ST. VINCENT PALLOTTI COLLEGE OF ENGINEERING & TECHNOLOGY, NAGPUR

(An autonomous institution affiliated to Rashtrasant Tukadoji Maharaj Nagpur University)

B. Tech. Scheme of Examination & Syllabus 2022-23

COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

Scheme of Examination – Seventh Semester

	Course Code	Course Title	Hours per Week			Credits	Maximum Marks		
			L	T	P		Continual Assessment	End Sem Examination	Total
1	22CS701T	Cyber Forensics	3	1	-	4	30	70	100
2	22CS701P	Cyber Forensics Lab	-	-	2	1	25	25	50
3	22CS702T	Machine Learning for Cyber Security	3	1	-	4	30	70	100
4	22CS703T	Professional Elective - III	4	-	-	4	30	70	100
5	22CS704P	Network Protocol Engineering Lab	-	-	2	1	25	25	50
6	22CS705P	Project - II	-	-	6	3	50	50	100
7	22CS761O	Open Elective - III	3	-	-	3	30	70	100
8	22CS706P	Summer/Winter Internship	-	-	-	2	50	-	50
9	22CS707P	Capstone Course - II	-	-	2	1	50	-	50
Total			**13**	**2**	**12**	**23**	**370**	**430**	**800**

	Professional Elective - III
22CS703T(i)	PE- III Threats and Malware Analysis
22CS703T(ii)	PE- III Information Security Audit and Monitoring
22CS703T(iii)	PE- III Information Security Analysis and Compliance using Big Data
	Open Elective - III
22CS761O(i)	OE - III Mobile App Security Analysis
22CS761O(ii)	OE- III Open Source and Open standards
22CS761O(iii)	OE- III Operational Research

Chairman - BoS	Dean – Academics	July 2025	1.0	Applicable for 2025-26
		Date of Release	Version	

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS701T	Cyber Forensics	3	1	-	4	30	70	100

Course Objectives	Course Outcomes
This course is intended • Analyze the core principles and techniques of cyber forensics and digital evidence management. • Apply standard procedures for evidence acquisition, analysis, and documentation. • Explore the tools and technologies used in the detection and investigation of cybercrimes. • Examine the legal and ethical aspects of cybercrime investigations.	**Students will be able to** • Comprehend the foundational concepts and scope of cyber forensics. • Analysed and interpret digital evidence using appropriate forensic tools. • Document forensic activities in accordance with legal and professional standards. • Conduct forensic investigations in compliance with cyber laws and ethical practices.

Unit I: Introduction to Cyber Forensics [8 Hrs]
1. Definition and scope of Cyber Forensics, 2.Categories of cybercrime and digital evidence, 3.Digital crime investigation process, 4.Forensic readiness and lab setup, 5.Chain of custody and integrity of evidence, 6.Legal considerations in cyber forensics, 7.Case Study: Introduction to a real-world cybercrime investigation.
Unit II: Evidence Acquisition and Preservation [8 Hrs]
1.Data acquisition techniques: live vs. static, 2.Imaging tools and write blockers, 3.Disk and file system analysis (FAT, NTFS, Ext), 4.RAM and volatile memory analysis, 5.Hashing techniques: MD5, SHA1, 6.Evidence preservation and documentation, 7.Lab: Creating and verifying forensic disk images.
Unit III: Legal and Ethical Aspects of Risk Management [6 Hrs]
1.Overview of forensic toolkits: FTK, Encase, Autopsy, 2.Email and browser forensics, 3.Log analysis and event correlation, 4.Mobile device forensics basics, 5.Steganography detection, 6.Lab: Analysing browser cache and email headers
Unit IV: Risk Analysis Techniques and Reporting [8 Hrs]
1. Network traffic capture and analysis (Wireshark), 2.IDS and firewall logs, 3.Investigating insider threats and APTs, 4.Malware behaviour analysis basics. 5.Memory dump analysis using Volatility, 6.Case Study: Tracing a ransomware attack
Unit V: Incident Response and Business Continuity Planning [6 Hrs]
1.Cyber laws and forensic standards (IT Act, GDPR, HIPAA), 2.Expert witness and courtroom presentation, 3.Forensic report writing and documentation standards, 4.Ethics in digital investigation, 5.Lab: Drafting a forensic investigation report

Text Books

S.N	Title	Authors	Edition	Publisher
1	Computer Forensics and Cyber Crime	Marjie T. Britz	4th Edition	Pearson
2	Guide to Computer Forensics and Investigations	Bill Nelson, Amelia Phillips, Chris Steuart	6th Edition	Cengage Learning

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Computer Forensics and Cyber Crime	Marjie T. Britz	4th Edition	Pearson
2	Guide to Computer Forensics and Investigations	Bill Nelson, Amelia Phillips, Chris Steuart	6th Edition	Cengage Learning

		July 2025	1.0	Applicable for 2025-26
Chairman - BoS	Dean – Academics	Date of Release	Version	

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS701P	Cyber Forensics Lab	-	-	2	1	25	25	50

Course Objectives	Course Outcomes
This course is intended • Analyse the principles and methodologies used in digital forensics and cyber investigations. • Identify and extract evidence from computers, mobile devices, and networks using forensic tools. • Ensure proper documentation, preservation, and presentation of digital evidence. • Gain knowledge of laws, ethics, and the legal framework related to cybercrime investigations.	**Students will be able to** • Comprehend the fundamental concepts of cyber forensics and digital evidence collection. • Utilize standard forensic tools to acquire and analyse data from digital devices. • Document forensic procedures to maintain the integrity and admissibility of evidence. • Apply forensics in real-world scenarios involving cybercrime investigations.

Expt. No.	Title of the Experiment	CO
1	Introduction to Cyber Forensics and Setup of a Lab Environment	CO1
2	Acquisition and Imaging of Digital Evidence using FTK Imager	CO1
3	File Recovery and Metadata Extraction from a Windows System	CO1,CO2
4	Analysing Web Browser Artefacts and Cache Files	CO2
5	Email Forensics: Header Analysis and Phishing Investigation	CO2,CO3
6	Memory Dump Analysis using Volatility Framework	CO2,CO3
7	Mobile Device Forensics using Open Source Tools	CO2,CO3
8	Network Packet Capture and Analysis using Wireshark	CO3
9	Detecting Hidden Files and Steganography Content	CO3
10	Reporting and Documentation of a Cyber Forensics Case Study	CO3,CO4
11	Legal Procedures and Chain of Custody Simulation	CO4

Text Books

S.N	Title	Authors	Edition	Publisher
1	Computer Forensics and Cyber Crime	Marjie T. Britz	4th Edition	Pearson
2	Guide to Computer Forensics and Investigations	Bill Nelson, Amelia Phillips, Chris Steuart	6th Edition	Cengage Learning

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Computer Forensics and Cyber Crime	Marjie T. Britz	4th Edition	Pearson
2	Guide to Computer Forensics and Investigations	Bill Nelson, Amelia Phillips, Chris Steuart	6th Edition	Cengage Learning

		July 2025	1.0	Applicable for 2025-26
Chairman - BoS	Dean – Academics	Date of Release	Version	

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS702T	Machine Learning for Cyber Security	3	1	-	4	30	70	100

Course Objectives	Course Outcomes
This course is intended to provide: • Explain the foundational concepts of Machine Learning (ML) and their relevance to cyber security applications. • Explore various ML techniques such as supervised, unsupervised, and reinforcement learning for solving security problems. • Analyze real-world cyber security datasets using ML algorithms to detect anomalies, intrusions, malware, and phishing attacks. • Develop models to predict and classify threats using popular ML libraries and frameworks. • Evaluate the performance and limitations of ML models in adversarial cyber environments and understand ethical concerns.	**Student will be able to:** • Explain the fundamental concepts of machine learning and its integration into cyber security systems. • Apply supervised learning for cyber threat classification tasks. • Implement unsupervised learning algorithms and anomaly detection techniques to identify irregular patterns and threats in network traffic. • Design and evaluate machine learning models by performing feature engineering and using appropriate evaluation metrics in a cyber-security context. • Demonstrate ethical and practical challenges of using ML in cyber defense.

Unit I Introduction to Machine Learning in Cyber Security **[8 Hrs]**

Introduction to Machine Learning: Definitions, Overview of machine learning and cyber security, Application areas of machine learning in cyber security, Challenges and limitations of machine learning in cyber security, Types (Supervised, Unsupervised, Reinforcement Learning), Role of ML in Cyber Security, Comparison of traditional vs. ML-based security systems, Basics of Data Preprocessing for Cyber Security, ML Pipeline in Security: Data Collection, Feature Engineering, Overview of popular ML tools: Scikit-learn, Pandas, NumPy, case study.

Unit II Supervised Learning for Threat Detection **[7 Hrs]**

Supervised Learning Concepts: Labels, Features, Training & Testing, Classification Algorithms: Decision Trees, Random Forests, Logistic Regression, and Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), case study.

Unit III Unsupervised Learning for Anomaly Detection **[8 Hrs]**

Unsupervised Learning Concepts: Clustering and Dimensionality Reduction, Clustering Algorithms: K-Means Clustering, DBSCAN, Anomaly Detection Techniques, Dimensionality Reduction: PCA (Principal Component Analysis) and Case Study: Detecting abnormal behavior in network traffic, case study.

Unit IV Feature Engineering & Model Evaluation **[6 Hrs]**

Importance of Feature Engineering in Cyber Security, Feature Selection Techniques, Feature Extraction Techniques, Model Evaluation in Cyber Contexts: ROC curve, AUC.

Unit V Adversarial Machine Learning **[7 Hrs]**

Types of cyber threats: malware, phishing, DDoS, Traditional vs AI-based Threat Detection Systems, Defensive Techniques: Adversarial Training, Robust Models, Case studies: Phishing URL detection using ML, Botnet traffic detection using clustering.

Text Books

S.N	Title	Authors	Edition	Publisher
1	Machine Learning and Security: Protecting Systems with Data and Algorithms	Clarence Chio, David Freeman	Second	O'Reilly Media, 2018
2	Hands-On Machine Learning for Cybersecurity	Soma Halder, Sinan Ozdemir	Third	Packt Publishing

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Machine Learning for Cybersecurity Cookbook	Emmanuel Tsukerman	Second	Packt Publishing, 2019
2	Applied Machine Learning for Cybersecurity	Aihua Liu	Third	Springer

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS703T	Professional Elective –III (Threat and Malware Analysis)	4	-	-	4	30	70	100

Course Objectives	Course Outcomes
This course is intended • To identify malware types based on static & behavioral analysis • To determine malware types & capabilities • To evaluate potential threat from malware activity	Student will be able to: • Understand CTI concepts, threat types, and intelligence lifecycle models. • Apply structured intelligence frameworks like MITRE ATT&CK and STIX for threat reporting. • Analyze CTI implementation using OSINT tools and organizational strategies. • Apply static and dynamic malware analysis using appropriate lab setups. • Evaluate malware detection techniques using signature and non-signature-based methods.

Unit-I	**10 Hrs**
Introduction to Cyber Threat Intelligence (CTI) Essential Terminology, Types of Threats, APTs & IoCs, Where to Begin? The Intelligence Cycle, The Diamond Model, Cyber Kill Chain, Cyber Threat Lifecycles & Frameworks	
Unit-II	**12Hrs**
Structured intelligence and business planning, MITRE ATT&CK Framework , STIX Language, Intelligence Reporting, Intelligence Report Structure, Collection Sources, Threat Intelligence Budgeting, Intelligence Analysts	
Unit-III	**12Hrs**
CTI Implementation Organizational Footprint, Primary Considerations for CTI Implementation, Developing the Core CTI Team, Introduction to OSINT, OSINT Platforms, OSINT Research Technologies, CTI Prioritization	
Unit-IV	**12Hrs**
Introduction to Malware Analysis History, Types of Malwares, Types of Malware Analysis, Malware Analysis Lab Setup, Static Malware Analysis, Dynamic Malware Analysis	
Unit-V	**14Hrs**
Malware Detection Techniques: Signature-based techniques: malware signatures, packed malware signature, metamorphic and polymorphic malware signature Non-signature based techniques: similarity-based techniques, machine-learning methods, invariant inferences.	

Text Books

S.N	Title	Authors	Edition	Publisher
1	Cyber Threat Intelligence: The No-Nonsense Guide for CISOs and Security Managers	Aaron Roberts.	First Edition	Apress Publishing.
2	The Threat Intelligence Handbook: A Practical Guide for Security Teams to Unlocking the Power of Intelligence.	Chris Pace		Cyber Edge Press

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Learning Malware Analysis	Monappa K A		Packt Publishing
2	Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software	by Michael Sikorski & Andrew Honig.		No Starch Press

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS704P	Network Protocol Engineering Lab	-	-	2	1	25	25	50

Course Objectives	Course Outcomes
This course is intended • Understand the differences between IT and OT networks, including their architecture and security requirements. • Familiarize with industry-standard tools for asset discovery, threat detection, and network monitoring in OT environments. • Apply cybersecurity frameworks and standards like IEC 62443 to design secure OT systems. • Develop hands-on skills in configuring network security measures including VLANs, firewalls, RBAC, and intrusion detection systems. • Plan and implement proactive OT cybersecurity practices including risk assessment, incident response, and patch management.	**Students will be able to** • Differentiate between IT and OT network architectures and identify unique security requirements for OT systems. • Demonstrate the ability to use tools like Armis, Nozomi, and Claroty CTD for asset classification and threat detection in OT environments. • Apply IEC 62443 zoning, conduits, and risk assessment principles to secure an industrial control system. • Configure and monitor OT security protocols using tools such as Wireshark, VLANs, firewalls, and Snort for network defense. • Design an effective incident response plan and implement system hardening techniques for enhanced OT cybersecurity posture.

Expt. No.	Title of the Experiment	CO
1	Compare IT vs OT Network Architecture and Security Requirements	CO1
2	Discover and Classify OT Assets Using Armis	CO2
3	Apply IEC 62443 Zoning and Conduit Concepts to a Sample OT System	CO3
4	Perform a Risk Assessment Based on IEC 62443-3-2 Guidelines	CO3
5	Configure Role-Based Access Control in an ICS Simulation (IEC 62443-3-3 SR 1.1)	CO3
6	Detect ICS Threats Using Nozomi Guardian (Simulated)	CO2
7	Analyze Threat Alerts Using Claroty Continuous Threat Detection (CTD)	CO2
8	Monitor OT Protocols (Modbus/DNP3) Using Wireshark	CO4
9	Implement VLANs and Firewalls to Segment an OT Network	CO4
10	Deploy Snort for Intrusion Detection in an Industrial Control Network	CO4
11	Design an Incident Response Plan for an OT Cybersecurity Scenario	CO5
12	Simulate Patch Management and System Hardening for OT Devices	CO5

Text Books

S.No.	Title	Authors	Edition	Publisher
1	Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems	Eric D. Knapp, Joel Langill	-	Syngress
2	Practical Industrial Internet of Things Security: A practitioner's guide to securing connected industries	Sravani Bhattacharjee, Gaurav Belani	-	Packt Publishing

Reference Books

S.No.	Title	Authors	Edition	Publisher
1	Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS	Tyson Macaulay & Bryan L. Singer	7th Edition	CRC Press
2	The Industrial Cybersecurity Handbook: A Practical Guide to Securing Your Organization's OT and ICS Environment	P.E. David J. Teumim	10th Edition	ISA (International Society of Automation)

		July 2025	1.0	Applicable for 2025-26
Chairman - BoS	Dean – Academics	Date of Release	Version	

ST. VINCENT PALLOTTI COLLEGE OF ENGINEERING & TECHNOLOGY, NAGPUR

(An autonomous institution affiliated to Rashtrasant Tukadoji Maharaj Nagpur University)

B. Tech. Scheme of Examination & Syllabus 2022-23

COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS761O(i)	OE-III Mobile App Security Analysis	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
Upon completion of this course, students will: • Understand mobile application platforms, especially Android and iOS architectures. • Identify and analyze common security threats, vulnerabilities, and risks in mobile apps. • Gain hands-on experience with tools and frameworks used in mobile app penetration testing. • Learn secure coding practices and techniques for secure app development. • Understand regulatory, legal, and ethical issues in mobile app security.	**Upon completion, students will be able to:** • Explain mobile OS architecture and app life cycles. • Identify security vulnerabilities and risks in mobile apps. • Demonstrate use of tools for mobile app security testing and forensics. • Recommend and implement secure coding and design principles. • Interpret legal and ethical considerations in mobile application security

Unit I **[9 Hrs]**

Introduction to Mobile Platforms and App Ecosystems, Overview of Mobile OS (Android, iOS), App architecture and life cycle, Application sandboxing, Permissions models, App store ecosystems & security models, Mobile threat landscape

Unit II **[9 Hrs]**

Mobile App Threats and Attack Vectors, OWASP Mobile Top 10 vulnerabilities , Static and dynamic analysis , Reverse engineering basics , Data storage insecurity , Insecure communication (HTTP vs HTTPS, SSL/TLS flaws) , Authentication & session management flaws

Unit III **[9 Hrs]**

Tools and Techniques for Mobile App Security Analysis , Introduction to mobile penetration testing , Tools: MobSF, Frida, Drozer, Apktool, Burp Suite , Code obfuscation and anti-debugging , Memory analysis and runtime instrumentation , Logging and forensic data in mobile devices

Unit IV **[9 Hrs]**

Secure Mobile App Development , Secure coding guidelines (Android/iOS) , Input validation, secure API usage , Secure data storage and encryption , Code signing and application integrity , Secure update mechanisms , DevSecOps practices in mobile CI/CD

Unit V **[9 Hrs]**

Legal, Ethical, and Compliance Aspects , Privacy regulations (GDPR, CCPA, IT Act India)
Secure mobile app policies & compliance , Ethical hacking and responsible disclosure , Incident response for mobile breaches , App security audits and reporting

Text Books

S.N	Title	Authors	Edition	Publisher
1	The Mobile Application Hacker's Handbook	Dominic Chell, Tyrone Erasmus, Shaun Colley	1 st Edition	Wiley (2015)
2	iOS Application Security: The Definitive Guide for Hackers and Developers	David Thiel	1 st Edition	No Starch Press (2016)

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Mobile Application Penetration Testing	Vijay Kumar Velu	1 st Edition	Packt Publishing (Mar 11, 2016)
2	Android Security Internals: An In-Depth Guide to Android's Security Architecture	Nikolay Elenkov	1 st Edition	No Starch Press (2014)

		July 2025	1.0	Applicable for 2025-26
Chairman - BoS	Dean – Academics	Date of Release	Version	

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS707P	Capstone Course - II	-	-	2	1	50	-	50

Course Objectives	Course Outcomes
This course is intended • Develop a deep understanding of enterprise-level routing, switching, and network services. • Design, implement, and troubleshoot complex network topologies using GNS3. • Apply knowledge of dynamic routing protocols, redundancy mechanisms, and traffic engineering. • Build and test virtual networks for real-world CCNP-level configurations using Cisco IOS images in GNS3.	**Students will be able to** • Design and simulate network topologies using GNS3. • Configure advanced routing protocols like EIGRP, OSPF, BGP, and MPLS. • Implement Layer 2 and Layer 3 security, redundancy, and troubleshooting techniques. • Perform complex network configurations using route maps, VRFs, VPNs, and policy-based routing. • Troubleshoot network issues using Cisco CLI and monitoring tools in a virtual environment.

Expt. No.	Title of the Experiment
1	Installation of GNS3 with cisco router and switches with xshell
2	Creating GNS3 network with RIP, EIGRP, OSPF.
3	MPLS Layer 3 VPN Configuration using VRF and MP-BGP
4	Route Redistribution Between OSPF, EIGRP, and BGP Using Route Maps
5	Advanced VLAN Setup with VTPv3, DTP, and Trunking
6	HSRP, VRRP, and GLBP Gateway Redundancy Configuration
7	Switchport Security with PortFast, BPDU Guard, and Root Guard
8	IPv4 and IPv6 Routing Troubleshooting Scenarios
9	Access Control Lists (ACL) – Standard, Extended, Named ACLs
10	GRE Tunnel and IPSec VPN Setup Between Routers
11	MPLS Layer 3 VPN Configuration using VRF and MP-BGP

Text Books

S.N	Title	Authors	Edition	Publisher
1	CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide	Bradley Edgeworth, Ramiro Garza Rios	Latest Edition	Cisco Press
2	CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide	Raymond Lacoste, Brad Edgeworth	Latest Edition	Cisco Press

		July 2025	1.0	Applicable for 2025-26.
Chairman - BoS	Dean – Academics	Date of Release	Version	