ST. VINCENT PALLOTTI COLLEGE OF ENGINEERING & TECHNOLOGY, NAGPUR

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

B. Tech. Scheme of Examination & Syllabus 2024 - 25

COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

SEMESTER V

Sr No	Course Category	CourseCode	Course Title	Hours per Week			Credits	Maximum Marks				Minimum Passing Marks	No. of Hours for ESE
				L	T	P		Mid-Sem Examination	Continual Assessment	End Sem Examination	Total		
1	PCC	**24CS501T**	Network Vulnerability Analysis and Penetration Testing	**3**	**-**	**-**	**3**	**20**	**20**	**60**	**100**	**45**	**3**
2	PCC	**24CS501P**	Network Vulnerability Analysis and Penetration Testing Lab	**-**	**-**	**2**	**1**	**-**	**25**	**25**	**50**	**25**	**-**
3	PCC	**24CS502T**	Foundation of Cryptography	**3**	**-**	**-**	**3**	**20**	**20**	**60**	**100**	**45**	**3**
4	PCC	**24CS502P**	Foundation of Cryptography Lab	**-**	**-**	**2**	**1**	**-**	**25**	**25**	**50**	**25**	**-**
5	PCC	**24CS503T**	Mobile App Security Analysis	**2**	**-**	**-**	**2**	**10**	**10**	**30**	**50**	**23**	**1.5**
6	PCC	**24CS504P**	Computer Lab	**-**	**-**	**2**	**1**	**-**	**25**	**25**	**50**	**25**	**-**
7	PEC	**24CS505T**	Program Elective - I	**3**	**-**	**-**	**3**	**20**	**20**	**60**	**100**	**45**	**3**
8	VSC	**24CS506P**	Technical Skill Development – II	**-**	**-**	**4**	**2**	**-**	**50**	**-**	**50**	**25**	**-**
9	SEC	**24CS541P**	Career Development – V	**-**	**-**	**2**	**1**	**-**	**50**	**-**	**50**	**25**	**-**
10	MDM	**24CS531M**	MDM – III (Refer the Basket)	**3**	**-**	**-**	**3**	**20**	**20**	**60**	**100**	**45**	**3**
Total				**14**	**-**	**12**	**20**	**90**	**265**	**345**	**700**	**-**	**-**

Multidisciplinary Minor – III	
24CS531M	Fundamentals of Blockchain Technology

Program Elective - I	
24CS505T(i)	Security Strategies in Windows and Linux
24CS505T(ii)	IOT and Security
24CS505T(iii)	Intrusion Detection and Prevention System

		July 2026	**NEP 2.1**	**Applicable for 2026 - 27**
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 2024-25

COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation			
						MSE	CA	ESE	Total
24CS501T	Network Vulnerability Analysis and Penetration Testing	3	-	-	3	20	20	60	100

Course Objectives	Course Outcomes
This course is intended to: 1. Explain the basic principles and techniques of how attackers can enter computer systems. 2. Put acquired knowledge into practice by performing ethical penetration tests and hiding the intrusion. 3. Evaluate the societal role of hacking from a social, ethical and economic standpoint.	**Students will be able to** 1. Perform analyses of data breaches and audits of information technology security. 2. Apply penetration testing methodologies to simulate real-world cyber-attacks in a controlled environment. 3. Evaluate the strengths and weaknesses of various information technology solutions regarding data security. 4. Independently present and perform demonstrations of pen tests for educational purposes. 5. Demonstrate the use of tools such as Nmap, Metasploit, and Wireshark for network analysis and testing.

Unit I **[9 Hrs]**

Introduction Ethics of Ethical Hacking: Why you need to understand your enemy's tactics, recognizing the gray areas in security, Vulnerability Assessment and Penetration Testing. Penetration Testing and Tools: Social Engineering Attacks: How a social engineering attack works, conducting a social engineering attack, common attacks used in penetration testing, preparing yourself for face-to-face attacks, defending against social engineering attacks.

Unit II **[9 Hrs]**

Physical Penetration Attacks: Why a physical penetration is important, conducting a physical penetration, Common ways into a building, Defending against physical penetrations. Insider Attacks: Conducting an insider attack, Defending against insider attacks. Metasploit: The Big Picture, Getting Metasploit, Using the Metasploit Console to Launch Exploits, Exploiting Client-Side Vulnerabilities with Metasploit, Penetration Testing with Metasploit's Meterpreter, Automating and Scripting Metasploit, Going Further with Metasploit.

Unit III **[9 Hrs]**

Managing a Penetration Test: planning a penetration test, structuring a penetration test, execution of a penetration test, information sharing during a penetration test, reporting the results of a Penetration Test. Basic Linux Exploits: Stack Operations, Buffer Overflows, Local Buffer Overflow Exploits, Exploit Development Process. Windows Exploits: Compiling and Debugging Windows Programs, Writing Windows Exploits, Understanding Structured Exception Handling (SEH), Understanding Windows Memory Protections (XPSP3, Vista, 7 and Server 2008), Bypassing Windows Memory Protections.

Unit IV **[9 Hrs]**

Web Application Security Vulnerabilities: Overview of top web application security vulnerabilities, Injection vulnerabilities, cross-Site scripting vulnerabilities, the rest of the OWASP Top Ten SQL Injection vulnerabilities, Cross-site scripting vulnerabilities. Vulnerability Analysis: Passive Analysis, Source Code Analysis, Binary Analysis.

Unit V **[9 Hrs]**

Client-Side Browser Exploits: Why client-side vulnerabilities are interesting, Internet explorer security concepts, history of client- side exploits and latest trends, finding new browser-based vulnerabilities heap spray to exploit, protecting yourself from client-side exploit. Malware Analysis: Collecting Malware and Initial Analysis: Malware, Latest Trends in Honeynet Technology, Catching Malware: Setting the Trap, Initial Analysis of Malware.

Text Books

S.N	Title	Authors	Edition	Publisher
1	Gray Hat Hacking - The Ethical Hackers Handbook	Allen Harper, Stephen Sims, Michael Baucom	III Edition	Tata Mc Graw-Hill.
2	The Web Application Hacker's Handbook-Discovering and Exploiting Security flaws	Dafydd Suttard, Marcus pinto	I Edition	Wiley Publishing

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Penetration Testing: Hands-on Introduction to Hacking"	Georgia Weidman	I Edition	Pearson edition
2	The Pen Tester Blueprint-Starting a Career as an Ethical Hacker	L. Wylie, Kim Crawly	I Edition	Wiley Publications

		July 2026	NEP 2.1	Applicable for 2026-27
Chairman - BoS	Dean – Academics	Date of Release	Version	

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
24CS501P	Network Vulnerability Analysis and Penetration Testing Lab	-	-	2	1	25	25	50

Course Objectives	Course Outcomes
This course is intended 1. Understand Security Concepts: Gain foundational knowledge of network security principles, protocols, and architectures. 2. Threat Identification: Develop skills to identify, analyze, and mitigate various network vulnerabilities and threats. 3. Security Mechanisms: Learn to implement and manage security tools, techniques, and policies to protect network infrastructure. 4. Incident Response: Equip learners with the ability to detect, respond to, and recover from network security breaches.	**Students will be able to** 1. Comprehend Security Fundamentals: Demonstrate a solid understanding of network security concepts, threats, and defense mechanisms. 2. Implement Security Measures: Apply appropriate tools and techniques to secure network infrastructures and ensure data integrity. 3. Analyze and Mitigate Threats: Identify and address potential network vulnerabilities and actively mitigate security risks. 4. Respond to Security Incidents: Develop strategies for effective incident detection, response, and recovery in real-world scenarios.

Experiment No.	Name of Experiment
1.	Installation of KALI & WINDOWS with bridge Connection.
2.	Social Engineering Attacks: - Setoolkit , Web Templet , Harvesting.
3.	Penetration Testing and Tools: - Wireshark, Nmap.
4.	Physical Penetration Attacks: -Tailgating, Lock Picking, Dumpster Diving
5.	Insider Attacks: - Data Theft, Sabotage.
6.	Metasploit: - Exploiting a Vulnerable Service, Creating a Reverse Shell.
7.	Managing a Penetration Test: - Planning and Scoping, Reconnaissance and Information Gathering.
8.	Basic Linux Exploits: - Sudo Privilege Escalation, Kernel Exploits.
9.	Windows Exploits: - Privilege Escalation with UAC Bypass, Identify Bypass Techniques.
10.	Web Application Security Vulnerabilities: - Cross-Site Scripting (XSS) .

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

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation			
						MSE	CA	ESE	Total
24CS502T	Foundation of Cryptography	3	-	-	3	20	20	60	100

Course Objectives	Course Outcomes
This course is intended to: 1. To provide deeper understanding into cryptography, its application to network security, threats/vulnerabilities to networks and countermeasures. 2. To explain various approaches to Encryption techniques, strengths of Traffic Confidentiality, Message Authentication Codes. 3. To familiarize Digital Signature Standard and provide solutions for their issues.	**Students will be able to** 1. Use symmetric and asymmetric key algorithms for cryptography 2. Design a security solution for a given application 3. Analyze Key Management techniques and importance of number Theory. 4. Understanding of Authentication functions the manner in which Message Authentication Codes and Hash Functions works. 5. To examine the issues and structure of Authentication Service and Electronic Mail Security.

Unit I **[9 Hrs]**

INTRODUCTION: Security trends, The OSI Security Architecture, Security Attacks, Security Services and Security Mechanisms, A model for Network security. CLASSICAL ENCRYPTION TECHNIQUES: Symmetric Cipher Modes, Substitute Techniques, Transposition Techniques, Rotor Machines, Stenography.

Unit II **[9 Hrs]**

BLOCK CIPHER AND DATA ENCRYPTION STANDARDS: Block Cipher Principles, Data Encryption Standards, the Strength of DES, Differential and Linear Crypt Analysis, Block Cipher Design Principles. ADVANCED ENCRYPTION STANDARDS: Evaluation Criteria for AES, the AES Cipher. MORE ON SYMMETRIC CIPHERS: Multiple Encryption, Triple DES, Block Cipher Modes of Operation, Stream Cipher and RC4. INTRODUCTION TO NUMBER THEORY: Prime Numbers, Fermat's and Euler's Theorem, Testing for Primality, The Chinese Remainder Theorem, Discrete logarithm.

Unit III **[9 Hrs]**

PUBLIC KEY CRYPTOGRAPHY AND RSA: Principles Public key crypto Systems, Diffie Hellman Key Exchange, the RSA algorithm, Key Management, Elliptic Curve Arithmetic, Elliptic Curve Cryptography. MESSAGE AUTHENTICATION AND HASH FUNCTIONS: Authentication Requirement, Authentication Function, Message Authentication Code, Hash Function, Security of Hash Function and MACs. HASH AND MAC ALGORITHM: Secure Hash Algorithm, Whirlpool, HMAC, CMAC. DIGITAL SIGNATURE: Digital Signature, Authentication Protocol, Digital Signature Standard.

Unit IV **[9 Hrs]**

AUTHENTICATION APPLICATION: Kerberos, X.509 Authentication Service, Public Key Infrastructure. EMAIL SECURITY: Pretty Good Privacy (PGP) and S/MIME. IP SECURITY: Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.

Unit V **[9 Hrs]**

AUTHENTICATION APPLICATION: Kerberos, X.509 Authentication Service, Public Key Infrastructure. EMAIL SECURITY: Pretty Good Privacy (PGP) and S/MIME. IP SECURITY: Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.

Text Books

S.N	Title	Authors	Edition	Publisher
1	Cryptography and Network Security - Principles and Practice	William Stallings	6th Edition	Pearson Education
2	Cryptography and Network Security	Atul Kahate	3rd Edition	Mc Graw Hill

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Cryptography and Network Security	Forouzan, Mukhopadhyay	3rd Edition	Mc Graw Hil
2	Information Security, Principles, and Practice	Mark Stamp	I Edition	Wiley India

		July 2026	NEP 2.1	Applicable for 2026-27
Chairman - BoS	Dean – Academics	Date of Release	Version	

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
24CS502P	Foundation of Cryptography Lab	-	-	2	1	25	25	50

Course Objectives	Course Outcomes
This course is intended 1. To introduce students to traditional encryption methods such as Caesar Cipher, Playfair Cipher, and Transposition techniques, including their design and limitations. 2. To study and simulate block cipher algorithms like DES and AES, focusing on their internal transformations and security principles. 3. To implement RSA algorithm, secure key exchange mechanisms, and understand public-key infrastructure concepts.	**Students will be able to** 1. Implement and analyze classical encryption techniques like Caesar, Playfair, and Transposition ciphers. 2. Simulate DES and AES operations, understanding their rounds, transformations, and practical significance. 3. Develop RSA-based encryption/decryption systems and perform secure key exchange and digital signature creation. 4. Analyze and simulate real-world security systems such as Kerberos, PGP, or IPSec, and apply hashing algorithms like SHA for integrity verification.

Experiment No.	Name of Experiment
1.	Implement Caesar Cipher encryption and decryption.
2.	Implement Playfair cipher using a 5×5 matrix.
3.	Implement transposition technique. Encrypt and decrypt messages using a keyword.
4.	Write a program to simulate Data Encryption Standard (DES) steps.
5.	Implement core steps of Advanced Encryption Standard (AES): • SubBytes • ShiftRows • MixColumns • AddRoundKey
6.	Implement RSA key generation, encryption, and decryption.
7.	Simulate secure key exchange between two users.
8.	Implement or use library functions to compute Secure Hash Algorithm (SHA).
9.	Create and verify a digital signature using RSA + hash function.
10.	Study and simulate any one: • Kerberos authentication • PGP email encryption • IPSec (Authentication Header / ESP)

Text Books

S.N	Title	Authors	Edition	Publisher
1	Classical and Modern Cryptography for Beginners	Rajkumar Banoth, Rekha Regar	1st Edition	Springer
2	Cryptography Algorithms	Massimo Bertaccini	2nd Edition	Packt Publishing

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation			
						MSE	CA	ESE	Total
24CS503T	Mobile App Security Analysis	2	-	-	2	10	10	30	50

Course Objectives	Course Outcomes
This course is intended to: 1. Introduce the architecture and life cycle of major mobile operating systems and applications. 2. Examine common security threats and vulnerabilities in mobile platforms. 3. Understand the concepts and methodologies behind mobile security testing and digital forensics. 4. Discuss secure coding principles and design strategies for mobile application development.	**Students will be able to** 1. Grasp core concepts of mobile platforms, app ecosystems, security, and common threats. 2. Analyze security vulnerabilities and risks in mobile applications. 3. Explain tools and techniques used for mobile application security testing and digital forensics.

Unit I	**[10 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	**[10 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	**[10 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 devicesSecure 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	

Text Books

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

Reference Books

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

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
24CS504P	Computer Lab	-	-	2	1	25	25	50

Course Objectives	Course Outcomes
This course is intended 1. To introduce the fundamentals of Java programming language. 2. To develop problem-solving skills using object-oriented concepts. 3. To provide hands-on experience with Java syntax, control structures, and basic OOP. 4. Develop solution to problems using collection classes, generics, streams, multithreading.	**Students will be able to** 1. Explain various data types, operators, control flow statements, iterative statements and apply it to develop a Java program. 2. Describe the concepts of objects, classes, interface and apply it to develop an object-oriented Java program. 3. Describe scope rules, storage classes, intricacies of constructors and apply it to develop a Java program. 4. Design efficient and reusable solutions using inheritance, polymorphism, method overloading, function overloading.

Experiment No.	Name of Experiment
1.	Write a Java program to demonstrate primitive and non-primitive data types.
2.	Implement a program to demonstrate arithmetic, relational, logical, and bitwise operators.
3.	Write programs using if, if-else, switch-case statements.
4.	Implement programs using for, while, do-while loops.
5.	Write programs to perform operations on arrays and strings.
6.	Create a class and instantiate objects.
7.	Demonstrate default, parameterized constructors.
8.	Implement an interface and an abstract class.
9.	Create programs demonstrating single and multilevel inheritance.
10.	Demonstrate runtime polymorphism using method overriding.

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

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation			
						MSE	CA	ESE	Total
24CS505T(ii)	PE – I IOT and Security	3	-	-	3	20	20	60	100

Course Objectives	Course Outcomes
This course is intended 1. To understand the architecture, components, and working principles of Internet of Things (IoT) systems. 2. To analyze security requirements, vulnerabilities, and threats associated with IoT devices and applications. 3. To apply cryptographic techniques and security mechanisms for designing secure IoT solutions.	**Students will be able to** 1. Explain the concepts, architecture, and enabling technologies of IoT systems. 2. Identify security threats, vulnerabilities, and attacks in IoT environments. 3. Analyze authentication, authorization, and access control mechanisms for IoT security. 4. Apply cryptographic techniques and secure communication protocols in IoT applications. 5. Design and develop secure IoT solutions to mitigate attacks and ensure end-to-end security.

Unit I	**[9 Hrs]**
Introduction of IoT : Definition, Characteristics, Physical design, Logical design, Functional blocks, Components in internet of things, Sensors and Actuators, M2M and IoT Technology, Fundamentals Devices and gateways	
Unit II	**[10 Hrs]**
Requirement of IoT Security: Security Requirements in IoT Architecture - Security in Enabling Technologies -Security Concerns in IoT Applications. Security Architecture in the Internet of Things, Security Requirements in IoT - Insufficient Authentication/Authorization – Insecure, Access Control - Threats to Access Control, Privacy, and Availability - Attacks Specific to IoT.	
Unit III	**[8 Hrs]**
IoT Vulnerabilities: Threats to Access Control, Privacy, and Availability - Attacks Specific to IoT. Vulnerabilities – Secrecy and Secret-Key Capacity-Authentication/Authorization for Smart Devices - Transport Encryption – Attack & Fault trees	
Unit IV	**[9 Hrs]**
Role of Cryptography in IoT Security: Cryptographic primitives and its role in IoT – Encryption and Decryption – Hashes – Digital Signatures – Random number generation – Cipher suites – key management fundamentals – cryptographic controls built into IoT messaging and communication protocols – IoT Node Authentication	
Unit V	**[9 Hrs]**
Attacks and Remedies : Basic attacks, User anonymity, Perfect forward secrecy, reply attack, offline password guessing attack, user impersonation attack, Man in middle attack, Smart card loss and stolen attack, Server spoofing attack, Denial of Service attack and Distributed DoS	

Text Books

S.N	Title	Authors	Edition	Publisher
1	Security and privacy in Internet of things (IoTs): Models, Algorithms, and Implementations	Hu, Fei	1st Edition	,CRC Press, 2016
2	Practical Internet of Things Security	Russell, Brian, and Drew Van Duren	1st Edition	Packt Publishing Ltd, 2016

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Rethinking the Internet of Things: a scalable approach to connecting everything	DeCosta, Francis, and Byron Henderson	1st Edition	Springer Nature, 2013

		July 2026	**NEP 2.1**	**Applicable for 2026-27**
Chairman - BoS	**Dean – Academics**	**Date of Release**	**Version**	

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation			
						MSE	CA	ESE	Total
24CS505T(iii)	PE – I Intrusion Detection and Prevention System	3	-	-	3	20	20	60	100

Course Objectives	Course Outcomes
This course is intended 1. To provide fundamental knowledge of intrusions, vulnerabilities, attacks, and various Intrusion Detection and Prevention Systems techniques used for securing computer networks and systems. 2. To understand the design, architecture, and operation of IDS and IPS technologies including host-based, network-based, anomaly-based, and hybrid detection systems. 3. To develop practical skills in configuring and using Snort, writing detection rules, managing alerts, and analyzing intrusion data using security monitoring tools.	**Students will be able to** 1. Understand the concepts of intrusions, vulnerabilities, attacks, and the need for Intrusion Detection and Prevention Systems. 2. Analyze different intrusion detection and prevention technologies including HIDS, NIDS, misuse detection, anomaly detection, and hybrid detection techniques. 3. Explain the architecture and components of IDS and IPS including sensors, agents, managers, and information flow mechanisms. 4. Apply alert management, correlation techniques, and cooperative intrusion detection methods for effective security monitoring and analysis. 5. Configure and use Snort for intrusion detection using rules, preprocessors, plugins, logging mechanisms, and database integration tools like ACID and SnortSnarf.

Unit I **[08 Hrs]**

Introduction: Introduction to Intrusions, Need of Intrusion Detection, Classification of Intrusion Detection Systems, Sources of Vulnerabilities, Attacks against various security objectives, countermeasures of attacks.

Unit II **[10 Hrs]**

Intrusion Detection and Prevention Technologies: Host-based intrusion detection system (HIDS), Network-based IDS, Information Sources for IDS, Host and Network Vulnerabilities and Countermeasures. Intrusion detection techniques, misuse detection: pattern matching, rule-based and state-based anomaly detection: statistical based, machine learning based, data mining-based hybrid detection.

Unit III **[10 Hrs]**

IDS and IPS Architecture: Tiered architectures, Single-tiered, Multi-tiered, Peer-to-Peer. Sensor: sensor functions, sensor deployment and security. Agents: agent functions, agent deployment and security. Manager component: manager functions, manager deployment and security. Information flow in IDS and IPS, defending IDS/IPS, Case study on commercial and open-source IDS.

Unit IV **[08 Hrs]**

Alert Management and Correlation Data fusion: Alert correlation, Pre-process, Correlation Techniques, Post-process, Alert Correlation architectures. Cooperative Intrusion Detection, Cooperative Discovery of Intrusion chain, Abstraction-based Intrusion Detection, Interest-based communication and cooperation, agent-based cooperation.

Unit V **[09 Hrs]**

Working with Snort Rules, Rule Headers, Rule Options, Snort Modes, Snort Configuration File (snort.conf), Plugins, Preprocessors, Output Modules, Alert and Logging Mechanisms, Writing and Testing Snort Rules, Using Snort with MySQL, ACID and SnortSnarf, Agent Development for Intrusion Detection, and Architecture Models of IDS and IPS.

Text Books

S.N	Title	Authors	Edition	Publisher
1	Intrusion Detection and Prevention Systems	Ali A. Ghorbani, Wei Lu, Mahbod Tavallaee	1st Edition	Springer
2	Snort IDS and IPS Toolkit	Jay Beale, Brian Caswell, Andrew Baker	1st Edition	Syngress

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Intrusion Detection	Rebecca Gurley Bace	1st Edition	Macmillan Technical Publishing
2	Network Intrusion Detection	Stephen Northcutt, Judy Novak	3rd Edition	New Riders Publishing

		July 2026	**NEP 2.1**	**Applicable for 2026-27**
Chairman - BoS	**Dean – Academics**	**Date of Release**	**Version**	

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
24CS506P	Technical Skill Development – II Linux Administration Lab	-	-	4	2	50	-	50

Course Objectives	Course Outcomes
This course is intended 1. Understand core Linux administration concepts through hands-on RHEL installation and system configuration. 2. Develop practical skills in user management, permissions, storage, and network services. 3. Apply Linux security mechanisms including ACL, SELinux, and system services. 4. Gain exposure to cloud-based Linux management and monitoring tools.	**Students will be able to** 1. Install and manage Linux systems using essential commands and file editors. 2. Configure users, permissions, and disks, LVM, and NFS services effectively. 3. Implement security controls using ACL, SELinux, and system daemons. 4. Monitor and administer Linux cloud environments using subscription manager and Cockpit.

Experiment No.	Name of Experiment
1.	Installation of RHEL with Basic Commands.
2.	Linux directory structure and file editors.
3.	Linux users management and group management
4.	Linux cloud subscription manager
5.	Exploring Linux cloud using Cockpit
6.	Linux File and Directory Permission
7.	Linux ACL permission
8.	Disk and Partition Management
9.	Linux disk cluster using LVM
10.	Linux security using SE Linux & System Demon
11.	NFS server configuration.

Text Books

S.N	Title	Authors	Edition	Publisher
1	UNIX and Linux System Administration Handbook	Evi Nemeth	1st Edition	Wesley Professional
2	Linux Administration: A Beginner's Guide	Wale Soyinka	2nd Edition	McGraw-Hill Education

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
24CS541P	Career Development – V	-	-	2	1	50	-	50

Course Objectives	Course Outcomes
To enhance students' aptitude, analytical reasoning, communication, teamwork, and professional presentation skills required for competitive examinations, higher education, and workplace success.	**CO1.** Students will be able to solve problems related to time and work, pipe and cisterns, geometry, mensuration, and analytical puzzles using logical and quantitative reasoning skills. **CO2.** Students will be able to apply concepts of time, speed, and distance and solve coding-decoding and direction sense problems accurately using analytical thinking. **CO3.** Students will be able to perform SWOC analysis, set SMART goals, and deliver effective self-introductions with confidence and professional communication skills. **CO4** Students will be able to conduct company profile presentations and participate effectively in table topic group discussions demonstrating teamwork, critical thinking, and spontaneous speaking skills. **CO5.** Students will be able to demonstrate improved verbal ability, grammar, vocabulary, reading comprehension, and active classroom participation for professional communication.

Unit I (15marks)	**[7Hrs]**
Time and Work, Chain Rule, Pipe and Cistern, Geometry and mensuration **Puzzles:-** Analytical puzzle, Tabular Puzzle, Box or Floor based Puzzle, Rank based Puzzle	
Unit II (10marks)	**[7Hrs]**
Time Speed and Distance:- Basic Problems, Average Speed, Relative Speed, Problems on Trains, Boats and Streams, Escalators, Directions sense Problems Coding and Decoding	
Unit III (5marks)	**[5Hrs]**
SWOC Analysis and SMART Goal Setting - for Personal and Professional Development **Self-Elevator Pitch –** Self Introduction, Confidence Building, and Professional Communication Skills (5marks)	
Unit IV (10marks)	**[6Hrs]**
Company Profile Group Presentation – Research, Team Coordination, and Presentation Techniques (5marks) **Table Topic Group Discussion –** Critical Thinking, Spontaneous Speaking, and Team Interaction	
Unit V (10marks)	**[3Hrs]**
Verbal Ability Quiz – Grammar, Vocabulary Building, and Reading Comprehension for Professional Communication **Continuous Assessment -** Attendance, Individual Engagement & Team Dynamics	

Text Books

S.N	Title	Authors	Edition	Publisher
1	Quantitative Aptitude By R. S. Aggarwal	R.S. Aggarwal		
2	Quantitative Aptitude	Shripad Deo		Allied Publication
3	A Modern Approach to Verbal & Non-Verbal Reasoning	R.S. Aggarwal		

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Quantitative Aptitude for CAT by Arun Sharma	Arun Sharma		
2	Developing Communication Skills	Krishna Mohan & Meera Banerji	2002	
3	Professional Communication Skills	Alok Jain	2006	S Chand & Company Ltd.
4	Personality Development & Soft Skills	Barun Mitra	2019	Cambridge University Oress

		July 2026	NEP 2.1	Applicable for 2026-27
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 2024-25

COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation			
						MSE	CA	ESE	Total
24CS531M	MDM – III Fundamentals of Blockchain Technology	3	-	-	3	20	20	60	100

Course Objectives	Course Outcomes
This course is intended to: 1. To explore the building blocks of Blockchain. 2. To analyze the significance of Distributed Ledger Technology and Smart Contract. 3. To exploit applications of Blockchain in real world scenarios and their impacts.	**Students will be able to** 1. Explore the Blockchain ecosystem and its services in real-world sceneries. 2. Apply and analyze the requirements of Distributed Ledger Technology. 3. Illustrate the Smart Contracts and their use cases. 4. Apply concepts to explain the structure and workflow of decentralized applications. 5. Acquaint the protocol and assess computational requirements of Blockchain Ecosystems.

Unit I **[9 Hrs]**

Foundations of Blockchain: Blockchain Architecture – Challenges – Applications – Blockchain Design Principles -The Blockchain Ecosystem - The consensus problem - Asynchronous Byzantine Agreement - AAP protocol and its analysis - peer-to-peer network – Abstract Models - GARAY model - RLA Model - Proof of Work (PoW) - Proof of Stake (PoS) based Chains – Hybrid models.

Unit II **[9 Hrs]**

Distributed Ledger Technology: Origin of Ledgers – Types and Features of Distributed Ledger Technology (DLT) - Role of Consensus Mechanism - DLT Ecosystem - Distributed Ledger Implementations – Blockchain - Ethereum - Public and Private Ledgers – Registries – Ledgers - Practitioner Perspective:Keyless Technologies.

Unit III **[9 Hrs]**

Smart Contracts: Anatomy of a Smart Contracts - Life Cycle - Usage Patterns - DLT-based smart contracts -Use Cases: Healthcare Industry and Property Transfer.

Unit IV **[9 Hrs]**

Decentralized Organization: Decentralization versus Distribution - Centralized-distributed (Ce-Di) organizations - Decentralized-distributed (De-Di) organizations - Decentralized Autonomous Organizations: Aragon, DAOstack, DAOhaus and Colony.

Unit V **[9 Hrs]**

Types of Blockchain Ecosystem: One-Leader Ecosystem - Joint Venture or Consortia Ecosystems - Regulatory Blockchain Ecosystems - Components in Blockchain Ecosystem: Leaders, Core Group, Active Participants, Users, Third-Party Service Providers - Governance for Blockchain Ecosystems.

Text Books

S.N	Title	Authors	Edition	Publisher
1	Blockchain enabled applications.	Dhillon, V., Metcalf, D., and Hooper, M	1st Edition	CA: Apress, Berkeley
2	Blockchains, digital assets, smart contracts, decentralized autonomous organizations	Diedrich, H., Ethereum	1st Edition	Packt Publishing

Refere nce Books

S.N	Title	Authors	Edition	Publisher
1	Distributed Ledger Technology: The Science of the Blockchain	Wattenhofer, R. P	2nd Edition	Createspace Independent Pub, Scotts Valley, California, US

		July 2026	NEP 2.1	Applicable for 2026-27
Chairman - BoS	Dean – Academics	Date of Release	Version	