cyber -Physical Systems - Need for a General Theory - Systems Engineering - Demarcation of Specific Systems - Classification of Systems - Maxwell's Demon as a System - Games and Uncertainty - Uncertainty and Probability Theory - Random Variables: Dependence and Stochastic Processes	
UNIT II - INFORMATION AND NETWORK	(9)
Data and Information - Information and Its Different Forms - Physical and Symbolic Realities - Network Types -Processes on Networks and Applications - Limitations	
UNIT III - DECISIONS AND ACTIONS	(9)
Forms of Decision Making – Optimization - Game Theory - Rule-Based Decisions - The Three Layers of Cyber-Physical Systems - Physical Layer, Measuring, and Sensing Processes - Data Layer and Informing Processes - Decision Layer and Acting Processes - Layer Based Protocols and Cyber-Physical Systems Design	
UNIT IV - DYNAMICS OF CYBER-PHYSICAL SYSTEMS	(9)
Introduction to Dynamics of Cyber-Physical Systems - Failures and Layer-Based Attacks - Enabling Information and Communication Technologies - Data Networks and Wireless Communications - Artificial Intelligence and Machine Learning - Decentralized Computing and Distributed Ledger Technology	

UNIT V - APPLICATIONS	(9)
Future Technologies: A Look at the Unknown Future - Cyber-Physical Industrial System - Cyber-Physical EnergySystem - Governance Models - Social Implications of the Cyber Reality - Case studies The Cyber Project	
TOTAL:45PERIODS	

TEXTBOOKS:
1. Pedro H. J. Nardelli, Cyber-physical Systems, Released May 2022, Publisher(s): Wiley-IEEE Press, ISBN: 9781119785163.
REFERENCES:
1. Rajeev Alur, Principles of Cyber Physical Systems, 1st Edition, MIT Press 2015. 2. Raj Rajkumar, Dionisio de Niz, Mark Klein Cyber-Physical Systems, Released December 2016, Publisher(s):Addison-Wesley Professional. ISBN: 9780133416169

Mapping of Cos with POs/PSOs														
Cos	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	3	-	3	-	3	3	-	-	-	3	-	-	3	3
2	3	-	-	-	3	-	-	-	-	3	-	-	3	3
3	3	3	-	-	3	-	-	-	-	3	-	-	3	3
4	3	-	-	-	3	3	-	-	-	3	-	-	3	3
5	3	3	3	-	3	3	-	-	-	3	-	-	3	3
CO (W.A)	3	3	3	-	3	3	-	-	-	3	-	-	3	3

22CCX08 - INTRUSION DETECTION SYSTEMS

(Common to 22CIX38)

		L	T	P	C
		3	0	0	3
PREREQUISITE: Nil					
Course Objective:		<ul style="list-style-type: none"> To provide students with a comprehensive understanding of how IDS work, their implementation, and their role in network security 			
Course Outcomes The student will be able to		Cognitive Level	Weightage of COs in End Semester Examination		
CO1	Gain practical skills in deploying and configuring IDS in different environments.	An	20%		
CO2	Differentiate various IDS technologies and configure a network using IDS tools.	An	20%		
CO3	Configure a server and its hosts for real-time Intrusion Detection	Ap	20%		
CO4	Select and install a IDS system such as Snort to secure the network.	An	20%		
CO5	Create comprehensive reports summarizing Snort activity, detected threats, and response actions.	C	20%		

UNIT I - INTRODUCTION	(9)
Understanding Intrusion Detection – Intrusion detection and prevention basics – IDS and IPS analysis schemes, Attacks, Detection approaches – Misuse detection – anomaly detection – specification-based detection – hybrid detection-methodologies-Signature & Anomaly based Detection, Stateful protocol analysis Types of IDS, Information sources Host based information sources, Network based information sources.	
UNIT II - THEORETICAL FOUNDATIONS OF DETECTION TECHNOLOGIES	(9)
Taxonomy of anomaly detection system – fuzzy logic – Bayes theory – Artificial Neural networks – Support vector machine - IDS TECHNOLOGIES: Components & Architecture-Typical components, Network Architectures Security capabilities - Information gathering capabilities, logging capabilities, detection & prevention capabilities. Network protocol-based IDS, Hybrid IDS, and Analysis schemes.	
UNIT III - NETWORK BASED IDS	(9)
Networking Overview- OSI layers. Components and Architecture - Typical components, Network architectures and sensor locations. Security capabilities Wireless IDPS – Wireless Networking overview-WLAN standards & components. Components Network Behavior analysis system.	

UNIT IV - HOST BASED IDS	(9)
Components and Architecture-Typical components, Network architectures, Agent locations, host architectures. Security capabilities-Logging, detection, prevention and other capabilities. Using & Integrating multiple IDPS technologies-Need for multiple IDPS technologies, Integrating different IDPS technologies-Other technologies with IDPS capabilities, Anti – malware technologies, Firewalls and Routers, Honeypots.	
UNIT V - APPLICATIONS AND SNORT TOOLS	(9)
Tool Selection and Acquisition Process - Bro Intrusion Detection – Prelude Intrusion Detection – Cisco Security IDS - Snorts Intrusion Detection – NFR security - Introduction to Snort, Working with Snort Rules,Snort configuration, Snort with MySQL, Running Snort on Multiple Network Interfaces.	
TOTAL (L:45) = 45 PERIODS	

TEXT BOOKS:
<ol style="list-style-type: none"> 1. Carl Endorf, Eugene Schultz and Jim Mellander” Intrusion Detection & Prevention”, 1st Edition, Tata McGraw-Hill, 2006. 2. Ali A. Ghorbani, Wei Lu, “Network Intrusion Detection and Prevention: Concepts and Techniques”, Springer, 2010.
REFERENCES:
<ol style="list-style-type: none"> 1. Stephen Northcutt, Judy Novak: “Network Intrusion Detection”, 3rd Edition, New Riders Publishing, 2002. 2. Paul E. Proctor, “The Practical Intrusion Detection Handbook “, Prentice Hall, 2001. 3. Rafeeq Rehman: “Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID,” 1st Edition, Prentice Hall, 2003

Mapping of COs with POs / PSOs														
COs	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	3			2									3	
2													3	
3	3		3		3									
4			3			2								3
5	3													
CO (W.A)	3		3	2	3	2							3	3

22CCX11 - MOBILE DEVICE SECURITY						
(Common to 22AIX26, 22CIX37)						
			L	T	P	C
			3	0	0	3
PREREQUISITE: NIL						
Course Objective:		<ul style="list-style-type: none"> To equip students with the knowledge and skills necessary to protect mobile devices and the data they hold. 				
Course Outcomes		Cognitive Level	Weightage of COs in End Semester Examination			
The Student will be able to						
CO1	Apply theoretical knowledge to solve real-world security problems and scenarios related to mobile communication.	Ap	20%			
CO2	Apply access control mechanisms and user authentication techniques to ensure that only authorized individuals can access device resources.	Ap	20%			
CO3	Analyze security testing results and vulnerability reports to prioritize and address application-level security issues.	An	20%			
CO4	List the various types of threats for MANET applications.	An	20%			
CO5	Discuss security challenges and attacks over mobile commerce services.	An	20%			

UNIT I - SECURITY ISSUES IN MOBILE COMMUNICATION	(9)
Mobile Communication History - Security – Wired Vs Wireless, Security Issues in Wireless and Mobile Communications, Security Requirements in Wireless and Mobile Communications, Security for Mobile Applications, Advantages and Disadvantages of Application-level Security.	
UNIT II - SECURITY OF DEVICE, NETWORK, AND SERVER LEVELS	(9)
Mobile Devices Security Requirements - Mobile Wireless network level Security, Server Level Security; Application - Level Security in Wireless Networks - Application of WLANs, Wireless Threats, Some Vulnerabilities and Attack Methods over WLANs, Security for IG Wi-Fi Applications, Security for GWi- Fi Applications, Recent Security Schemes for Wi-Fi Applications.	
UNIT III - APPLICATION-LEVEL SECURITY IN CELLULAR NETWORKS	(9)
Generations of Cellular Networks - Security Issues and attacks in cellular networks - GSM Security for applications - GPRS Security for applications - UMTS security for applications - 3G security for applications -Some of Security and authentication Solutions.	

UNIT IV- APPLICATION-LEVEL SECURITY IN MANETS	(9)
MANETs-Applications of MANETs, MANET Features, Security Challenges in MANETs; Security Attacks on MANETs - External Threats for MANET applications, Internal threats for MANET Applications, Some of the Security Solutions; Ubiquitous Computing - Need for Novel Security Schemes for UC Security Challenges for UC, Security Attacks on UC networks, Some of the security solutions for UC.	
UNIT V - SECURITY FOR MOBILE COMMERCE APPLICATION	(9)
M-commerce Applications - M-commerce Initiatives - Security Challenges in Mobile E-commerce - Types of Attacks on Mobile E-commerce - A Secure M-commerce Model Based on Wireless Local Area Network – Some of M - Commerce Security Solutions.	
TOTAL:45PERIODS	

TEXTBOOKS:
1. Pallapa Venkata ram, Satish Babu, “Wireless and Mobile Network Security”, 1st Edition, Tata McGraw Hill,2010.
2. Man Ho Au, Raymond Choo,” Mobile Security and Privacy”,1st Edition, Syngress Publisher,2016

REFERENCES:
1. Frank Adelstein, K.S.Gupta , “Fundamentals of Mobile and Pervasive Computing”, 1st Edition, Tata McGraw Hill 2005.
2. Randall k. Nichols, Panos C. Lekkas, “Wireless Security Models, Threats and Solutions”, 1st Edition, Tata McGraw Hill, 2006.
3. Bruce Potter and Bob Fleck, “802.11 Security”, 1st Edition, SPD O'REILLY 2005.
4. James Kempf, “Guide to Wireless Network Security, Springer. Wireless Internet Security - Architecture and Protocols”, 1st Edition, Cambridge University Press, 2008.

Mapping of Cos with POs/PSOs														
Cos	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	3	-	3	3	3	3	-	-	-	3	-	-	3	3
2	3	3	3	3	3	3	-	-	-	3	-	-	3	3
3	3	-	3	3	3	-	-	-	-	3	-	-	3	3
4	3	-	3	3	3	-	-	-	-	3	-	-	3	3
5	3	3	3	3	3	3	-	-	-	3	-	-	3	3
CO (W.A)	3	1.2	3	3	3	1.8	-	-	-	3	-	-	3	3

22CCX12 - MALWARE ANALYSIS							
<i>(Common to 22AIX27)</i>							
				L	T	P	C
				3	0	0	3
PREREQUISITE: Nil							
Course Objective:		<ul style="list-style-type: none"> To provide students with a comprehensive understanding of malware analysis, including techniques, tools, and methodologies used to dissect, analyze, and mitigate malicious software. 					
Course Outcomes The Student will be able to		Cognitive Level	Weightage of COsin End Semester Examination				
CO1	Identify various malwares the behavior of malwaresin real world applications.	Ap	20%				
CO2	Implement different malware analysis techniques.	C	20%				
CO3	Analyze the malware behavior in windows andandroid.	An	20%				
CO4	Create detection signatures and Indicators of Compromise (IOCs) to identify malware detection engineering.	C	20%				
CO5	Conduct static analysis on Windows executables andDLLs to extract meaningful information without execution.	An	20%				

UNITI-MALWARE ANALYSIS	(9)
Malware Components and Distribution – Malware Packers – Persistence Mechanisms - Network Communication- Code Injection - Process Hollowing and API Hooking - Stealth and Rootkits	
UNITII-MALWARE CLASSIFICATION	(9)
Static Analysis – Dynamic Analysis – Memory Forensics with Volatility -Malware Pay load Dissection andClassification	
UNITIII-MALWARE REVERSE ENGINEERING	(9)
Debuggers and Assembly Language – Debugging Tricks for Unpacking Malware- Debugging Code Injection-Armoring and Evasion: The Anti-Techniques-Fileless, Macros, and Other Malware Trends	
UNITIV- DETECTION ENGINEERING	(9)
Antivirus Engines - IDS/IPS and Snort / Suricata Rule Writing – Malware Sand box Internals – Binary Instrumentation For Reversing Automation	

UNIT V - ANALYZING MALICIOUS WINDOWS PROGRAMS	(9)
Analyzing Malicious Windows Programs – The Windows API -Types and Hungarian Notation-File System Functions-Shared Files-Files Accessible via Namespaces - Alternate Data Streams - The Windows Registry.	
TOTAL:45PERIODS	

TEXTBOOKS:
<ol style="list-style-type: none"> 1 Malware Analysis and Detection Engineering, A Comprehensive Approach to Detect and Analyze Modern Malware by Abhijit Mohanta,Anoop Saldanha, 2020,Publisher(s): Apress, ISBN:9781484261934 2 Michael Sikorski and Andrew Honig,“PracticalMalwareAnalysis”byNoStarchPress,2012,ISBN: 9781593272906
REFERENCES:
<ol style="list-style-type: none"> 1. Jamie Butler and Greg Hoglund, “Rootkits: Subverting the Windows Kernel” by 2005, Addison-Wesley Professional. 2. Bruce Dang, Alexandre Gazet, Elias Bacchanalian, Sebastien Josse, “Practical Reverse Engineering:x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation”, 2014.

Mapping of Cos with Pos / PSOs														
Cos	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	3		3											
2				3									3	
3	3												3	3
4	3				3									3
5		3											3	
CO (W.A)	3	3	3	3	3	0	0	0	0	0	0	0	3	3

22CCX13- DIGITALFORENSICS					
(Common to 22AIX28)					
		L	T	P	C
		3	0	0	3
PREREQUISITE: NIL					
Course Objective:	<ul style="list-style-type: none"> To focuses on the methods and techniques used to investigate and analyzedigital evidence. 				
Course Outcomes The Student will be able to		Cognitive Level	Weightage of COsin End Semester Examination		
CO1	Explain the basics of digital forensics process.	Ap	20%		
CO2	Describe about digital crime and investigations procedures.	An	20%		
CO3	Outline the Frameworks, Standards and Methodologiesfor digital forensics.	Ap	20%		
CO4	Identify the digital evidences and tools for iOS devices	Ap	20%		
CO5	Create clear and detailed forensic reports that summarize findings, methodologies, and conclusions, suitable for legal proceedings or organizational review.	C	20%		

UNIT I - INTRODUCTION	(9)
Introduction - Computer Forensics Fundamentals, Types of Computer Forensics Technology, Types of Computer Forensics Systems; Vendor and Computer Forensics Services.	
UNIT II - COMPUTER FORENSIC EVIDENCE AND CAPTURE	(9)
Computer forensics evidence and capture - Data Recovery - Evidence Collection and Data Seizure - Duplication and Preservation of Digital Evidence - Computer Image Verification and Authentication.	
UNIT III - COMPUTER FORENSIC ANALYSIS	(9)
Discover of Electronic Evidence - Identification of Data, Reconstructing Past Events - Fighting against Macro Threats; Tactics of the Military - Tactics of Terrorist and Rogues - Tactics of Private Companies.	
UNIT IV - INFORMATION OPERATIONS	(9)
Arsenal and Surveillance Tools - Hackers and Theft of Components, Contemporary Computer Crime, Identity Theft and Identity Fraud; Organized Crime & Terrorism - Applying the First Amendment to Computer Related Crime, The Fourth Amendment and other Legal Issues.	

UNITY – DIGITAL FORENSIC CASES	(9)
Developing Forensic Capabilities – Searching and Seizing Computer Related Evidence, Processing Evidence and Report Preparation, - Future Issues.	
TOTAL (L:45) = 45 PERIODS	

TEXT BOOKS:
<ol style="list-style-type: none"> 1. John R. Vacca, “Computer Forensics: Computer Crime Scene Investigation”, Cengage Learning, 2nd Edition, 2005. 2. Marjie T Britz, “Computer Forensics and Cyber Crime: An Introduction”, Pearson Education, 2nd Edition, 2008.
REFERENCES:
<ol style="list-style-type: none"> 1. Cyber security – Understanding of cybercrimes, computer forensics and Legal perspectives by Nina Godbole and Sunit Belapure – Wiley India Publication 2019. 2. The basics of digital Forensics (Latest Edition)–The primer for getting started in digital forensics by John Sammons–Elsevier Syngress Imprint 2015. 3. Practical Digital Forensics – Richard Boddington [PACKT] Publication, Open-source community 2010. 4. Majid Yar, “Cybercrime and Society”, SAGE Publications Ltd, Hardcover, 2nd Edition, 2013.

Mapping of COs with POs / PSOs														
COs	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	3												3	
2	3	3											3	
3		3	3											3
4				3									3	
5							3							
CO (W.A)	3	3	3	3			3						3	3

22CCX14 - DATA ANALYTICS FOR CYBERSECURITY						
			L	T	P	C
			3	0	0	3
PREREQUISITE: NIL						
Course Objective:		<ul style="list-style-type: none"> To enhance cybersecurity measures, improve threat detection, and support incident response efforts. 				
Course Outcomes The student will be able to		Cognitive Level	Weightage of COs In End Semester Examination			
CO1	Gain knowledge of Big Data storage systems like HDFS and processing models like MapReduce and YARN.	An	20%			
CO2	Analyze data by utilizing clustering and classification algorithms.	An	20%			
CO3	Implement and evaluate association rules and various recommendation system approaches.	Ap	20%			
CO4	Perform real-time analytics and sentiment analysis using stream data.	An	20%			
CO5	Analyze Big Data using tools like Hive and HBase, and explore Big Data.	An	20%			

UNIT I - INTRODUCTION TO BIGDATA	(9)
Evolution of Big data; Best Practices for Big data Analytics; Big data characteristics; Validating; The Promotion of the Value of Big Data; Big Data Use Cases; Characteristics of Big Data Applications - Perception and Quantification of Value; Understanding Big Data Storage; HDFS; Map Reduce and YARN–Map Reduce Programming Model.	
UNIT II - CLUSTERING AND CLASSIFICATION	(9)
Advanced Analytical Theory and Methods- Overview of Clustering, K-means, Use Cases; Overview of the Method - Determining the Number of Clusters, Diagnostics, Reasons to Choose and Cautions; Classification- Decision Trees, Overview of a Decision Tree, The General Algorithm, Decision Tree Algorithms, Evaluating a Decision Tree, Decision Trees in R; Naïve Bayes – Bayes’ Theorem, Naïve Bayes Classifier.	
UNIT III – ASSOCIATION AND RECOMMENDATION SYSTEM	(9)
Advanced Analytical Theory and Methods- Association Rules, Overview, Apriori Algorithm, Evaluation of Candidate Rules; Finding Association & finding similarity; Recommendation System- Collaborative Recommendation, Content Based Recommendation, Knowledge Based Recommendation, Hybrid Recommendation Approaches.	

UNIT- IV STREAM MEMORY	(9)
Introduction to Streams Concepts; Stream Data Model and Architecture - Stream Computing, Sampling Data in aStream, Filtering Streams, Counting Distinct Elements in a Stream; Estimating moments; Counting oneness in aWindow – Decaying Window; Real time Analytics Platform (RTAP) applications; Case Studies; Real Time Sentiment Analysis.	
UNIT V - NO SQL DATA MANAGEMENT FOR BIG DATA AND VISUALIZATION	(9)
No SQL Databases- Schema-less Models; Increasing Flexibility for Data Manipulation; Key Value Stores-DocumentStores, Tabular Stores, Object Data Stores; Graph Databases Hive; Sharding; HBase – Analyzing big data with twitter; Big data for E-Commerce; Big data for blogs; Review of Basic Data Analytic Methods using.	
TOTAL(L:45):45PERIODS	

TEXTBOOKS:
<ol style="list-style-type: none"> 1. Anand Rajaraman and Jeffrey David Ullman, "Mining of Massive Datasets", Cambridge University Press, 2012. 2. David Loshin," Big Data Analytics: From Strategic Planning to Enterprise Integration with Tools, Techniques, NoSQL and Graph", Morgan Kauffmann/Elsevier Publishers, 2013
REFERENCES:
<ol style="list-style-type: none"> 1. EMC Education Services, "Data Science and Big Data Analytics: Discovering, Analyzing, Visualizing and Presenting Data", Wiley publishers, 2015. 2. Bart Baesens, "Analytics in a Big Data World: The Essential Guide to Data Science and its Applications",Wiley Publishers, 2015. 3. Dietmar Jannach and Markus Zanker, "Recommender Systems: An Introduction", Cambridge UniversityPress, 2010 4. Kim H. Pries and Robert Dunnigan, "Big Data Analytics: A Practical Guide for Managers" CRC Press, 2015

Mapping of Cos with Pos / PSOs														
Cos	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	3	3											3	3
2		3											3	3
3			3	3									3	3
4				3			3						3	3
5		3											3	3
CO (W.A)	3	3	3	3	0	0	3	0	0	0	0	0	3	3

22CCX15 - VULNERABILITY ASSESSMENT AND PENETRATION TESTING					
		L	T	P	C
		3	0	0	3
PREREQUISITE: NIL					
Course Objective:		<ul style="list-style-type: none"> This course covers Metasploit attacks, information gathering tools, and automated/manual vulnerability assessments. It includes wireless hacking techniques and web vulnerability assessments, providing students with essential skills for comprehensive security evaluations. 			
Course Outcomes The Student will be able to		Cognitive Level	Weightage of COsin End Semester Examination		
CO1	Analyze the different phases involved in the penetration testing process.	Ap	20%		
CO2	Identify different approaches and tools used in information gathering during penetration Testing	An	20%		
CO3	Discuss the function of vulnerability scanners and their role in identifying and assessing Security vulnerabilities using tools.	Ap	20%		
CO4	Summarize wireless network vulnerability analysis process	An	20%		
CO5	Identify key challenges associated with web hacking and build solutions with professional ethics.	An	20%		

UNIT I- TESTING PROCESS	(9)
Introduction – Terminologies – Categories of penetration testing – Types of penetration test – Vulnerability Assessment-Risk Assessment-Methodology	
UNIT II - INFORMATION GATHERING	(9)
Information gathering techniques – Active, passive and sources of information gathering – Approaches and tools – Trace routes, neo trace, what web, net craft, X code exploit scanner and NS lookup - Zone Transfer with Host Command – DNS Cache Snooping – Sniffing SNMP Passwords-SNMP Brute Force and Dictionary	
UNIT III - HOST DISCOVERY AND EVADING TECHNIQUES	(9)
Host discovery – Scanning for open ports and services – Types of port-Vulnerability scanner function – Pros and cons – Vulnerability assessment with NMAP – Testing SCADA environment with NMAP – Nessus vulnerability scanner – Safe check – Silent dependencies – Port range-vulnerability data resources	
UNIT IV - WIRELESS VULNERABILITY	(9)
Introduction-Requirements-Uncovering Hidden SSIDs-Turning on the Monitor Mode-Placing Your Wireless Adapter in Monitor Mode-Cracking a WPA/WPA2 Wireless Network -Capturing Packets Capturing the Four-Way Handshake-Reducing the Delay-Evil Twin Attack-Scanning the Neighbors Spoofing the MAC-Setting Up a Fake Access Point-Remote file inclusion	

UNITV - WEB VULNERABILITY	(9)
Attacking the Authentication-Brute Force and Dictionary Attacks-Types of Authentication-Crawling Restricted Links-Testing for the Vulnerability-Authentication Bypass with Insecure Cookie Handling XSSvulnerability -SQL Injection Attacks-Cross-Site Request Forgery-File Inclusion Vulnerabilities Testing a website for SSI injection	
TOTAL (L:45) = 45 PERIODS	

TEXT BOOKS:
1. Rafay Baloch, Ethical Hacking and Penetration Testing Guide, CRC Press, First Edition,2015
REFERENCES:
1. Prakhar Prasad, Mastering Modern Web Penetration Testing, Packt Publishing, First Edition, 2016.
2. Abhinav Singh, Metasploit Penetration Testing Cookbook, Wailings, Prentice Hall, 2010. Packt Publishing, First Edition, 2012.

Mapping of COs with POs / PSOs														
COs	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	2	3											3	3
2		3			3								3	3
3		2		3	3								3	3
4	3												3	3
5		3	3					3					3	3
CO (W.A)	1	3	3	3	3	0	0	3	0	0	0	0	3	3

22CCX16 - INFORMATION SYSTEM SECURITY MANAGEMENT
(Common to 22CSX24,22ITX24)

L	T	P	C
3	0	0	3

PREREQUISITE: Nil

Course Objective:

- To focus on the strategies and practices required to protect information systems and manage security effectively within an organization.

Course Outcomes The Student will be able to		Cognitive Level	Weightage of COs in End Semester Examination
CO1	Apply theoretical knowledge to practical problems, demonstrating the ability to develop and implement security solutions based on frameworks.	Ap	20%
CO2	Analyze and explore the information security controls	An	20%
CO3	Assess and evaluate the risk management practices of information security.	Ap	20%
CO4	Identify the disasters and recovering from them with appropriate decisions.	An	20%
CO5	Apply various recovery strategies, such as data backup and restoration, alternative site arrangements, and failover solutions, to ensure effective recovery.	Ap	20%

UNIT I - INFORMATION SECURITY PRINCIPLES AND FRAMEWORK (9)

Information Security- Assets and Types - Threat, Vulnerability, Risk and Impact - Information Security Policy Concepts - Need for Information Security. Organization and Responsibilities: Organizational Policy, Standards and Procedures - Information Security Governance - Information Assurance Programme Implementation - Security Incident Management - Legal Framework: Security Standards and Procedures.

UNIT II - SECURITY LIFE CYCLE AND CONTROLS (9)

Information Security Life Cycle - Testing, Audit, Review and Controls - Systems Development and Support - General Controls - People Security - User Access Controls - Technical Security - Protection from Malicious Software - Physical Security - Different Uses of Controls.

UNIT III - SECURITY MANAGEMENT MODELS AND PERFORMANCE MEASUREMENT (9)

Blueprints - Frameworks and Security Models - Security Architecture Models - Various Access Control Models - Information Security Performance Measurement.

UNIT IV - RISK ASSESSMENT & RISK MANAGEMENT	(9)
Threats and its Categories - Vulnerabilities and its Categories - Risk - Calculation of Overall Risk – Risk Identification - Risk Analysis - Risk Evaluation - Risk Control - Risk Termination - Risk Reduction – Risk Transfer - Risk Tolerance - Overall Risk Assessment. Risk Management Framework and Process – ManagingRisk - Risk Treatment- Alternative Risk Management Methodologies.	
UNIT V - DISASTER RECOVERY AND BUSINESS CONTINUITY MANAGEMENT	(9)
Disaster Recovery Process and policy - Relationship between Disaster Recovery and Business ContinuityManagement - Resilience and Redundancy - Approaches to Writing and Implementing Plans - Need for Documentation - Maintenance and Testing.	
TOTAL (L:45) = 45 PERIODS	

TEXT BOOKS:

1. Andy Taylor, David Alexander, Amanda Finch and David Sutton, “Information Security Principles”,2020, Third Edition, BCS, United Kingdom.
2. Michael E. Whitman and Herbert J. Mattord, “Management of Information Security”, 2018, Sixth Edition, Cengage Learning, United States of America.

REFERENCES:

1. Calder, A., and Watkins, S. G., “Information security risk management for ISO27001/ISO27002”, 2018, Third Edition, IT Governance Ltd, United States of America.
2. Susanto, H., and Almunawar, M. N, “Information security management systems: A novel framework and software as a tool for compliance with information security standards”, 2018, First Edition, Apple Academic Press, New York.

22CCX17 – CYBER SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE				
		L	T	P
		3	0	0
PREREQUISITE : NIL				
Course Objective:	<ul style="list-style-type: none"> To Focuses students with the knowledge and skills necessary to effectively manage cybersecurity initiatives, align them with organizational goals, and ensure compliance with relevant regulations and standards. 			
Course Outcomes The Student will be able to		Cognitive Level	Weightage of COsin End Semester Examination	
CO1	Ability to identify threats and introduction Governance.	Ap	20%	
CO2	Create and implement communication plans to ensure effective reporting and communication of IT governance issues, performance, and strategic alignment to stakeholders.	C	20%	
CO3	Analyze the impacts of climate change on environmental governance and develop strategies for adaptation and mitigation.	An	20%	
CO4	Demonstrate the ability to apply theoretical knowledge to practical situations, developing and implementing industry governance solutions.	An	20%	
CO5	Establish systems for monitoring and evaluating the performance of financial institutions against governance standards and regulatory requirements.	An	20%	

UNIT I - INTRODUCTION	(9)
Act Locally, Impact Globally – Governance – Risk – Compliance and Internal Controls – GRC and Globalization – Growth of Global Trade – Simple Suggestion to Improve Governance, Risk Management and Compliance (GRC) – A Risk-Based Approach to ICFR – COSO – Time to Rethink the corporate tax.	
UNIT II - GOVERNANCE IT	(9)
Role of internal Audit – Risk and Resolution – Last Mile of Finance – Fraud and Corruption – Fighting Corruption Remains a losing battle - IT Governance Overview – ISO 27001 and ISO 17799 - COBIT.	
UNIT III - ENVIRONMENTAL GOVERNANCE	(9)
The Impact of Environmental Legislation on High – Tech Supply Chains – Environmental Compliance and Enforcement in China – The Trajectory of Environmental Regulation: A Strategic Approach for industry – Environmental Compliance in India – Latin American Environmental Compliance: Environmental Biotechnology – Policy Developments in the United States related to chemicals and electronic waste.	

UNIT IV - INDUSTRY GOVERNANCE	(9)
Electronics Global Homologation: Removing Regulatory Barriers to Trade – Protecting the Innocent: The Information Security and Privacy Battle – Shippers Compliance in Freight Transportation and Logistics – Pharmaceutical – Public Sector Transparency.	
UNIT V - FINANCIAL SERVICES GOVERNANCE	(9)
Financial Services Regulation and Corporate Governance – Insurance Industry and Solvency II – Islamic Finance – Corporate Governance and Risk Management in Africa.	
TOTAL (L:45) = 45 PERIODS	

TEXT BOOKS:
1. Anthony Tarantino, “Governance, Risk and Compliance Handbook”, John Wiley & Sons, Inc, 2008.
REFERENCES:
1. Mark S Merkow , Jim Breithaupt, “Information Security: Principles and Practice”, Pearson Education Inc., New Delhi, 2014.
2. Charles P. Pfleeger and Sari Lawrence Pfleeger, “Analyzing Computer Security: A Threat / Vulnerability / Counter measure Approach”, Pearson Education, New Delhi, 2012.
3. Michael E Whitman, Herbert J Mattord, “Principles of Information Security”, Cengage Learning, USA, 2014.

Mapping of COs with POs / PSOs														
COs	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1		3					3							
2	3												3	
3				3			3							3
4			3										3	
5	3													3
CO (W.A)	3	3	3	3			3						3	3

22CCX18 – HARDWARE SECURITY					
		L	T	P	C
		3	0	0	3
PREREQUISITE: NIL					
Course Objective:	<ul style="list-style-type: none"> This course focuses concepts from diverse fields of study such as cryptography, hardware design, circuit testing, algorithms and machine learning. 				
Course Outcomes The student will be able to		Cognitive Level	Weight age of COs In End Semester Examination		
CO1	Apply principles of secure hardware design, including redundancy, fail-safes, and robust encryption, to create resilient hardware systems.	Ap	20%		
CO2	Analyze the performance impacts of implementing hardware security primitives, including the trade-offs between security and performance.	An	20%		
CO3	Apply Differential Power Analysis methods to extract secret keys by analyzing variations in power consumption during cryptographic operations.	Ap	20%		
CO4	Implement power management techniques and strategies to reduce power consumption and improve energy efficiency in ICs.	Ap	20%		
CO5	Develop measures to mitigate the effects of hardware Trojans, including redundancy, isolation, and error detection mechanisms.	C	20%		
UNIT I – MODERN HARDWARE DESIGN					(9)
Introduction – Mapping an algorithm to hardware – Binary GCD Processor – Enhancing the performance of a hardware design – modelling of the computational elements of the gcd processor.					
UNIT II –HARDWARE DESIGN OF THE ADVANCED ENCRYPTION STANDARD					(9)
Algorithmic and Architectural Optimizations for AES Design - Circuit for the AES S-Box -Implementation of the Mix Column Transformation - An Example Reconfigurable Design for the Rijndael Cryptosystem - Single Chip Encryptor/Decryptor					
UNIT III – SIDE – CHANNEL HARDWARE					(9)
Types of Side Channel Attacks - Kocher’s Seminal Works - Power Attacks - Fault Attacks - Cache Attacks - Scan Chain-Based Attacks - Scan Chain-Based Attacks on Cryptographic Implementations - Scan Attack on Trivium - Testability of Cryptographic Designs					

UNIT IV – Hardware Trojans	(9)
Introduction - Trojan Taxonomy and Examples - Multi-Level Attack - Effect of Hardware Trojan on Circuit Reliability - Hardware Trojan Insertion by Direct Modification of FPGA Configuration Bitstream-Statistical Approach for Trojan Detection	
UNIT V – SIDE-CHANNEL ANALYSIS TECHNIQUES FOR HARDWARE TROJANS DETECTION	(9)
Motivation for the Proposed Approaches - Multiple-Parameter Analysis-Based Trojan Detection - Integration with Logic-Testing Approach - Obfuscation-Based Trojan Detection/Protection - Integrated Framework for Obfuscation - A FPGA-Based Design Technique for Trojan Isolation - A Design Infrastructure Approach to Prevent Circuit Malfunction.	
TOTAL(L:45):45PERIODS	

TEXTBOOKS:
1. Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, "Hardware Security: Design, Threats, and Safeguards", CRC Press https://www.routledge.com/Hardware-Security-Design-Threats-and-Safeguards/Mukhopadhyay-Chakraborty/p/book/9781439895832
REFERENCES:
1. Ahmad-Reza Sadeghi and David Naccache (eds.): Towards Hardware-intrinsic Security: Theory and Practice, Springer. 2. Ted Huffmire et al: Handbook of FPGA Design Security, Springer. 3. Stefan Mangard, Elisabeth Oswald, Thomas Popp: Power analysis attacks - revealing the secrets of smart cards. Springer 2007. 4. Doug Stinson, Cryptography Theory and Practice, CRC Press.

Mapping of Cos with Pos / PSOs														
COs	POs												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
1	3													3
2		3			3									
3		3	3		3							3		
4	3	3	3											
5														3
CO (W.A)	3	3	3	-	-	-	-	-	-	-	-	-	3	-