SRI INDU INSTITUTE OF ENGINEERING AND TECHNOLOGY

(An Autonomous Institution)

B.Tech. in COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)
COURSE STRUCTURE & YEAR SYLLABUS

(BR22 Regulations)

Applicable from Academic Year: 2022-23 BATCH

IV YEAR I SEMESTER

S. No.	Course Code	Course Title	L	T	P	Credits
1	CS703PC	Vulnerability Assessment & Penetration Testing	3	0	0	3
2	CS704PC	Network Management Systems and Operations	3	0	0	3
3		Professional Elective - IV	3	0	0	3
4		Professional Elective - V	3	0	0	3
5		Open Elective - II	3	0	0	3
6	CS723PC	Vulnerability Assessment & Penetration Testing Lab	0	0	2	1
7	CS724PC	Network Management Systems and Operations Lab	0	0	2	1
8	CS713PC	Project Stage - I	0	0	6	3
		Total	**15**	**0**	**14**	**20**

IV YEAR II SEMESTER

S.No.	Course Code	CourseTitle	L	T	P	Credits
1	MBA801HS	Organizational Behavior	3	0	0	3
2		Professional Elective – VI	3	0	0	3
3		Open Elective – III	3	0	0	3
4	CS801PC	Project Stage – II including Seminar	0	0	22	11
		Total	**9**	**0**	**22**	**20**

***MC – Satisfactory/Unsatisfactory**

Professional Elective – IV

CS751PE	Edge Analytics
CS752PE	Web & Database Security
CS753PE	Information System Audit & Assurance
CS754PE	Social Media Security
CS755PE	Deep Learning

Professional Elective – V

CS765PE	Quantum Computing
CS757PE	Data Analytics for Fraud Detection
CS758PE	5G Technologies
CS759PE	Security Incident & Response Management (SOC)
CS760PE	Authentication Techniques

Professional Elective – VI

CS846PE	Quantum Cryptography
CS847PE	IoT Cloud Processing and Analytics
CS848PE	Cloud Security
CS849PE	Digital Watermarking and Steganography
CS850PE	Data Privacy

Open Electives (OE–II)

CS792OE	Information System Audit & Assurance
CS793OE	Social Media Security

Open Electives (OE–III)

CS882OE	Data Privacy
CS883OE	5G Technologies

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

(Course code: CS703PC)

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

- Give an introduction to Vulnerability Assessment and Penetration Testing.
- To be familiar with the Penetration Testing and Tools.
- To get an exposure to Metasploit exploitation tool, Linux exploit and Windows exploit.
- To gain knowledge on Web Application Security Vulnerabilities, Vulnerability analysis and Malware analysis.

Course Outcomes

- Learn to handle the vulnerabilities of a Web application
- Able to learn various penetration testing tools.
- Knowledge on Metasploit, Linux exploit and windows exploit tools
- Analyze various vulnerabilities

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 scripting vulnerabilities, the rest of the OWASP Top Ten SQL Injection vulnerabilities, Cross-site scripting vulnerabilities. **Vulnerability Analysis:** Passive Analysis, Source Code Analysis, Binary Analysis.

UNIT- V

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.

NETWORK MANAGEMENT SYSTEMS AND OPERATIONS

(Course code: CS704PC)

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

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.

EDGE ANALYTICS (Professional Elective – IV)

(Course code: CS751PE)

B.Tech. IV Year I Sem.

L	T	P	C
3	0	0	3

Prerequisites

1. A basic knowledge of “Python Programming”.

Course Objectives

- The aim of the course is to introduce the fundamentals of Edge Analytics
- The course gives an overview of – Architectures, Components, Communication Protocols and tools used for Edge Analytics

Course Outcomes

- Understand the concepts of Edge Analytics, both in theory and in practical application
- Demonstrate a comprehensive understanding of different tools used at edge analytics
- Formulate, Design and Implement the solutions for real world edge analytics

UNIT- I

Introduction to Edge Analytics

What is edge analytics, Applying and comparing architectures, Key benefits of edge analytics, Edge analytics architectures, Using edge analytics in the real world.

UNIT- II

Basic edge analytics components, Connecting a sensor to the ESP-12F microcontroller, KOM-MICS smart factory platform, Communications protocols used in edge analytics, Wi-Fi communication for edge analytics, Bluetooth for edge analytics communication, Cellular technologies for edge analytics communication, Long-distance communication using LoRa and Signfox for edge analytics.

UNIT- III

Working with Microsoft Azure IoT Hub, Cloud Service providers, Microsoft Azure, Exploring the Azure portal, Azure ioT Hub, Using the Raspberry Pi with Azure IoT edge, Connecting our Raspberry Pi edge device, adding a simulated temperature sensor to our edge device.

UNIT- IV

Using Micropython for Edge Analytics, Understanding Micropython, Exploring the hardware that runs MicroPython, Using MicroPython for an edge analytics application, Using edge intelligence with microcontrollers, Azure Machine Learning designer, Azure IoT edge custom vision.

UNIT- V

Designing a Smart Doorbell with Visual Recognition setting up the environment, Writing the edge code, creating the Node-RED dashboard, Types of attacks against our edge analytics applications, Protecting our edge analytics applications

Text Book:

1. Hands-On Edge Analytics with Azure IoT: Design and develop IoT applications with edge
   analytical solutions including Azure IoT Edge by Colin Dow

Reference Books:

1. Learn Edge Analytics - Fundamentals of Edge Analytics: Automated analytics at source using Microsoft Azure by Ashish Mahajan

WEB & DATABASE SECURITY (Professional Elective – IV)

(Course code: CS752PE)

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

Course Objectives

- Give an Overview of information security
- Give an overview of Access control of relational databases

Course Outcomes:

- Understand the Web architecture and applications
- Understand client side and server-side programming
- Understand how common mistakes can be bypassed and exploit the application
- Identify common application vulnerabilities

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

INFORMATION SYSTEM AUDIT AND ASSURANCE (Professional Elective – IV)

(Course code: CS753PE)

B.Tech. IV Year I Sem.

L	T	P	C
3	0	0	3

Course Objectives:

- Develop Expertise in System Auditing and Control.
- Master Business Continuity and Disaster Recovery Planning.

Course Outcomes:

- Acquire knowledge of the COBIT framework and its application in auditing and assurance services.
- Develop expertise in Internal Control and Information System Audit.
- Learn standard practices, policies, audit planning, and risk assessment to be able to do thorough audits of computer systems.
- Learn to evaluate and manage risks effectively.
- Learn to conduct business impact analyses and develop appropriate disaster recovery strategies.

UNIT - I

System Audit and Assurance: Characteristics of Assurance services, Types of Assurance 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 Information System Audit: Standard practices, policies, Audit planning, Risk Assessment, Information gathering techniques, Vulnerabilities, System security testing, Conducting audits for Banks.

UNIT - IV

Audit Control: 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: Data backup/storage, Developing appropriate Disaster recovery strategy, Business Impact analysis.

TEXT BOOK:

1. Information System Audit and Assurance; D. P. Dube, Ved Prakash Gulati; Tata McGraw- Hill Education, 01-Jan2005

REFERENCE BOOKS:

1. William Stallings and Lawrie Brown, Computer Security: Principles and Practice, Pearson Education.
2. Martin Weiss and Michael G. Solomon, Auditing IT Infrastructures For Compliance (Information Systems Security & Assurance), Jones and Bartlett Publishers, Inc.

SOCIAL MEDIA SECURITY (Professional Elective – IV)

(Course code: CS754PE)

B.Tech. IV Year I Sem.

L	T	P	C
3	0	0	3

Course Objectives

- Give introduction about the social networks, its use, the need of security in social data

Course Outcomes

- Learn about browser’s risks
- Learn about Social Networking,
- Understand the risks while using social media.
- Understand security of different web browsers.
- 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 Networks Crowdsourcing and Ethics, Authors: Altshuler Y, EloviciY, Cremers A.B, Aharony N, Pentland A. (Eds.)
2. Socialmediasecurity 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.

DEEP LEARNING (Professional Elective – IV)

(Course code: CS755PE)

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

Course Objectives:

- To understand deep Learning algorithms and their applications in real-world data

Course Outcomes:

- Understand machine learning basics and neural networks
- Understand optimal usage of data for training deep models
- Apply CNN and RNN models for real-world data
- Evaluate deep models
- Develop deep models for real-world problems

UNIT - I

Machine Learning Basics

Learning Algorithms, Capacity, Over fitting and Under fitting, Hyper parameters and Validation Sets, Estimators, Bias and Variance, Maximum Likelihood Estimation, Bayesian Statistics, Supervised Learning Algorithms, Unsupervised Learning Algorithms, Stochastic Gradient Descent, Building a Machine Learning Algorithm, Challenges Motivating Deep Learning

Deep Feed forward Networks Learning XOR, Gradient-Based Learning, Hidden Units, Architecture Design, Back-Propagation and Other Differentiation Algorithms

UNIT - II

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, Learning vs Pure Optimization, Challenges in Neural Network Optimization, Basic Algorithms, Parameter Initialization Strategies, Algorithms with Adaptive Learning Rates

UNIT - III

Convolution Networks

The Convolution Operation, Motivation, Pooling, Convolution and Pooling as an Infinitely Strong Prior, Variants of the Basic Convolution Function, Structured Outputs, Data Types, Efficient Convolution Algorithms, Random or Unsupervised Features

UNIT - IV

Recurrent and Recursive Nets

Unfolding Computational Graphs, Recurrent Neural Networks, Bidirectional RNNs, Encoder-Decoder Sequence-to-Sequence Architectures, Deep Recurrent Networks, Recursive Neural Networks, The Challenge of Long-Term Dependencies, Echo State Networks, Leaky Units and Other Strategies for Multiple Time Scales, The Long Short-Term Memory and Other Gated RNNs, Optimization for Long- Term Dependencies, Explicit Memory

UNIT - V

Practical Methodology: Performance Metrics, Default Baseline Models, Determining Whether to Gather More Data, Selecting Hyperparameters, Debugging Strategies, Example: Multi-Digit Number Recognition

Applications: Large-Scale Deep Learning, Computer Vision, Speech Recognition, Natural Language Processing, Other Applications.

TEXT BOOK:

1. Deep Learning by Ian Goodfellow, Yoshua Bengio and Aaron Courville, MIT Press.

REFERENCE BOOKS:

1. The Elements of Statistical Learning. Hastie, R. Tibshirani, and J. Friedman, Springer.
2. Probabilistic Graphical Models. Koller, and N. Friedman, MIT Press.
3. Bishop. C.M., Pattern Recognition and Machine Learning, Springer, 2006.
4. Yegnanarayana, B., Artificial Neural Networks PHI Learning Pvt. Ltd, 2009.
5. Golub, G.,H., and Van Loan, C.,F., Matrix Computations, JHU Press, 2013.
6. Satish Kumar, Neural Networks: A Classroom Approach, Tata McGraw-Hill Education, 2004.

QUANTUM COMPUTING (Professional Elective – V)

(Course code: CS765PE)

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

Course Objectives

- To introduce the fundamentals of quantum computing
- The problem-solving approach using finite dimensional mathematics

Course Outcomes

- Understand basics of quantum computing
- Understand physical implementation of Qubit
- Understand Quantum algorithms and their implementation
- Understand The Impact of Quantum Computing on Cryptography

UNIT - I

History of Quantum Computing: Importance of Mathematics, Physics and Biology. Introduction to Quantum Computing: Bits Vs Qubits, Classical Vs Quantum logical operations

UNIT - II

Background Mathematics: Basics of Linear Algebra, Hilbert space, Probabilities and measurements. Background Physics: Paul's exclusion Principle, Superposition, Entanglement and super-symmetry, density operators and correlation, basics of quantum mechanics, Measurements in bases other than computational basis. Background Biology: Basic concepts of Genomics and Proteomics (Central Dogma)

UNIT - III

Qubit: Physical implementations of Qubit. Qubit as a quantum unit of information. The Bloch sphere Quantum Circuits: single qubit gates, multiple qubit gates, designing the quantum circuits. Bell states.

UNIT - IV

Quantum Algorithms: Classical computation on quantum computers. Relationship between quantum and classical complexity classes. Deutsch’s algorithm, Deutsch’s-Jozsa algorithm, Shor’s factorization algorithm, Grover’s search algorithm.

UNIT - V

Noise and error correction: Graph states and codes, Quantum error correction, fault-tolerant Computation. Quantum Information and Cryptography: Comparison between classical and quantum information theory. Quantum Cryptography, Quantum teleportation

TEXT BOOK:

1. Nielsen M. A., Quantum Computation and Quantum Information, Cambridge.

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. I: Basic Concepts, Vol II.
3. Basic Tools and Special Topics, World Scientific. Pittenger A. O., An Introduction to Quantum Computing Algorithms.

DATA ANALYTICS FOR FRAUD DETECTION (Professional Elective – V)

(Course code: CS757PE)

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

3 0 0 3

Course Objectives

- Discuss the overall process of how data analytics is applied
- Discuss how data analytics can be used to better address and identify risks
- Help mitigate risks from fraud and waste for our clients and organizations

Course Outcomes

- Formulate reasons for using data analysis to detect fraud.
- Explain characteristics and components of the data and assess its completeness.
- Identify known fraud symptoms and use digital analysis to identify unknown fraud symptoms.
- Automate the detection process.
- 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

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

5G TECHNOLOGIES (Professional Elective – V)

(Course code: CS758PE)

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

3 0 0 3

Course Objectives:

- Knowledge on the concepts of 5G and 5G technology and drivers, understand 5G network
  architecture, components, features and their benefits.

Course Outcomes:

- Understand 5G and 5G Broadband Wireless Communications
- Understand 5G wireless Propagation Channels
- Understand the significance of radio access technologies for 5G
- Analyze Device-to-device (D2D) communications
- Learn Massive MIMO propagation channel models

UNIT - I

Overview of 5G Broadband Wireless Communications: Mobile communications generations: from 1G to 4G, Rationale of 5G - requirements, Standardization activities.

UNIT - II

The 5G wireless Propagation Channels: Channel model requirements, Propagation scenarios and challenges in the 5G modeling, Channel Models for mmWave, MIMO Systems.

UNIT - III

The 5G radio-access technologies: Access design principles for multi-user communications – Orthogonal Frequency Division Multiplexing (OFDM), Filter Bank Multi-Carriers (FBMC) and Universal Filtered Multi-Carrier (UFMC), Multiple Access Techniques – Orthogonal Frequency Division Multiple Accesses (OFDMA), Non-Orthogonal Multiple Accesses (NOMA).

UNIT - IV

Device-to-Device (D2D) Communications– Extension of 4G D2D standardization to 5G, radio resource management for mobile broadband D2D, multi-hop and multi-operator D2D communications.

UNIT - V

Millimeter-wave Communications – Spectrum and Regulations, Deployment scenarios, Beam-forming, physical layer techniques. Massive MIMO propagation channel models, Pilot design for Massive MIMO, Resource allocation and transceiver algorithms for massive MIMO, Fundamentals of baseband and RF implementations in massive MIMO.

TEXT BOOKS:

1. Afif Osseiran, Jose.F. Monserrat, Patrick Marsch, “Fundamentals of 5G Mobile Networks” , Cambridge University Press.

REFERENCE BOOKS:

1. Jonathan Rodriguez, “Fundamentals of 5G Mobile Networks”, John Wiley & Sons.
2. Amitabha Ghosh and Rapeepat Ratasuk “Essentials of LTE and LTE-A”, Cambridge University Press
3. Athanasios G.Kanatos, Konstantina S.Nikita, Panagiotis Mathiopoulos, “New Directions in Wireless Communication Systems from Mobile to 5G”, CRC Press.
4. Theodore S. Rappaport, Robert W. Heath, Robert C. Danials, James N. Murdock “Millimeter Wave Wireless Communications”, Prentice Hall Communications.
5. Martin Sauter “From GSM From GSM to LTE–Advanced Pro and 5G: An Introduction to Mobile Networks and Mobile Broadband”, Wiley-Blackwell.

SECURITY INCIDENT AND RESPONSE MANAGEMENT (Professional Elective – V)
(Course code: CS759PE)

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

3 0 0 3

Prerequisites:

1. Knowledge of information security and applied cryptography.
2. Knowledge of Operating Systems.

Course Objectives:

- Give an introduction to the preparation of inevitable incidents, incident detection and characterization.
- To get exposure to live data collection and forensic duplication.
- To gain knowledge on data collection in Windows, Unix and Mac OS Systems.

Course Outcomes:

- Learn how to handle the incident response management.
- Perform live data collection and forensic duplication.
- Identify network evidence.
- Analyze data to carry out an investigation.
- 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 Characterizatio**n: 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, Analyze 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 Systems: 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.

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.

AUTHENTICATION TECHNIQUES (Professional Elective – V)

(Course code: CS760PE)

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

3 0 0 3

Course Objectives:

- Knowledge on concept of authentication types, protocols, physical identification and various authentication algorithms

Course Outcomes:

- Understand different types of authentication techniques
- Understand authentication and Key Transport using Key Cryptography
- Understand different biometric techniques used in authentication.
- Understand the procedure of local authentication and Authentication by Addresses.
- 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 themiddle 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.

INFORMATION SYSTEM AUDIT AND ASSURANCE (Open Elective – II)

(Course code: CS792OE)

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

3 0 0 3

Course Objectives:

- Develop Expertise in System Auditing and Control.
  Master Business Continuity and Disaster Recovery Planning.

Course Outcomes:

- Acquire knowledge of the COBIT framework and its application in auditing and assurance services.
- Develop expertise in Internal Control and Information System Audit.
- Learn standard practices, policies, audit planning, and risk assessment to be able to do thorough audits of computer systems.
- Learn to evaluate and manage risks effectively.
- Learn to conduct business impact analyses and develop appropriate disaster recovery strategies

UNIT - I

System Audit and Assurance: Characteristics of Assurance services, Types of Assurance 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 Information System Audit: Standard practices, policies, Audit planning, Risk Assessment, Information gathering techniques, Vulnerabilities, System security testing, Conducting audits for Banks.

UNIT - IV

Audit Control: 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: Data backup/storage, Developing appropriate Disaster recovery strategy, Business Impact analysis.

TEXT BOOKS:

1. Information System Audit and Assurance; D. P. Dube, Ved Prakash Gulati; Tata McGraw- Hill Education, 01-Jan2005

REFERENCE BOOKS:

1. William Stallings and Lawrie Brown, Computer Security: Principles and Practice, Pearson Education
2. Martin Weiss and Michael G. Solomon, Auditing IT Infrastructures For Compliance (Information Systems Security & Assurance), Jones and Bartlett Publishers, Inc

SOCIAL MEDIA SECURITY (Open Elective – II)

(Course code: CS793OE)

B.Tech. IV Year I Sem.

L	T	P	C
3	0	0	3

Course Objectives

- Give introduction about the social networks, its use, the need of security in social data

Course Outcomes

- Learn about browser’s risks
- Learn about Social Networking,
- Understand the risks while using social media.
- Understand security of different web browsers.
- 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 Networks Crowd sourcing 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,
3. Applications, and Perspectives, CRC press

VULNERABILITY ASSESSMENT & PENETRATION TESTING LAB

(Course code: CS723PC)

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

0 0 2 1

Course Objectives:

- Learning Penetration Testing methodologies
- Monitoring the network traffic
- To understand the host and services discovery

Course Outcomes:

- Design for monitoring network traffic.
- Perform different penetration testing methods.
- Design different types of vulnerabilities scanning.
- Understand web application assessment.

List of Experiments:

1. Implement Monitoring of Network Traffic using
   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.

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.

NETWORK MANAGEMENT SYSTEMS AND OPERATIONS LAB

(Course code: CS724PC)

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

0 0 2 1

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 Trouble shooting techniques.
- Exploring the various network management tools.

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. Analyze 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.

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

ORGANIZATIONAL BEHAVIOUR

(Course code: MBA801HS)

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

3 0 0 3

Course Objectives:

- This course demonstrates individual, group behavior aspects: The dynamics of organizational climate, structure and its impact on Organizations.

Course Outcomes:

- Students understand their personality, perception and attitudes for overall development and further learn the importance of group behavior in the organizations.

UNIT - I Organizational Behaviour

Definition, need and importance of organizational behaviour – Nature and scope – Frame work – Organizational behaviour models.

UNIT - II Individual Behaviour

Personality – types – Factors influencing personality – Theories – Learning – Types of learnersThe learning process – Learning theories – Organizational behaviour modification, Misbehaviour– Types – Management Intervention. Emotions - Emotional Labour – Emotional Intelligence – Theories. Attitudes – Characteristics – Components – Formation – Measurement-Values. Perceptions – Importance – Factors influencing perception – Interpersonal perception-Impression Management. Motivation – importance – Types – Effects on work behavior.

UNIT - III Group Behaviour

Organization structure – Formation – Groups in organizations – Influence – Group dynamics – Emergence of informal leaders and working norms – Group decision making techniques – Team building - Interpersonal relations – Communication – Control.

UNIT - IV Leadership and Power

Meaning – Importance – Leadership styles – Theories of leadership – Leaders Vs Managers – Sources of power – Power centers – Power and Politics.

UNIT - V Dynamics of Organizational Behaviour

Organizational culture and climate – Factors affecting organizational climate – Importance. Job satisfaction – Determinants – Measurements – Influence on behavior. Organizational change – Importance – Stability Vs Change – Proactive Vs Reaction change – the change process – Resistance to change – Managing change. Stress – Work Stressors – Prevention and Management of stress – Balancing work and Life. Organizational development – Characteristics – objectives –. Organizational effectiveness

TEXT BOOKS:

1. Stephen P. Robins, Organisational Behavior, PHI Learning / Pearson Education, 11th edition, 2008.
2. Fred Luthans, Organisational Behavior, McGraw Hill, 11th Edition, 2001.

REFERENCE BOOKS:

1. Schermerhorn, Hunt and Osborn, Organisational behavior, John Wiley, 9th Edition, 2008.
2. Udai Pareek, Understanding Organisational Behaviour, 2nd Edition, Oxford Higher Education, 2004.

QUANTUM CRYPTOGRAPHY (Professional Elective – VI)

(Course code: CS846PE)

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

3 0 0 3

Prerequisites:

1. Quantum computing

Course Objectives

- Objective of the course is to build quantum-preparedness for the post quantum era.

Course Outcomes

- Basic understanding about quantum information and computation.
- Understand attack Strategies on QKD Protocols
- Analyze and understand statistical analysis of QKD Networks in Real-Life Environment
- Apply Quantum-cryptographic networks

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, StatisticalAnalysis 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).

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.

IOT CLOUD PROCESSING AND ANALYTICS (Professional Elective – VI)
(Course code: CS847PE)

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

3 0 0 3

Course Objectives

- To analyze the data generated from IoT device, store in cloud, to be able to manage IoT data stored in cloud

Course Outcomes

- Learn IoT Big data challenges
- Integrate Cloud and Big Data for IOT analytics
- Analyze sensor data streams for events
- Know open source framework for IoT analytics
- Review tools for semantic and data stream analytics

UNIT - I

Introducing IoT Analytics

IoT Data and BigData, Challenges of IoT Analytics, Applications, IoT Analytics Lifecycle and Techniques IoT

Cloud and Big Data Integration for IoT Analytics Introduction, IaaS, PaaS and SaaS Paradigms, Requirements of IoT Big Data Analytics, Platform3, Functional Architecture, Data Analytics for the IoT, Data Collection Using Low-power, Longrange Radios, WAZIUP Software Platform, iKaaS Software Platform

UNIT - II

Searching the Internet of Things

Introduction, A Search Architecture for Social and Physical Sensors, Local Event Retrieval, Using Sensor Metadata Streams to Identify Topics of Local, Events in the City, Venue Recommendation

UNIT - III

Development Tools for IoT Analytics Applications Introduction, Related Work, The VITAL Architecture for IoT Analytics Applications, VITAL Development Environment, Development Examples

UNIT - IV

An Open Source Framework for IoT Analytics as a Service Introduction, Architecture for IoT Analytics-as-a-Service, Sensing-as-a-Service Infrastructure Anatomy, Scheduling, Metering and Service Delivery, Sensing-as-a-Service Example, From Sensing-as-a- Service to IoT-Analytics-as-a-Service

UNIT - V

A Review of Tools for IoT Semantics and Data Streaming Analytics Introduction, Related Work, Semantic Analysis, Tools and Platforms

Data Analytics for Smart Cities

Introduction, Cloud-based IoT Analytics, Cloud-based City Platform, Solutions, Edge, State of the Art, Edge-based City Platform, Workflow ,Task and Topology, IoT-friendly Interfaces, Use Case of Edge based Data Analytics

TEXT BOOKS:

1. Building Blocks for IoT Analytics by John Soldatos, River Publisher

REFERENCE BOOKS:

1. Analytics for the Internet of Things (IoT)by Andrew miller, Packt Publishing.
2. Big Data Analytics for Internet of Things by Tausifa Jan Saleem, Mohammad Ahsan Chishti, Wiley Publishing.

CLOUD SECURITY (Professional Elective – VI)

(Course code: CS848PE)

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

3 0 0 3

Pre-requisites:

1. Computer Networks, Cryptography and Network Security, Cloud Computing.

Course Objectives:

- To understand the fundamentals concepts of cloud computing.
- To understand the cloud security and privacy issues.
- To understand the Threat Model and Cloud Attacks
- To understand the Data Security and Storage

Course Outcomes:

- Acquire the knowledge on fundamentals concepts of cloud computing.
- Distinguish the various cloud security and privacy issues.
- Analyze the various threats and Attack tools
- Understand the Data Security and Storage concepts.

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, DataSecurity 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.

DIGITAL WATERMARKING AND STEGANOGRAPHY (Professional Elective – VI)

(Course code: CS849PE)

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

3 0 0 3

Course Objectives:

- To learn about the watermarking models and message coding
- To learn about watermark security and authentication.
- To learn about steganography Perceptual models

Course Outcomes:

- Know the History and importance of watermarking and steganography.
- Analyze Applications and properties of watermarking and steganography.
- Demonstrate Models and algorithms of watermarking.
- Possess the passion for acquiring knowledge and skill in preserving authentication of Information.
- 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 &analyzing errors: Informed Embedding, Informed CodingStructured dirty-paper codes, Message errors, False positive errors, False negative errors, ROCcurves – 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.

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.

DATA PRIVACY (Professional Elective – VI)

(Course code: CS850PE)

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

3 0 0 3

Course Objectives:

- Instill an understanding of the essential importance of data privacy.
- Classify the necessary statistical and computational techniques essential for data sharing, particularly emphasizing applications in social and health sciences.
- Develop the foundational principles in architecture, algorithms, and technology for the preservation and maintenance of data privacy.

Course Outcomes:

- Outline essential rules and principles for safeguarding privacy and personally identifiable information.
- Develop data that facilitates meaningful statistical inference while minimizing the exposure of sensitive information.
- Identify potential threats related to different types of anonymized data.
- Classify and evaluate methods for generating test data with a focus on both privacy and utility considerations.

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 Privacyand 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.

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.

5G TECHNOLOGIES (Open Elective – III)

(Course code: CS883OE)

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

3 0 0 3

Course Objectives:

- Knowledge on the concepts of 5G and 5G technology and drivers, understand 5G network architecture, components, features and their benefits.

Course Outcomes:

- Understand 5G and 5G Broadband Wireless Communications
- Understand 5G wireless Propagation Channels
- Understand the significance of radio access technologies for 5G
- Analyze Device-to-device (D2D) communications
- Learn Massive MIMO propagation channel models

UNIT - I

Overview of 5G Broadband Wireless Communications: Mobile communications generations: from 1G to 4G, Rationale of 5G - requirements, Standardization activities.

UNIT - II

The 5G wireless Propagation Channels: Channel model requirements, Propagation scenarios and challenges in the 5G modeling, Channel Models for mmWave, MIMO Systems.

UNIT - III

The 5G radio-access technologies: Access design principles for multi-user communications – Orthogonal Frequency Division Multiplexing (OFDM), Filter Bank Multi-Carriers (FBMC) and Universal Filtered Multi-Carrier (UFMC), Multiple Access Techniques – Orthogonal Frequency Division Multiple Accesses (OFDMA), Non-Orthogonal Multiple Accesses (NOMA).

UNIT - IV

Device-to-Device (D2D) Communications– Extension of 4G D2D standardization to 5G, radio resource management for mobile broadband D2D, multi-hop and multi-operator D2D communications.

UNIT - V

Millimeter-wave Communications – Spectrum and Regulations, Deployment scenarios, Beam-forming, physical layer techniques.

Massive MIMO propagation channel models, Pilot design for Massive MIMO, Resource allocation and transceiver algorithms for massive MIMO, Fundamentals of baseband and RF implementations in massive MIMO.

TEXT BOOK:

1. Afif Osseiran, Jose.F. Monserrat, Patrick Marsch, “Fundamentals of 5G Mobile Networks” , Cambridge University Press.

REFERENCE BOOKS:

1. Jonathan Rodriguez, “Fundamentals of 5G Mobile Networks”, John Wiley & Sons.
2. Amitabha Ghosh and Rapeepat Ratasuk “Essentials of LTE and LTE-A”, Cambridge University Press
3. Athanasios G. Kanatos, Konstantina S.Nikita, Panagiotis Mathiopoulos, “New Directions in Wireless Communication Systems from Mobile to 5G”, CRC Press.
4. Theodore S. Rappaport, Robert W. Heath, Robert C. Danials, James N. Murdock “Millimeter Wave Wireless Communications”, Prentice Hall Communications.
5. Martin Sauter “From GSM From GSM to LTE–Advanced Pro and 5G: An Introduction to Mobile Networks and Mobile Broadband”, Wiley-Blackwell.

DATA PRIVACY (Open Elective – III)

(Course code: CS882OE)

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

Course Objectives:

- Instill an understanding of the essential importance of data privacy.
- Classify the necessary statistical and computational techniques essential for data sharing, particularly emphasizing applications in social and health sciences.
- Develop the foundational principles in architecture, algorithms, and technology for the preservation and maintenance of data privacy.

Course Outcomes:

- Outline essential rules and principles for safeguarding privacy and personally identifiable information.
- Develop data that facilitates meaningful statistical inference while minimizing the exposure of sensitive information.
- Identify potential threats related to different types of anonymized data.
- Classify and evaluate methods for generating test data with a focus on both privacy and utility considerations.

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 Privacyand 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 protectingQuasi-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 BOOK:

1. Nataraj Venkataramanan, Ashwin Sriram, Data Privacy: Principles and Practice, 2016, 1st
   Edition, Taylor & Francis. (ISBN No.: 978-1-49-872104-2), United Kingdom.

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.