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 & 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	2	25	25	50
3	22CS702T	Machine Learning in Cyber Security	3	1	-	4	30	70	100
4	22CS703T	Elective-III	4	-	-	4	30	70	100
5	22CS704P	Network Protocol engineering Lab	-	-	2	1	25	25	50
6	22CS705P	Project-II	-	-	4	4	100	100	200
7	22CS706T	Open Elective-III	4	-	-	4	30	70	100
8	22CS707T	Summer/winter Internship	-	-	-	2	-	50	50
9	22CS708P	Capstone courses II*	-	-	2	1	25	25	50
Total			**14**	2	**10**	26	**250**	**425**	**700**

	Elective - III
22CS703T(i)	Threats and Malware Analysis
22CS703T(ii)	Information Security Audit and Monitoring
22CS703T(iii)	Information Security Analysis and Compliance using Big Data
	Open Elective - III
22CS706T(i)	Mobile App Security Analysis
22CS706T(ii)	Open Source and Open standards
22CS706T(iii)	Operational Research

SEVENTH SEMESTER

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

Course Objectives	Course Outcomes
This course is intended 1. Understand the core principles and techniques of cyber forensics and digital evidence management. 2. Apply standard procedures for evidence acquisition, analysis, and documentation. 3. Explore the tools and technologies used in the detection and investigation of cybercrimes. 4. Examine the legal and ethical aspects of cybercrime investigations.	**Students will be able to** 1. Comprehend the foundational concepts and scope of cyber forensics. 2. Analysed and interpret digital evidence using appropriate forensic tools. 3. Document forensic activities in accordance with legal and professional standards. 4. 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

		June 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		
22CS701P	Cyber Forensics Lab.	-	-	2	1	CA	ESE	Total
						25	25	50

Course Objectives	Course Outcomes
This course is intended 1. Understand the principles and methodologies used in digital forensics and cyber investigations. 2. Identify and extract evidence from computers, mobile devices, and networks using forensic tools. 3. Ensure proper documentation, preservation, and presentation of digital evidence. 4. Gain knowledge of laws, ethics, and the legal framework related to cybercrime investigations.	**Students will be able to** 1. Comprehend the fundamental concepts of cyber forensics and digital evidence collection. 2. Utilize standard forensic tools to acquire and analyse data from digital devices. 3. Document forensic procedures to maintain the integrity and admissibility of evidence. 4. Apply forensics in real-world scenarios involving cybercrime investigations.

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

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

		June 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 in Cyber Security	3	1	-	4	30	70	100

Course Objectives	Course Outcomes
This course is intended to provide:	**Student will be able to:**
• 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.	• Describe the basics of machine learning techniques and their taxonomy. • Apply supervised and unsupervised learning methods to cyber security datasets. • Build and train ML models for threat detection, malware analysis, and phishing detection. • Analyze the effectiveness of ML-based solutions in real-time cyber threats. • Demonstrate ethical and practical challenges of using ML in cyber defense.

Unit I Introduction to Machine Learning in Cyber Security **[6 Hrs]**

Introduction to Machine Learning: Definitions, Types (Supervised, Unsupervised, Reinforcement Learning), Role of ML in Cyber Security,Comparison of traditional vs. ML-based security systems,Types of cyber threats: malware, phishing, DDoS, insider threats, etc. ,Basics of Data Preprocessing for Cyber Security,Overview of popular ML tools: Scikit-learn, Pandas, NumPy.

Unit II Supervised Learning for Threat Detection **[8 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). Application: Intrusion Detection Systems (IDS), Hands-on: Using ML models for malware and spam classification, Evaluation Metrics: Accuracy, Precision, Recall, F1-Score and Confusion Matrix.

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

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

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

Importance of Feature Engineering in Cyber Security, Feature Selection Techniques, Feature Extraction Techniques, Cross-validation and Hyper parameter Tuning (GridSearchCV, RandomSearchCV), Model Evaluation in Cyber Contexts: ROC curve, AUC, PR curve.

Unit V Adversarial Machine Learning & Case Studies **[8 Hrs]**

Introduction to Adversarial Machine Learning, Attacks on ML Models: Evasion, Poisoning, and Model Inversion. Defensive Techniques: Adversarial Training, Robust Models, Case Studies: Phishing URL detection using ML, Malware classification with dynamic/static analysis, 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

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

SEVEN SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
22CS703T	PE-III (Threat And Malware Ananlysis)	4	-	-	4	CA	ESE	Total
						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	Students will be able to • Use intelligence models for identifying and classifying threats • Apply structured intelligence methods using frameworks • Apply standard techniques for CTI implementation. • Conduct deep malware analysis using static and dynamic analysis processes. • Analyze and detect malware using signature-based and non-signature-based techniques

Unit I **[7Hrs]**

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 **[8Hrs]**

Structured Intelligence & Business PlanningMITRE ATT&CK Framework, STIX Language, Intelligence Reporting, Intelligence Report Structure, Collection Sources, Threat Intelligence Budgeting, Intelligence Analysts

Unit III **[7Hrs]**

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 [7Hrs]

Introduction to Malware AnalysisHistory, Types of Malwares, Types of Malware Analysis, Malware Analysis Lab Setup, Static Malware Analysis, Dynamic Malware Analysis

Unit V [7Hrs]

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	Michael Sikorski & Andrew Honig		No Starch Press

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

Course Code	Course Name	Th	Tu	Pr	Credits	:valuation		
22CS704P	**Network Protocol and Engineering Lab**			**2**	**1**	**CA**	**ESE**	**Total**
						25	**25**	**50**

Course Objectives	Course Outcomes
This course is intended ● **Understand Security Concepts**: Gain foundational knowledge of network security principles, protocols, and architectures. ● **Threat Identification**: Develop skills to identify, analyze, and mitigate various network vulnerabilities and threats. ● **Security Mechanisms**: Learn to implement and manage security tools, techniques, and policies to protect network infrastructure. ● **Incident Response**: Equip learners with the ability to detect, respond to, and recover from network security breaches.	**Students will be able to** ● **Comprehend Security Fundamentals**: Demonstrate a solid understanding of network security concepts, threats, and defense mechanisms. ● **Implement Security Measures**: Apply appropriate tools and techniques to secure network infrastructures and ensure data integrity. ● **Analyze and Mitigate Threats**: Identify and address potential network vulnerabilities and actively mitigate security risks. ● **Respond to Security Incidents**: Develop strategies for effective incident detection, response, and recovery in real-world scenarios.

Expt. No.	Title of the experiment
1	Interpreting Ping and Traceroute Output. 25
2	Demonstrating Distribution Layer Functions
3	Placing ACLs
4	Exploring Different LAN Switch Options
5	Implementing an IP Addressing Scheme
6	Examining Network Address Translation (NAT)
7	Observing Static and Dynamic Routing
8	Configuring Ethernet and Serial Interfaces
9	Configuring a Default Route
10	Configuring Static and Default Routes
11	Configuring RIP
12	Planning Network-based Firewalls

Text Books

S.N	Title	Authors	Edition	Publisher
1	Programming with Java	Primer, E.Balaguruswamy	6th Edition	TMH
2	The Complete Reference Java	Herbert Schildt	7th Edition	Tata McGraw Hill

SEVENTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS706(i)T	OE-III Mobile App Security Analysis	3			3	30	70	100

Course Objectives	Course Outcomes
Upon completion of this course, students will: 1. Understand mobile application platforms, especially Android and iOS architectures. 2. Identify and analyze common security threats, vulnerabilities, and risks in mobile apps. 3. Gain hands-on experience with tools and frameworks used in mobile app penetration testing. 4. Learn secure coding practices and techniques for secure app development. 5. Understand regulatory, legal, and ethical issues in mobile app security.	Upon completion, students will be able to: 1. Explain mobile OS architecture and app life cycles. 2. Identify security vulnerabilities and risks in mobile apps. 3. Demonstrate use of tools for mobile app security testing and forensics. 4. Recommend and implement secure coding and design principles. 5. 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)