
# DEPARTMENT

# OF

# COMPUTER SCIENCE AND ENGINEERING

# (CYBER SECURITY)

## B. Tech.

## *R22-COURSE STRUCTURE & SYLLABUS*

**IV YEAR I SEMESTER**

| S.No. | Course Code | Course Title | Category | L | T | P | Credits |
|---|---|---|---|---|---|---|---|
| 1 | 22CY4111 | Vulnerability Assessment & Penetration Testing | PC | 3 | - | - | 3 |
| 2 | 22CY4112 | Network Management Systems and Operations | PC | 3 | - | - | 3 |
| 3 | **Professional Elective–IV** | | | | | | |
| | 22CY4171 | Web & Database Security | PE | 3 | - | - | 3 |
| | 22CY4172 | Computer Security & Audit Assurance | | | | | |
| | 22CY4173 | Social Media Security | | | | | |
| | 22CY4174 | Authentication Techniques | | | | | |
| 4 | **Professional Elective–V** | | | | | | |
| | 22IT4177 | Deep Learning | PE | 3 | - | - | 3 |
| | 22AM4175 | Quantum Computing | | | | | |
| | 22CY4175 | Data Analytics for Fraud Detection | | | | | |
| | 22CY4176 | Security Incident & Response Management (SOC) | | | | | |
| 5 | | **Open Elective–II** | OE | 3 | - | - | 3 |
| 6 | 22CY4151 | Vulnerability Assessment & Penetration Testing lab | PC | - | - | 2 | 1 |
| 7 | 22CY4152 | Network Management Systems and Operations Lab | PC | - | - | 2 | 1 |
| 8 | 22CY4181 | Internship | PW | - | - | 2 | 1 |
| 9 | 22CY4182 | Project Stage–I | PW | - | - | 4 | 2 |
| | | **Total** | | **15** | **0** | **10** | **20** |

**IV YEAR II SEMESTER**

| S.No. | Course Code | Course Title | Category | L | T | P | Credits |
|---|---|---|---|---|---|---|---|
| 1 | 22MB4211 | Organizational Behaviour | HS | 3 | - | - | 3 |
| 2 | **Professional Elective–VI** | | | | | | |
| | 22CY4271 | Quantum Cryptography | PE | 3 | - | - | 3 |
| | 22CY4272 | Cloud Security | | | | | |
| | 22CY4273 | Digital Water marking and Steganography | | | | | |
| | 22CY4274 | Data Privacy | | | | | |
| 3 | | **Open Elective–III** | OE | 3 | - | - | 3 |
| 4 | 22CY4281 | Project Stage–II Including Seminar | PW | 0 | - | 22 | 11 |
| | | **Total** | | **9** | - | **22** | **20** |

**Open Electives offered by the Department of Computer Science and Engineering ( Cyber Security) to other departments**

| S.No. | Open Elective | Subject Code | Subject Name | Credits |
|---|---|---|---|---|
| 1. | Open Elective–I | 22CY3261 | Introduction to Cyber Security | **3** |
| | | 22CY3262 | Ethical Hacking | |
| 2. | Open Elective–II | 22CY4161 | Computer Security & Audit Assurance | **3** |
| | | 22CY4162 | Social Media Security | |
| 3. | Open Elective–III | 22CY4261 | Data Privacy | **3** |
| | | 22CY4262 | Cyber Laws | |
| | | | **Total** | **9** |

**22CY4111: VULNERABILITY ASSESSMENT AND PENETRATION TESTING**

**B.Tech. IV Year I Sem.**

| L | T | P | C |
|---|---|---|---|
| 3 | 0 | 0 | 3 |

**Prerequisites**

1. Knowledge in information security.
2. Knowledge on Web Application.

**Course Objectives**

1. To introduce ethical hacking, penetration testing, and social engineering techniques.
2. To explain physical and insider threats along with Metasploit exploitation tools.
3. To describe the planning and execution of penetration tests and exploit development.
4. To explore top web vulnerabilities and methods of vulnerability analysis.
5. To discuss browser-based exploits and malware analysis methods.

**Course Outcomes**

1. Differentiate ethical hacking tactics and identify common social engineering attacks.
2. Implement penetration tests using Metasploit for client-side vulnerabilities.
3. Demonstrate basic Linux and Windows exploitation using buffer overflow techniques.
4. Analyse applications using passive, source code, and binary analysis.
5. Conduct initial malware analysis and recognize client-side attack vectors.

**UNIT- I**

**Introduction**

Ethics of Ethical Hacking: Why you need to understand your enemy's tactics, recognizing the Gray areas in security, Vulnerability Assessment and Penetration Testing.

**Penetration Testing and Tools:**

Social Engineering Attacks: How a social engineering attack works, conducting a social engineering attack, common attacks used in penetration testing, preparing yourself for face-to-face attacks, defending against social engineering attacks.

**UNIT- II**

**Physical Penetration Attacks:** Why a physical penetration is important? conducting a physical penetration, Common ways into a building, defending against physical penetrations.

**Insider Attacks:** Conducting an insider attack, defending against insider attacks.

**Metasploit:** The Big Picture, Getting Metasploit, Using the Metasploit Console to Launch Exploits, Exploiting Client-Side Vulnerabilities with Metasploit, Penetration Testing with Metasploit's Meterpreter, Automating and Scripting Metasploit, Going Further with Metasploit.

**UNIT- III**

**Managing a Penetration Test:** planning a penetration test, structuring a penetration test, execution of a penetration test, information sharing during a penetration test, reporting the results of a Penetration Test.

**Basic Linux Exploits:** Stack Operations, Buffer Overflows, Local Buffer Overflow Exploits, Exploit Development Process.

**Windows Exploits:** Compiling and Debugging Windows Programs, Writing Windows Exploits, Understanding Structured Exception Handling (SEH), Understanding Windows Memory Protections (XPSP3, Vista, 7 and Server 2008), Bypassing Windows Memory Protections.

**UNIT- IV**

**Web Application Security Vulnerabilities:**

Overview of top web application security vulnerabilities, Injection vulnerabilities, cross-Site cripting vulnerabilities, the rest of the OWASP Top Ten SQL Injection vulnerabilities, Cross-site scripting vulnerabilities.

**Vulnerability Analysis:**

Passive Analysis, Source Code Analysis, Binary Analysis.

**UNIT- V**

**Client-Side Browser Exploits:**

Why client-side vulnerabilities are interesting, Internet explorer security concepts, history of client-side exploits and latest trends, finding new browser-based vulnerabilities heap spray to exploit, protecting yourself from client-side exploit.

**Malware Analysis:** Collecting Malware and Initial Analysis: Malware, Latest Trends in Honeynet Technology, Catching Malware: Setting the Trap, Initial Analysis of Malware.

**TEXT BOOKS:**

1. Gray Hat Hacking-The Ethical Hackers Handbook", Allen Harper, Stephen Sims, Michael Baucom, 3rd Edition, Tata Mc Graw-Hill.
2. The Web Application Hacker's Handbook-Discovering and Exploiting Security flaws", Dafydd Suttard, Marcus pinto, 1st Edition, Wiley Publishing.

**REFERENCE BOOKS:**

1. "Penetration Testing: Hands-on Introduction to Hacking", Georgia Weidman, 1st Edition, No Starch Press.
2. The Pen Tester Blueprint-Starting a Career as an Ethical Hacker ", L. Wylie, Kim Crawly, 1st Edition, Wiley Publications.

## 22CY4112: NETWORK MANAGEMENT SYSTEMS AND OPERATIONS

**B.Tech. IV Year I Sem.**

| L | T | P | C |
|---|---|---|---|
| 3 | 0 | 0 | 3 |

**Prerequisites:**

- Computer Networks, Operating Systems

**Course Objectives:**

1. To introduce network management concepts and challenges.
2. To explain configuration issues in multi-vendor networks.
3. To outline fault detection and performance analysis techniques.
4. To highlight network security policies and access control.
5. To demonstrate the use of network management tools.

**Course Outcomes:**

1. Identify key elements and challenges in network management.
2. Distinguish configuration parameters and their dependencies.
3. Assess faults and optimize network performance.
4. Evaluate network security controls and access mechanisms.
5. Apply network management tools for monitoring and control.

**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, reachability 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 BOOK:**


1. Automated Network Management Systems, D. Comer, Prentice Hall, 2006, ISBN No. 0132393085.
2. Network Management: Principles and Practice, Author: Mani Subramanian, Publisher: Pearson Education, Edition: 2nd Edition.
3. Network Management Fundamentals, Author: Alexander Clemm, Publisher: Cisco press


**REFERENCE BOOKS:**


1. Nagios Core Administration Cookbook - Second Edition, Tom Ryder, 2016, Packt Publishing, ISBN: 781785889332.
2. Terraform: Up and Running, Yevgeniy Brikman, 2017, O'Reilly Media, Inc., ISBN: 9781491977088
3. Applied Network Security Monitoring, Chris Sanders, Jason Smith, Syngress publications.

**22CY4171: WEB & DATABASE SECURITY**
**(Professional Elective – IV)**

**B.Tech. IV Year I Sem.** **L T P C**
**3 0 0 3**

**Prerequisites**

- Web Technologies, DBMS, Cryptography basics

**Course Objectives**

1. To describe web security, cryptography, and digital identification.
2. To investigate threats to server and application security.
3. To summarize database access control models and trust issues.
4. To explore techniques for database security and recovery.
5. To discuss privacy and security in mobile and location-based systems.

**Course Outcomes:**

1. Explain web security issues and cryptographic principles.
2. Assess server and application-level security.
3. Compare access control models for relational and XML databases.
4. Analyse data recovery and watermarking in secure databases.
5. Demonstrate privacy enforcement in mobile and cloud-based systems.

**UNIT - I**

The Web Security, The Web Security Problem, Risk Analysis and Best Practices Cryptography and the Web: Cryptography and Web Security, Working Cryptographic Systems and Protocols, Legal Restrictions on Cryptography, Digital Identification

**UNIT - II**

The Web's War on Your Privacy, Privacy-Protecting Techniques, Backups and Anti-Theft, Web Server Security, Physical Security for Servers, Host Security for Servers, Securing Web Applications

**UNIT - III**

Database Security: Recent Advances in Access Control, Access Control Models for XML, Database Issues in Trust Management and Trust Negotiation, Security in Data Warehouses and OLAP Systems

**UNIT - IV**

Security Re-engineering for Databases: Concepts and Techniques, Database Watermarking for Copyright Protection, Trustworthy Records Retention, Damage Quarantine and Recovery in Data Processing Systems, Hippocratic Databases: Current Capabilities and

**UNIT - V**

Future Trends Privacy in Database Publishing: A Bayesian Perspective, Privacy-enhanced Location-based Access Control, Efficiently Enforcing the Security and Privacy Policies in a Mobile Environment

**TEXT BOOKS:**

1. Web Security, Privacy and Commerce Simson GArfinkel, Gene Spafford, O'Reilly.
2. Handbook on Database security applications and trends Michael Gertz, Sushil Jajodia

**REFERENCE BOOKS:**

1. Andrew Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications, O'reilly
2. Jonathan LeBlanc Tim Messerschmidt, Identity and Data Security for Web Development -Best Practices, O'reilly
3. McDonald Malcolm, Web Security for Developers, No Starch Press, US

## 22CY4172: COMPUTER SECURITY & AUDIT ASSURANCE
## (Professional Elective – IV)

**B.Tech. IV Year I Sem.** **L T P C**
**3 - - 3**

**Prerequisites**
- Information Security, Networking Fundamentals

**Course Objectives:**
1. To state the basic concepts in information systems security, including security technology and principles.
2. To acquire knowledge about software security and trusted systems and IT security management
3. To understand audit, standard practices and policies.
4. To explain concepts related to various cryptographic tools.
5. To understand and implement disaster recovery planning control

**Course Outcomes:**
1. State the requirements and mechanisms for identification and authentication.
2. Explain and compare the various access control policies and models as well as the assurance of these models.
3. Understand various standard practices and policies in conducting audits.
4. Understand and analyse the significance of Network Security and Control, Internet Banking Risks and Control.
5. Developing appropriate disaster recovery strategy.

**UNIT - I**
System Audit and Assurance – Characteristics of Assurance services, Types of Assurances services, Certified Information system auditor, Benefits of Audits for Organization, COBIT.

**UNIT - II**
Internal Control and Information system Audit - Internal Control, Detective control, Corrective Control, Computer Assisted Audit Tools and Techniques.

**UNIT - III**
Conducting Audit – Standard practices, policies, Audit planning, Risk Assessment, Information gathering techniques, Vulnerabilities, System security testing, conducting Audits for Banks.

**UNIT - IV**
Network Security and Control, Internet Banking Risks and Control, Operating System Risks and Control, Operational Control Overview.

**UNIT - V**
Business Continuity and Disaster Recovery Planning Control – Data backup/storage, Developing appropriate Disaster recovering strategy, Business Impact analysis.

TEXT BOOK:

1. Information System Audit and Assurance; D. P. Dube, Ved Prakash Gulati; Tata McGraw- Hill Education, 01 Jan 2005.

2. William Stallings and Lawrie Brown, Computer Security: Principles and Practice, Pearson education

**REFERENCE BOOKS**:

1. Martin Weiss and Michael G. Solomon, Auditing IT Infrastructures for Compliance (Information Systems Security & Assurance), Jones and Bartlett Publishers, Inc.

2. Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM by Regner Sabillon

## 22CY4173: SOCIAL MEDIA SECURITY
## (Professional Elective – IV)

**B.Tech. IV Year I Sem.**

| L | T | P | C |
|---|---|---|---|
| 3 | 0 | 0 | 3 |

**Prerequisites**

- Web Technologies, Cyber Laws and Ethics

**Course Objectives**

1. To introduce social media platforms and related security concerns.
2. To discuss cyber threats in social media.
3. To evaluate social media campaigns and content management.
4. To investigate risks of data leakage and misuse.
5. To develop security and privacy policies for social platforms.

**Course Outcomes**

1. Learn about browser's risks
2. Learn about Social Networking,
3. Understand the risks while using social media.
4. Understand security of different web browsers.
5. Understand threats and safety measures involved using an email communication

**UNIT – I**

Introduction to Social Media, Understanding Social Media, Different Types and Classifications, The Value of Social Media, Cutting Edge Versus Bleeding Edge, The Problems That Come With Social Media, Is Security Really an Issue? Taking the Good With the Bad

**UNIT - II**

Dark side Cyber-crime, Social Engineering, Hacked accounts, cyber stalking, cyber bullying, predators, phishing, hackers

**UNIT – III**

Being bold versus being overlooked Good social media campaigns, Bad social media campaigns, sometimes it's better to be overlooked, social media hoaxes, The human factor, Content management, Promotion of social media

**UNIT - IV**

Risks of Social media Introduction Public embarrassment, Once it's out there, it's out there False information, Information leakage, Retention and archiving, Loss of data and equipment

**UNIT – V**

Policies and Privacy Blocking users controlling app privacy, Location awareness, Security Fake accounts passwords, privacy and information sharing

**TEXT BOOKS:**

1. Interdisciplinary Impact Analysis of Privacy in Social Networks,Recognizing Your Digital Friends, Encryption for Peer-to-Peer Social NetworksCrowdsourcing and Ethics, Authors: Altshuler Y, EloviciY, Cremers A.B, Aharony N, Pentland A. (Eds.)
2. Social media security https://www.sciencedirect.com/science/article/pii/B97815974998660000

**REFERENCE BOOKS:**

1. Michael Cross, Social Media Security Leveraging Social Networking While Mitigating Risk.
2. Online Social Networks Security, Brij B. Gupta, Somya Ranjan Sahoo, Principles, Algorithm, Applications, and Perspectives, CRC press.

## 22CY4174: AUTHENTICATION TECHNIQUES
## (Professional Elective – IV)

**B.Tech. IV Year I Sem.** **L T P C**
**3 0 0 3**

**Prerequisites**

- Cryptography and Network Security, Operating Systems.

**Course Objectives:**

1. To introduce authentication methods and attack defences.
2. To analyse public-key protocols and key agreements.
3. To describe biometric authentication techniques.
4. To explore local and address-based authentication methods.
5. To explain indirect and enterprise authentication protocols.

**Course Outcomes:**

1. Understand different types of authentication techniques
2. Understand authentication and Key Transport using Key Cryptography
3. Understand different biometric techniques used in authentication.
4. Understand the procedure of local authentication and Authentication by Addresses.
5. Apply various authentication protocols in different environments and their representation

**UNIT - I**

**Introduction to Authentication:** Protocol Architectures, Cryptographic tools, Adversary capabilities, Goals for authentication and key establishment, Tools for verification of Protocols
**Authentication Tokens:** Tokens, Network Password Sniffing, One-Time Passwords, Man in the middle Attack, IP Hijacking, Incorporating a PIN, Enrolling Users

**UNIT- II**

**Authentication and Key Transport Using Public Key Cryptography:** Entity Authentication Protocols: Protocols in ISO/IEC 9798-3, Protocols in ISO/IEC 9798-5, SPLICE/AS, Key Transport Protocols**.**
**Key Agreement Protocols:** Introduction, Diffie-Hellman Key Agreement, MTI Protocols, Diffie-Hellman based protocols with Basic Message Format, Diffie-Hellman based protocols with explicit authentication**.**

**UNIT- III**

**Biometrics:** Biometrics, Uses of Biometrics, Biometric Techniques, How Biometrics Work, taking a Biometric Reading, Feedback During Biometric Input, forging a Physical Trait, Building and Matching Patterns, A Trivial Hand Geometry Biometric, Enrolling a User, Biometric Accuracy, Biometric Encryption, Authenticity of Biometric Data, The Problem of Biometric Exploitation

**UNIT- IV**

**Local Authentication:** Laptops and Workstations, Workstation Encryption, File Encryption, Volume Encryption, Encryption for Data Protection, Shortcut Attacks on Encryption, Trial-and-Error Attacks on Encryption, Theoretical Guess-Rate Limitations, Key-Handling Issues, Key-Handling Policies, Key Escrow and Crypto Politics
**Authentication by Address:** Telephone Numbers as Addresses, Identification via Dial-Back, Dial-Up Identification: Caller ID, Network Addresses, Denial of Service Attacks, Effective Source Authentication, Unix Local Network Authentication, Remote Procedure Calls, NFS, and NIS, Authenticating a Geographical Location**.**

**UNIT- V**

**Indirect Authentication:** Indirect Authentication, Network Boundary Control, One-Time Password Products, LAN Resource Control, RADIUS Protocol, Protecting RADIUS Messages, RADIUS Challenge Response, Encrypted Connections and Windows NT, Encrypted Connections, Integrity Protection, Politics, Encryption, and Technical Choices, Windows NT Secure Channels, Secure Channel Keying, Attacks on Secure Channels, Computers' Authentication Secrets

**TEXT BOOKS:**


1. "Protocols for Authentication and Key Establishment", Colin Boyd and Anish Mathuria, springer, 202.
2. "Authentication: From Passwords to Public Keys", Smith, R. E. (2002), United Kingdom: Addison-Wesley.


**REFERENCE BOOKS:**


1. Biometrics Authentication: A Practical Guide to Fingerprint, Face, Iris, and Speech Recognition by Anil Jain, Arun Ross, and Karthik Nandakumar
2. Kerberos: The Protocol and Its Applications by William Stallings
3. Biometrics Technologies and verification Systems, John Vacca, , Elsevier Inc., 2007.
4. Pattern Classification, Richard O. Duda, David G.Stork, Peter E. Hart, Wiley 2007.

**22AM4175: QUANTUM COMPUTING**
**(Professional Elective – V)**

**B.Tech. IV Year I Sem.** **L T P C**
**3 0 0 3**

**Prerequisites:**

1. Linear Algebra

**Course Objectives: The objective of this course is to:**

1. To introduce the fundamentals of quantum computing
2. To introduce problem-solving approach using finite dimensional mathematics
3. To learn the basic quantum logical operations and algorithms for processing quantum information.
4. To learn the basic knowledge about the practical use of quantum algorithms and quantum programming skills.
5. To learn the basic quantum logical operations and algorithms for processing quantum information.

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

1. To Understand basics of quantum computing
2. To Understand physical implementation of Qubit
3. To Understand Quantum algorithms and their implementation
4. To Understand the Impact of Quantum Computing on Cryptography
5. To Understand simple quantum algorithms and information channels in the quantum circuit model

**UNIT – I**

**Introduction to Essential Linear Algebra:** Some Basic Algebra, Matrix Math, Vectors and Vector Spaces, Set Theory. Complex Numbers: Definition of Complex Numbers, Algebra of Complex Numbers, Complex Numbers Graphically, Vector Representations of Complex Numbers, Pauli Matrice, Transcendental Numbers.

**UNIT – II**

**Basic Physics for Quantum Computing:** The Journey to Quantum, Quantum Physics Essentials, Basic Atomic Structure, Hilbert Spaces, Uncertainty, Quantum States, Entanglement.

**Basic Quantum Theory**: Further with Quantum Mechanics, Quantum Decoherence, Quantum Electrodynamics, Quantum Chromodynamics, Feynman Diagram Quantum Entanglement and QKD, Quantum Entanglement, Interpretation, QKE.

**UNIT – III**

**Quantum Architecture:** Further with Qubits, Quantum Gates, More with Gates, Quantum Circuits, The D-Wave Quantum Architecture. Quantum Hardware: Qubits, How Many Qubits Are Needed? Addressing Decoherence, Topological Quantum Computing, Quantum Essentials.

**UNIT – IV**

Quantum Algorithms: What Is an Algorithm? Deutsch's Algorithm, Deutsch-Jozsa Algorithm, Bernstein-Vazirani Algorithm, Simon's Algorithm, Shor's Algorithm, Grover's Algorithm.

**UNIT – V**

**Current Asymmetric Algorithms:** RSA, Diffie-Hellman, Elliptic Curve.

**The Impact of Quantum Computing on Cryptography:**

Asymmetric Cryptography, Specific Algorithms, Specific Applications.

**TEXT BOOKS:**


1. Nielsen M. A., Quantum Computation and Quantum Information, Cambridge University Press
2. Dr. Chuck Easttom, Quantum Computing Fundamentals, Pearson


**REFERENCE BOOKS:**


1. Quantum Computing for Computer Scientists by Noson S. Yanofsky and Mirco A. Mannucci
2. Benenti G., Casati G. and Strini G., Principles of Quantum Computation and Information, Vol. Basic Concepts. Vol. Basic Tools and Special Topics, World Scientific.
3. Pittenger A. O., An Introduction to Quantum Computing Algorithms.

**22IT4177: DEEP LEARNING**
**(Professional Elective – V)**

**B.Tech. IV Year I Sem.** **L T P C**
**3 0 0 3**

**Prerequisite(s):** Artificial Intelligence

**Course Objectives:** Develop ability to

- Understand various learning models.
- Learn feed forward neural networks for learning
- Learn to use auto encoders and regularization
- Understand Convolution Neural Networks for learning
- Understand Recurrent Neural Networks for learning

**Course Outcomes (COs)**

- Analyze various learning models.
- Use feed forward neural networks for learning
- Highlight the importance of auto encoders and regularization
- Apply Convolution Neural Networks for learning
- Apply Recurrent Neural Networks for learning

**UNIT I**

**Introduction-** Historical Trends in Deep Learning, McCulloch Pitts Neuron, Thresholding Logic, Perceptron, Perceptron Learning Algorithm. Representation Power of MLPs, Sigmoid Neurons, Gradient Descent, Feed forward Neural Networks, Representation Power of Feed forward Neural Networks.

**UNIT II**

**Feed Forward Neural Networks: -** Back propagation, Gradient Descent (GD), Momentum Based GD, Nesterov Accelerated GD, Stochastic GD, AdaGrad, RMS Prop, Adam, Eigenvalues and Eigenvectors, Eigenvalue Decomposition, Basis Principal Component Analysis and its interpretations, Singular Value Decomposition.

**UNIT III**

**Auto encoders:-** Relation to PCA, Regularization in auto encoders, Denoising auto encoders, Sparse auto encoders, Contractive auto encoders, Regularization: Bias Variance Tradeoff, L2 regularization, early stopping, Dataset augmentation, Parameter sharing and tying, Injecting noise at input, Ensemble methods, Dropout, Greedy Layer wise Pre-training, Better activation functions, better weight initialization methods, Batch Normalization.

**UNIT IV**

**Convolutional Neural Network: -** The Convolution Operation, Motivation, Pooling,Convolution and Pooling as an Innitely Strong Prior, Variants of the Basic Convolution Function, Structured Outputs, Data Types, LeNet, AlexNet, ZF-Net, VGGNet, GoogLeNet,ResNet, Visualizing Convolutional Neural Networks, Guided Back propagation, Deep Dream, Deep Art, Fooling Convolutional Neural Networks.

**UNIT V**

**Recurrent Neural Networks**-Back propagation through time (BPTT), Vanishing and Exploding Gradients, Truncated BPTT, GRU, LSTMs, Encoder Decoder Models, Attention Mechanism, Attention over images.

**Text Books:**

**1.** Good fellow. I., Bengio.Y. and Courville.A., " Deep Learning", MITPress, 2016.

**References:**

1. Ragav Venkatesan, Baoxin Li, "Convolutional Neural Networks in Visual Computing", CRC Press, 2018.
2. Navin Kumar Manaswi, "Deep Learning with Applications Using Python", A press, 2018.
3. John D Kelleher "Deep Learning" (The MIT Press Essential Knowledge series) The MIT Press,2019.
4. Daniel Graupe "Deep Learning Neural Networks: Design and Case Studies", World Scientific Publishing Co Pte Ltd, 2016.
5, Rajiv Chopra "Deep Learning", Khanna Book Publishing ,2018.

.

## 22CY4175: DATA ANALYTICS FOR FRAUD DETECTION
**(Professional Elective – V)**

**B.Tech. IV Year I Sem.** **L T P C**
**3 0 0 3**

**Prerequisites**

- Probability and Statistics, Data Mining, Python for Data Analysis.

**Course Objectives**

1. To introduce the concept of fraud and the need for analytics.
2. To describe the data analysis cycle and data preparation.
3. To explain standard analytical tests for fraud detection.
4. To illustrate advanced techniques for detecting fraud patterns.
5. To discuss fraud schemes in payroll and reimbursements.

**Course Outcomes**

1. Formulate reasons for using data analysis to detect fraud.
2. Explain characteristics and components of the data and assess its completeness.
3. Identify known fraud symptoms and use digital analysis to identify unknown fraud symptoms.
4. Automate the detection process.
5. Verify results and understand how to prosecute fraud

**UNIT - I**

**Introduction:** Defining Fraud, Anomalies versus Fraud, Types of Fraud, Assess the Risk of Fraud, Fraud Detection, Recognizing Fraud, Data Mining versus Data Analysis and Analytics, Data Analytical Software, Anomalies versus Fraud within Data, Fraudulent Data Inclusions and Deletions

**UNIT - II**

The Data Analysis Cycle, Evaluation and Analysis, Obtaining Data Files, Performing the Audit, File Format Types, Preparation for Data Analysis, Arranging and Organizing Data Statistics and Sampling, Descriptive Statistics, Inferential Statistics

**UNIT - III**

**Data Analytical Tests:** Benford's Law, Number Duplication Test, Z-Score, Relative Size Factor Test, Same-Same-Same Test, Same-Same-Different Test

**UNIT - IV**

**Advanced Data Analytical Tests**

Correlation, Trend Analysis, GEL-1 and GEL-2, Skimming and Cash Larceny, Billing schemes: and Data Familiarization, Benford's Law Tests, Relative Size Factor Test, Match Employee Address to Supplier data

**UNIT - V**

Payroll Fraud, Expense Reimbursement Schemes, Register disbursement schemes

**TEXT BOOK:**

1. Fraud and Fraud Detection: A Data Analytics Approach by Sunder Gee, Wiley
2. Data Analytics: The Magic Tool of Fraud Detection by by Kelechukwu Aku | 29 August 2022

**REFERENCE BOOKS:**

1. Blokdyk Gerardus, Data analysis techniques for fraud detection, Create space Independent Publishing Platform
2. Leonard W. Vona, Fraud Data Analytics Methodology: The Fraud Scenario Approach to Uncovering Fraud in Core Business Systems, Wiley.

## 22CY4176: SECURITY INCIDENT AND RESPONSE MANAGEMENT
## (Professional Elective – V)

**B.Tech. IV Year I Sem.** **L T P C**
**3 0 0 3**

**Prerequisites:**
- Knowledge of information security and applied cryptography.
- Knowledge of Operating Systems.
- Digital Forensics

**Course Objectives:**
1. To introduce incident response preparation and scope definition.
2. To outline live data collection and forensic duplication.
3. To explore network evidence and enterprise services analysis.
4. To clarify Windows forensic analysis and memory artifacts.
5. To explain investigation techniques for macOS and applications.

**Course Outcomes:**
1. Learn how to handle the incident response management.
2. Perform live data collection and forensic duplication.
3. Identify network evidence.
4. Analyse data to carry out an investigation.
5. Knowledge on investigation on Mac and Windows OS systems

**UNIT- I**

**Introduction**: Preparing for the inevitable incident: Real-world incident, IR management incident handbook, Pre-incident preparation, preparing the Organization for Incident Response, Preparing the IR team, preparing the Infrastructure for Incident Response.

**Incident Detection and Characterization:** Getting the investigation started on the right foot, collecting initial facts, Maintenance of Case Notes, Understanding Investigative Priorities.

**Discovering the scope of Incident:** Examining initial data, Gathering and reviewing preliminary evidence, determining a course of action, Customer data loss scenario, automated clearing fraud scenario.

**UNIT- II**

**Data Collection:** Live Data Collection: When to perform live response, selecting a live response tool, what to collect, collection best practices, Live data collection on Microsoft Windows Systems, Live Data Collection on Unix-based Systems.

**Forensic Duplication:** Forensic Image Formats, Traditional duplication, live system duplication, Duplication of Enterprise Assets.

**UNIT- III**

**Network Evidence:** The case for network monitoring, Types for network monitoring, setting up a Network Monitoring System, Network Data, Analysis, Collect Logs Generated from Network Events. **Enterprise Services**: Network Infrastructure Services, Enterprise Management Applications, Web servers, Database Servers.

**UNIT- IV**

**Data Analysis:** Analysis Methodology: Define Objectives Know your data, access your data, analyse your data, Evaluate Results.

**Investigating Windows Systems**: NTFS and File System analysis, prefetch, Event logs, Scheduled Tasks, The Windows Registry, Other Artifacts of Interactive Sessions, Memory Forensics, Alternative Persistence Mechanisms.

**UNIT- V**

**Investigating Mac OS X System**s: HFS and File System Analysis, Core Operating Systems data. **Investigating Applications**: What is Application Data? Where is application data stored? General Investigation methods, Web Browser, Email Clients, Instant Message Clients.

**TEXT BOOK:**

1. "Incident Response and Computer Forensics", Jason T. Luttgens, Mathew Pepe and Kevin Mandia, 3rd Edition, Tata McGraw-Hill Education.
2. "Cyber Security Incident Response-How to Contain, Eradicate, and Recover from Incidents", Eric. C. Thompson, Apress.

**REFERENCE BOOKS:**

1. "Cyber Security Incident Response-How to Contain, Eradicate, and Recover from Incidents", Eric. C. Thompson, Apress.
2. "The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk", N.K. McCarthy, Tata McGraw-Hill.

## 22CY4151: VULNERABILITY ASSESSMENT & PENETRATION TESTING LAB

**B.Tech. IV Year I Sem.**

| L | T | P | C |
|---|---|---|---|
| 0 | 0 | 2 | 1 |

**Course Objectives:**

1. To learn and apply penetration testing methodologies across various scenarios.
2. To monitor and analyse network traffic using open-source tools.
3. To discover hosts and services on a network.
4. To understand and perform vulnerability scanning and assessment.
5. To assess web application security using practical tools.

**Course Outcomes:**

1. Design solutions for monitoring network traffic using tools like Wireshark and tcpdump.
2. Perform host and service discovery using tools such as Nmap and Masscan.
3. Execute vulnerability scanning using tools like OpenVAS and SQLmap.
4. Carry out internal and external penetration testing techniques.
5. Assess web application vulnerabilities using tools like Nikto, Burp Suite, and OWASP ZAP.

**List of Experiments:**

1. Implement Monitoring of Network Trafficking
    a. wireshark
    b. tcpdump
    c. Nagios
    d. solarwinds
2. Implement Host & Services Discovery using Nmap, massscan.
3. Implement Vulnerability Scanning using OpenVAS, Zapproxy, SQLmap.
4. Implement Internal Penetration Testing.
    a. Mapping
    b. Scanning
    c. Gaining access through CVE's
    d. Sniffing POP3/FTP/Telnet Passwords
    e. ARP Poisoning
    f. DNS Poisoning
5. Implement External Penetration Testing.
    a. Evaluating external Infrastructure.
    b. Creating topological map & identifying IP address of target.
    c. Lookup domain registry for IP information.
    d. Examining use of IPV6 at remote location.
6. Implement Vulnerability scanning with Nessus.
7. Implement Vulnerability scanning with openvas.
8. Implement Web application assessment with nikto.
9. Implement Web application assessment with burp suite.
10. Implement Web application assessment with owaspzap,

**TEXT BOOKS:**

1. " Gray Hat Hacking-The Ethical Hackers Handbook", Allen Harper, Stephen Sims, Michael Baucom, 3rd Edition, Tata Mc Graw-Hill.

2. " The Web Application Hacker's Handbook-Discovering and Exploiting Security flaws", Dafydd Suttard, Marcus pinto, 1st Edition, Wiley Publishing.

3. "Penetration Testing: A Hands-On Introduction to Hacking", Author: Georgia Weidman, Publisher: No Starch Press

**REFERENCE BOOKS:**

1. "Penetration Testing: Hands-on Introduction to Hacking", Georgia Weidman, 1st Edition, No Starch Press.
2. " The Pen Tester Blueprint-Starting a Career as an Ethical Hacker ", L. Wylie, Kim Crawly, 1st Edition, Wiley Publications.

## 22CY4152: NETWORK MANAGEMENT SYSTEMS AND OPERATIONS LAB

**B.Tech. IV Year I Sem.**

| L | T | P | C |
|---|---|---|---|
| 0 | 0 | 2 | 1 |

**Course Objectives:**

1. To gain practical experience in discovering and mapping networks.
2. To implement network security policies and ensure compliance.
3. To automate network tasks using configuration management tools.
4. To diagnose faults and monitor traffic using industry tools.
5. To enforce network security through configuration and monitoring.

**Course Outcomes:**

1. Analyse and document network infrastructure using discovery tools like Nmap.
2. Implement and test policy compliance using tools such as Snort or pfSense.
3. Automate network configurations and updates using Ansible.
4. Diagnose network issues using Wireshark, Nagios, and tcpdump.
5. Apply security tools for traffic monitoring and threat detection.

**List of Experiments:**

1. Network Discovery and Mapping
   A. Utilize tools like Nmap and Wireshark to perform network discovery.
   B. Create a visual map of the network infrastructure.
   C. Analyse the implications of the network structure on management strategies.

2. Policy Implementation and Compliance
   A. Use tools like Snort or Suricata for intrusion detection.
   B. Implement firewall rules with tools such as iptables or pfSense.
   C. Assess compliance with security policies and regulatory requirements.

3. Automation with Ansible
   A. Set up Ansible for network configuration management.
   B. Automate routine tasks such as software updates and configuration changes.
   C. Evaluate the impact of automation on efficiency and responsiveness.
4. Fault Detection with Wireshark and Nagios
5. Protocol Analysis with Tcpdump
6. Traffic Analysis with Wireshark and Bandwidthd
7. Traffic Measurement with Ntopng
8. Threat Modeling with OWASP Cornucopia
9. Risk Assessment with OpenVAS
10. Firewall Configuration with pfSense
11. Network Discovery with Nmap
12. Security Enforcement with Snort

**TEXT BOOK:**

1. Automated Network Management Systems, D. Comer, Prentice Hall, 2006, ISBN No. 0132393085.
2. "Practical Network Automation: Leverage the power of Python and Ansible to optimize your network", Author: Abhishek Ratan, Publisher: Packt Publishing

**REFERENCE BOOKS:**

1. Nagios Core Administration Cookbook - Second Edition, Tom Ryder, 2016, Packt Publishing, ISBN: 781785889332.
2. Terraform: Up and Running, Yevgeniy Brikman, 2017, O'Reilly Media, Inc., ISBN: 9781491977088

## 22CY4181: INTERNSHIP

**B.Tech. IV Year I Sem.**

| L | T | P | C |
|---|---|---|---|
| 0 | 0 | 2 | 1 |

## 22CY4182: PROJECT STAGE I

**B.Tech. IV Year I Sem.**

| L | T | P | C |
|---|---|---|---|
| 0 | 0 | 4 | 2 |

## 22MB4211: ORGANIZATIONAL BEHAVIOUR

**B.Tech. IV Year II Sem.**

| L | T | P | C |
|---|---|---|---|
| 3 | 0 | 0 | 3 |

**Course Objectives:**

1) To analyse the behaviour of individuals and groups in organizations in terms of the key factors that influence organizational behaviour.
2) To understand the potential effects of organizational level factors (such as structure, culture and change) on organizational behaviour.
3) To evaluate the potential effects of important developments in the external environment (such as globalization and advances in technology) on organizational behaviour.
4) To analyse organizational behavioural issues in the context of organizational behaviour theories, models and concepts
5) To understand the concepts of leadership and Behavioural Performance Management.

**Course Outcomes:**

1) The students able to analyse the behaviour of individuals and groups in organizations in terms of the key factors that influence organizational behaviour.
2) The students able to understand the potential effects of organizational level factors (such as structure, culture and change) on organizational behaviour.
3) The students able to evaluate the potential effects of important developments in the external environment (such as globalization and advances in technology) on organizational behaviour.
4) The students able to analyse organizational behavioural issues in the context of organizational behaviour theories, models and concepts
5) The students able to understand the concepts of leadership and Behavioural Performance Management.

**UNIT - I**

Introduction to OB - Definition, Nature and Scope –Environmental and organizational context – Impact of IT, globalization, Diversity, Ethics, culture, reward systems and organizational design on Organisational Behaviour. Cognitive Processes-I : Perception and Attribution: Nature and importance of Perception – Perceptual selectivity and organization -Social perception – Attribution Theories – Locus of control – Attribution Errors –Impression Management.

**UNIT - II**

Cognitive Processes-II: Personality and Attitudes - Personality as a continuum – Meaning of personality - Johari Window and Transactional Analysis - Nature and Dimension of Attitudes – Job satisfaction and organisational commitment-Motivational needs and processes- Work-Motivation Approaches Theories of Motivation- Motivation across cultures- Positive organizational behaviour: Optimism – Emotional intelligence – Self-Efficacy.

**UNIT - III**

Dynamics of OB-I: Communication – types - interactive communication in organizations –barriers to communication and strategies to improve the follow of communication – Decision Making: Participative decision-making techniques – creativity and group decision making. Dynamics of OB –II Stress and Conflict: Meaning and types of stress –Meaning and types of conflict - Effect of stress and intra-individual conflict - strategies to cope with stress and conflict.

**UNIT - IV**

Dynamics of OB –III Power and Politics: Meaning and types of power – empowerment -Groups Vs. Teams – Nature of groups –dynamics of informal groups – dysfunctions of groups and teams – teams in modern work place.

**UNIT - V**

Leading High performance: Job design and Goal setting for High performance- Quality of Work Life- Socio technical Design and High-performance work practices – Behavioural Performance management: reinforcement and punishment as principles of Learning –Processof Behavioural modification - Leadership theories - Styles, Activities and skills of Great Leaders.

**TEXT BOOKS:**


1. Luthans, Fred: Organizational Behaviour 10/e, McGraw-Hill, 2009
2. Mc Shane: Organizational Behaviour, 3e, TMH, 2008
3. Nelson: Organizational Behaviour, 3/e, Thomson, 2008.
4. New strom W. John& Davis Keith, Organisational Behaviour-- Human Behaviour atWork, 12/e, TMH, New Delhi, 2009.
5. Pierce and Gardner: Management and Organisational Behaviour: An Integratedperspective, Thomson, 2009.
6. Robbins, P. Stephen, Timothy A. Judge: Organisational Behaviour, 12/e,PHI/Pearson, New Delhi, 2009.
7. PareekUdai: Behavioural Process at Work: Oxford & IBH, New Delhi, 2009.


**REFERENCE BOOKS**:


1. Schermerhorn: Organizational Behaviour 9/e, Wiley, 2008.
2. Hitt: Organizational Behaviour, Wiley, 2008
3. Aswathappa: Organisational Behaviour, Himalaya, 2009
4. Mullins: Management and Organisational Behaviour, Pearson, 2008.
5. McShane, Glinow: Organisational Behaviour--Essentials, TMH, 2009.
6. Ivancevich: Organisational Behaviour and Management, 7/e, TMH, 2008.

## 22CY4271: QUANTUM CRYPTOGRAPHY
**(Professional Elective – VI)**

**B.Tech. IV Year II Sem.**

| L | T | P | C |
|---|---|---|---|
| 3 | 0 | 0 | 3 |

**Prerequisites:**
- Quantum computing, Cryptography and Network Security.

**Course Objectives**
1. To introduce quantum information theory and QKD basics.
2. To describe error correction in QKD using adaptive protocols.
3. To identify and explain attack strategies on QKD systems.
4. To analyse statistical methods in quantum key networks.
5. To demonstrate the application of QKD in real-world scenarios.

**Course Outcomes**
1. Explain QKD, entropy, and secure communication concepts.
2. Compare error correction strategies in quantum systems.
3. Evaluate the security of QKD under various attacks.
4. Interpret data routing in QKD networks.
5. Apply QKD models in real-world secure communication.

**UNIT - I**
Quantum Information Theory, Unconditional Secure Authentication, Entropy, Quantum Key Distribution, Quantum Channel, Public Channel, QKD Gain, Finite Resources

**UNIT - II**
Adaptive Cascade Introduction, Error Correction and the Cascade Protocol, Adaptive Initial Block-Size Selection, Fixed Initial Block-Size, Dynamic Initial Block-Size, Examples

**UNIT - III**
Attack Strategies on QKD Protocols: Introduction, Attack Strategies in an Ideal Environment, Individual Attacks in an Realistic Environment QKD Systems: Introduction, QKD Systems

**UNIT - IV**
Statistical Analysis of QKD Networks in Real-Life Environment: Statistical Methods, Statistical Analysis QKD Networks Based on Q3P: QKD Networks, PPP, Q3P, Routing, Transport

**UNIT - V**
Quantum-Cryptographic Networks from a Prototype to the Citizen: The SECOQC Project, How to Bring QKD into the "Real" Life The Ring of Trust Model: Introduction, Model of the Point of Trust, Communication in the Point of Trust Model, Exemplified Communications, A Medical Information System Based on the Ring of Trust

**TEXT BOOK:**
1. Kollmitzer C., Pivk M. (Eds.), Applied Quantum Cryptography, Lect. Notes Phys. 797 (Springer, Berlin Heidelberg 2010).
2. Introduction to Quantum Cryptography by Thomas Vidick and Stephanie Wehner

**REFERENCE BOOKS:**
1. Gerald B. Gilbert, Michael Hamrick, and Yaakov S. Weinstein, Quantum Cryptography, World Scientific Publishing.
2. Gilles Van Assche, Quantum Cryptography and Secret-Key Distillation, Cambridge University Press.

## 22CY4272: CLOUD SECURITY
## (Professional Elective – VI)

**B.Tech. IV Year II Sem.** **L T P C**
**3 0 0 3**

**Pre-requisites:**
- Computer Networks, Cryptography and Network Security, Cloud Computing.

**Course Objectives:**
1. To introduce cloud models and basic security concepts.
2. To discuss cloud security and privacy at various layers.
3. To outline threats and attacks in cloud environments.
4. To explain data security and storage practices.
5. To illustrate advanced cloud security and management tools.

**Course Outcomes:**
1. Distinguish between cloud service and deployment models.
2. Evaluate privacy and security mechanisms at all cloud layers.
3. Classify types of attacks and security tools in the cloud.
4. Analyse data protection strategies in cloud environments.
5. Implement access control and configuration management in cloud setups.

**UNIT - I**

**Overview of Cloud Computing:** Introduction, Definitions and Characteristics, Cloud Service Models, Cloud Deployment Models, Cloud Service Platforms, Challenges Ahead.
**Introduction to Cloud Security:** Introduction, Cloud Security Concepts, CSA Cloud Reference Model, NIST Cloud Reference Model, NIST Cloud Reference Model.

**UNIT - II**

**Cloud Security and Privacy Issues:** Introduction, Cloud Security Goals/Concepts, Cloud Security Issues, Security Requirements for Privacy, Privacy Issues in Cloud.
**Infrastructure Security:** The Network Level, the Host Level, The Application Level, SaaS Application Security, PaaS Application Security, IaaS Application Security.

**UNIT – III**

**Threat Model and Cloud Attacks:** Introduction, Threat Model- Type of attack entities, Attack surfaces with attack scenarios, A Taxonomy of Attacks.
**Attack Tools**: Network-level attack tools, VM-level attack tools, VMM attack tools, Security Tools, VMM security tools.

**UNIT - IV**

**Information Security Basic Concepts**: an Example of a Security Attack, Cloud Software Security Requirements, Rising Security Threats.
**Data Security and Storage:** Aspects of Data Security, Data Security Mitigation, Provider Data and Its Security.

**UNIT - V**

**Evolution of Security Considerations**: Security Concerns of Cloud Operating Models, Identity Authentication, Secure Transmissions, Secure Storage and Computation, Security Using Encryption Keys, Challenges of Using Standard Security Algorithms, Variations and Special Cases for Security Issues with Cloud Computing, Side Channel Security Attacks in the Cloud.
**Security Management in the Cloud**: Security Management Standards, Availability Management, Access Control, Security Vulnerability, Patch, and Configuration Management.

**TEXT BOOKS:**
1. Cloud Security Attacks, Techniques, Tools, and Challenges by Preeti Mishra, Emmanuel S Pilli, Jaipur R C Joshi Graphic Era, 1st Edition published 2022 by CRC press.
2. Cloud Security and Privacy by Tim Mather, Subra Kumaraswamy, and Shahed Lati First Edition, September 2019.
3. Cloud Computing with Security and Scalability, Concepts and Practices by Naresh Kumar Sehgal, Pramod Chandra P. Bhatt, John M. Acken · Springer International Publishing 2022.

**REFERENCE BOOKS:**
1. Essentials of Cloud Computing by K. Chandrasekaran Special Indian Edition CRC press.
2. Cloud Computing Principles and Paradigms by Rajkumar Buyya, John Wiley.

## 22CY4273: DIGITAL WATERMARKING AND STEGANOGRAPHY
## (Professional Elective – VI)

**B.Tech. IV Year II Sem.** **L T P C**
**3 0 0 3**

**Pre-requisites:**
- Cryptography and Network Security

**Course Objectives:**
1. To introduce information hiding techniques and applications.
2. To explain watermarking with side information and error analysis.
3. To describe perceptual models and robust embedding methods.
4. To discuss watermark security and authentication methods.
5. To explore steganography and steganalysis techniques.

**Course Outcomes:**
1. Know the History and importance of watermarking and steganography
2. Analyse Applications and properties of watermarking and steganography.
3. Demonstrate Models and algorithms of watermarking.
4. Possess the passion for acquiring knowledge and skill in preserving authentication of Information
5. Identify the theoretic foundations of steganography and steganalysis.

**UNIT - I**
**Introduction:** Information Hiding, Steganography and Watermarking, History of watermarking, Importance of digital watermarking, Applications and Properties, Evaluating watermarking systems. Watermarking models & message coding, Notation, Communications, Communication-based models, Geometric models, Mapping messages into message vectors, Error correction coding, Detecting multi-symbol watermarks.

**UNIT - II**
**Watermarking with side information &analysing errors:** Informed Embedding, Informed Coding – Structured dirty-paper codes, Message errors, False positive errors, False negative errors, ROC curves – Effect of whitening on error rates.

**UNIT - III**
**Perceptual models:** Evaluating perceptual impact, General form of a perceptual model, Examples of perceptual models, Robust watermarking approaches, Redundant Embedding, Spread Spectrum Coding, Embedding in Perceptually significant coefficients.

**UNIT - IV**
**Watermark security & authentication:** Security requirements, Watermark security and cryptography, Attacks, Exact authentication, Selective authentication, Localization, Restoration.

**UNIT - V**
**Steganography:** Steganography communication, Notation and terminology, Information, theoretic foundations of steganography, Practical steganographic methods, Minimizing the embedding impact, Steganalysis.

**TEXT BOOKS:**
1. Digital Watermarking and Steganography, Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, Morgan Kaufmann Publishers, New York, 2008.
2. Digital Watermarking and Steganography by Frank Y. Shih

**REFERENCE BOOKS:**
1. Techniques and Applications of Digital Watermarking and Contest Protection, Michael Arnold, Martin Schmucker, Stephen D. Wolthusen, Artech House, London, 2003.
2. Digital Watermarking for Digital Media, Juergen Seits, IDEA Group Publisher, New York, 2005.
3. Disappearing Cryptography – Information Hiding: Steganography & Watermarking, PeterWayner, Morgan Kaufmann Publishers, New York, 2002.

## 22CY4274: DATA PRIVACY
## (Professional Elective – VI)

**B.Tech. IV Year II Sem.** **L T P C**
**3 0 0 3**

**Pre-requisites:**
- Cryptography and Network Security, DBMS

**Course Objectives:**
1. To introduce data privacy principles and anonymization methods.
2. To discuss anonymization techniques for multidimensional data.
3. To explain privacy protection for complex data types.
4. To analyse threats to anonymized datasets.
5. To demonstrate privacy-preserving data mining and test data generation.

**Course Outcomes:**
1. Identify principles and techniques for protecting personal data.
2. Apply k-anonymity, l-diversity, and t-closeness.
3. Develop anonymization strategies for complex data.
4. Assess vulnerabilities in anonymized datasets.
5. Construct privacy-preserving synthetic and test data.

**UNIT - I**

**Introduction to Data Privacy**: Overview of Data Privacy, Importance of Data Privacy, Protecting Sensitive Data, Use Cases for Data Sharing, Methods of Protecting Data, Balancing Data Privacy and Utility, Introduction to Anonymization Design Principles.

**Nature of Data in the Enterprise:** Multidimensional Data, Transaction Data, Longitudinal Data, Graph Data, Time Series Data.

**UNIT - II**

**Static Data Anonymization I**: Multidimensional Data: -Introduction, Classification of Privacy-Preserving Methods, Classification of Data in a Multidimensional Data: Protecting explicit identifiers protecting Quasi-identifiers, Group Based Anonymization: k-Anonymization, I-Diversity, t-Closeness, Algorithm Comparison.

**UNIT - III**

**Static Data Anonymization II**: Complex Data Structures- Introduction, Privacy Preserving Graph Data, Privacy-Preserving Time Series Data, Privacy Preservation of Longitudinal Data, Privacy Preservation of Transaction Data.

**UNIT - IV**

**Threats to Anonymized Data**: Threats to Anonymized Data, Threats to Data Structures, Multidimensional Data, Longitudinal Data, Graph Data, Time Series Data, Transaction Data, Threats by Anonymization Techniques: Randomization, k-Anonymization, l-diversity, t-closeness.

**UNIT - V**

**Privacy-Preserving Data Mining:** Introduction, Data Mining: Key Functional Areas of Multidimensional Data, Privacy-Preserving Test Data Manufacturing, Test Data Fundamentals, Privacy Preservation of Test Data.

**Synthetic Data Generation:** Introduction, Synthetic Data and Their Use, Privacy and Utility in Synthetic Data, Dynamic Data Protection: Tokenization Introduction, Understanding Tokenization, Use Cases for Dynamic Data Protection, Benefits of Tokenization Compared to Other Methods, Components for Tokenization.

**TEXT BOOKS:**

1. Nataraj Venkataramanan, Ashwin Sriram, *Data Privacy: Principles and Practice*, 2016, 1st Edition, Taylor & Francis. (ISBN No.: 978-1-49-872104-2), United Kingdom.
2. L. Sweeney, Computational Disclosure Control: A Primer on Data Privacy Protection, MIT ComputerScience,2002.

**REFERENCE BOOKS:**

1. B. Raghunathan, the Complete Book of Data Anonymization: From Planning to Implementation, 1st Edition, CRC press.
2. L. Sweeney, Computational Disclosure Control: A Primer on Data Privacy Protection, MIT Computer Science, 2002.
3. Nishant Bhajaria, Data Privacy: A runbook for engineers, Manning Publications.

## 22CY4281: PROJECT STAGE II INCLUDING SEMINAR

**B.Tech. IV Year II Sem.**

| L | T | P | C |
|---|---|---|---|
| 0 | 0 | 22 | 11 |