FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS501T	Theory of Computation	3	1	-	4	30	70	100

Course Objectives	Course Outcomes
This course is intended • To study the theoretical foundation of finite state machines and its application. • To study formal languages and related grammar. • To study basic computational function related to finite automaton.	Students will be able to • Design the Finite State Machine with mathematical representation. • Define regular expression for the given Finite State Machine and vice verse. • Represent context free grammar in various forms along with its properties. • Design Push Down Automaton and Turing Machine as FSM and its various representation. • Differentiate between decidable and undecidable problems.

Unit I	**[7Hrs]**
Strings, Alphabet, Language operations, Finite state machine definitions, Finite automation model, Acceptance of strings and language, Non deterministic finite automation, Deterministic finite automation, Equivalence between NFA and DFA, Conversion of NFA into DFA, Moore and Mealy machines.	
Unit II	**[7Hrs]**
Regular sets, Regular expressions, Identity Rule, Manipulation of regular expressions, Equivalence between RE and FA, Inter conversion, Pumping lemma, Closure properties of regular sets(proofs not required), Chomsky hierarchy of languages, Regular grammars, Right linear and left linear grammars, Equivalence between regular grammar and finite automation, Inter conversion between RE and RG.	
Unit III	**[7Hrs]**
Context free grammar, Derivation trees (Syntax tree and Parse tree), Ambiguous Grammar, Context Free Language (CFL), Closure properties of CFL, Normal Form of grammar: Chomsky Normal form, Greibach normal form.	
Unit IV	**[8Hrs]**
Push Down Automaton, Turing Machine: Definition, Model of TM, Design of TM, Universal Turing Machine, Types of TM's (proofs not required), Turing Computable Functions, Linear bounded automaton.	
Unit V	**[7Hrs]**
Decidability and Undecidability of problems, Properties of recursive & recursively enumerable languages, Halting problems, Post correspondence problem, Ackerman function, Church's Hypothesis, Recursive Function: Basic functions and operations on them, Primitive recursive function, μ-recursive function, Bounded Minimization, Unbounded Minimization.	

Text Books

S.N	Title	Authors	Edition	Publisher
1	Theory of Computer Science, Automata, Languages and Computation	K. L. P. Mishra and N. Chandrasekaran	3rd Edition	PHI Learning.
2	Introduction to Automata Theory, Languages and Computation	J.E.Hopcraft,R. Motwani, J. D Ullman	2nd Edition	Pearson Education, Aisa

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Introduction to Theory of Computation	Sipser	2nd Edition	Cengage publications
2	An Introduction to Formal Languages and Automata	Peter Linz	2nd Edition	Pearson Education, Aisa
3	Introduction to Languages and the theory of Automata	John Martin	2nd Edition	TMH Publication

		July 2024	1.0	Applicable for 2024-25
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 & ENGINEERING (CYBER SECURITY)

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS502T	Security Policy and Implementation	3	1	-	4	30	70	100

Course Objectives	Course Outcomes
This course is intended ● To analyze the need for security policies, procedures and security awareness. ● To understand the types & approaches of policy designing. ● To identify security policies considerations & implement them. ● To critique existing security policy for its effectiveness and completeness.	**Students will be able to** ● Recognize the suitable cybersecurity policies based upon an organization's IT infrastructure. ● Design clear, concise and compliant cybersecurity policies. ● Effectively enforce cybersecurity policies and oversee their updation in organizations
Unit I : The Need for IT Security Policy Frameworks	**[8Hrs]**
Introduction to Security Policies, Information Systems Security, Information Assurance Information systems Security Policies, Business Drivers for Information Security Policies.	
Unit II: : Role of Governance and Business	**[8Hrs]**
Compliance Laws – India, Compliance Laws – International, Seven Domains of IT Infrastructure, Business Challenges & Policies to Mitigate the Risks, Information Security Policy Implementation Issues	
Unit III: Policy Framework & Designing	**[6Hrs]**
Program Framework Policy, Business Considerations for Framework, Information Assurance Considerations, IT Security Standards & Frameworks, How to Design, Organize, Implement & Maintain IT Security Policies, IT Security Policy Framework Approaches	
Unit IV: Types of Policies	**[8Hrs]**
User Domain Policies, IT Infrastructure Security Policies, Data Classification and Handling Policies, Risk Management Policies, Incident Response Team (IRT) Policies, Special Access Policies, Physical Security Policy, DLP Policies,	
Unit V	**[6Hrs]**
Project 1 – Research on Existing and/or Lack of Cybersecurity Polices in Local IT Companies, Analyse the Results and Generate a Comprehensive & Customised List of Cybersecurity Policies for the Companies	

Text Books

S.N	Title	Authors	Edition	Publisher
1	Security Policies and implementation Issues	Robert Johnson & Chick Easttom. Jones & Bartlett Learning	Third Edition	. Wiley Publishing.
2	Computer Security Handbook	y Seymour Bosworth, M.E. Kabay & Eric Whyne	Fifth Edition	Wiley Publishing

Reference Books

S.N	Title	Authors	Edition	Publisher
1	The Cyber Crime Law and Practices	CS Mamta Binani	1st Edition	The Institute of Company Secretaries of India

		July 2024	1.0	Applicable for 2024-25
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 & ENGINEERING (CYBER SECURITY)

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS503T	Network Vulnerability Analysis and Penetration Testing	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
This course is intended to • Explain the basic principles and techniques of how attackers can enter computer systems. • Put acquired knowledge into practice by performing ethical penetration tests and hiding the intrusion. • Evaluate the societal role of hacking from a social, ethical and economic standpoint.	**Students will be able to** • Perform analyses of data breaches and audits of information technology security. • Evaluate the strengths and weaknesses of various information technology solutions regarding data security. • Independently present and perform demonstrations of pen tests for educational purposes.

Unit I **[6Hrs]**

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 **[8Hrs]**

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 **[8Hrs]**

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 **[8Hrs]**

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 **[8Hrs]**

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	Author	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 2024	1.0	Applicable for
Chairman - BoS	Dean – Academics	Date of Release	Version	2024-25

B. Tech. Scheme of Examination & Syllabus 2022-23
COMPUTER SCIENCE & ENGINEERING (CYBER SECURITY)

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS503P	Network Vulnerability Analysis and Penetration Testing Lab	-	-	2	1	25	25	50

Course Objectives	Course Outcomes
This course is intended • Explain the basic principles and techniques of how attackers can enter computer systems. • Put acquired knowledge into practice by performing ethical penetration tests and hiding the intrusion. • Evaluate the societal role of hacking from a social, ethical and economic standpoint.	**Students will be able to** • Perform analyses of data breaches and audits of information technology security. • Evaluate the strengths and weaknesses of various information technology solutions regarding data security. • Independently present and perform demonstrations of pen tests for educational purposes.

Expt. No.	Title of the 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 :-Windows pass Crecking.
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	Gray Hat Hacking - The Ethical Hackers Handbook,	Allen Harper, Stephen Sims, Michael Baucom	III Edition	Tata Mc Graw-Hill.

Reference Books

S N	Title	Author	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

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)

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS504T(i)	PE-I Introduction to Cloud Security	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
This course is intended ● Learning basics of cloud and challenges in its implementation. ● Understanding the cloud environment and its security issues. ● Understanding the various ways to secure cloud programming environments.	**Students will be able to** ● Articulate the concepts of cloud computing, its various deployment and service models and vulnerabilities. ● Develop solutions based on the concept of virtualization, resource management and migration. ● Design measures for cloud data security and identity management. ● Provide recommendations for Cloud Infrastructure Security based on cloud compliance and policies.

Unit I **[7Hrs]**

Introduction: Evolution of Cloud Computing, Cloud Fundamentals: Cloud Definition, Evolution, Architecture, Cloud Characteristics – Elasticity in Cloud – On-demand Provisioning, Applications, deployment models - Public, Private and Hybrid Clouds, and service models - Infrastructure as a Service (IaaS) - Resource Virtualization: Server, Storage, Network. Platform as a Service (PaaS) - Cloud platform & Management: Computation, Storage. Software as a Service (SaaS) - Anything as a service (XaaS), Security as a service. Vulnerability Issues and Security Threats, Security Challenges

Unit II **[8Hrs]**

Definition, Understanding and Benefits of Virtualization. Implementation Level of Virtualization, Virtualization Structure/Tools and Mechanisms, Issues with virtualization, virtualization technologies and architectures, introduction to Various Hypervisors, virtualization of data centers, and Virtual Machine level Security, Virtualization security Issues

Unit III **[7Hrs]**

Resource Management and Load Balancing : Distributed Management of Virtual Infrastructures, Resource management, Load Balancing. Interoperability, Migration and Fault Tolerance: Issues with interoperability, Cloud Migration, Migration of virtual Machines and techniques. Fault Tolerance Mechanisms. Risk Assessment on Cloud Migration

Unit IV **[7Hrs]**

Cloud Data Security and Storage : Cloud storage: Introduction to Storage Systems, Cloud Storage Concepts, Data in the cloud- Cloud file systems. Data level Security, Data Protection (rest, at transit, in use), Data Information lifecycle, Cloud Data Audit, Multi-tenancy Issues.

Unit V **[7Hrs]**

Identity and Access Management : Introduction to Identity and Access Management, IAM Challenges, IAM Architecture, IAM Standards and Protocols for Cloud Services, Cloud Authorization Management.

Text Books

S.N	Title	Authors	Edition	Publisher
1	Distributed and cloud computing from Parallel Processing to the Internet of Things	Kai Hwang, Geoffrey C. Fox and Jack J. Dongarra	1st Edition	Morgan Kaufmann, Elsevier – 2012
2	Cloud Security and Privacy An Enterprise Perspective on Risks and Compliance	Tim Mather, SubraKumaraswamy, and Shahed Latif	1st Edition	O'Reilly 09

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Cloud Computing Bible	Barrie Sosinsky	1st Edition	john Wiley & Sons
2	Cloud Computing Principles and Paradigms	Ronald L. Krutz,Russell Dean Vines,	1st Edition	Wiley Publishers.

		July 2024	1 .0	Applicable for 2024-25
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 & ENGINEERING (CYBER SECURITY)

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS504T(ii)	PE-I Security Strategies in Windows & Linux	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
This course is intended ● To identify the vulnerabilities in Windows & Linux operating system. ● To analyze the security architecture of Windows and Linux operating system. ● To analyze the best practices to respond and recover from a security breach.	**Students will be able to** ● Recognize the attack surface on different versions & flavors of Windows & Linux operating systems. ● Design strategic security plans for operating system security in Windows & Linux. ● Administer layered security controls in Windows & Linux operating systems

Unit I : Microsoft Windows Security Situation **[8Hrs]**

Information Systems Security, Microsoft EULA Microsoft Windows & Applications IT Infrastructure, Anatomy of Microsoft Windows Vulnerabilities, Windows OS Components & Architecture, Access control & Authentication, Users, Groups & Active Directory, Windows Attack Surfaces and Mitigation, Windows Security Monitoring & Maintenance

Unit II: : Managing & Maintaining Microsoft Windows Security **[8Hrs]**

Access Controls in Windows, Windows Encryption Tools & Technologies, Windows Protection from Malware, Group Policy Control in Windows, Windows Security Profile & Audit Tools, Windows Backup & Recovery Tools, Windows Network Security, Windows Security Administration

Unit III: : Microsoft Windows Operating System and Application Security Trends and Directions **[6Hrs]**

Windows Operating System Hardening, Microsoft Application Security, Windows Incident Handling & Management, Windows and the Security Lifecycle, Best Practices for Windows and Application Security.

Unit IV: Linux Overview and Security Brief **[8Hrs]**

Security Threats to Linux, Basic Components of Linux Security, User Privileges and Permissions, Filesystems, Volumes and Encryption, Securing Services, Networks, Firewalls, SELinux, AppArmor, Networked Filesystems & Remote Access, Networked Application Security, Kernel Security Risk Mitigation

Unit V: Building a Layered Linux Security Strategy **[6Hrs]**

Managing Security Alerts & Updates, Building & Maintaining a Security Baseline, Testing & Reporting, Detecting & Responding to Security Breaches, Best Practices & Emerging Technology

Text Books

S.N	Title	Authors	Edition	Publisher
1	Security Strategies in Windows Platforms and Applications	Michael G. Solomon. Jones and Bartlett Learning	Third Edition	Willey Publication
2	Security Strategies in Linux Platforms and Applications	Michael Jang & Ric Messier. Jones and Bartlett Learning	Second Edition	Willey Publication

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Security Strategies in Linux Platforms and Applications	Michael Jang & Ric Messier. Jones and Bartlett Learning	Second Edition	Willey Publication

		July 2024	1	Applicable for 2024-25
Chairman - BoS	Dean – Academics	Date of Release	Version	

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS504T(iii)	PE-I IOT and Security	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
This course is intended • Ability to understand the Security requirements in IoT • Examine in detail IoT device vulnerabilities • Understand how these vulnerabilities should be addressed and mitigated • Understand the IoT authentication and Cloud Security.	Students will be able to • Secure a connected IoT product from scratch. • Identify the main threats and attacks on IoT products and services. • Build and deploy secure IoT solutions • Examine End-to-End IoT Security in detail.

Unit I	**[7Hrs]**
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	**[8Hrs]**
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	**[7Hrs]**
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	**[7Hrs]**
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	**[7Hrs]**
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	DaCosta, Francis, and Byron Henderson	1st Edition	Springer Nature, 2013

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS561O(i)	OE-I Basics of Ethical Hacking	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
This course is intended • Understand the fundamental principles, methodologies, and ethical considerations of hacking and develop practical skills in footprinting, scanning, enumeration, and system hacking techniques. • Learn advanced hacking methodologies, including denial of service attacks, session hijacking, and web server exploitation. • Gain proficiency in identifying and exploiting common web application vulnerabilities. • Understand network hacking techniques, including SQL injection, wireless networking hacking, and evading intrusion detection systems (IDS) and firewalls. • Learn about viruses, worms, and physical security measures to protect information assets.	Students will be able to • Students can explain the ethical considerations and legal implications of hacking activities. With footprinting, scanning, and enumeration activities to gather information about target systems. • Students can identify common vulnerabilities in systems and networks and demonstrate proficiency in exploiting them. • Students can analyze web application vulnerabilities and employ appropriate techniques to exploit them. • Students can demonstrate proficiency in network hacking techniques, including SQL injection, wireless networking hacking, and evasion of IDS and firewalls. • Students can explain the characteristics of viruses, worms, and physical security measures and propose strategies to mitigate their impact.

Unit I	**[7Hrs]**
Introduction to Ethical Hacking: Hacking Methodology, Process of Malicious Hacking: Footprinting and Scanning, Footprinting, Scanning, Enumeration, System Hacking and Trojans System Hacking,Trojans. Black Box Vs White Box Techniques.	
Unit II	**[7Hrs]**
Hacking Methodology: Denial of Service, Sniffers, Session Hijacking, Hacking Web Servers:Session Hijacking, Hacking Web Servers.	
Unit III	**[7Hrs]**
Web Application Vulnerabilities and Web Techniques: Web Application Vulnerabilities, Web Based Password Cracking Techniques.	
Unit IV	**[8Hrs]**
Web and Network Hacking: SQL Injection, Hacking Wireless Networking, Viruses and Worms, Physical Security, Linux Hacking.	
Unit V	**[7Hrs]**
Evading IDS and Firewalls, Report Writing & Mitigation : Evading IDS and Firewalls, Introduction to Report Writing & Mitigation, Requirements for low-level reporting & high-level reporting of Penetration testing results, Demonstration of vulnerabilities and Mitigation of issues identified including tracking.	

Text Books

S.N	Title	Authors	Edition	Publisher
1	The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws.	Dafydd Stuttard, Marcus Pinto,	First Edition	Wiley Publications
2	Title: "Ethical Hacking and Countermeasures: Attack Phases.	EC-Council	First Edition	EC-Council

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Hacking: The Art of Exploitation	Jon Erickson	Second Edition	No Starch Press
2	Penetration Testing: A Hands-On Introduction to Hacking.	Georgia Weidman	Second Edition	No Starch Press

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS561O (ii)	OE-I Security in IOT	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
This course is intended • Ability to understand the Security requirements in IoT • Examine in detail IoT device vulnerabilities • Understand how these vulnerabilities should be addressed and mitigated • Understand the IoT authentication and Cloud Security.	Students will be able to • Secure a connected IoT product from scratch. • Identify the main threats and attacks on IoT products and services. • Build and deploy secure IoT solutions • Examine End-to-End IoT Security in detail.

Unit I	**[7Hrs]**
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	**[8Hrs]**
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	**[7Hrs]**
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	**[7Hrs]**
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	**[7Hrs]**
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	DaCosta, Francis, and Byron Henderson	1st Edition	Springer Nature, 2013

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)

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS561O(iii)	OE-I Fundamentals of Cryptography	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
This course is intended • Learn fundamentals of cryptography and its application to network security. • Understand network security threats, security services, and countermeasures. • Understand vulnerability analysis of network security.	**Students will be able to** • Understand and explain the risks faced by computer systems and networks. • Analyse Cryptographic techniques. • Identify and analyze security problems in computer systems and networks. • Explain how standard security mechanisms work. • Understand security mechanisms to protect computer systems and networks.

Unit I **[6Hrs]**

Security Fundamentals:
Introduction of information Security, Security goals, Security Services and mechanisms, Attacks, Authentication, Authorization, Chipher Techniques : substitution and transposition ciphers, One-time Pad, Block chipher and Stream Cipher.

Unit II **[8Hrs]**

Cryptography:
Symmetric and Asymmetric Cryptographic Techniques : DES, AES, Attacks on DES, Modes of operations, Linear cryptanalysis and differential cryptanalysis, Public key algorithms, RSA, Hash functions- SHA-1, MD5

Unit III **[8Hrs]**

Key management
Generation, Distribution, updation, Digital certificate, X.509 certificates, Digital signatures, Diffie hellman key exchange, One way authentication, Kerberos.

Unit IV **[8Hrs]**

Network Security
Security concerns, Introduction to IPSEC, Tunnel mode, Transport mode, Introduction to handshake protocols, Record layer protocol, Internet Key Exchnage protocol(IKE)

Unit V **[8Hrs]**

Security in Networks:
Threats in networks, Network Security Controls – Architecture, Encryption, Content Integrity, Strong Authentication, Access Controls, Wireless Security, Honeypots, Traffic flow security, Firewalls – Design and Types of Firewalls, Personal Firewalls, IDS, Email Security – PGP,S/MIME

Text Books

S.N	Title	Authors	Edition	Publisher
1	Applied Cryptography- Protocols, Algorithms and source code in “c”	Bruice Schneier	II Edition	Wiley India Pvt ltd
2	Network Security and Cryptography	Bernard Menzees	I Edition	Cengage Learning

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Cryptography and Network Security Principal and Practice	Wiiliam Stalling	I Edition	Pearson edition
2	Cryptography and Network Security	Berouz Forouzan	I Edition	Tata Mc Graw Hill

		July 2024	1.0	Applicable for 2024-25
Chairman - BoS	Dean – Academics	Date of Release	Version	

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS505P	Computer Lab-III	-	-	2	1	25	25	50

Course Objectives	Course Outcomes
This course is intended • To introduce java compiler and eclipse platform. • To write programs using abstract classes. • To write programs for solving real world problems using java collection frame work. • To write multithreaded programs. • To write GUI programs using swing controls in Java.	**Students will be able to** • Design programs for solving real world problems using java collection frame work. • Create programs using abstract classes. • Implement multithreaded programs. • Understand the concept of package and exception handling • Create GUI programs using swing controls in Java.

Expt. No.	Title of the experiment
1	Installation of eclipse IDE and introduction of JAVA.
2	Demonstration of Class and Object, Pattern Programming with JAVA.
3	Program to demonstrate Type Casting and Type Conversion.
4	Program to implement inheritance with JAVA.
5	Program to implement abstract class.
6	Program to implement multithreading.
7	Program to implement package.
8	Program to implement exception handling using try and multiple catch blocks.
9	Program to handle user defined exception using throw keyword.
10	Program to implement swing control with java.

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		
						CA	ESE	Total
22AS501T	Economics and Management	3	-	-	3	30	70	100

Course Objectives	Course Outcomes
● The course examines how the economics, business and industrial management practices are related and how business decision is taken.	● Apply managerial economics concept in business analysis and business decision making. ● Explain relationships between production and costs and understand different forms of market structures. ● Asses impact of macroeconomics and government policies on business and economy. ● Recognize the functions of management and marketing management for business decisions. ● Explore role of financial management in business and decision making.

Unit I	**[8Hrs]**
Economics, Classification of economics, Industrial economics, Applications of Industrial economics. Types of Business structures, Consumer demand, Law of Demand, Determinants of demand, Demand forecasting, Law of supply, Utility, Law of diminishing marginal Utility, Types of Elasticity of demand	
Unit II	**[8Hrs]**
Concept of Production, Factors of Production, Laws of return, Cost concepts and types of cost, cost curves, Market Structures- Perfect competition, Monopoly, Oligopoly, and Monopolistic competition. Business cycles, optimum size of firm.	
Unit III	**[8Hrs]**
The functions of central bank, Inflation, Deflation, Recession. Measures to control Inflation, National income, GDP, GNP, Monetary and fiscal policy of government. Liberalization, Privatization and Globalization	
Unit IV	**[8Hrs]**
Definition of management, functions of management – planning, organizing, directing, Controlling, Introduction to human resources Management, Marketing Management, Concepts of Marketing, Marketing mix, Methods of pricing, Marketing mix. channels of distribution, advertising and sales promotion.	
Unit V	**[8Hrs]**
Financial Management, nature and scope of financial management, Sources of finance, Types of capital, Brief outline of profit and loss account, balance sheet, Budgets and types of budgets, Ratio analysis, Principles of costing	

Text Books

S. N	Title	Authors	Edition	Publisher
1.	Managerial Economics	D.N. Dwivedi	8th	Vikas Publishing
2.	Modern Economic Theory	K.K. Dewett	2005	S. Chand Publisher
3.	Industrial Management	Dr.I.K. Chopde, Dr.A.M. Sheikh	Revised edition	S. Chand Publisher

Reference Books

S. N	Title	Authors	Edition	Publisher
1.	Industrial Organization and Industrial economics	T.R. Banga, S.C. Sharma	2006	Khanna Publishers

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)

FIFTH SEMESTER

Course Code	Course Name	Th	Tu	Pr	Credits	Evaluation		
						CA	ESE	Total
22CS506P	Technical Skill Development-II	-	-	2	1	50	-	50

Course Objectives	Course Outcomes
This course is intended ● To identify the vulnerabilities in Windows & Linux operating system. ● To analyze the security architecture of Windows and Linux operating system. ● To analyze the best practices to respond and recover from a security breach.	**Students will be able to** ● Recognize the attack surface on different versions & flavors of Windows & Linux operating systems. ● Design strategic security plans for operating system security in Windows & Linux. ● Administer layered security controls in Windows & Linux operating systems

Unit I : Microsoft Windows Security Situation **[8Hrs]**

Information Systems Security, Microsoft EULA Microsoft Windows & Applications IT Infrastructure, Anatomy of Microsoft Windows Vulnerabilities, Windows OS Components & Architecture, Access control & Authentication, Users, Groups & Active Directory, Windows Attack Surfaces and Mitigation, Windows Security Monitoring & Maintenance

Unit II: : Managing & Maintaining Microsoft Windows Security **[8Hrs]**

Access Controls in Windows, Windows Encryption Tools & Technologies, Windows Protection from Malware, Group Policy Control in Windows, Windows Security Profile & Audit Tools, Windows Backup & Recovery Tools, Windows Network Security, Windows Security Administration

Unit III: : Microsoft Windows Operating System and Application Security Trends and Directions **[6Hrs]**

Windows Operating System Hardening, Microsoft Application Security, Windows Incident Handling & Management, Windows and the Security Lifecycle, Best Practices for Windows and Application Security.

Unit IV: Linux Overview and Security Brief **[8Hrs]**

Security Threats to Linux, Basic Components of Linux Security, User Privileges and Permissions, Filesystems, Volumes and Encryption, Securing Services, Networks, Firewalls, SELinux, AppArmor, Networked Filesystems & Remote Access, Networked Application Security, Kernel Security Risk Mitigation

Unit V: Building a Layered Linux Security Strategy **[6Hrs]**

Managing Security Alerts & Updates, Building & Maintaining a Security Baseline, Testing & Reporting, Detecting & Responding to Security Breaches, Best Practices & Emerging Technology

Text Books

S.N	Title	Authors	Edition	Publisher
1	Security Strategies in Windows Platforms and Applications	Michael G. Solomon. Jones and Bartlett Learning	Third Edition	Willey Publication
2	Security Strategies in Linux Platforms and Applications	Michael Jang & Ric Messier. Jones and Bartlett Learning	Second Edition	Willey Publication

Reference Books

S.N	Title	Authors	Edition	Publisher
1	Security Strategies in Linux Platforms and Applications	Michael Jang & Ric Messier. Jones and Bartlett Learning	Second Edition	Willey Publication