IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)

Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

Sr. No.	Course Type	Course Code	Course Title	Scheme			Credits
				L	T	P	
1	PCC	CB15	Cloud Computing	2	1	–	3
2	PEC	CB02	Professional Elective -II	2	1	–	3
3	PEC	CB03	Professional Elective -III	2	1	–	3
4	IOC	CB02	Interdisciplinary Open Course-II	3	–	–	3
5	LC	CB15(P)	Cloud Computing Lab	–	–	2	1
6	LC-PEC	CB03(P)	Professional Elective-III Lab	–	–	2	1
7	PROJ	CB04	Project-II	–	–	8	4
8	PROJ	CB05	Evaluation of Internship-II	–	–	6	3
Total Academic Engagement and Credits				**9**	**3**	**18**	**21**
				30			

- Professional Elective–II

(A) Vulnerability Assessment of Application Security
(B) Cyber Laws & Forensics
(C) Cyber Security Assessment and Risk Analysis
(D) Semantic Web & Ontologies

-Professional Elective–III

(A) Soft Computing
(B) Ethical Hacking
(C) Bit Coin & Cryptocurrency Technology
(D) Cybercrime Intelligence and Threat Management

-Interdisciplinary Open Course-II

CS01Digital Marketing & SEO
FT (B) Occupation Health and First Aid
Green Technology

•

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

PCC-CB15	Cloud Computing	2L:1T:0P (3hrs.)	3 Credits

Pre-requisite: Nil

Course Objective: The objective of this course is to provide students with the comprehensive and in-depth knowledge of Cloud Computing concepts, technologies, architecture and applications.

Course Contents: (40hrs)

Module 1: **(06hrs.)**

Introduction of Grid and Cloud computing, characteristics, components, business and IT perspective, cloud services requirements, cloud models, Security in public model, public verses private clouds, Cloud computing platforms: Amazon EC2, Platform as Service: Google App Engine, Microsoft Azure, Utility Computing, Elastic Computing.

Module 2: **(08hrs.)**

Cloud services- SAAS, PAAS, IAAS, cloud design and implementation using SOA, conceptual cloud model, cloud stack, computing on demand, Information life cycle management, cloud analytics, information security, virtual desktop infrastructure, storage cloud.

Module 3: **(10hrs.)**

Virtualization technology: Definition, benefits, sensor virtualization, HVM, study of hypervisor, logical partitioning- LPAR, Storage virtualization, SAN, NAS, cloud server virtualization, virtualized data center.

Module 4: **(10hrs.)**

Cloud security fundamentals, Vulnerability assessment tool for cloud, Privacy and Security in cloud, Cloud computing security architecture: Architectural Considerations- General Issues, Trusted Cloud computing, Secure Execution Environments and Communications, Microarchitectures; Identity Management and Access control Identity management, Access control, Autonomic Security, Cloud computing security challenges: Virtualization security management- virtual threats, VM Security Recommendations, VM-Specific Security techniques, Secure Execution Environments and Communications in cloud.

Module 5: **(06hrs.)**

SOA and cloud, SOA and IAAS, cloud infrastructure benchmarks, OLAP, business intelligence, e-Business, ISV, Cloud performance monitoring commands, issues in cloud computing. QOS issues in cloud, mobile cloud computing, Inter cloud issues, Sky computing, Cloud Computing Platform, Xen Cloud Platform, Eucalyptus, Open Nebula, Nimbus, T Platform, Apache Virtual Computing Lab (VCL), Anomaly Elastic Computing Platform.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)

Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

Course Outcome:

1. Explain the core concepts of the cloud computing paradigm
2. Demonstrate knowledge of virtualization
3. Explain the core issues of cloud computing such as security, privacy, and interoperability.
4. Choose the appropriate technologies, algorithms, and approaches for the related issues.
5. Identify problems, and explain, analyze, and evaluate various cloud computing solutions.

List of Text/ Reference Books:

1. Dr.Kumar Saurabh, “Cloud Computing", Wiley India.
2. Ronald Krutz and Russell Dean Vines, "Cloud Security", Wiley-India.
3. Judith Hurwitz, R.Bloor, M.Kanfman, F.Halper, "Computing for Dummies", Wiley India Edition.
4. Anthony T.Velte Toby J.Velte, Cloud Computing A Practical Approach", TMH.
5. Barrie Sosinsky, “Cloud Computing Bible", Wiley India.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

PEC-CB02(A)	Vulnerability Assessment of Application Security	2L:1T:0P (3hrs.)	3 Credits

Pre-requisite: Nil

Course Objective: Understanding Vulnerability Assessment, Differences between a bug bounty and a client-initiated pentest, Detecting SQL Injection flaws. Also covering the Extracting data using Insecure Direct Object Reference (IDOR) Flaws, Discovering Authentication methods.

Course Contents: (40 hrs.)

Module1: **(07hrs.)**

Configuring Burp Suite: Setting up proxy listeners, Working with non-proxy-aware clients, Creating target scopes in Burp Suite, Working with target, Additional browser add-ons that can be used to manage proxy Settings, Setting system-wide proxy for non-proxy-aware clients, Setting up Android and iOS to work with Burp Suite, Differences between a bug bounty and a client-initiated pentest, Why Burp Suite?: Types and features, Crawling. Why Burp Suite Scanner?: Auditor/Scanner, Understanding the insertion points. Detailed Stages of an application pentest, Features of Burp Suite.

Module2: **(12hrs.)**

Preparing for an Application Penetration Test and Identifying Vulnerabilities: Setup of vulnerable web applications, Reconnaissance, and file discovery: Using Burp for content and file discovery. Testing for authentication via Burp, Detecting SQL injection flaws, Detecting OS command injection, Detecting XSS vulnerabilities, Detecting XML-related issues such as XXE, Detecting SSTI, Detecting SSRF, Detecting CSRF, Detecting Insecure Direct Object References, Detecting security misconfigurations, Detecting insecure deserialization, Detecting OAuth-related issues, Detecting broken authentication.

Module3: **(7hrs.)**

Detecting and Exploiting Vulnerabilities: Data exfiltration via a blind Boolean-based SQL injection, Executing OS commands using an SQL injection, Executing an out-of-band command injection, Stealing session credentials using XSS, Taking control of the user's browser using XSS, Extracting server files using XXE vulnerabilities, Performing out-of-data extraction using XXE and Burp Suite collaborator, Exploiting SSTI vulnerabilities to execute server commands.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

Module4: **(07hrs.)**

Exploiting Vulnerabilities Using Burp Suite: Using SSRF/XSPA to perform internal port scans. Using SSRF/XSPA to extract data from internal machines, Extracting data using Insecure Direct Object Reference (IDOR) Flaws. Exploiting security misconfigurations, Directory listings, Default credentials, Untrusted HTTP methods. Using insecure deserialization to execute OS commands, Exploiting crypto vulnerabilities, Brute forcing HTTP basic authentication, Brute forcing forms, Bypassing file upload restrictions.

Module5: **(07hrs.)**

Writing Burp Suite Extensions and Breaking the Authentication: Setting up the development environment, Writing a Burp Suite extension: Burp Suite's API, Modifying the user-agent using an extension. Executing the extension, Performing information gathering, Port scanning, Discovering Authentication method. Exploiting and Exfiltrating Data from a Large Shipping Corporation: Discovering Blind SQL injection: Automatic scan, SQLMap detection, Intruder detection

Course Outcome:

1. Work with Proxies and non-proxy-aware clients
2. Set up Vulnerable web applications
3. Identify XSS, XML, SSTI, SSRF, and CSRF vulnerabilities
4. Exploit crypto vulnerabilities
5. Discover Blind SQL injection

List of Text/ Reference Books:

1. Hands-on Penetration Testing for Web Applications: Run Web Security Testing on Modern Applications Using Nmap, Burp Suite and Wireshark by Richa Gupta.
2. Practical Web Penetration Testing: Secure web applications using Burp Suite, Nmap, Metasploit, and more by Gus Khawaja.
3. Hands-On Application Penetration Testing with Burp Suite: Use Burp Suite and its features by Carlos A. Lozano, Dhruv Shah, et al.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

PEC-CB02(B)	Cyber Laws & Forensics	2L:1T:0P (3hrs.)	3 Credits

Prerequisite: Nil

Course Objective: Analyze and resolve security issues in an organization to secure an IT infrastructure.

Course Contents: (40 hrs.)

Module 1: **(08 hrs.)**

Cybercrimes and Attacks Introduction, Classifications of Cybercrimes: E-Mail Spoofing, Spamming, Cyber defamation, Industrial Spying/Industrial Espionage, Hacking, Software Piracy, Password Sniffing, Credit Card Frauds, Cyber stalking, Botnets, Phishing, Pharming, Man-in-the-Middle attack, Password Cracking, Key loggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Malware, Ransomware, Types of Identity Theft, Techniques of ID Theft, Cyber terrorism, Browser Attacks, Reverse Engineering, Cross site scripting

Module 2: **(06 hrs.)**

Cyber Security Concepts Introduction to Cyber Security, Cyber Security Goals, Cyber Security policy, Domain of Cyber Security Policy, Elements, Cyber Security Evolution, Implementing Hardware Based Security, Software Based Firewalls, Security Standards, Assessing Threat Levels, Forming an Incident Response Team, Reporting Cybercrime, Difference between cyber forensics and cyber security

Module 3: **(12 hrs.)**

Cyber Forensics Fundamentals Introduction to cyber forensics, needs of cyber forensic, cyber forensic and digital evidences, Internet Fraud, Storage Fundamentals, File System Concepts, challenges in cyber forensic, Data and Evidence Recovery- Deleted File Recovery, Data Recovery Tools, Data Recovery Procedures and Ethics, Preserve and safely handle original media, Document a "Chain of Custody", Complete time line analysis of computer files based on file creation, file modification and file access, Recover Internet Usage Data, Recover Swap Files/Temporary Files/Cache Files, Introduction to Encase Forensic Edition, Forensic Tool Kit (FTK) and other commonly used forensic tools.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

Module 4: **(08 hrs.)**

Cyber Forensics Investigation Introduction to Cyber Forensic Investigation, Investigation Tools, e- Discovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, Email Recovery, Encryption and Decryption methods, Search and Seizure of Computers, Recovering deleted evidences, Password Cracking.

Module 5: **(06 hrs.)**

Cyber Laws Introduction to IT laws & Cyber Crimes, Cyber Laws, IPR, Legal System of Information Technology, Social Engineering.

Course Outcomes:

1. Define and explain the concepts of cyber crime and its classification.
2. Delineate the components online frauds, intrusions, virtual crimes and hacking.
3. Knowledge of different act's in cyber security
4. List the various parts of IT act related to electronic records.
5. Knowledge of different Cyber Security tools.

List of Text / Reference Books:

1. Nina Godbole and Sunit Belpure , Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley
2. Jennifer L. Bayuk, J. Healey, P. Rohmeyer, Marcus Sachs, Jeffrey Schmidt, Joseph Weiss Cyber Security Policy Guidebook, John Wiley & Sons 2012.
3. Vivek sood, Cyber law simplified, Tata Mc GrawHill, Education (India).
4. Eoghan Casey, Handbook of digital forensic and investigation.
5. Clint P Garrison, Digital forensic for network, internet and cloud computing.
6. Panagiotis Kandlis, Digital crime and forensic science in cyberspace, information society S.A Greece IDEA Group Publishing

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

PEC-CB02(C)	Cyber Security Assessment and Risk Analysis	2L:1T:0P (3hrs.)	3 Credits

Prerequisite: Nil

Course Objective: This course describes the concepts of risk management and analysis in information security. It also covers the various Contingency Planning components. It will also discuss incident response options, and design an Incident Response Plan for sustained organizational operations

Course Contents: (40 hrs.)

Module 1: **(08hrs.)**

Information Security Overview: Introduction: Introduction to Information Security, History and Understanding the Information system, basics of information systems, Impact of information system.

Building Blocks of Information Security: Introduction, Basic principles of Information Security, security related basic terms and definitions, three pillars of Information security, Information classification, criteria and terms for classification, Information security risk analysis.

Module 2: **(08hrs.)**

Threats and Vulnerability of a System

Threats: Cyber threat categorization, sources, motivation, type, technical vs. non-technical (e.g. attacks to cooling systems to disrupt cyber systems), threat actors, exploitation of cyber vulnerabilities leading to impact and associated likelihood. Vulnerabilities: Sources of cyber vulnerability, complexity of modern software, attack surface of modern systems, development of software for functionality and not with security considerations, existing known and zero-day system vulnerabilities, vulnerability databases and open information.

Module 3: **(08hrs.)**

Security Planning

Security investigation: Need for Security - Business Needs - Threats – Attacks - secure software development - Legal, Ethical and Professional Issues in Information Security. Planning for security: Information security planning and governance – policy and practices-

Module 4: **(08hrs.)**

Security Planning and Awareness

Security Blueprint and Implementation- Blueprints for Security, Training and Awareness Programs, Business Continuity and Disaster Recovery Strategies **Security Frameworks and**

Approaches- Information Security Planning Process

Module 5: **(08hrs.)**

Risk Management and Cybersecurity Controls

Risk evaluation and associated selection of risk treatment options, effects and selection of risk avoidance, mitigation, transfer, acceptance (or a combination thereof), risk management as an iterative process, risk profile stemming from modifications in an organization's environment, building an organization's cyber security control environment from the results of risk analysis, introduction to basic Cybersecurity controls. Case study on security planning and management in any organizations.

Course Outcome:

1. Understand the fundamentals of information security, including its basic principles, terminologies, and the process of information classification and risk analysis.
2. Analyze various types of cyber threats and system vulnerabilities, including their sources, motivations, and impacts on modern information systems.
3. Evaluate the need for secure software development and interpret legal, ethical, and professional responsibilities in information security planning.
4. Design and implement effective security strategies, including security blueprints, awareness training, and continuity plans to enhance organizational security posture.
5. Apply risk management principles to identify, evaluate, and mitigate cybersecurity risks, and recommend appropriate security controls for organizational protection.

List of Text/Reference Books:

1. Information System Security best practices framework- Nina Godbole- John Willey
2. "Security Risk Management: Building an Information Security Risk Management Program from the Ground Up", by Evan Wheeler
3. "The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)", by Anne Kohnke and Dan Shoemaker
4. Michael E Whitman and Herbert J Mattord, "Principles of Information Security", Vikas Publishing House, New Delhi, 2003
5. Micki Krause, Harold F. Tipton, "Handbook of Information Security Management", Vol 1-CRC Press LLC, 2004.
6. Cyber Forensics: Understanding Information Security Investigations (Springer's Forensic Laboratory Science Series by Jennifer Bayuk Sep 9, 2010

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

PEC-CB02(D)	Semantic Web & Ontologies	2L:1T:0P (3hrs.)	3 Credits

Pre-requisite: Nil

Course Objective: The objective of this course is to familiarize the students about Semantic Web Vision and able to understand XML, RDF, Querying Ontology.

Course Contents: (40 hrs.)

Module 1: **(6 hrs.)**
Semantic Web: Building Models , Calculating with knowledge, Exchanging Information, Semantic Web Technologies ,Types of Web :Smart Web Dumb Web, Applications ,Semantic Data ,Search Engine for Semantic Web

Module 2: **(8 hrs.)**
Semantic Modeling: Modeling for human communication, Explanation and prediction, Mediating Variability: Variation Classes, Variation Layers, Expressivity in Modeling.

Module 3: **(10 hrs.)**
Resource Description Language RDF : Introduction , Advanced features , simple ontologies in RDF Schema, encoding of special data structures, RDF formal semantics ,syntactic reasoning with deduction rules ,Distributing data across web , Managing data from multiple sources .

Module 4: **(10 hrs.)**
Web Ontology Language OWL: OWL syntax and Intuitive semantics, OWL species, Owl formal semantics: Description Logics, Model-Theoretic Semantics of OWL, Automated reasoning with OWL, Ontology Matching and Distributed Information

Module 5: **(6 hrs.)**
Semantic Web Application Architecture: RDF Parser/Serializer, RDF store: RDF data standards and Interoperability of RDF stores , RDF query engines , SPARQL: Query language for RDF , conjunctive Queries for OWL DL ,RDF backed web portals , Data federation . Ontology Engineering: Constructing Ontologies manually, Reusing Existing Ontologies, Semiautomatic Ontology Acquisition, Ontology Mapping.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)

Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

Course Outcome:

1. Understand the architecture, technologies, and applications of the Semantic Web, and distinguish between various types of web data models.
2. Apply semantic modeling principles to represent human communication, explain variability, and assess the expressivity of different models.
3. Construct and manage RDF-based knowledge structures, including ontologies, using formal semantics and reasoning techniques.
4. Analyze and implement Web Ontology Language (OWL) constructs for knowledge representation, including automated reasoning and ontology matching.
5. Develop semantic web applications using RDF tools, SPARQL queries, and ontology engineering methods for data integration and federation.

Text/Reference Books:

1. Hitzler, Markus, Rudolph , Foundations of Semantic Web Technologies" , Chapman Hall/CRC,2009,ISBN 9781420090505
2. Allemang , Hendler , " Semantic Web for the working Ontologist" 2nd ed. Elsevier Pub
3. Liang Yu , " Introduction to the Semantic Web and Semantic Web Services", Chapman Hall/CRC
4. Antoniou , Harmelen , "A semantic Web Primer", PHI Pub.
5. Rajendra Akerkar ," Foundations of Semantic Web" , Narosa Publishing ,New Delhi

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

PEC-CB03(A)	Soft Computing	2L:1T:0P (3hrs.)	3 Credit

Pre-requisite: Analysis and Design of Algorithm

Course Objective: The objective of this course is to familiarize the students with different soft computing tools to use them to be able to solve complex problems.

Course Contents: (42 hrs.)

Module 1: **(08 hrs.)**
Introduction to Neural Network: Concept, biological neural network, comparison of ANN with biological NN, evolution of artificial neural network, Basic models, Types of learning, Linear separability, XOR problem, McCulloch-Pitts neuron model, Hebb rule.

Module 2: **(08hrs.)**
Supervised Learning: Perceptron learning, Single layer/multilayer, Adaline, Madaline, Back propagation network, RBFN, Application of Neural network in forecasting, data compression and image compression.

Module 3: **(08hrs.)**
Unsupervised learning: Introduction, Fixed weight competitive nets, Kohonen SOM, Counter Propagation networks, (Theory, Architecture, Flow Chart, Training Algorithm and applications). Introduction to Convolutional neural networks (CNN) and Recurrent neural networks (RNN)**.**

Module 4: **(08hrs.)**
Fuzzy Set: Introduction, Basic Definition and Terminology, Properties and Set-theoretic Operations, Fuzzy Relations, Membership Functions and their assignment, Fuzzy rules and fuzzy Reasoning, Fuzzy if-then Rules, Fuzzy Inference Systems. Application of Fuzzy logic in solving engineering problems.

Module 5: **(10hrs.)**
Genetic Algorithm: Introduction to GA, Simple Genetic Algorithm, terminology and operators of GA (individual, gene, fitness, population, data structure, encoding, selection, crossover, mutation, convergence criteria). Reasons for working of GA and Schema theorem, GA

optimization problems like TSP (Travelling salesman problem), Network design routing. Introduction to Ant Colony optimization (ACO) and Particle swarm optimization (PSO).

Course Outcomes:

1. State basic concept of Neural Network
2. Illustrate various concepts supervised learning, data and image compression
3. Describe the concept of unsupervised learning.
4. Apply fuzzy logic concepts to solve real world problem.
5. Design and implement the real world problem through Genetic algorithm

List of Text / Reference Books:

1. S.N. Shivnandam, “Principle of soft computing”, Wiley.
2. S. Rajshekaran and G.A.V. Pai, “Neural Network, Fuzzy logic And Genetic Algorithm”, PHI.
3. Jack M. Zurada, “Introduction to Artificial Neural Network System” JAico Publication.
4. Simon Haykins, “Neural Network- A Comprehensive Foundation”
5. Timothy J.Ross, “Fuzzy logic with Engineering Applications”, McGraw-Hills.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

PEC-CB03(B)	Ethical Hacking	2L:1T:0P (3hrs.)	3 Credit

Pre-requisite: Nil

Course Objective: To equip students with foundational knowledge and practical skills in ethical hacking and penetration testing, enabling them to understand attack vectors, identify system vulnerabilities, analyze social engineering threats, and apply appropriate tools and methodologies within a legal and ethical framework to enhance cybersecurity.

Course Contents: (40 hrs.)

Module 1: **(08hrs.)**

Ethical Hacking: Introduction, Networking & Basics, Foot printing and scanning: Information Gathering, Determining the Network Range, Identifying Active Machines, Finding Open Ports and Access Points, OS Fingerprinting Services, Mapping the Network Attack Surface. Google Hacking, Scanning, Windows Hacking, Linux Hacking.

Module 2: **(08hrs.)**

The Business Perspective: Business Objectives, Security Policy, Previous Test Results, Business Challenges Planning for a Controlled Attack: Inherent Limitations, Imposed Limitations, Timing is Everything, Attack Type, Source Point, Required Knowledge, Multi-Phased Attacks, Teaming and Attack Structure, Engagement Planner, The Right Security Consultant, The Tester, Logistics, Intermediates, Law Enforcement.

Module 3: **(08hrs.)**

Preparing for a Hack: Technical Preparation, Managing the Engagement Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance, Steganography, Cryptography, Wireless Hacking, Firewall & Honeypots, IDS & IPS, Vulnerability, Penetration Testing.

Module 4: **(08hrs.)**

Enumeration: Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase Exploitation: Intuitive Testing, Evasion, Threads and Groups, Operating Systems, Password Crackers, RootKits, applications, Wardialing, Network, ServicesDoS attacks and Areas of Concern.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

Module 5: **(08hrs.)**

Reverse Engineering: Email Hacking, Incident Handling & Response, Bluetooth Hacking, Mobile Phone Hacking Basic ethical hacking tools and usage of these tools in a professional environment. Legal, professional and ethical issues likely to face the domain of ethical hacking. Ethical responsibilities, professional integrity and making appropriate use of the tools and techniques associated with ethical hacking.

Course Outcome:

1. Describe and understand the basics of the ethical hacking and Gain the knowledge of the use and availability of tools to support an ethical hack.
2. Gain the knowledge of interpreting the results of a controlled attack.
3. Understand the role of politics, inherent and imposed limitations and metrics for planning of a test.
4. Perform the foot printing and scanning.
5. Demonstrate the techniques for system hacking and Detect and prevent the security attacks in different environments.

Text/Reference Books:

1. Certified Ethical Hacker, Version 9, Second Edition, Michael Gregg, Pearson IT Certification.
2. Hacking the Hacker, Roger Grimes, Wiley.
3. The Unofficial Guide to Ethical Hacking, Ankit Fadia, Premier Press.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

PEC-CB03(C)	**Bitcoin and Cryptocurrency Technology**	**2L:1T:0P (3hrs.)**	**3 Credit**

Pre-requisite:

Course Objective:
This course introduces students to cryptography and cryptocurrencies, focusing on Bitcoin's technology, its decentralized nature, and its various applications. Students will learn about cryptographic primitives**,** the security mechanisms behind Bitcoin, and the consensus protocols that make decentralized systems possible.

Course Contents: (40 hrs.)

Module 1: **(08hrs.)**
Introduction to Crypto and Cryptocurrencies: Cryptographic building blocks ("primitives") and reason about their security. Constructing Simple Cryptocurrencies, Decentralization in Bitcoin, Bitcoin's consensus mechanism and its security. Technical methods and clever incentive engineering. Mechanics of Bitcoin: Components of the Bitcoin protocol, transactions, script, blocks, and the peer-to-peer network, Different ways of storing Bitcoin keys, Security measures, and various types of services that allow trade and transact with bitcoins.

Module 2: **(08hrs.)**
Bitcoin Mining Who are the miners, Introduction to mining, Operations of mining and miners, Business model for miners, their have on the environment. Bitcoin and Anonymity: Concept of Bitcoin anonymity, improving Bitcoin's anonymity and privacy, Bitcoin's role in Silk Road and other hidden marketplaces.

Module 3: **(08hrs.)**
Community, Politics, and Regulation, Bitcoin and cryptocurrency technology touches the world of people, Community, politics within Bitcoin and the way that Bitcoin interacts with politics, and law enforcement and regulation issues.

Module 4: **(08hrs.)**
Alternative Mining Puzzles: Issues and problems with mining, energy consumption aspect,

Requirement of specialized hardware, how mining can be re-designed in alternative cryptocurrencies.

Module 5: **(08hrs.)**

Bitcoin as a Platform: Bitcoin potential to support applications other than currency. Properties of Bitcoin that makes this possible, Alternative cryptocurrencies, The Future of Bitcoin, The use of Bitcoin technology for decentralizing property, markets

Course Outcome:

1. Understand the foundational concepts of cryptography and cryptocurrencies, including the cryptographic building blocks, Bitcoin's decentralization, consensus mechanism, and security features.
2. Analyze Bitcoin mining, its business model, environmental impact, and understand the concept of Bitcoin anonymity and privacy.
3. Evaluate the intersection of Bitcoin and cryptocurrency technology with community, politics, law enforcement, and regulatory issues.
4. Assess the challenges and limitations of Bitcoin mining, including energy consumption and the need for specialized hardware, and explore alternative mining puzzles.
5. Explore Bitcoin's potential beyond currency, including its application as a decentralized platform for property and markets, and investigate the future of Bitcoin and alternative cryptocurrencies.

Text/Reference Books:

1. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.
2. Schar, F., & Berentsen, A. (2020). Bitcoin, Blockchain, and Cryptoassets: A Comprehensive Introduction. MIT press.
3. Cole Ruiz, Bitcoin and Cryptocurrency Technologies, 2022
4. Cliff Davison, Bitcoin and Cryptocurrency Technologies, 2022

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

PEC-CB03(D)	Cybercrime Intelligence and Threat Management	2L:1T:0P (3hrs.)	3 Credit

Pre-requisite: Nil.

Course Objective: This course introduces students to the basic elements of Cyber Security and its role in the real world, familiarizes them with various types of cyber-attacks and cyber-crimes, helps them understand the broad concepts of the technical, social, and legal aspects of Cyber Security and provides insights into the application of Cyber Security to resolve vulnerabilities and security problems.

Course Content: (40 Hrs)

Module 1: **(06hrs.)**

Introduction to Cyber Security

Overview of Cyber Security, Types of Vulnerability, Computer Criminals, CIA Triad, Cyber Threats:- Cyber Warfare-Cyber Crime-Cyber terrorism-Cyber Espionage.

Global Internet Governance – Challenges and Constraints, Need for a Comprehensive Cyber Security Policy, Need for a Nodal Authority, Need for an International convention on Cyberspace.

Module 2: **(08hrs.)**

Cyber Security Vulnerabilities and Cyber Security Assessments

Cyber Security Vulnerabilities-Overview, vulnerabilities in software and Hardware, Security system administration, Threats for Open Access to Organizational Data, Weak Authentication, Poor Cyber Security Awareness and Training.

Cyber Security Assessments- Overview, Access control, Audit, Authentication, Biometrics, Cryptography, Deception, Denial of Service Filters, Ethical Hacking, Firewalls, Intrusion Detection Systems, Response, Scanning, Security policy, Threat Management.

Module 3: **(10hrs.)**

Introduction to Cyber Crime and its implication on mobile and wireless devices

Cybercrime: Introduction to cyber-crime, intellectual property in the cyberspace, dimension of cybercrimes, mindset and skills of hackers and other cyber criminals.

Introduction to Cybercrime in Mobile and Wireless Devices, Proliferation of Mobile and Wireless Devices, Credit card Frauds in Mobile and Wireless Computing, Security Challenges in Mobile Devices and wireless devices, Types of Attacks on Mobile and wireless devices, Organizational Security Policies and Measures for securing Mobile and wireless devices.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

Module 4: **(06hrs.)**

Cyber Forensics

Introduction to Cyber Forensics, Handling Preliminary Investigations, Controlling an Investigation, Conducting disk-based analysis, Investigating Information-hiding, Scrutinizing E-mail, Validating E-mail header information, Tracing Internet access, Tracing memory in real-time.

Module 5: **(10hrs.)**

Forensic Tools and Processing of Electronic Evidence

Introduction to Forensic Tools, Usage of Slack space, tools for Disk Imaging, Data Recovery, Vulnerability Assessment Tools, Encase and FTK tools, Anti Forensics and probable counters, retrieving information, process of computer forensics and digital investigations, processing of digital evidence, digital images, damaged SIM and data recovery, multimedia evidence, retrieving deleted data: desktops, laptops and mobiles, retrieving data from slack space, renamed file, ghosting, compressed files.

Course Outcome:

1. Describe the basic elements of Cyber Security and its role in real world with operational and organizational security Aspects
2. Understand various cyber-attacks, types of cybercrimes and cyber laws
3. To protect oneself from cyber-attacks and ultimately and understanding of securing entire Internet community from such attacks
4. Comprehend the purpose of Cyber Crime and its implication on mobile and wireless devices.
5. Understand the basics of computer forensics.

Text/Reference Books:

1. W.A.Coklin, G.White, Principles of Computer Security: Fourth Edition, McGraw Hill, 2016
2. Anand Shinde, Introduction to Cyber Security: Guide to the World of Cyber Security, 2021.
3. John Vacca, Computer Forensics: Computer Crime Scene Investigation, 2015
4. Cyber Forensics by Dejey & S. Murugan, OXFORD UNIVERSITY PRES, 2018
5. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press, First Edition, 2016.
6. Introduction to Cyber Security, Chwan-Hwa(john) Wu,J. David Irwin, CRC Press T & F Group, 2013
7. Fundamentals of Forensic Science, Manjugouda R Patil, Dr.C.F.Mulimani, First Edition. 2020

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

IOC-CB02(C)	Digital Marketing & SEO	3L:0T:0P (3hrs.)	3 Credit

Pre-requisite:

Course Objective: The objective of subject is to facilitate students to understand digital marketing and its importance.

Course Contents: (40 hrs.)

Module 1: (06 hrs)
Digital Marketing: Introduction, Moving from Traditional to Digital Marketing, Integrating Traditional and Digital Marketing, Reasons for Growth. Need for a comprehensive Digital Marketing Strategy. Concepts: Search Engine Optimization (SEO); Concept of Pay Per Click

Module 2: (08 hrs)
Social Media Marketing: Introduction, Process - Goals, Channels, Implementation, Analyze. Tools: Google and the Search Engine, Facebook, Twitter, YouTube and LinkedIn. Issues: Credibility, Fake News, Paid Influencers; Social Media and Hate/ Phobic campaigns. Analytics and linkage with Social Media. The Social Community.

Module 3: (10 hrs)
Email Marketing: Introduction, email marketing process, design and content, delivery, discovery. Mobile Marketing: Introduction and concept, Process of mobile marketing: goals, setup, monitor, analyze; Enhancing Digital Experiences with Mobile Apps. Pros and Cons; Targeted advertising. Issues: Data Collection, Privacy, Data Mining, Money and Apps, Security, Spam. Growth Areas.

Module 4: (06hrs)
Managing Digital Marketing: Content Production; Video based marketing; Credibility and Digital Marketing; IoT; User Experience; Future of Digital Marketing.

Module 5: (10 hrs)
SEO Analytics, Monitoring & Reporting : Google Search Console (GSC), Key Sections & Features of GSC; How to monitor SEO progress with Key Features of GSC: Overview, Performance, URL Inspection, Coverage, Sitemaps, Speed, Mobile Usability, Backlinks, Referring Domains, Security & Manual Actions, How to do SEO Reporting.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

Course Outcome:

1. Understand the concept of digital marketing and its real-world iterations.
2. Articulate innovative insights of digital marketing enabling a competitive edge.
3. Understand how to create and run digital media based campaigns.
4. Identify and utilize various tools such as social media etc.
5. Understand how to do SEO Audit.

List of Text / Reference Books:

1. Dodson, Ian, "The Art of Digital Marketing - The Definitive Guide to Creating Strategic", Targeted, and Measurable Online Campaigns. Wiley, 2016.
2. Ryan, Damien, "Understanding Digital Marketing - Marketing Strategies for Engaging the Digital Generation", Kogan Page Limited, 2008.
3. Gupta, Sunil, "Driving Digital Strategy" Harvard Business Review Press, 2018.
4. Tuten, Tracy L. and Solomon, Michael R. "Social Media Marketing", Sage, 3rd edition 2017.
5. Bhatia, Puneet S." Fundamentals of Digital Marketing", Pearson, 2nd edition, 2019.
6. Kotler, Philip "Marketing 4.0: Moving from Traditional to Digital", Wiley, 1st edition, 2017.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

LC-CB15(P)	Cloud Computing Lab	0L:0T:2P (2hrs.)	1 Credit

Pre-requisite: Nil

Course Objective: The objective of this course is to provide hands-on experience with cloud platforms, virtualization, storage integration, cloud security, and performance monitoring, enabling students to design, deploy, and manage cloud-based solutions effectively.

Course Contents: (20hrs)

Module 1: **(04hrs.)**
Introduction to Cloud and Service Models- Overview of cloud computing: Characteristics, models, and benefits, Introduction to cloud platforms: AWS, Azure, and Google Cloud, Hands-on with instance creation (EC2, Azure VM), Practical understanding of SaaS, PaaS, IaaS with real-life use cases.

Module 2: **(04hrs.)**
Virtualization and VM Management- Fundamentals of virtualization: Definition, need, and benefits, Introduction to hypervisors: Type 1 vs Type 2 (e.g., Xen, VirtualBox), Installation and configuration of VMs using VirtualBox/Vmware.

Module 3: **(04hrs.)**
Cloud Storage and Data Access- Understanding cloud storage models: Object vs block vs file storage, Integrating APIs: Google Drive API / Dropbox API for data access, Practical implementation of cloud-based data access in apps, Overview of Virtual Desktop Infrastructure (VDI), Setting up and accessing VDI environments (using AWS WorkSpaces or simulation).

Module 4: **(04hrs.)**
Security and Identity Management in Cloud- Basics of cloud security: Threats, vulnerabilities, and attack surfaces, Identity and Access Management (IAM): Roles, policies, permissions, Hands-on with AWS IAM or Azure Active Directory.

Module 5: **(04hrs.)**
Monitoring and Performance Optimization- Importance of monitoring in cloud environments, Introduction to AWS CloudWatch, Azure Monitor, GCP Operations, Resource usage monitoring: CPU, memory, disk, network, Real-time alerting, logs, and metrics dashboard.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

Course Outcome:

1. Demonstrate understanding of cloud computing fundamentals and effectively deploy instances on major cloud platforms such as AWS, Azure, and Google Cloud.
2. Configure and manage virtual machines and hypervisors, and apply virtualization techniques for efficient resource utilization.
3. Implement cloud storage solutions and integrate APIs for data access, including deploying and managing virtual desktop infrastructure.
4. Apply cloud security concepts using identity and access management tools, and perform vulnerability assessments using standard security tools.
5. Monitor and analyze cloud resource performance using platform-specific tools, and implement optimization strategies for efficient cloud operations.

List of Text/ Reference Books:

1. Dr.Kumar Saurabh, Cloud Computing", Wiley India.
2. Ronald Krutz and Russell Dean Vines,"Cloud Security", Wiley-India.
3. Judith Hurwitz, R.Bloor, M.Kanfman, F.Halper,"Computing for Dummies", Wiley India Edition.
4. Anthony T.Velte Toby J.Velte, Cloud Computing A Practical Approach", TMH.
5. Barrie Sosinsky, Cloud Computing Bible", Wiley India.

List of Experiments:

1. Install Virtualbox / VMware Workstation with different flavours of linux or windows OS on top of windows7 or 8.
2. Install a C compiler in the virtual machine created using virtual box and execute Simple Programs
3. Install Google App Engine. Create hello world app and other simple web applications using python/java.
4. Install Google App Engine. Create hello world app and other simple web applications using Eclipse
5. Create, Deploy and Launch Virtual Machines in Openstack.
6. Use GAE launcher to launch the web applications.
7. Simulate a cloud scenario using CloudSim and run a scheduling algorithm that is not present in CloudSim.
8. Find a procedure to transfer the files from one virtual machine to another virtual machine.
9. Find a procedure to launch virtual machine using trystack (Online Openstack Demo Version)
10. Install Hadoop single node cluster and run simple applications like wordcount.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

LC-PEC-CB03(P)	Soft Computing Lab	0L:0T:2P (2hrs.)	1 Credit

Pre-requisite: Analysis and Design of Algorithm

Course Objective: The objective of this course is to introduce the fundamentals of neural networks, fuzzy logic, and evolutionary algorithms, emphasizing their models, learning methods, and applications. The course aims to develop understanding of supervised and unsupervised learning, CNNs, RNNs, fuzzy systems, and optimization techniques like GA, ACO, and PSO for solving real-world problems.

Course Contents: (20 hrs.)

Module 1: **(04 hrs.)**
Introduction to Neural Network: Concept, biological neural network, Types of learning, Linear separability, XOR problem, McCulloch-Pitts neuron model, Hebb rule.

Module 2: **(04hrs.)**
Supervised Learning: Application of Neural network in forecasting, data compression and image compression.

Module 3: **(04hrs.)**
Unsupervised learning, Introduction to Convolutional neural networks (CNN) and Recurrent neural networks (RNN)**.**

Module 4: **(04hrs.)**
Fuzzy Set: Introduction, Basic Definition and Terminology, Properties and Set-theoretic Operations, Fuzzy Relations, Application of Fuzzy logic in solving engineering problems.

Module 5: **(04hrs.)**
Genetic Algorithm: Introduction to GA, Simple Genetic Algorithm, Introduction to Ant Colony optimization (ACO) and Particle swarm optimization (PSO).

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

Course Outcomes:

1. State basic concept of Neural Network
2. Illustrate various concepts supervised learning, data and image compression
3. Describe the concept of unsupervised learning.
4. Apply fuzzy logic concepts to solve real world problem.
5. Design and implement the real world problem through Genetic algorithm

List of Text / Reference Books:

1. S.N. Shivnandam, “Principle of soft computing”, Wiley.
2. S. Rajshekaran and G.A.V. Pai, “Neural Network , Fuzzy logic And Genetic Algorithm”, PHI.
3. Jack M. Zurada, “Introduction to Artificial Neural Network System” JAico Publication.
4. Simon Haykins, “Neural Network- A Comprehensive Foundation”
5. Timothy J.Ross, “Fuzzy logic with Engineering Applications”, McGraw-Hills.

List of Experiments:

1. Form a perceptron net for basic logic gates with binary input and output.
2. Using Adaline net, generate XOR function with bipolar inputs and targets.
3. Calculation of new weights for a Back propagation network, given the values of input pattern, output pattern, target output, learning rate and activation function.
4. Design fuzzy inference system for a given problem.
5. Maximize the function y =3x2 + 2 for some given values of x using Genetic algorithm.
6. Implement Travelling salesman problem using Genetic Algorithm.
7. Optimisation of problem like Job shop scheduling using Genetic algorithm

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

LC-PEC-CB03(P)	Ethical Hacking Lab	0L:0T:2P (2hrs.)	1 Credit

Pre-requisite: Nil

Course Objective: To equip students with foundational knowledge and practical skills in ethical hacking and penetration testing, enabling them to understand attack vectors, identify system vulnerabilities, analyze social engineering threats, and apply appropriate tools and methodologies within a legal and ethical framework to enhance cybersecurity.

Course Contents: (20 hrs.)

Module 1: **(04hrs.)**
Introduction to Ethical Hacking, Footprinting and Scanning: Information gathering Identifying open ports, OS fingerprinting, Google Hacking, Windows and Linux basics for hacking

Module 2: **(04hrs.)**
Understanding security policies and limitations, Planning for a controlled attack, Types of attacks: DoS, Role of a security consultant and tester (basic overview)

Module 3: **(04hrs.)**
Reconnaissance techniques: Social engineering, Internet reconnaissance, Introduction to steganography and cryptography, Introduction to Honeypots, Basics of penetration testing

Module 4: **(04hrs.)**
Enumeration Techniques, Exploitation Concepts: Password cracking, Rootkits, Web-based attacks, Session hijacking (conceptual)

Module 5: **(04hrs.)**
Introduction to Reverse Engineering (basic exposure), Email Hacking concepts, Mobile & Bluetooth, Hacking (brief overview), Commonly used hacking tools, Ethical, legal, and professional responsibilities

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

Course Outcome:

1. Describe and understand the basics of the ethical hacking and Gain the knowledge of the use and availability of tools to support an ethical hack.
2. Gain the knowledge of interpreting the results of a controlled attack.
3. Understand the role of politics, inherent and imposed limitations and metrics for planning of a test.
4. Perform the foot printing and scanning.
5. Demonstrate the techniques for system hacking and Detect and prevent the security attacks in different environments.

Text/Reference Books:

1. Certified Ethical Hacker, Version 9, Second Edition, Michael Gregg, Pearson IT Certification.
2. Hacking the Hacker, Roger Grimes, Wiley.
3. The Unofficial Guide to Ethical Hacking, Ankit Fadia, Premier Press

List of Experiments:

1. List the tools for Ethical Hacking.
2. Implement Foot-printing and Reconnaissance using tools.
3. Setup a honey pot and monitor the honey pot on network.
4. Create a social networking website login page using phishing techniques.
5. Write a code to demonstrate DoS attacks.
6. Install rootkits and study variety of options.
7. Study of Techniques uses for Web Based Password Capturing.
8. Implement passive scanning, active scanning, session hijacking, cookies extraction using Burp suit tool.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

LC-PEC-CB03(P)	**Bit Coin & Cryptocurrency Technology Lab**	**0L:0T:2P (2hrs.)**	**1 Credit**

Pre-requisite:

Course Objective: To equip students with foundational knowledge and practical skills in blockchain technology, focusing on cryptographic principles, consensus mechanisms, privacy, regulation, and hands-on cryptocurrency transaction and smart contract development.

Course Contents: (20 hrs.)

Module 1: **(04hrs.)**
Cryptographic Foundation: Hashing with SHA-256 using Python, Encryption: AES & RSA (PyCryptodome), Public/private key generation and digital signing (ECDSA)

Module 2: **(04hrs.)**
Blockchain Mechanisms & Privacy: Proof-of-Work simulation, Mining logic and nonce handling, Bitcoin anonymity and transaction tracing using explorers.

Module 3: **(04hrs.)**
Case Studies & Regulation: Study of Silk Road or similar incidents, International regulatory approaches (overview).

Module 4: **(04hrs.)**
Consensus Models & Energy Use: Comparison of PoW and PoS (Ethereum testnet demo), Mining calculators and energy simulation.

Module 5: **(04hrs.)**
Transactions & Smart Contracts: Create & broadcast Bitcoin Testnet transactions, Deploy basic smart contracts or tokens, Intro to Hyperledger: chaincode interaction and query.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

Course Outcome:

1. Apply cryptographic techniques to secure digital transactions using tools like Python and ECDSA.
2. Simulate blockchain mechanisms such as Proof-of-Work mining and transaction validation.
3. Analyze privacy, anonymity, and traceability in cryptocurrency systems using blockchain explorers.
4. Evaluate legal and regulatory frameworks governing cryptocurrency across different jurisdictions.
5. Demonstrate hands-on skills in creating, broadcasting, and scripting cryptocurrency transactions and deploying smart contracts.

Text/Reference Books:

1. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.
2. Schar, F., & Berentsen, A. (2020). Bitcoin, Blockchain, and Cryptoassets: A Comprehensive Introduction. MIT press.
3. Cole Ruiz, Bitcoin and Cryptocurrency Technologies, 2022
4. Cliff Davison, Bitcoin and Cryptocurrency Technologies, 2022

List of Experiments:

1. Implement basic cryptographic primitives and hash functions using Python (SHA-256, AES /RSA).
2. Simulate a simple cryptocurrency transaction using ECDSA for signing.
3. Simulate Proof-of-Work (PoW) mining with nonce and difficulty target.
4. Trace transactions using blockchain explorers and analyze anonymity (e.g., CoinJoin).
5. Case study on Bitcoin regulation (e.g., Silk Road, country-wise policies).
6. Compare PoW with PoS through simulation and study mining resource consumption.
7. Create and broadcast a transaction on the Bitcoin Testnet using bitcoin-cli or Electrum.
8. Deploy a basic smart contract or token on a compatible testnet.
9. Interact with a blockchain network using Hyperledger Fabric (invoke/query chaincode).
10. Develop a simple blockchain-based app for asset transfer or reward tracking.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

LC-PEC-CB03(P)	Cybercrime Intelligence and Threat Management Lab	0L:0T:2P (2hrs.)	1 Credit

Pre-requisite:

Course Objective: The main objectives of this course is

1. To gain hands-on experience in identifying cyber vulnerabilities and investigating cybercrime.
2. To use security tools for digital forensics, vulnerability assessments, and threat detection.
3. To understand and simulate real-world cyber-attacks and forensic responses.

Course Contents: (20 hrs.)

Module 1: **(04hrs.)**
Introduction to Cyber Security- CIA Triad, current global cyber threats (e.g., ransomware, cyber espionage), threat intelligence websites (like Kaspersky ThreatMap or VirusTotal).

Module 2: **(04hrs.)**
Vulnerabilities and Security Assessment- **v**ulnerability scanning (Nmap, Nikto), Basic password cracking and firewall rule setup, Intrusion detection using Snort

Module 3: **(04hrs.)**
Cyber Crime and Mobile Threats- Phishing & social engineering simulation, Wi-Fi sniffing using, Wireshark, Mobile malware scenario (conceptual demo).

Module 4: **(04hrs.)**
Cyber Forensics- Disk imaging and deleted file recovery (FTK Imager / Autopsy / Recuva), Email header and browser artifact analysis.

Module 5: **(04hrs.)**
Mini Project / Case Study- real-world cybercrime case (e.g., Sony hack, Pegasus spyware), forensic report, ransomware attack in a controlled virtual lab and data recovery, threat detection and alert system using Python and basic machine learning.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

Course Outcome:

1. Demonstrate understanding of cyber security fundamentals by analyzing the CIA triad and evaluating global cyber threats using real-time intelligence tools.
2. Conduct vulnerability assessments using industry-standard tools to identify system and network weaknesses and simulate intrusion detection mechanisms.
3. Analyze and simulate cybercrime scenarios including phishing, social engineering, and mobile threats, and document forensics response strategies.
4. Apply digital forensic techniques to recover and investigate digital evidence from various media and perform comprehensive forensic analysis.
5. Develop practical solutions to real-world cyber threats through case studies, simulations, and mini projects involving threat detection and mitigation techniques.

Text/Reference Books:

1. William Stallings, "Network Security Essentials: Applications and Standards", Pearson Education.
2. Chuck Easttom, "Computer Security Fundamentals", Pearson.
3. Nelson, Phillips, and Steuart, "Guide to Computer Forensics and Investigations", Cengage Learning.

List of Experiments:

1. Demonstrate the CIA Triad with real-world examples and use threat intelligence platforms.
2. Perform vulnerability scanning using Nmap and Nikto.
3. Execute password cracking with John the Ripper or Hashcat in a lab setup.
4. Configure a basic firewall rule set and simulate intrusion detection using Snort.
5. Simulate a phishing attack using SET (Social Engineering Toolkit).
6. Capture Wi-Fi packets using Wireshark and identify sniffed data.
7. Perform disk imaging and deleted file recovery using FTK Imager / Recuva.
8. Analyze a mobile malware scenario and prepare a forensics response report.
9. Investigate a real-world cybercrime case and create a brief forensic summary.
10. Build a basic Python-based threat detection or alert system (mini project).

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

PROJ-CB04	Project-II	0L:0T:8P (8hrs.)	4 Credit

Pre-requisite: Knowledge of subjects of respective stream.

Course Objective: To develop ability in the students to apply some of the theoretical concepts and programming knowledge, in real life engineering problems.

Course outcome:

1. Acquire practical knowledge within the chosen area of technology for project development.
2. Identify, analyze and handle programming projects with a comprehensive and systematic approach.
3. Contribute as an individual or in a team in development of technical projects.
4. Develop effective communication skills for presentation of project related activities.
5. Formulate and propose a plan for creating a solution for the problems identified.
6. Report and present the finding of the study conducted in the preferred domain.

IPS Academy, Institute of Engineering & Science

(A UGC Autonomous Institute, Affiliated to RGPV, Bhopal)
Scheme Based on AICTE Flexible Curriculum

Department of Computer Science & Engineering

Bachelor of Technology (B.Tech.)

Computer Science & Engineering (IOT and Cyber Security Including Block Chain Technology) (CSITCS)

VII Semester

PROJ-CB05	**Evaluation of Internship-II**	**0L:0T:6P (6hrs.)**	**3 Credits**

Prerequisite: Nil.

Course Objective:
The primary purpose of doing an academic internship is to better understand the theories, ideas, and practices of discipline or major by actively engaging in a "hands-on," work-based, learning experience.

Course Outcome: On successful completion of the course, the student will be able to:

1. To explore career alternatives prior to graduation.
2. To develop communication, interpersonal and other critical skills in the job interview process.
3. To Assess interests and abilities in their field of study.
4. To Identify, write down, and carry out performance objectives related to their job assignment
5. To Integrate theory and practice.