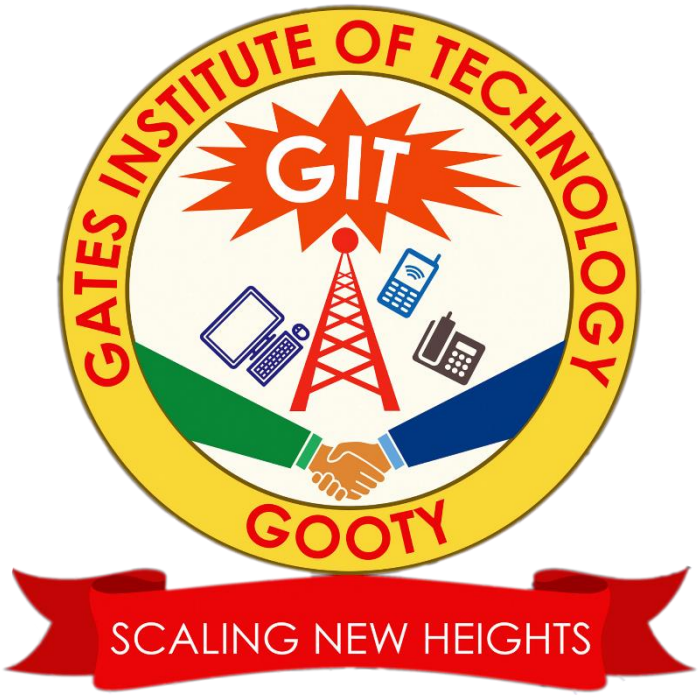


Gates Institute of Technology
(UGC Autonomous)
Gooty, Ananthapuramu Dist. – 515 002 (AP) India

==========

B. Tech (Regular-Full time)

(Effective for the students admitted into I B.Tech from the Academic B.Tech 2023-24 onwards)

CSE – CYBER SECURITY

COURSE STRUCTURE

&

SYLLABUS

IV B.Tech I Semester (CSE-Cyber Security)

S.No.	Course Code	Title	L	T	P	Credits
1	23CST29b	Blockchain Technology	3	0	0	3
2	23MBTU4a 23MBTU4a 23MBTU4a	**Management Course- II** 1. Business Ethics and Corporate Governance 2. E-Business 3. Management Science	2	0	0	2
3	23CST29a 23CYT04a 23CST24 23CYT04b 23CST23e	**Professional Elective - IV** 1. Software Architecture & Design Patterns 2. Network Management Systems and Operations 3. Deep Learning 4. Malware Analysis & Reverse Engineering 5. Agentic AI Engineering	3	0	0	3
4	23CST29c 23CYT05a 23CST30b 23CYT05b 23CST30d	**Professional Elective –V** 1. Augmented Reality and Virtual Reality 2. Intrusion Detection and Prevention System 3. Metaverse 4. Cyber Laws and Security Policies 5. AI Powered Application Development	3	0	0	3
5		**Open Elective-III**	3	0	0	3
6		**Open Elective-IV**				3
7	23CYP05	**Skill Enhancement Course** Ethical Hacking	0	1	2	2
8	23CST39	**Audit Course** Gender Sensitization	2	0	0	-
9	23CSEII	Evaluation of Industry Internship	-	-	-	2
		Total	**16**	**1**	**02**	**21**

Open Elective – III

S.No	Course Code	Course Name	Offered by the Dept.
1	23CET24	Building Materials and Services	CIVIL
2	23CET25	Environmental Impact Assessment	
3	23EET22	Smart Grid Technologies	EEE
4	23MET23	3D Printing Technologies	ME
5	23ECT12	Microprocessors and Microcontrollers	ECE
6	23BST30	Wavelet transforms and its Applications	Mathematics
7	23BST31	Smart Materials And Devices	Physics
8	23BST34	Introduction to Quantum Mechanics	
9	23BST32	Green Chemistry And Catalysis For Sustainable Environment	Chemistry
10	23BST33	Employability Skills	Humanities

IV B.Tech I Semester

Open Elective – IV

S.No	Course Code	Course Name	Offered by the Dept.
1	23CET26	Geo-Spatial Technologies	CIVIL
2	23CET27	Solid Waste Management	
3	23EET25	Electric Vehicles	EEE
4	23MET24	Total Quality Management	ME
5	23ECT29	Transducers and Sensors	ECE
6	23BST35	Introduction to Quantum Computing	CSE & Allied
7	23BST36	Financial Mathematics	Mathematics
8	23BST37	Sensors And Actuators For Engineering Applications	Physics
9	23BST38	Chemistry Of Nanomaterials and Applications	Chemistry
10	23CET26	Literary Vibes	Humanities
11	23BST40	Advance Aptitude & Critical Thinking	Mathematics

IV B.Tech II Semester (CSE-Cyber Security)

S.No.	Course code	Title	Category	L	T	P	Credits
1	23CSIAP	Internship		-	-	-	4
2		Project		-	-	-	8
Total							**12**

IV B.Tech I Semester

23CST29b	BLOCK CHAIN TECHNOLOGY	L	T	P	C
		3	0	0	3

Course Objectives:

- Understand how block chain systems (mainly Bit coin and Ethereum) work and to securely interact with them.
- Design, build, and deploy smart contracts and distributed applications.
- Integrate ideas from block chain technology into their own projects.

Course Outcomes (CO):

After completion of the course, students will be able to

1. Demonstrate the foundation of the Block chain technology and understand the processes in payment and funding.
2. Identify the risks involved in building Block chain applications.
3. Review of legal implications using smart contracts.
4. Choose the present landscape of Blockchain implementations and Understand Crypto currency markets
5. Examine how to profit from trading crypto currencies.

UNIT - I Introduction Lecture 8Hrs

Introduction, Scenarios, Challenges Articulated, Block chain, Block chain Characteristics, Opportunities Using Block chain, History of Block chain. Evolution of Block chain: Evolution of Computer Applications, Centralized Applications, Decentralized Applications, Stages in Block chain Evolution, Consortia, Forks, Public Block chain Environments, Type of Players in Block chain Ecosystem, Players in Market.

UNIT - II Block chain Concepts Lecture 9Hrs

Block chain Concepts: Introduction, Changing of Blocks, Hashing, Merkle-Tree, Consensus, Mining and Finalizing Blocks, Currency aka tokens, security on block chain, data storage on block chain, wallets, coding on block chain: smart contracts, peer-to-peer network, types of block chain nodes, risk associated with bloc chain solutions, life cycle of block chain transaction.

UNIT - III Architecting Block chain solutions Lecture 9Hrs **Architecting**

Block chain solutions: Introduction, Obstacles for Use of Block chain, Block chain Relevance Evaluation Framework, Block chain Solutions Reference Architecture, Types of Block chain Applications. Cryptographic Tokens, Typical Solution Architecture for Enterprise Use Cases, Types of Block chain Solutions, Architecture Considerations, Architecture with Block chain Platforms, Approach for Designing Block chain Applications.

UNIT - IV Ethereum Block chain Implementation Lecture 8Hrs

Ethereum Block chain Implementation: Introduction, Tuna Fish Tracking Use Case, Ethereum Ecosystem, Ethereum Development, Ethereum Tool Stack, Ethereum Virtual Machine, Smart Contract Programming, Integrated Development Environment, Truffle Framework, Ganache, Unit Testing, Ethereum Accounts, My Ether Wallet, Ethereum Networks/Environments, Infura, Ether scan, Ethereum Clients, Decentralized Application, Metamask, Tuna Fish Use Case Implementation, Open Zeppel in Contracts .

UNIT - V Hyper ledger Block chain Implementation Lecture 8Hrs

Hyper ledger Implementation: Introduction, Use Case – Car Ownership Tracking, Hyper ledger Fabric, Hyper ledger Fabric Transaction Flow, FabCar Use Case Implementation, Invoking Chain code Functions Using Client Application.

Advanced Concepts in Block chain: Introduction, Inter Planetary File System (IPFS), Zero Knowledge Proofs, Oracles, Self-Sovereign Identity, Block chain with IoT and AI/ML Quantum Computing and Block chain, Initial Coin Offering, Block chain Cloud Offerings, Block chain and its Future Potential.

Textbooks:

1. Ambadas, Arshad Sarfarz Ariff, Sham "Block chain for Enterprise Application Developers", Wiley, 2020
2. Andreas M. Antonopoulos, "Mastering Bitcoin: Programming the Open Blockchain", O'Reilly, 2017

Reference Books:

1. Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions, Joseph Bambara, Paul R. Allen, Mc Graw Hill.
2. Blockchain: Blueprint for a New Economy, Melanie Swan, O'Reilly

Online Learning Resources:

https://github.com/blockchainedindia/resources

Course Code		L	T	P	C
23MBTU4a	**NESS ETHICS AND CORPORATE GOVERNANCE**	**2**	**0**	**0**	**2**
	Semester	**IV-I**			

Course Objectives:

1. To make the student understand the principles of business ethics
2. To enable them in knowing about the ethics in management
3. To facilitate the student role in corporate culture
4. To impart knowledge about the fair-trade practices
5. To encourage the student in knowing about the corporate governance

Course Outcomes (CO): Student will be able to

- Understand the Ethics and different types of Ethics.
- Understand business ethics and ethical practices in management
- Understand the role of ethics in management
- Apply the knowledge of professional ethics & technical ethics
- Analyze corporate law, ethics, codes & principles
- Evaluate corporate governance & corporate scams.

UNIT-I		Lecture Hrs: 7

Introduction – Meaning – Nature, Scope, significance, Loyalty, and ethical behavior.. Value systems - Business Ethics - Types, Characteristics, Factors, Contradictions and Ethical Practices in Management -Corporate Social Responsibility – Issues of Management – Crisis Management.

UNIT-II		Lecture Hrs: 7

Introduction- Ethics in production, finance, Human resource management and Marketing Management - The Ethical Value System – Universalism, Utilitarianism, Distributive Justice, Social Contracts, Individual Freedom of Choice, Professional Codes; Culture and Ethics – Ethical Values in different Cultures - Culture and Individual Ethics – professional ethics and technical ethics.

UNIT-III		Lecture Hrs: 7

Introduction - Meaning, definition, Nature, and significance – Key elements of corporate culture, shared values, beliefs and norms, rituals, symbols and language - Types of corporate culture, hierarchical culture, market driven culture – Organization leadership and corporate culture, leadership styles and their impact on culture, transformational leadership and culture change.

UNIT-IV		Lecture Hrs: 7

Law and Ethics -Agencies enforcing Ethical Business Behavior - Legal Impact – Environmental Protection, Fair Trade Practices, legal Compliances, Safeguarding Health and wellbeing of Customers – Corporate law, Securities and financial regulations, corporate governance codes and principles.

UNIT-V		Lecture Hrs: 7

Introduction - Meaning – Corporate governance code, transparency & disclosure -Role of auditors, board of directors and shareholders. Global issues, accounting and regulatory frame work - Corporate scams - Committees in India and abroad, corporate social responsibility. BoDs composition, Cadbury Committee - Various committees - Reports - Benefits and Limitations.

Textbooks:
1. Murthy CSV: Business Ethics and Corporate Governance, HPH July 2017 2. Bholananth Dutta, S.K. Podder – Corporation Governance, VBH. June 2010
Reference Books:
1. Dr. K. Nirmala, KarunakaraReaddy. Business Ethics and Corporate Governance, HPH 2. H.R.Machiraju: Corporate Governance, HPH, 2013 3. K. Venkataramana, Corporate Governance, SHBP. 4. N.M.Khandelwal. Indian Ethos and Values for Managers

Course Code	**E-BUSINESS**	**L**	**T**	**P**	**C**
23MBTU4b		**2**	**0**	**0**	**2**
	Semester	**IV-I**			

Course Objectives:

1. To provide knowledge on emerging concept on E-Business related aspect.
2. To understand various electronic markets & business models.
3. To impart the information about electronic payment systems & banking.
4. To create awareness on security risks and challenges in E-commerce.
5. To the students aware on different e-marketing channels & strategies.

Course Outcomes (CO): Student will be able to

- Remember E-Business & its nature, scope and functions.
- Understand E-market-Models which are practicing by the organizations
- Apply the concepts of E-Commerce in the present globalized world.
- Analyze the various E-payment systems & importance of net banking.
- Evaluate market research strategies & E-advertisements.
- Understand importance of E-security & control.

UNIT-I		Lecture Hrs: 7

Introduction – Nature, meaning, significance, functions and advantages - Definition of Electronic Business - Functions of Electronic Commerce (EC)-Advantages & Disadvantages of E-Commerce –E-Commerce and E-Business, Internet Services, Online Shopping- E-Commerce Opportunities for Industries.

UNIT-II		Lecture Hrs: 7

Introduction –E-Shops-E-Malls E-Groceries - Portals - Vertical Portals-Horizontal Portals - Advantages of Portals - Business Models- Business to Business (B2B)-Business to Customers(B2C) - Business to Government(B2G)-AuctionsB2B Portals in India

UNIT-III		Lecture Hrs: 7

Introduction to electronic payment systems (EPS) -Types of electronic payments - Credit/debit cards, e-wallets, UPI, and crypto currencies -Smart cards and digital wallets: Features and usage -Electronic Fund Transfer (EFT): Role in business transactions -Infrastructure requirements and regulatory aspects of e-payments

UNIT-IV		Lecture Hrs: 7

Security risks and challenges in electronic commerce - Cyber threats - Phishing, hacking, identity theft, and malware - Digital Signatures & Certificates - Security protocols over public networks (HTTP, SSL, TLS) -Firewalls in securing ebusiness platforms.

UNIT-V		Lecture Hrs: 7

Introduction – Online Marketing – Advantages of Online Marketing – Internet Advertisement – Advertisement Methods – Conducting Online Market Research– – E-marketing planning: Online branding, social media marketing, and email marketing - E-business strategies: Digital advertising, content marketing, and analytics – E-Customer Relationship Management (eCRM) E-supply chain management (e-SCM)

Textbooks:

1. Arati Oturkar & Sunil Khilari. E-Business. Everest Publishing House, 2022
2. P.T.S Joseph. E-Commerce, Fourth Edition, Prentice Hall of India, 2011

Reference Books:
Reference Books: 1. Debjani, Kamalesh K Bajaj. E-Commerce, Second Edition Tata McGraw-Hill's, 2005 2. Dave Chaffey.E-Commerce E-Management, Second Edition, Pearson, 2012. 3. Henry Chan. E-Commerce Fundamentals and Application, RaymondLeathamWiley India 2007 4. S. Jaiswal. E-Commerce GalgotiaPublication Pvt Ltd., 2003.

IV B.Tech I Semester

Course Code	MANAGEMENT SCIENCE	L	T	P	C
23MBTU4c		**2**	**0**	**0**	**2**
	Semester	**IV-I**			

Course Objectives:

1. To provide fundamental knowledge on Management, Administration, Organization & its concepts.
2. To make the students understand the role of management in Production
3. To impart the concept of HRM in order to have an idea on Recruitment, Selection, Training & Development, job evaluation and Merit rating concepts
4. To create awareness on identify Strategic Management areas & the PERT/CPM for better Project Management
5. To make the students aware of the contemporary issues in modern management

Course Outcomes (CO): Student will be able to

- Remember the concepts & principles of management and designs of organization in a practical world
- Understand the knowledge of Work-study principles & Quality Control techniques in industry
- Apply the process of Recruitment & Selection in organization.
- Analyze the concepts of HRM & different training methods.
- Evaluate PERT/CPM Techniques for projects of an enterprise and estimate time & cost of project & to analyze the business through SWOT.
- Create awareness on contemporary issues in modern management & technology.

UNIT-I		Lecture Hrs: 7

Management - Concept and meaning - Nature-Functions - Management as a Science and Art and both. Schools of Management Thought - Taylor‘s Scientific Theory-Henry Fayol‘s principles - Elton Mayo‘s Human relations - Organizational Designs - Line organization - Line & Staff Organization - Functional Organization - Matrix Organization - Project Organization - Committee form of Organization - Social responsibilities of Management.

UNIT-II		Lecture Hrs: 7

Principles and Types of Plant Layout - Methods of Production (Job, batch and Mass Production), Work Study - Statistical Quality Control- Material Management - Objectives - Inventory-Functions - Types, Inventory Techniques - EOQ-ABC Analysis - Marketing Management - Concept - Meaning - Nature-Functions of Marketing - Marketing Mix - Channels of Distribution - Advertisement and Sales Promotion - Marketing Strategies based on Product Life Cycle.

UNIT-III		Lecture Hrs: 7

HRM - Definition and Meaning – Nature - Managerial and Operative functions - Job Analysis - Human Resource Planning(HRP) - Employee Recruitment-Sources of Recruitment - Employee Selection - Process - Employee Training and Development - methods - Performance Appraisal Concept - Methods of Performance Appraisal – Placement - Employee Induction - Wage and Salary Administration.

UNIT-IV		Lecture Hrs: 7

Definition& Meaning - Setting of Vision - Mission - Goals - Corporate Planning Process - Environmental Scanning - Steps in Strategy Formulation and Implementation - SWOT Analysis - Project Management - Network Analysis - Programme Evaluation and Review Technique (PERT)

- Critical Path Method (CPM) Identifying Critical Path - Probability of Completing the project within given time - Project Cost- Analysis - Project Crashing (Simple problems).		
UNIT-V		Lecture Hrs: 7
Customer Relations Management(CRM) - Total Quality Management (TQM) - Six Sigma Concept - Supply Chain Management(SCM) - Enterprise Resource Planning (ERP) - Performance Management – employee engagement and retention - Business Process Re-engineering and Bench Marking - Knowledge Management – change management – sustainability and corporate social responsibility.		
Textbooks:		
1. Frederick S. Hillier, Mark S. Hillier. Introduction to Management Science, October 26, 2023 2. A.R Aryasri, Management Science, TMH, 2019		
Reference Books:		
1. Stoner, Freeman, Gilbert.Management, Pearson Education, New Delhi, 2019. 2. 2. Koontz & Weihrich, Essentials of Management, 6/e, TMH, 2005. 3. Thomas N.Duening & John M.Ivancevich, Management Principles and Guidelines, Biztantra. 4. Kanishka Bedi, Production and Operations Management, Oxford University Press, 2004. 5. Samuel C.Certo, Modern Management, 9/e, PHI, 2005		

23CST29a	**SOFTWARE ARCHITECTURE AND DESIGN PATTERNS**	**L**	**T**	**P**	**C**
		3	**0**	**0**	**3**

Course Objectives:

After completing this course, the student should be able to:

- To understand the concept of patterns and the Catalog.
- To discuss the Presentation tier design patterns and their affect on: sessions, client access, validation and consistency.
- To understand the variety of implemented bad practices related to the Business and Integration tiers.

Course Outcomes:

- To highlight the evolution of patterns.
- To learn how to add functionality to designs while minimizing complexity
- To learn what design patterns really are, and are not
- To know about specific design patterns.
- To learn how to use design patterns to keep code quality high without over design.

UNIT I Lecture 9Hrs

Envisioning Architecture: The Architecture Business Cycle, What is Software Architecture, Architectural patterns, reference models, reference architectures, architectural structures and views. Creating an Architecture: Quality Attributes, Achieving qualities, Architectural styles and patterns, designing the Architecture, Documenting software architectures, Reconstructing Software Architecture.

UNIT II Lecture 8Hrs

Analyzing Architectures: Architecture Evaluation, Architecture design decision making, ATAM, CBAM. Moving from one system to many: Software Product Lines, Building systems from off the shelf components, Software architecture in future.

UNIT III Lecture 9Hrs

Patterns: Pattern Description, Organizing catalogs, role in solving design problems, Selection andusage.Creational and Structural patterns: Abstract factory, builder, factory method, prototype, singleton, adapter, bridge, composite, façade, flyweight.

UNIT IV Lecture 8Hrs

Behavioural patterns: Chain of responsibility, command, Interpreter, iterator, mediator, memento, observer, state, strategy. template method, visitor.

UNIT V Lecture 8Hrs

Case Studies: A-7E – A case study in utilizing architectural structures, The World Wide Web - a case study in interoperability, Air Traffic Control – a case study in designing for high availability, Celsius Tech – a case study in product line development

TEXT BOOKS:

1. Software Architecture in Practice, second edition, Len Bass, Paul Clements & Rick Kazman, Pearson Education, 2003.
2. Design Patterns, Erich Gamma, Pearson Education.

REFERENCES:

1. Beyond Software architecture, Luke Hohmann, Addison wesley, 2003.
2. Software architecture, David M. Dikel, David Kane and James R. Wilson, Prentice Hall PTR, 2001
3. Software Design, David Budgen, second edition, Pearson education, 2003
4. Head First Design patterns, Eric Freeman & Elisabeth Freeman, O'REILLY, 2007.
5. Design Patterns in Java, Steven John Metsker& William C. Wake, Pearson education, 2006 6. J2EE Patterns, Deepak Alur, John Crupi& Dan Malks, Pearson education, 2003.
7. Design Patterns in C#, Steven John metsker, Pearson education, 2004.
8. Pattern Oriented Software Architecture, F.Buschmann&others, John Wiley & Sons.

23CYT04a	NETWORK MANAGEMENT SYSTEMS AND OPERATIONS (Professional Elective-IV)	L	T	P	C
		3	0	0	3

Course Objectives:

- Comprehensive understanding of network management.
- Learn about network configurations, security policies, and risk assessments.
- Learn about diagnosing and troubleshooting network faults, performance assessment, and optimization.

Course Outcomes:

- Understanding the challenges and structure of network management in the context of the Internet.
- Defining network management and comprehending its scope, challenges, and variety in multivendor environments.
- Identifying and diagnosing network faults, understanding trouble reports, and learning troubleshooting techniques.
- Exploring the various network management tools.

UNIT - I

The Network Management Challenge: Introduction, The Internet and Network Management, Internet Structure, Managing an Entity, Internal and External policies, The state of Network Management, Network Management in the Gartner Model, Benefits of Automation, The Lack of Industry Response, Distributed Systems and new abstractions.

A Review of Network Elements and Services: Introduction, Network Devices and Network Services, Network Elements and Element Management, Effect of physical organization on Management, Examples of Network Elements and Services, Basic Ethernet Switch, VLAN Switch, Access Point for a Wireless LAN,Cable Modem System, DSL Modem System and DSLAM, CSU/DSU used in Wide Area Digital Circuits, Channel Bank, IP Router, Firewall, DNS Server, DHCP Server, Web Server, HTTP Load Balancer.

UNIT - II

The Network Management Problem: Introduction, What is Network Management? The scope of Network Management, variety and multi-vendor environments, element and network management systems, scale and complexity, types of networks, classification of devices.

Configuration and Operation: Introduction, Intuition for configuration, configuration and protocol layering, dependencies among configuration parameters, seeking a more precise definition of configuration, configuration and temporal consequences, configuration and global consistency, global state and practical systems, configuration and default values, partial state, automatic update and recovery, Interface paradigm and incremental configuration, commit and rollback during configuration, automated rollback and timeout, snapshot, configuration, and partial state, separation of setup and activation.

UNIT - III

Fault Detection and Correction: Introduction, Network Faults, Trouble Reports, Symptoms, and causes, Troubleshooting and Diagnostics, Monitoring, Baselines, Items that can be Monitored, Alarms, Logs, and Polling, Identifying the cause of a Fault, Human Failure and Network Faults, Protocol Layering and Faults, Hidden Faults and Automatic Correction, Anomaly Detection and Event Correlation, Fault Prevention.

Performance Assessment and Optimization: Introduction, aspects of performance, Items that can be measured, measures of network performance, application and endpoint sensitivity, degraded service, variance in traffic and congestion, congestion, delay and utilization, local and end-to-end measurements, passive observation Vs. active probing, bottlenecks and future planning, capacity Planning, planning the capacity of a switch, planning the capacity of a router, planning the capacity of an Internet connection, measuring peak and average traffic on a link, estimated peak utilization and 95th percentile, the relationship between average and peak utilization.

UNIT - IV

Security: Introduction, The illusion of a secure network, security as a process, security terminology and concepts, management goals related to security, Risk Assessment, Security policies, acceptable use policy, basic technologies used for security, management issues and security, Security architecture: Perimeter Vs. Resources, element coordination and firewall unification, resource limits and denial of service, management of authentication, access control and user authentication, management of wireless networks, security of the network, role-based access control, audit trails and security logging, key management.

UNIT - V

Management Tools and Technologies: Introduction, the principle of most recent change, the evolution of Management tools, management tools as applications, using a separate network for management, types of management tools, physical layer testing tools, reach ability and connectivity tools (ping), packet analysis tools, discovery tools, device interrogation interfaces and tools, event monitoring tools, triggers, Urgency Levels, and Granularity, events, Urgency Levels and traffic, performance monitoring tools, flow analysis tools, routing and traffic engineering tools, Configuration tools, Security Enforcement tools, Network Planning tools, Integration of Management tools, NOCs and Remote Monitoring, Remote CLI Access, Remote Aggregation Of Management Traffic.

TEXT BOOKS:

1. Automated Network Management Systems, D. Comer, Prentice Hall, 2006, ISBN No. 0132393085.

REFERENCE BOOKS:

1. Navies Core Administration Cookbook - Second Edition, Tom Ryder, 2016, Packet Publishing, ISBN: 781785889332.
2. Territory: Up and Running, Yevgeniy Brickman, 2017, O'Reilly Media, Inc., ISBN: 9781491977088
3. Applied Network Security Monitoring, Chris Sanders, Jason Smith, Singers publications.

23CST24	DEEP LEARNING	L	T	P	C
		2	1	0	3

Course Objectives:

- Demonstrate the major technology trends driving Deep Learning
- Build, train, and apply fully connected deep neural networks
- Implement efficient (vectorized) neural networks
- Analyse the key parameters and hyper parameters in a neural network's architecture

Course Outcomes:

After completion of the course, students will be able to

- Demonstrate the mathematical foundation of neural network
- Describe the machine learning basics
- Differentiate architecture of deep neural network
- Build a convolutional neural network
- Build and train RNN and LSTMs

UNIT-I Lecture 8Hrs

Linear Algebra: Scalars, Vectors, Matrices and Tensors, Matrix operations, types of matrices, Norms, Eigen decomposition, Singular Value Decomposition, Principal Components Analysis.
Probability and Information Theory: Random Variables, Probability Distributions, Marginal Probability, Conditional Probability, Expectation, Variance and Covariance, Bayes' Rule, Information Theory. Numerical Computation: Overflow and Underflow, Gradient-Based Optimization, Constrained Optimization, Linear Least Squares.

UNIT-II Lecture 9Hrs

Machine Learning: Basics and Under fitting, Hyper parameters and Validation Sets, Estimators, Bias and Variance, Maximum Likelihood, Bayesian Statistics, Supervised and Unsupervised Learning, Stochastic Gradient Descent, Challenges Motivating Deep Learning. Deep Feed forward Networks: Learning XOR, Gradient-Based Learning, Hidden Units, Architecture Design, Back-Propagation and other Differentiation Algorithms.

UNIT-III Lecture 8Hrs

Regularization for Deep Learning: Parameter Norm Penalties, Norm Penalties as Constrained Optimization, Regularization and Under-Constrained Problems, Dataset Augmentation, Noise Robustness, Semi-Supervised Learning, Multi-Task Learning, Early Stopping, Parameter Tying and Parameter Sharing, Sparse Representations, Bagging and Other Ensemble Methods, Dropout, Adversarial Training, Tangent Distance, Tangent Prop and Manifold Tangent Classifier. Optimization for Training Deep Models: Pure Optimization, Challenges in Neural Network Optimization, Basic Algorithms, Parameter Initialization Strategies, Algorithms with Adaptive Learning Rates, Approximate Second-Order Methods, Optimization Strategies and Meta-Algorithms.

UNIT-IV Lecture 9Hrs

Convolutional Networks: The Convolution Operation, Pooling, Convolution, Basic Convolution Functions, Structured Outputs, Data Types, Efficient Convolution Algorithms, Random or Unsupervised Features, Basis for Convolutional Networks.

UNIT V Lecture 8Hrs

Sequence Modeling: Recurrent and Recursive Nets: Unfolding Computational Graphs, Recurrent Neural Networks, Bidirectional RNNs, Encoder-Decoder Sequence-to-Sequence Architectures, Deep Recurrent Networks, Recursive Neural Networks, Echo State Networks, LSTM, Gated RNNs, Optimization for Long-Term Dependencies, Auto encoders, Deep Generative Models.

Text books:

1. Ian Good fellow, Yoshua Bengio, Aaron Courville, “Deep Learning”, MIT Press,2016.
2. Josh Patterson and Adam Gibson, “Deep learning: A practitioner's approach”, O'Reilly Media, First Edition,2017.

Reference Books:

1. Fundamentals of Deep Learning, Designing next-generation machine intelligence algorithms, Nikhil Buduma, O’Reilly, Shroff Publishers,2019.
2. Deep learning Cook Book, Practical recipes to get started Quickly, Douwe Osinga, O’Reilly, Shroff Publishers,2019.

Online Learning Resources:

1. https://keras.io/datasets/
2. http://deeplearning.net/tutorial/deeplearning.pdf
3. https://arxiv.org/pdf/1404.7828v4.pdf
4. https://www.cse.iitm.ac.in/~miteshk/CS7015.html
5. https://www.deeplearningbook.org
6. https://nptel.ac.in/courses/106105215

23CYT04b	MALWARE ANALYSIS & REVERSE ENGINEERING (Professional Elective-IV)	L	T	P	C
		3	0	0	3

Course Objectives:

- To understand different types of malware and their behaviors.
- To analyze malware using static and dynamic techniques.
- To learn reverse engineering fundamentals and binary analysis.
- To use industry-standard tools for malware analysis and debugging.
- To develop countermeasures against modern malware threats.

Course Outcomes (COs):

After completing this course, students will be able to:

1. Identify and classify different types of malware.
2. Perform static and dynamic analysis using specialized tools.
3. Reverse engineer binaries to understand their execution logic.
4. Apply anti-analysis and deobfuscation techniques for malware analysis.
5. Develop and implement effective malware defence strategies.

UNIT 1: Introduction to Malware and Threat Landscape

Overview of Cyber Threats and Malware - Types of Malware: Viruses, Worms, Trojans, Ransom ware, Root kits, Spyware, Bonnets - Infection Vectors and Attack Mechanisms - Malware Lifecycle and Behaviour- Case Studies of Notorious Malware (Winery, Stunt, Zeus, Maria).

UNIT 2: Malware Analysis Techniques

Malware Analysis Environment Setup (Virtual Machines, Sandboxing)-Static Analysis: File Signatures and PE Headers-String Extraction and Hashing-Signature-Based DetectionDynamic Analysis: Process Monitoring and Behavioural Analysis- API Calls and Network Traffic Analysis- Sandboxing with Cuckoo.

UNIT 3: Reverse Engineering Fundamentals

Introduction to Disassembly and Debugging- Assembly Language Basics for Reverse Engineering- Understanding Executable File Formats (PE, ELF)-Introduction to Reverse Engineering Tools: IDA Pro, Hydra, Olli Debug, x64dbg-Debugging and Binary Analysis Techniques.

UNIT 4: Advanced Malware Analysis & Reverse Engineering

Code Obfuscation and Anti-Reverse Engineering Techniques - Unpacking and Decrypting Malware - API Hooking and Process Injection- Shellcode Analysis and Exploit Techniques-Memory Forensics for Malware Investigation.

UNIT 5: Malware Defence, Detection, and Case Studies

Signature-Based vs. Behaviour -Based Detection - Machine Learning for Malware Detection- Evasion Techniques Used by Modern Malware- Incident Response and Forensic Analysis-Case Study: Analyzing a Real-World Malware Sample.

Textbooks:

1. **Malware Analysis:** Michael Sikorski & Andrew Honing, *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*, No Starch Press, 2012.
2. **Reverse Engineering:** Bruce Dang, Alexander Gazet, Elias Bachaalany, *Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation*, Wiley, 2014.

Reference Books:

1. Chris Eagle, *The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassemble*, No Starch Press, 2011.
2. Cameron Malian, Eagan Casey, James Aquiline, *Malware Forensics: Investigating and Analyzing Malicious Code*, Singers, 2008.

Tools and Resources:

- **Disassembly & Debugging:** IDA Pro, Hydra, Olli Debug, x64dbg
- **Network & System Monitoring:**Wire shark, Process Monitor, Process Explorer
- **Sandboxing & Forensics:** Cuckoo Sandbox, Volatility, Regnum

IV B.Tech I Semester

23CST23e	**Agentic AI Engineering**	**3**	**-**	**-**	**3**

Prerequisite: Knowledge of Python programming and Artificial Intelligence concepts. Course Objectives:

- **To provide foundational knowledge of intelligent AI agents, their architectures, and operational principles.**
- **To equip students with the skills to design, develop, and orchestrate AI agents using modern frameworks and platforms.**
- **To enable students to build, deploy, and evaluate agentic AI solutions for real-world applications.**

Course Outcomes:

After successful completion of the course, students will be able to:

CO1 : Explain the principles, architectures, and types of intelligent AI agents.

CO2 : Develop AI agents using memory management, tool calling, and agent development platforms.

CO3: Build LLM-powered agents using planning, orchestration, RAG, and workflow automation techniques.

CO4: Analyze the coordination, collaboration, and workflow design of multi-agent systems.

CO5: Analyze agent deployment architectures and emerging trends in Agentic AI.

Unit I: Foundations of AI Agents **Lecture 9 Hrs**

Evolution of AI Agents and Agentic AI, Characteristics and Architecture of Intelligent Agents, Types of AI Agents, Agent Environment and Lifecycle, Reasoning and Decision-Making Concepts, Applications of AI Agents.

Unit II: Agent Design and Development **Lecture 8 Hrs**

Goal-Oriented and Task-Oriented Agents, Agent Memory and Context Management, Tool Calling and Function Calling, Coding Agents using Frameworks and Developing Agents using Low-Code/No-Code Platforms (n8n, Zapier, Make), Designing Domain-Specific Agents, Agent Testing and Evaluation.

Unit III: LLM-Powered Agents and Agent Workflows **Lecture 9 Hrs**

Large Language Models as Agent Brains, Agent Planning and Task Decomposition, Agent Orchestration and Workflow Management, Retrieval-Augmented Generation (RAG) for Agents, Workflow Automation using AI Agents, AI Coding and Knowledge Agents, Human-in-the-Loop Systems.

Unit IV: Multi-Agent Systems and Collaboration **Lecture 8 Hrs**

Fundamentals of Multi-Agent Systems, Agent Coordination and Collaboration, Multi-Agent Workflow Design, Enterprise Workflow Automation, Enterprise AI Agent Applications, Case Studies of Multi-Agent Solutions.

Unit V: Agent Deployment and Emerging Trends **Lecture 8 Hrs**

Agent Deployment Architectures, Monitoring and Maintenance of Agent Systems, Emerging Trends in Agentic AI.

Design and Development of Multi-Agent Systems for Domain-Specific Applications such as Banking, Agriculture, Healthcare.

Text Books

1. Karthik Ramgopal, Designing Autonomous AI Agents, O'Reilly Media, 2024.
2. Paul Iusztin and Maxime Labonne, AI Engineering: Building Applications with Foundation Models, O'Reilly Media, 2025.

Reference Books

1. Valentino Zocca and Ram Sriharsha, Building LLM Powered Applications, Packt Publishing, 2024.
2. Jay Alammar and Maarten Grootendorst, Hands-On Large Language Models, O'Reilly Media, 2024.
3. Michael Wooldridge, An Introduction to MultiAgent Systems, 2nd Edition, Wiley, 2009.
4. Noah Gift and Alfredo Deza, Practical MLOps: Operationalizing Machine Learning Models, 2nd Edition, O'Reilly Media, 2024.

		L	T	P	C
23CST29c	**Augmented Reality and Virtual Reality (Professional Elective-V)**	**3**	**0**	**0**	**3**

Course Outcomes: At the end of the Course the student will be able to:

CO1: Describe the concept of virtual reality and Communication Media. (L2)

CO2: Understand current virtual reality hardware and software. (L2)

CO3: Understand various modelling approaches. (L2)

CO4: Illustrate the concepts of Human Factors and Applications of VR. (L2)

CO5: Build a Virtual Reality Application. (L3)

UNIT - I **(10 Lectures)**

INTRODUCTION TO VIRTUAL REALITY (VR): Defining Virtual Reality, Key elements of virtual reality experience, Virtual Reality, Telepresence, Augmented Reality and Cyberspace.

Bird's-Eye View: Hardware, Software, Human Physiology and Perception.

Learning Outcomes: At the end of the unit, students will be able to

1. Compare Virtual and Augmented Reality. (L2)
2. Outline the history of Virtual Reality. (L2)
3. Understand the Human Physiology and perception.(L2)

UNIT-II **(10 Lectures)**

Input Devices: (Trackers, Navigation, and Gesture Interfaces): Three-dimensional position trackers, navigation and manipulation, interfaces and gesture interfaces**.**

Output Devices: Graphics displays, sound displays & hap tic feedback.

Learning Outcomes: At the end of the unit, students will be able to

1. Classify different input devices. (L2)
2. Understand the navigation and manipulation. (L2)
3. Illustrate the use of different output devices. (L2)

UNIT-III **(10 Lectures)**

Modelling: Geometric modelling, Kinematics modelling, Physical modelling, Behaviour modelling, Model management.

Learning Outcomes: At the end of the unit, students will be able to

1. Demonstrate the usage of modelling.(L2)
2. Classify modelling techniques. (L2)
3. Understand the Model Management.(L2)

UNIT-IV **(10 Lectures)**

Augmented Reality (AR): Taxonomy, Technology and Features of Augmented Reality, AR Vs VR, Challenges with AR, AR systems and functionality, Augmented Reality Methods, Visualization Techniques for Augmented Reality, Enhancing interactivity in AR Environments, Evaluating AR systems

AR software development: AR software, Camera parameters and camera calibration, Marker-based augmented reality, AR Toolkit.

Learning Outcomes: At the end of the unit, students will be able to

1. Illustrate the challenges of Augmented Reality.(L2)
2. Understand different VR applications. (L2)
3. Understand the use of AR Software and Toolkit(L2)

UNIT-V **(10 Lectures)**

Interaction & Audio: Interaction - Motor Programs and Remapping, Locomotion, Manipulation, Social Interaction. Audio -The Physics of Sound, The Physiology of Human Hearing, Auditory Perception, Auditory Rendering. Interaction - Motor Programs and Remapping, Locomotion, Manipulation, Social Interaction. Audio -The Physics of Sound, The Physiology of Human Hearing, Auditory Perception, Auditory Rendering. (from Text Book2)

Learning Outcomes: At the end of the unit, students will be able to

1.explain key interactions to manipulate, navigate and interact in a Virtual World. (L2)
2.identify the role of Immersion in VR..(L1)
3.develop an application with VR experience. (L3)

TEXT BOOKS:

1. Virtual Reality Technology, Second Edition, Gregory C. Burden& Philippe Coiffed, John Wiley & Sons, Inc, 2017.
2. Virtual Reality, Steven M. Lavelle, Cambridge University Press, 2016.

REFERENCES:

1. Rajesh K.Maurya, *Computer Graphics with Virtual Reality System*, 3rd Edition, Wiley Publication, 2018.
2. William R. Sherman and Alan B. Craig, *Understanding Virtual Reality Interface, Application, and Design*, 2nd Edition, Morgan Kaufmann Publishers, Elsevier, 2019.
3. Gregory C.Burdea, Philippe Coiffet, *Virtual Reality Technology*, 2nd Edition, Wiley,2017.
4. K.S. Hale and K. M. Stanley, *Handbook on Virtual Environments*, 2nd Edition, CRC Press, 2015.

WEB REFERENCES:

1. http://vr.cs.uiuc.edu/vrbook.pdf
2. https://nptel.ac.in/courses/106/106/106106138/

IV B.Tech I Semester

23CYT05a	INTRUSION DETECTION AND PREVENTION SYSTEM (Professional Elective-V)	L	T	P	C
		3	0	0	3

Course Description

This course covers a comprehensive range of topics related to intrusion detection, prevention, and analysis, with a specific focus on the practical application of the Snort tool. Students will gain knowledge about the historical context, various types of threats, response strategies, and hands-on experience with Snort for intrusion detection and prevention.

Course Objectives:

1. Comprehend the historical evolution and key concepts of intrusion detection and audit techniques.
2. Gain skills to effectively use various IDS and IPS technologies, including hybrid approaches.
3. Develop the ability to independently install, configure, and use Snort in diverse scenarios.
4. Foster analytical skills for intrusion detection, encompassing vulnerability analysis and response strategy formulation.
5. Explore advanced techniques, including ACID and Snort Scarf, and understand different IDS and IPS architecture models.

Course Outcomes:

1. Articulate the historical evolution of intrusion detection, define key concepts, and understand cybersecurity importance.
2. Demonstrate proficiency in deploying various IDS and IPS technologies, informed by threat assessments.
3. Install, configure, and use Snort for intrusion detection across multiple network interfaces.
4. Ability to analyze intrusions, conduct vulnerability assessments, and formulate responses aligned with security policies.
5. Apply advanced techniques, including ACID and Snort Scarf, and develop custom agents for tailored intrusion detection solutions. Understand different architecture models of IDS and IPS.

UNIT-I **9 Hrs**

History of Intrusion detection, Audit, Concept and definition , Internal and external threats to data, attacks, Need and types of IDS, Information sources Host based information sources, Network based information sources.

UNIT-II **9 Hrs**

Intrusion Prevention Systems, Network IDs, protocol based IDs ,Hybrid IDs, Analysis schemes, thinking about intrusion. A model for intrusion analysis techniques, Responses requirement of responses, types of responses mapping, responses to policy Vulnerability analysis, credential analysis, non credential analysis.

UNIT-III **9 Hrs**

Introduction to Snort, Snort Installation Scenarios, Installing Snort, Running Snort on Multiple Network Interfaces, Snort Command Line Options. Step-By-Step Procedure to Compile and Install Snort Location of Snort Files, Snort Modes Snort Alert Modes

UNIT-IV **9 Hrs**

Working with Snort Rules, Rule Headers, Rule Options, The Snort Configuration File etc. Plugging, Pre-processors and Output Modules, Using Snort with MySQL

UNIT-V **9 Hrs**

Using ACID and Snort Scarf with Snort, Agent development for intrusion detection, Architecture models of IDs and IPs.

TEXT BOOKS:

1. Rafael Redman : ― Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID,‖ 1st Edition, Prentice Hall , 2003.

REFERENCES:

1. Christopher Krueger,Fredrik Valour, Giovanni Vegan: ―Intrusion Detection and Correlation Challenges and Solutions‖, 1st Edition, Springer, 2005.
2. Carl Endure, Eugene Schultz and Jim Millender― Intrusion Detection & Prevention‖, 1st Edition, Tata McGraw-Hill, 2004.
3. Stephen Northcutt, Judy Novak : ―Network Intrusion Detection‖, 3rd Edition, New Riders Publishing, 2002.
4. T. Fahringer, R. Prod an, ―A Text book on Grid Application Development and Computing Environment‖. 6th Edition, Khans Publishers, 2012.

IV B.Tech I Semester

23CST30b	METAVERSE	L	T	P	C
	(Professional Elective –V)	3	0	0	3

The main objectives of the course are to:
1. Present and discuss Metaverse characteristics, concepts and layers.
2. Explain and analyse Metaverse technologies, tools, platforms, and applications.
3. Discuss design theories and practices relevant to the Metaverse.
4. Explore cyber security and cybercrime in the Metaverse.
5. Examine open challenges in the Metaverse.

Course Out comes:

After completion of the course students are expected to be able to:
1. Under stand the characteristics, and interdisciplinary nature of the Metaverse, the opportunities and risks it presents.
2. Analyze Metaverse layers, the technologies used in creating them, as well as design theories and practices for Metaverse.
3. Examine and discuss Metaverse platforms, applications and the latest technological developments in this area.
4. Identify cyber security issues, understand cybercrime, and discuss the open challenges.
5. Building Metaverse Applications

Unit-I Lecture 9Hrs

Metaverse fundamentals: Metaverse evolution, Metaverse importance and characteristics, the interdisciplinary nature of the Metaverse, Metaverse opportunities and risks, Computer-mediated communication (social presence theory, social information processing theory, media richness theory, cyborg theory), Avatar-mediated communication.

Unit-II Lecture 8Hrs

The seven layers of Metaverse: ExperienceDiscovery, Creator economy, Spatial computing, Decentralization, Human interface, Infrastructure

Metaverse Technologies part I: AR/VR/MR/XR, 3D reconstruction, Game engines, Smart glasses, wearables, haptic devices, headsets and headwear.

Unit-III Lecture 9Hrs

Metaverse technologies part II: Blockchain, smart contracts, tokens, NFTs, Cryptography, Artificial Intelligence (AI), Internet of Things (IoT), Edge computing and 5G, 6G.Design theories and practices: Social presence and co-presence, Motion sickness and cybersickness, Uncanny valley, Sense of self-location, sense of agency and sense of body ownership, Universal simulation principle, Prototyping, Evaluation techniques (qualitative and quantitative).

Unit-IV Lecture 9Hrs

Tools and technologies for Metaverse UX and UI: Tools and services for avatar systems, Spatial user interface design, Cross-platform user experience design, Multimodal user interface, Technologies and devices for human computer interaction in Metaverse, Metaverse platforms: Decentraland, SANDBOX, Roblox, Axie Infinity, uHive, Hyper Nation, Nakamoto (NAKA), Metahero (HERO), Star

Atlas (ATLAS), Bloktopia (BLOK), Stageverse, Spatial, PalkaCity, Viverse, Sorare, Illuvium, Upland, Second Life, Sansar, Sensorium Galaxy

Unit-V Lecture 9Hrs

Metaverse applications - part I: Gaming and entertainment, Travel and tourism, Education and learning, Remote working, Commerce and business, Metaverse applications - part II: Real estate, Banking and Finance, Healthcare, Social media, Fashion, Metaverse and cyber security: Cyber security concerns in Metaverse: Social engineering attacks, Data theft, Decentralization vs vulnerabilities, Cyber security risks in Metaverse: process, people, technology, Metaverse and cybercrime: Scam and theft, Rug pull, Money manipulation and wash trading, Money laundering, Metaverse challenges and open issues: Persistency, Interoperability and scalability, Maturity, Regulation, Usefulness and ease-of-use, Privacy and data security, Content creation, NFTs and creator economy, Social, legal and ethical issues in the Metaverse

Text books

The Metaverse, Terry Winters, Independently published, 2021, ISBN: 979-8450959283

Reference Books:

1. Ball, M., 2022, "The Metaverse and How It Will Revolutionize Everything", Liveright, ISBN: 978-1324092032

2. Damar, M. (2021). Metaverse shape of your life for future: A bibliometric snapshot. Journal ofMetaverse, 1(1), 1–8.

3. Day, J. (2022) Metaverse will see cyber warfare attacks unlike anything before: 'Massively elevated', February 28.
https://www.express.co.uk/news/science/1570844/metaverse-news-cyber-warfare-attacks-virtual-worlds-russia-china-spt.

4. Polyviou, A., Sharma K., Pappas, I.O.(2023). Training in the metaverse: Employing physiological data to improve how we build metaverses for businesses. The next generation internet: The role of metaverses, AR, VR, MR, and digital twins, Temple University Institute for Business and Information Technology Link: https://ibit.temple.edu/nextgenerationinternet

5. QuHarrison T. , Keeney, S., 2022, "The Metaverse Handbook: Innovating for the Internet's NextTectonic Shift", Wiley, ISBN: 978-1119892526

6. The mistocleous, M., Christodoulou, K., & Katelaris, L. (2023). An Educational Metaverse Experiment: The first on-chain and in- Metaverse academic course. Information Systems. EMCIS2022. Lecture Notes in Business Information Processing, Springer, Cham.

7. Stephenson, N., 1992, "Snow Crash", ISBN: 978-055338

23CYT05b	CYBER LAWS AND SECURITY POLICIES (Professional Elective-V)	L	T	P	C
		3	0	0	3

Course Objectives:

- Gain an understanding of the evolution and jurisprudence of cyber law in India, including the IT Act 2000.
- Learn about digital signatures, e-governance, and their legal implications under the IT Act.
- Understand the legal framework for electronic contracts, their formation, and international perspectives.
- Explore taxation issues in cyberspace, cybercrimes, electronic evidence, and their adjudication under the IT Act.

Course Outcomes

- Learn evolution and key aspects of Indian cyber law, including recent amendments.
- Gain knowledge about the legalities of digital signatures and the role of e-governance in the IT Act.
- Develop an understanding of the legalities involved in electronic contracts and international conventions.
- Adapt in understanding and analyzing cybercrime, electronic evidence, and intellectual property rights in the context of IT.

UNIT - I

Introduction: History of Internet and World Wide Web, Need for cyber law, Cybercrime on the rise, Important terms related to cyber law.
Cyber law in India: Need for cyber law in India, History of cyber law in India.
Information Technology Act, 2000: Overview of other laws amended by the IT Act, 2000, National Policy on Information Technology 2012.

UNIT - II

Overview of the Information Technology Act, 2000: Applicability of the Act, Important provisions of the Act: Digital signature and Electronic signature, Digital Signature under the IT Act, 2000, E- Governance Attribution, Acknowledgement and Dispatch of Electronic Records, Certifying Authorities, Electronic Signature Certificates, Duties of Subscribers, Penalties and Offences, Intermediaries.

UNIT - III

Overview of rules issued under The IT Act, 2000, Electronic Commerce, Electronic Contracts, CyberCrimes, Cyber Frauds.

UNIT - IV

Regulatory Authorities: Department of Electronics and Information Technology, Controller of Certifying Authorities (CCA), Cyber Appellate Tribunal, Indian Computer Emergency Response Team (ICERT), Cloud Computing, Case Laws.

UNIT - V

Introduction to Cybercrime and procedure to report Cyber crime: procedure to report cybercrime, some basic rules for safe operations of the computer and internet, the criminal law (amendment) act, 2013: legislative remedies for online harassment and cyberstalking in India.

TEXT BOOKS:

1. Text book on ―Cyber Law‖,**2 Ed Rap 2023**, PaganDug gal, Universal Law Publishing.
2. Text book on ―Indian Cyber law on Cybercrimes‖, PaganDug gal,

REFERENCE BOOKS:

1. Debby Russell and Sr. G.T Gingili, "Computer Security Basics (Paperback)‖, 2nd Edition, O'Reilly Media, 2006.
2. Thomas R. Pettier, ―Information Security policies and procedures: A Practitioner's Reference‖, 2nd Edition Prentice Hall, 2004.
3. Kenneth J. Knapp, ―Cyber Security and Global Information Assurance: Threat Analysis andResponse Solutions‖, IGI Global, 2009.
4. Thomas R Pettier, Justin Pettier and John Blackley,‖ Information Security Fundamentals‖, 2nd Edition, Prentice Hall, 1996.

23CST30d	**AI Powered Application Development**	**L**	**T**	**P**	**C**
		3	**-**	**-**	**3**

Course Objectives:

- **To provide knowledge of AI-powered application development using modern software engineering and Python programming concepts.**
- **To enable students to design and develop full-stack applications integrated with AI models, APIs, and databases.**
- **To equip students with skills to build, deploy, and evaluate AI-powered applications for real-world scenarios.**

Prerequisite: Knowledge of Python programming, databases, and Artificial Intelligence concepts.

Course Outcomes:

After successful completion of the course, students will be able to: CO1: Explain the fundamentals of AI-powered application development.

CO2: Develop full-stack AI applications using frontend, backend, and database technologies.

CO3: Integrate LLMs and SLMs into applications using AI services, APIs, and SDKs.

CO4: Analyze the design and implementation of AI-powered application features.

CO5: Analyze deployment, scaling, and monitoring strategies for AI-powered applications.

Unit I: Application Development (9 Hrs)

Introduction to AI-Powered Applications, Software Development Life Cycle (SDLC), Agile Methodology and Scrum Basics, AI Application Development Lifecycle, Lambda Functions, map() and filter(), Iterators and Generators, Object-Oriented Programming Concepts, Exception Handling, Modules and Packages, Working with JSON Data.

Unit-II: Full-Stack AI Application Development (9 Hrs)

Web Application Architecture, MVC and MVT Design Patterns, Frontend Development using React.js, RESTful API Development, Database Integration using Python and ORM, CRUD Operations, Integration of Frontend and Backend Applications.

Unit III: AI Model Integration for Applications (9 Hrs)

Introduction to Large Language Models (LLMs) and Small Language Models (SLMs), AI Service Integration using APIs, Working with AI SDKs and Frameworks, Integrating LLMs and SLMs into Python Applications, Prompt Engineering Fundamentals, AI Response Processing and Validation.

Unit IV: Building AI-Powered Applications (9 Hrs)

Design of AI-Powered Application Features, Conversational AI and Chatbots, Document Analysis and Knowledge Applications, AI Content Generation Applications AI Agents and Productivity Applications, Case Studies of AI-Powered Applications.

Unit V: Deployment and Scaling (8 Hrs)

Application Deployment Fundamentals, Containerization Concepts, Cloud Deployment Basics, Scaling AI Applications, Logging and Monitoring, Capstone Project Design and Implementation.

Text Books

1. Eric Matthes, Python Crash Course, 3rd Edition, No Starch Press, 2023.
2. William S. Vincent, Django for APIs, 5th Edition, WelcomeToCode, 2024.
3. Paul Iusztin and Maxime Labonne, AI Engineering: Building Applications with Foundation Models, O'Reilly Media, 2025.

Reference Books

1. Valentino Zocca and Ram Sriharsha, Building LLM Powered Applications, Packt Publishing, 2024.
2. Jay Alammar and Maarten Grootendorst, Hands-On Large Language Models, O'Reilly Media, 2024.
3. Simon Holmes, Clive Harber, Tomomi Imura, Noel Hurst, Christian Kaindl, The React Workshop, 2nd Edition, Packt Publishing, 2024.
4. Noah Gift and Alfredo Deza, Practical MLOps: Operationalizing Machine Learning Models, 2nd Edition, O'Reilly Media, 2024.

23CYP05	**Ethical Hacking (Skill Enhancement Course)**	**L**	**T**	**P**	**C**
		0	**1**	**2**	**2**

Course Description :

Ethical Hacking is one of the most popular courses with the increase in people's interest in internet security and ways for keeping one's personal security safe and secure from different peoples. This course cover tools and techniques that are used by hackers and penetration testers and topics in general namely Ethical Hacking, Website, System Hacking & Security and Mobile & Wireless Security.

Course Objectives:

The objective of this course is to make students to,

1. To learn about the importance of information security.
2. To learn different scanning and enumeration methodologies and tools.
3. To understand various hacking techniques and attacks.
4. To be exposed to programming languages for security professionals.
5. To get familiarized with the different phases in penetration testing.

Course Outcomes:

Upon completion of this course, the student should be able to,

1. Understand how to secure the information.
2. Defend hacking attacks and protect data assets.
3. Defend a computer against a variety of security attacks using various tools.
4. Practice and use safe techniques on the World Wide Web.
5. Get familiarized with the different phases in penetration testing.

UNIT-I **9 Hrs**

Introduction to Hacking: Introduction to Hacking – Importance of Security – Elements of Security – Phases of an Attack – Types of Hacker Attacks – Activism – Vulnerability Research – Introduction to Foot printing – Information Gathering Methodology – Foot printing Tools – WHOIS Tools – DNS Information Tools – Locating the Network Range – Meta Search Engines.

a) Write a Python program to perform a WHOIS lookup on a domain.
b) Write a Python program to extract DNS records (A, MX, NS) for a given domain.
c) Write a Python script to scan open ports on a target machine using the socket module.
d) Write a program to implement a basic key logger for ethical testing (Ensure responsible use).
e) Write a Python program to identify hidden files in a given directory.

UNIT-II **9 Hrs**

Scanning and Enumeration: Introduction to Scanning – Objectives – Scanning Methodology – Tools – Introduction to Enumeration – Enumeration Techniques – Enumeration Procedure – Tools.

a) Write a Python program to perform a basic network scan using the socket module.
b) Write a Python script to scan open ports on a target IP using neap (requires python-neap library).
c) Write a Python program to identify live hosts in a network using ICMP (Ping Sweep).
d) Write a Python program to extract system and network details using OS commands (e.g., ipconfig, ifconfig).
e) Write a Python script to enumerate user accounts and shared resources on a remote system using SMB (requires impacted library).

UNIT-III **9 Hrs**

System Hacking: Introduction – Cracking Passwords – Password Cracking Websites – Password Guessing – Password Cracking Tools – Password Cracking Counter measures – Escalating Privileges –Executing Applications –Key loggers and Spyware.

a) Write a Python program to generate a list of common password combinations for brute-force attacks.
b) Write a Python script to perform a dictionary-based password attack on a hashed password file.
c) Write a Python program to implement a basic key logger to record keystrokes (for ethical testing only).
d) Write a Python script to detect running key loggers or spyware processes on a system.
e) Write a Python program to encrypt and decrypt passwords using a hashing algorithm (e.g., SHA-256).

UNIT-IV **9 Hrs**

Programming for Security Professionals: Programming Fundamentals – C language – HTML – Perl – Windows OS Vulnerabilities – Tools for Identifying Vulnerabilities – Countermeasures – Linux OS Vulnerabilities – Tools for Identifying Vulnerabilities – Countermeasures.

a) Write a Python script to detect buffer overflow vulnerabilities by monitoring input size.
b) Write a Python script to check an HTML file for XSS (Cross-Site Scripting) vulnerabilities using rages.
c) Write a Python script to analyze system logs and detect multiple failed login attempts (brute force detection).
d) Write a Python program to scan a Windows system for open ports and weak password policies.
e) Write a Python script to list all SUID/SGID files on a Linux system that may pose security risks.

UNIT-V **9 Hrs**

Penetration Testing: Introduction – Security Assessments – Types of Penetration Testing- Phases of Penetration Testing – Tools – Choosing Different Types of Pen-Test Tools – Penetration Testing Tools.

a) Write a Python script to perform an automated vulnerability scan using neap (requires python-neap library).
b) Write a Python script to perform banner grabbing to detect service versions running on open ports.
c) Write a Python program to perform a brute-force attack on an SSH server using a wordlist (ethical testing only).
d) Write a Python script to detect and analyze network packets using scrappy for penetration testing.
e) Write a Python program to automate SQL Injection detection on a website using requests and Beautiful Soup.

Text Books:

1. Ec-Council, ―Ethical Hacking and Countermeasures: Attack Phases‖, Delmar Engage Learning, 2009.
2. Michael T. Simpson, Kent Beckman, James E. Corley, ―Hands-On Ethical Hacking and Network Defence‖, Engage Learning, 2012.

Reference Books:

1. Patrick Engebretson, ―The Basics of Hacking and Penetration Testing – Ethical Hacking and Penetration Testing Made Easy‖, Singers Media, Second Revised Edition, 2013.
2. Jon Erickson, ―Hacking: The Art of Exploitation‖, No Starch Press, Second Edition, 2008.
3. Daniel G. Graham, Ethical Hacking: A Hands-on Introduction to Breaking In, William Pollock, 2021.