VIGNANA BHARATHI Institute of Technology

(An UGC Autonomous Institution, Approved by AICTE, Affiliated by JNTUH, Accredited by NBA & NAAC)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

(CYBER SECURITY)

B.Tech -R21-COURSE STRUCTURE & SYLLABUS

IV YEAR I SEMESTER

S. No.	Course Code	Course Title	Category	L	T	P	Credits
1	21CY4111	Vulnerability Assessment & Penetration Testing	PC	3	1	-	3
2	21CY4112	Computer Security and Audit Assurance	PC	3	-	-	3
	21CY4171	Edge Analytics	PE-III	3	-	-	3
	21CY4172	Web & Database Security					
	21CY4173	Social Media Security					
	21CY4174	Deep Learning					
	21CY4175	Authentication Techniques	PE-IV	3	-	-	2
	21CY4176	Quantum Computing					
	21CY4177	Data Analytics for Fraud Detection					
	21CY4178	Security Incident & Response Management					
5		**Open Elective – III**	OE	3	-	-	3
6	21CY4151	Vulnerability Assessment & Penetration Testing lab	PC	-	-	2	1
7	21CY4182	Mini Project*	PW	-	-	4	2
		Total Credits	**41**	**15**	**1**	**6**	**17**

IV YEAR II SEMESTER

S. No.	Course Code	Course Title	Category	L	T	P	Credits
1	21MB4212	Fundamentals of Management and Organizational Behavior	HS	3	-	-	3
	21CY4271	Quantum Cryptography	PE	3	-	-	3
	21CY4272	Cloud Security					
	21CY4273	Digital Watermarking and Steganography					
	21CY4274	Data Privacy					
3	21CY4275	Malware Analysis	PE	3	-	-	3
	21CY4276	Enterprise Security					
	21CY4277	Device Hacking					
	21CY4278	Security Governance and Risk Management					
4	21CY4281	Major Project		-	-	20	10
			Total	9	-	20	19

21CY4111: Vulnerability Assessment & Penetration Testing

B.Tech. IV Year I Sem. **L T P C**
3 1 - 3

Prerequisites:

- Knowledge in information security.
- Knowledge on Web Application.

Course Objectives:

1. Understand the ethics of hacking and the importance of ethical hacking, as well as develop knowledge and skills in vulnerability assessment and penetration testing.
2. Comprehend and analyze various types of attacks in cybersecurity, Gain proficiency in using Metasploit for penetration testing.
3. Develop management and reporting skills for penetration test. Explore and exploit vulnerabilities in operating systems.
4. Gain knowledge of web application security vulnerabilities and acquire skills in vulnerability analysis.
5. Develop skills in malware analysis and client-side browser exploits.

Course Outcomes:

1. Evaluate the ethical considerations and legal implications in conducting ethical hacking activities using appropriate tools.
2. Analyze and defend against social engineering, physical penetration, and insider attacks using automating penetration testing processes.
3. Manage and report penetration tests effectively and develop and execute Linux and Windows exploits, bypassing memory protections.
4. Analyze and mitigate web application security vulnerabilities and Conduct vulnerability analysis.
5. Evaluate and protect against client-side browser exploits.

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,7andServer2008), 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.

TEXTBOOKS:

1. Gray Hat Hacking-The Ethical Hackers Handbook, Allen Harper, Stephen Sims, MichaelBaucom,3rd Edition, Tata McGraw-Hill.
2. The Web Application Hacker's Hand Book-Discovering and Exploiting Security flaws, Dafydd Suttard, Marcuspinto,1st Edition, Wiley Publishing.

REFERENCEBOOKS:

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.

21CY4112: Computer Security & Audit Assurance

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

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

21CY4171: Edge Analytics

(Professional Elective – III)

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

Prerequisites

A basic knowledge of "Python Programming"

Course Objectives:

1. To introduce the fundamentals of Edge Analytics
2. To give an overview of Architectures, Components, Communication Protocols and tools used for Edge Analytics.
3. To give an overview of Microsoft Azure.
4. To use Micropython for Edge Analytics.
5. To develop edge analytics application

Course Outcomes:

1. Understand the concepts of Edge Analytics, both in theory and in practical application.
2. Demonstrate a comprehensive understanding of different tools used at edge analytics.
3. Experiment with edge devices by working with Microsoft Azure IoT Hub.
4. Develop edge analytics applications using Micropython.
5. 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 Sign fox 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.
2. The Analytics Edge by Dimitris Bertsimas, Allison K O'Hair and William R Pulleyblank Dynamic Ideas, 2016. ISBN: 978-0989910897.

REFERENCE BOOKS:

1. Learn Edge Analytics - Fundamentals of Edge Analytics: Automated analytics at source using Microsoft Azure by Ashish Mahajan.
2. Edge & Fog Analytics: The New Analytics Interface Kindle Edition by Abdallah Bari

21CY4172: Web & Database Security
(Professional Elective – III)

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

3 - - 3

Course Objectives:

1. To equip students with a comprehensive understanding of web security principles, cryptography, and digital identification.
2. To educate students about the threats to user privacy posed by the web and equip them with privacy-protecting techniques.
3. To familiarize students with recent advancements in database security, access control models, and trust management techniques.
4. To equip students with the knowledge and skills necessary to assess the security vulnerabilities in databases.
5. To explore emerging trends and cutting-edge techniques in privacy protection for database publishing.

Course Outcomes:

1. Understand the fundamental concepts of web security, including the importance of protecting sensitive data and maintaining the confidentiality, integrity, and availability of web resources.
2. Identify common security risks and vulnerabilities associated with web servers, proxies and clients.
3. Explore advanced access control models and their application in database security.
4. Evaluate the current capabilities of Hippocratic Databases in preserving data privacy.
5. Assess the challenges and potential solutions for efficiently enforcing security and privacy policies in mobile computing environments.

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 Antitheft, 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, Data base Issues in Trust Management and Trust Negotiation, Security in Data Ware houses and OLAP Systems

UNIT-IV

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

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

TEXTBOOKS:

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

REFERENCEBOOKS:

1. Andrew Hoffman, Web Application Security: Exploitation and Counter measures 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.

21CY4173: Social Media Security
Professional Elective-III)

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

Course Objectives:

1. Give introduction about the social networks
2. To demonstrate the usage of social media.
3. To understand the need of security in social data.
4. To become familiar in the Phishing attacks
5. To demonstrate the basic concepts of Policies and Privacy

Course Out comes:

1. Learn about browser's risks.
2. Learn about Social Networking, Understand the risks while using social media. Guidelines for social networking.
3. Understand how to secure different web browsers.
4. Understand how an e-mail works, learn threats involved using an email communication, safety measures while using e-mail.
5. Understand privacy issues, assess security implications, and design policies for user privacy and data protection.

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 Cybercrime, Social Engineering, Hacked accounts, cyberstalking, cyberbullying, predators, phishing, hackers.

UNIT–III

Being bold versus being overlooked Good social media campaigns, Bad social media campaigns, Sometimes it's better to be over looked, 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

TEXTBOOKS:

1. Inter disciplinary 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, Elo vici Y, Cremers A.B, A harony N, Pentl and A. (Eds.).
2. Social Media Security: Leveraging Social Networking While Mitigating Risk by Michael Cross
3. Social media security https://www.sciencedirect.com/science/article/pii/B978159749986600000

REFERENCEBOOKS:

1. Online Social Networks Security, Brij B. Gupta, Somya Ranjan Sahoo, Principles, Algorithm, Applications, and Perspectives, CRC press.
2. Social Media Security: Protecting Your Digital Life C P Kumar

21CY4174: Deep Learning

(Professional Elective – III)

B.Tech. IV Year I Sem.

L	T	P	C
3	-	-	3

Course Objectives: Students will be able to:

1. TounderstandcomplexityofDeepLearningalgorithmsandtheirlimitations
2. To learn about Convolutional Neural Networks
3. TobecapableofperformingexperimentsinDeepLearningusingreal-worlddata.
4. To learn about Applications of Deep Learning to NLP.
5. To understand Analogy reasoning.

Course Outcomes:

1. Implement deep learning algorithms, understand neural networks and traverse the layers of data.
2. Learn topics such as convolutional neural networks, recurrent neural networks, training deep networks and high-level interfaces.
3. Understand applications of Deep Learning to Computer Vision.
4. Analyze and understand applications of Deep Learning to NLP.
5. Understanding the concepts of recurrent neural networks.

UNIT-I

Introduction: Feed forward Neural networks, Gradient descent and the back-propagation algorithm, Unit saturation, the vanishing gradient problem, and ways to mitigate it. RelU Heuristics for avoiding bad local minima, Heuristics for faster training, Nestors accelerated gradient descent, Regularization, Dropout

UNIT-II

Convolutional Neural Networks: Architectures, convolution/pooling layers, Recurrent Neural Networks: LSTM, GRU, Encoder Decoder architectures. Deep Unsupervised Learning: Auto encoders, Variational Auto-encoders, Adversarial Generative Networks, Auto-encoder and DBM Attention and memory models, Dynamic Memory Models.

UNIT-III

Applications of Deep Learning to Computer Vision: Image segmentation, object detection, automatic image captioning, Image generation with Generative adversarial networks, video to text with LSTM models, Attention Models for computer vision tasks.

UNIT-IV

Applications of Deep Learning to NLP: Introduction to NLP and Vector Space Model of Semantics, Word Vector Representations: Continuous Skip-Gram Model, Continuous Bag-of-Words model (CBOW), Glove, Evaluations and Applications in word similarity

UNIT-V

Analogy reasoning: Named Entity Recognition, Opinion Mining using Recurrent Neural Networks: Parsing and Sentiment Analysis using Recursive Neural Networks: Sentence Classification using Convolutional Neural Networks, Dialogue Generation with LSTMs.

TEXTBOOKS:

1. Deep Learning by Ian Good fellow, Yoshua Bengio and Aaron Courville, MIT Press.
2. The Elements of Statistical Learning by T. Hastie, R. Tibs hirani, and J. Fried man, Springer.
3. Probabilistic Graphical Models. Koller, and N. Friedman, MIT Press.

REFERENCEBOOKS:

1. Bishop, C, M., Pattern Recognition and Machine Learning, Springer,2006.
2. Yegnanarayana, B., Artificial Neural Networks PHI Learning Pvt. Ltd,2009.
3. Golub, G., H., and Van Loan, C.F., Matrix Computations, JHU Press, 2013.
4. Satish Kumar, Neural Networks: A Classroom Approach, TataMcGraw-HillEducation,2004.

21CY4175: Authentication Techniques

(Professional Elective – IV)

B.Tech. IV Year I Sem. **L T P C**
3 - - 2

Course Objectives:

1. Knowledge on concept of authentication types, protocols, physical identification and various authentication algorithms.
2. To learn text ad voice-based authentication techniques.
3. To learn different types of digital identification.
4. To acquire knowledge of different international standards and policies for authentication
5. To explore different tools used for authentication.

Course Outcomes

1. Understand different types of authentication techniques
2. Understand text based and voice-based authentication techniques
3. Analyze different digital identification techniques
4. Understand significance of authentication algorithms and its standards.
5. Apply various authentication protocols in multi-server environment and their representation.

UNIT-I:

DefinitionofAuthentication,Identification/verification,Stagesandstepsofauthentication,Authentication Entity : User, Device and Application; Authentication attributes: Source, Location, Path, Time duration etc.; Authentication Types : Direct / Indirect, One Way / Mutual, On demand/
Periodic/Dynamic/Continuousauthentication,Assisted/Automatic;3Factorsofauthentication;Passwords,Generation of passwords of varied length and of mixed type, OTP, passwords generation using entity identity credentials; Secure capture, processing, storage, verification and retrieval of passwords;

UNIT-II:

Physical identification using smart cards, remote control device, proximity sensors, surveillance camera, authentication in Card present / Card Not Present transactions as ATM/ PoS Device, mobile phone, wearable device and IoT device-based authentication; single sign-on; Symmetric Key Generation, Key Establishment, Key Agreement Protocols;

UNIT-III:

Biometrics – photo, face, iris, retinal, handwriting, signature, fingerprint, palm print, hand geometry, voice – Text based and text independent voice authentication, style oftalking, walking, writing, key strokes, gait etc. multi-modal biometrics.

UNIT-IV:

Matching algorithms, Patterns analysis, errors, performance measures, ROC Curve; Authentication Standards–International, UIDAI Standard. Kerberos, X.509 Authentication Service, Public Key Infrastructure, Scanners and Software; Web Authentication Methods: Http based, Token Based, O Auth and API.

UNIT-V:

User authentication protocols in multi-server environment, BAN Logic, Representation of authentication protocols using BAN Logic, Random Oracle Model, Scyther Tools, Prover if tool, Chebyshev Chaotic Map, Fuzzy Extractor, Fuzzy Extractor Map, Bloom Filter, LU Decomposition based User Authentication, Block chain-based authentication.

TEXTBOOKS:

1. Protocols for Authentication and Key Establishment, Colin Boyd and Anish Mathuria, springer, 2021
2. Guide to Biometrics, Rund M. Bolle, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, Jonathan H. Connell, Springer2009.

REFERENCE BOOKS:

1. Digital Image Processing using MATLAB, Rafael C. Gonzalez, Richard Eugene Woods, 2nd Edition, Tata Mc Graw-Hill Education 2010.
2. Biometric System and Data Analysis: Design, Evaluation, and data Mining, Ted Dunstone and Neil Yager, Springer.
3. Biometrics Technologies and verification Systems, John Vacca, ElsevierInc.,2007.
4. Pattern Classification, RichardO. Duda, David G. Stork, Peter E. Hart, Wiley 2007.

21CY4176: Quantum Computing

(Professional Elective – IV)

B.Tech. IV Year I Sem. **L T P C**
3 - - 2

Course Objectives:

1. To introduce the fundamentals of quantum computing
2. The problem-solving approach using finite dimensional
3. mathematics
4. To acquire knowledge of quantum architecture and its essentials
5. Knowledge of quantum algorithms
6. To understand the Impact of Quantum Computing on Cryptography

Course Outcome s:

1. Understand basics of quantum computing
2. Understand basic quantum theory and its essentials
3. Understand physical implementation of Qubit
4. Understand Quantum algorithms and their implementation
5. Understand the Impact of Quantum Computing on Cryptography

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 Electro dynamics, 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.

TEXTBOOKS:

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

REFERENCE BOOKS:

1. Quantum Computing for Computer Scientists by No son 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.

21CY4177: Data Analytics for Fraud Detection (Professional Elective – IV)

B.Tech. IV Year I Sem. **L T P C**
3 - - 2

Course Objectives:

1. To discuss the overall process of how data analytics is applied.
2. To discuss how data analytics can be used to better address and identify risks.
3. To discuss about data analytical tests
4. To acquire knowledge of advanced data analytical tests.
5. To help mitigate risks from fraud and waste for our clients and organizations.

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. Identifyknownfraudsymptomsandusedigitalanalysistoidentifyunknownfraudsymptoms.
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 with in 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

Pay roll Fraud, Expense Reimbursement Schemes, Registered disbursement schemes.

TEXTBOOK:

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

REFERENCEBOOKS:

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.

21CY4178: Security Incident & Response Management
(Professional Elective –IV)

B.Tech. IV Year I Sem. **L T P C**
3 - - 2

Prerequisites:

- Knowledge in information security and applied cryptography.
- Knowledge in Operating Systems and Networking Fundamentals.
- Knowledge on Ethical and Legal Considerations

Course Objectives:

1. Understand the Real-World Incident Landscape and Learn how to create an organizational incident response plan.
2. Understand Live Data Collection in Incident Response and Identify the types of data that should be collected during live data acquisition
3. Understand the Importance of Network Monitoring and Set Up an Effective Network Monitoring System.
4. Understand Analysis Methodology and Learn various methods to access and retrieve data from different sources securely
5. Understand HFS+ and File System Analysis and Learn how to conduct file system analysis to extract valuable information for incident investigations.

Course Outcomes:

1. To understand the importance of preparation, documentation, and prioritization, and be capable of leading or contributing effectively to incident response efforts within their organizations.
2. Implementing live data collection on both Windows and Unix systems, selecting appropriate live response tools, and understanding the significance of forensic duplication in incident response investigations.
3. Analyze network traffic and data to detect security incidents in enterprise environments
4. Identify data analysis methodologies and possess specialized knowledge in investigating Windows-based systems.
5. Understanding of investigating Mac OS X systems and applications

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, Data base 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.

TEXTBOOKS:

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.

REFERENCEBOOKS:

1."The Computer Incident Response Planning Handbook: Executable Plans for Protecting a Information at Risk", N. K. McCarthy, Tata McGraw-Hill.
2. Incident Handling and Response: A Holistic Approach for an efficient Security Incident Management by Jithin Alex

21CY4151: Vulnerability Assessment & Penetration Testing lab

B.Tech. IV Year I Sem. **L T P C**
- - 2 1

Course Objectives: This lab session focuses on training the students in:

1. Penetration Testing methodologies.
2. Monitoring the network traffic and
3. To understand the host and services discovery

Course Outcomes:

1. Design for monitoring network traffic
2. Perform different penetration testing methods
3. Design different types of vulnerabilities scanning
4. Understand web application assessment

List of Experiments:

1. Monitoring Network Traffic
2. Host& Services Discovery using Nmap
3. Vulnerability Scanning using OpenVAS
4. 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. 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. Different types of vulnerability scanning
7. Vulnerability scanning with Nessus
8. Web application assessment with nikto & burp suite

TEXTBOOKS:

1. "Gray Hat Hacking-The Ethical Hackers Handbook", Allen Harper, Stephen Sims, MichaelBaucom,3rd Edition, Tata McGraw-Hill.
2. "The Web Application Hacker's Handbook-Discovering and Exploiting Security flaws", Dafydd Suttard, Marcu's pinto,1stEdition, Wiley Publishing.

REFERENCEBOOKS:

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.

21CY4181: Mini Projects

B.Tech. IV Year I Sem.

L	T	P	C
-	-	4	2

21MB4212: Fundamentals of Management and Organizational Behavior

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

Course Objective:

- To understand the fundamentals of management, history and evolution of management theories
- To analyze various dimensions of organizational planning and organizing.
- To understand the functions of staffing, Directing and controlling.
- To understand the fundamental concepts of Organizational Behaviour.
- To analyze and evaluate the various dimensions of Cognitive process and Stress related issues in Organizational Behaviour.

Course Outcomes: After the completion of the course, student should be able to

- Understand the fundamentals of management and contribution of management thinkers.
- Analyze the relevance and importance of planning and organizing.
- Understand the importance of organizing, types of organizational structures and various function of human resource management
- Understand fundamental concepts of organizational behaviour
- Analyze and evaluate the various dimensions of cognitive process and stress related issues in organizational behaviour.

UNIT- I
Introduction to Management: Definition, Nature and Scope, Functions, Managerial Roles, Levels of Management, Managerial Skills, Challenges of Management; Evolution of Management.
Approaches- Classical Scientific and Administrative Management; The Behavioral approach; The Quantitative approach; The Systems Approach; Contingency Approach, IT Approach.

UNIT – II
Planning and Organizing: General Framework for Planning - Planning Process, Types of Plans, Principles of Organization: Organizational Design & Organizational Structures; Departmentalization, Delegation; Empowerment, Centralization, Decentralization, Recentralization.

UNIT- III
Staffing: Functions of HRM.
Leadership: Leadership Styles; Leadership theories.
Motivation - Types of Motivation; Motivational Theories - Needs Hierarchy Theory, Two Factor Theory, Theory X, Theory Y and Theory Z.
Communication: Types of communication, Importance, Communication Process and communication Barriers.
Controlling: Process of controlling, Types of Control

UNIT- IV

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

UNIT- V

Cognitive Processes-II: Personality and Attitudes - Personality as a continuum – Meaning of personality - Johari Window and Transactional Analysis - Nature and Dimension of Attitudes- 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.

TEXT BOOKS:

1. Management Essentials, Andrew DuBrin, 9e, Cengage Learning, 2012.
2. Fundamentals of Management, Stephen P. Robbins, Pearson Education, 2009
3. Principles and Practice of Management, L. M. Prasad, S. Chand, 2019, New Delhi.
4. Robbins, P. Stephen, Timothy A. Judge: Organisational Behaviour, 12/e, PHI/Pearson, NewDelhi, 2009.

REFERENCES:

1. Newstrom W. John & Davis Keith, Organisational Behaviour-- Human Behaviour at Work, 12/e,TMH, New Delhi, 2009.
2. Luthans, Fred: Organizational Behaviour 10/e, McGraw-Hill, 2009.

21CY4271: Quantum Cryptography (Professional Elective – VI)

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

Course Objectives:

1. To build quantum-preparedness for the post quantum era.
2. To understand quantum information and computation.
3. To Understand attack Strategies on QKD Protocols.
4. To understand statistical analysis of QKD Networks in Real-Life Environment.
5. To apply Quantum-cryptographic networks.

Course Outcomes:

1. Basic understanding about Quantum Information and Computation.
2. Understand about Quantum adaptive cascade protocol and its blocks.
3. Understand attack Strategies on QKD Protocols.
4. Analyze and understand statistical analysis of QKD Networks in Real-Life Environment.
5. 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 a 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 Proto type 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

TEXTBOOK:

1. KollmitzerC., PivkM. (Eds.), Applied Quantum Cryptography, Lect.NotesPhys.797(Springer, Berlin Heidelberg 2010).
2. Introduction to Quantum Cryptography by Thomas Vidick and Stephanie Wehner

REFERENCEBOOKS:

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.

21CY4272: Cloud Security

(Professional Elective – VI)

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

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

Course Objectives:

1. To understand the fundamentals concepts of cloud computing.
2. To understand the cloud security and privacy issues.
3. To understand the Threat Model and Cloud Attacks.
4. To understand the Data Security and Storage.
5. To analyze Security Management in the Cloud.

Course Outcome

1. Ability to acquire the knowledge on fundamentals concepts of cloud computing.
2. Able to distinguish the various cloud security and privacy issues.
3. Able to analyze the various threats and Attack tools.
4. Able to understand the Data Security and Storage.
5. Able to analyze the Security Management in the Cloud.

UNIT-I

Over view 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.

Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

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.

Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

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.

Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

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.

Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

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.

Note: Laboratory practice will be imparted with the help of relevant case studies as and when required.

TEXTBOOKS:

1. Cloud Security Attacks, Techniques, Tools, and Challenges by Preeti Mishra, Emmanuel S Pilli, Jaipur RCJoshiGraphicEra,1st Editionpublished 2022by CRC press.
2. Cloud Computing with Security Concepts and Practices Second Edition by Naresh Kumar Sehgal Pramod Chandra, P. Bhatt John M. Acken,2nd Edition Springer nature Switzerland AG2020.
3. Cloud Security and Privacy by Tim Mather, Subra Kumara swamy, and Shahed Lati First Edition, September 2019.

REFERENCEBOOKS:

1. Essentials of Cloud Computing by K. Chandra Sekaran Special Indian Edition CRC press.
2. Cloud Computing Principles and Paradigms by Rajkumar Buyya, John Wiley.

21CY4273: Digital Watermarking and Steganography

(Professional Elective – VI)

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

Course Objectives:

1. To learn about the water marking models and message coding.
2. To learn about the watermarking side information &analyzing errors
3. To learn about water mark security and authentication.
4. To learn about watermarking perceptual models.
5. To learn about steganography.

Course Outcomes:

1. Know the History and importance of water marking and steganography.
2. Analyze Applications and properties of water marking 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 theoretic foundations of steganography and steganalysis.

UNIT-I

Introduction: Information Hiding, Steganography and Watermarking – History of watermarking–Importanceofdigitalwatermarking–Applications–Properties–Evaluating water marking 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

Water marking with side information & analyzing 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

Water mark security & authentication: Security requirements–Water mark 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

TEXTBOOK:

1.Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, "Digital Water marking and Steganography", Margan Kaufmann Publishers, NewYork,2008.

2. Digital Watermarking and Steganography by Frank Y. Shih

REFERENCEBOOK:

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, "Digital Water marking", Margan Kaufmann Publishers, NewYork,2003.
2. Data Hiding and Its Applications: Digital Watermarking and Steganography by David Meg´ıas, Wojciech Mazurczyk, et al.

21CY4274: Data Privacy

(Professional Elective – VI)

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

Course Objectives:

1. The objective of this course is to provide fundamental concepts of data privacy.
2. Explores architectural, algorithmic and technological foundations for the maintenance of the privacy of individuals.
3. To conduct a comprehensive survey of techniques
4. To learn the concepts of confidentiality of organizations, and the protection of sensitive information, despite the requirement that information be released publicly or semi-publicly.
5. To explore the intersection of technology, policy, privacy, and freedom of information acts.

Course Outcomes:

1. Discuss the concepts of privacy into day's environment.
2. understanding of data explosion, statistics, data sharing practices, protection, privacy and risk measurements.
3. Impact of automation is changing the concepts and expectations concerning privacy and the increasingly interconnected issue of security.
4. Analyze how emerging issues are affecting society and business, with a concentration on how information security must shape corporate practices.
5. Explaintheknowledgeoftheroleofprivateregulatoryandself-helpefforts.

UNIT-I:

Introduction- Fundamental Concepts, Definitions, Statistics, Data Privacy Attacks, Data linking and profiling, access control models, role-based access control, privacy policies, their specifications, languages and implementation, privacy policy languages, privacy indifferent domains-medical, financial, etc.

UNIT-II:

Data explosion-Statistics and Lack of barriers in Collection and Distribution of Person-specific information, Mathematical model for characterizing and comparing real-world data sharing practices and policies and for computing privacy and risk measurements, Demographics and Uniqueness, **Protection Models**-Null-map, k-map, Wrong map

UNIT-III:

Survey of techniques- Protection models (null-map, k-map, wrong map), Disclosure control, Inferring entity identities, Strength and weaknesses of techniques, entry specific databases.

UNIT-IV:

Computation systems for protecting delimited data-MinGen, Data fly, Mu-Argus, k-Similar, Protecting textual documents: Scrub.

UNIT-V:

Technology, Policy, Privacy and Freedom- Medical privacy legislation, policies and best practices, Examination of privacy matters specific to the World Wide Web, Protections provided by the Freedom of Information Act or the requirement for search warrants.

TEXTBOOKS:

1. B. Raghunathan, The Complete Book of Data Anonymization: From Planning to Implementation,1st Edition, AuerbachPub,2013.
2. L. Sweeney, Computational Disclosure Control: A Primer on Data Privacy Protection, MIT ComputerScience,2002.

REFERENCEBOOKS:

1. Nishant Bhajaria Data Privacy: A run book for engineers, Manning Publications.
2. Gwen Kennedy, Data Privacy Law: A Practical Guide to the GDPR, ISBN-13:978-0999512722, ISBN-10:0999512722.

21CY4275: Malware Analysis
(Professional Elective-V)

B.Tech. IV Year II Sem. **L T PC**
3 - - 3

Prerequisite: Basic knowledge of Computer Networks and various types of attacks.

Course Objectives:

1. To analyze malware evolution, types, and conduct static and dynamic malware analysis effectively.
2. To understand X86 architecture, analyze Windows programs, and employ anti-static analysis techniques proficiently.
3. To conduct live and dead malware analysis, analyze malware traces, and employ anti-dynamic analysis techniques adeptly.
4. To understand malware functionalities and employ covert malware launching methods skillfully.
5. To utilize signature-based and non-signature-based techniques for malware detection, including Android malware characterization.

Course Outcomes:

1. Master static and dynamic malware analysis for effective cyber defense.
2. Enhance malware detection through proficient static analysis techniques.
3. Conduct real-time malware analysis with adept dynamic analysis skills.
4. Utilize covert malware launching methods for robust cybersecurity measures
5. Employ diverse malware detection techniques, including Android malware characterization, for enhanced cybersecurity.

UNIT-I:

INTRODUCTION: Introduction to malware, OS security concepts, malware threats, evolution of malware, malware types-viruses, worms, rootkits, Trojans, bots, spyware, adware, logic bombs, malware analysis, static malware analysis, dynamic malware analysis

UNIT-II:

STATIC ANALYSIS:X86 Architecture- Main Memory, Instructions, Opcodes and Endianness, Operands, Registers, Simple Instructions, The Stack, Conditionals, Branching, Rep Instructions, C Main Method and Offsets. Antivirus Scanning, Fingerprint for Malware, Portable Executable File Format, The PE File Headers and Sections, The Structure of a Virtual Machine, Reverse-Engineering- x86 Architecture, recognizing c code constructs in assembly, c++ analysis, Analyzing Windows programs, Anti-static analysis techniques- obfuscation, packing, metamorphism, polymorphism.

UNIT-III:

DYNAMIC ANALYSIS: Live malware analysis, dead malware analysis, analyzing traces of malware- system-calls, api-calls, registries, network activities. Anti-dynamic analysis techniques-anti-vm, runtime-evasion techniques, , Malware Sandbox, Monitoring with Process

Monitor, Packet Sniffing with Wireshark, Kernel vs. User-Mode Debugging, OllyDbg, Breakpoints, Tracing, Exception Handling, Patching.

UNIT-IV:

Malware Functionality: Downloader, Backdoors, Credential Stealers, Persistence Mechanisms, Privilege Escalation, Covert malware launching- Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection.

UNIT-V:

Malware Detection Techniques: Signature-based techniques: malware signatures, packed malware signature, metamorphic and polymorphic malware signature non-signature-based techniques: similarity-based techniques, machine-learning methods, invariant inferences.

Android Malware: Malware Characterization, Case Studies –Plankton, DroidKungFu, AnserverBot, Smartphone (Apps) Security.

Text Books:

1. Practical malware analysis The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig ISBN-10: 159327-290-1, ISBN-13: 978-1-59327-290-6, 2012 2
2. Computer viruses: from theory to applications by Filiol, Eric Springer Science & Business Media, 2006
3. Android Malware by Xuxian Jiang and Yajin Zhou, Springer ISBN 978-1-4614-7393-0, 2005

Reference Books:

1. Hacking exposed™ malware & rootkits: malware & rootkits security secrets & Solutions by Michael Davis, Sean Bodmer, Aaron Lemasters, McGraw-Hill, ISBN: 978-0-07-159119-5, 2010
2. Windows Malware Analysis Essentials by Victor Marak, Packt Publishing, 2015

21CY4276: Enterprise Security
(Professional Elective-V)

B.Tech. IV Year II Sem. **L T PC**

3 - - 3

Prerequisite: Computer Networks, Information Systems architecture, Risk management.

Course Objective

1. To understand enterprise security fundamentals, common attacks, compliance, and architectural origins.
2. To grasp the SABSA® Model, its application, systems engineering role, and control systems concept
3. To develop contextual security architectures aligned with business goals and assess operational risks
4. To design comprehensive logical, physical, and component security architectures.
5. To manage operational security, policies, risks, and assurance effectively

Course Outcomes

1. Identify attacks and compliance standards for proactive security measures.
2. Apply the SABSA® Model for robust security designs.
3. Develop security architectures aligned with business goals
4. Design comprehensive security architectures seamlessly.
5. Manage operational security, policies, and compliance effectively.

UNIT-I

Introduction: What is enterprise Security, Importance of Enterprise Security, Fundamental best practices of Enterprises Security, Common Enterprise attacks, difference types of compliances and standards, The Origins of Architecture, Managing Complexity, Information Systems Architecture, Enterprise Security Architecture.

UNIT-II

Security Architecture Model: The SABSA® Model, The SABSA® Matrix, SABSA Matrix for the Operational Layer, The Role of Systems Engineering, The Need for Systems Engineering in Security Architectures, The Control System Concept,

UNIT-III

Strategy and Planning: **Contextual Security Architecture**- Business Needs for Information Security, Digital Business, Operational Continuity and Stability, Safety-Critical Dependencies, Business Goals, Success Factors and Operational Risks, Operational Risk Assessment, Business Processes and Their Need for Security, Organization and Relationships Affecting Business Security Needs, Location Dependence of Business Security Need, Time Dependency of Business Security Need.

Conceptual Security Architecture: Conceptual Thinking. Security Strategies and Architectural Layering, Security Entity Model and Trust Framework, Security Domain Model.

UNIT-IV

Design, Logical Security Architecture, Physical Security Architecture, Component Security Architecture,

UNIT-V

Operations, Operational Security Architecture, Security Policy Management, Operational Risk Management, Assurance Management.

,

Text Books:

1. Enterprise Security Architecture: A Business-Driven Approach by John Sherwood, Andrew Clark, David Lynas.
2. Next-Generation Enterprise Security and Governance by Abu Barkat, Mohiuddin Ahmed

Reference Books:

1. Mastering Enterprise Security Architecture: A Comprehensive Guide To Become An Enterprise Security Architect by Cybellium Ltd.
2. Implementing Enterprise Cybersecurity with Opensource Software and Standard Architecture by Anand Handa, Rohit Negi, et al.
3. Enterprise Information Security Architecture A Complete Guide - 2021 Edition by Gerardus Blokdyk.

21CY4277: Device Hacking
(Professional Elective-V)

B.Tech. IV Year II Sem. **L T PC**
3 - - 3

Prerequisite: Computer Networks, Operating Systems, Cloud Computing, IOT Fundamentals

Course Objectives

1. To develop proficiency in password cracking techniques to secure operating systems.
2. To conduct wireless network penetration tests to strengthen encryption protocols.
3. To analyze malware components and implement sniffing techniques for network security.
4. To evaluate cloud threats and conduct penetration tests for enhanced cloud security.
5. To identify IoT threats and implement security measures for IoT ecosystems."

Course Outcomes

1. Understand system hacking methodologies and techniques.
2. Analyze WPA/WPA2 authentication modes and vulnerabilities.
3. Explore different types of malwares and their propagation methods
4. Evaluate cloud security controls and best practices
5. Analyze IoT hacking techniques and threats.

UNIT-1

Operating System Hacking: System Hacking Techniques / methodologies, Password Cracking, Privilege Escalation, Keyloggers and spywares, Hiding Files. Root kits**.**

UNIT-II

Hacking Wireless networks: Wi-Fi Security, WPA/WPA2 Encryption, WPA/WPA2 Authentication modes, wireless hacking methodology, wireless attacks

UNIT-III

Malware Threats: Malware and its propagation methods, malware components, Types malware: trojan, virus, worm, Ransomware, adware**,** Malware analysis and Countermeasures**.**

Sniffing: Sniffing Concepts, types of sniffing, types of active sniffing attacks.

UNIT-IV

Cloud Hacking: Cloud Computing and types of cloud, cloud deployment models, benefits of cloud computing, Popular cloud providers: AWS, Common threats to cloud services, Popular attacks on cloud, cloud security controls and best practices, Cloud penetration testing procedure and procedure.

UNIT-V

IOT Hacking: What is IOT, how does it works, IOT Architecture, Applications of IOT, IOT Communication models, Challenges with IOT, IOT Attacks and threats, IOT Countermeasures.

Text Books:

1. Hacking: The Art of Exploitation" by Jon Erickson
2. "Hacking Exposed Wireless: Wireless Security Secrets & Solutions" by Johnny Cache, Joshua Wright, and Vincent Liu
3. “Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software” by Michael Sikorski and Andrew Honig

Reference Books:

1. "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" by Tim Mather, Subra Kumaraswamy, and Shahed Latif
2. "Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities" by Nitesh Dhanjani
3. "Penetration Testing IoT Devices: A Practical Guide to Testing IoT Systems and Understanding IoT Security" by Aaron Guzman and Aditya Gupta

21CY4278: SECURITY GOVERNANCE AND RISK MANAGEMENT
(Professional Elective-V)

B.Tech. IV Year II Sem. **L T PC**
3 - - 3

Prerequisite: Information Security Fundamentals, Risk Management Fundamentals:

Course Objectives

1. To be able to understand governance origins, roles, and benefits for effective security governance
2. To be able to align security strategies, manage risks, assure processes, deliver value, and optimize resources.
3. To be able to define risk management responsibilities, set objectives, and conduct gap analysis.
4. To be able to craft robust security strategies, allocate resources, and navigate constraints effectively.
5. To be able to define and measure metrics for security program development and support CISO decisions.

Course Outcomes

1. Identify governance origins, roles, and benefits for effective security practices.
2. Align strategies, manage risks, assure processes, deliver value, and optimize resources for security.
3. Define responsibilities, set objectives, and conduct gap analysis for enhanced risk management.
4. Craft strategies, allocate resources, and navigate constraints for actionable security plans.
5. Define and measure metrics, aiding decision-making for CISOs and security management.

UNIT-I:

Governance Overview: Origins of Governance, Governance Definition, Information Security Governance, Six Outcomes of Effective Security Governance, Benefits of Good Governance.

Roles and Responsibilities: The Board of Directors, Executive Management, Security Steering Committee, The CISO **Strategic Metrics**: Governance Objectives.

UNIT-II:

Information Security Outcomes: Strategic Alignment, Risk Management, Business Process Assurance/Convergence, Value Delivery, Resource Management, Resource Management **Security Governance Objectives**: Security Architecture, CobiT, Capability Maturity Model.

UNIT-III:

Risk Management Objectives: Risk Management Responsibilities, Managing Risk Appropriately, Determining Risk Management Objectives.

Current State: Current State of Security, Current State of Risk Management, Gap Analysis—Unmitigated Risk
Practical Technical Scenarios (Ptss), DrivesCobit5, Framework Principles.

UNIT-IV:

Developing a Security Strategy: Failures of Strategy, Attributes of a Good Security, Strategy Resources, Strategy Constraints, Sample Strategy Development.

Implementing Strategy: Action Plan Intermediate Goals, Action Plan Metrics, Reengineering, Inadequate Performance, Elements of Strategy.

UNIT-V:

Security Program Development Metrics: Information Security Program Development Metrics, Program Development Operational Metrics

Information Security Management Metrics: Management Metrics, Security Management Decision Support Metrics, CISO Decisions, Information Security Operational Metrics.

Text Books:

1. Information Security Governance Simplified: From the Boardroom to the Keyboard by Todd Fitzgerald
2. Information Security Governance A Practical Development and Implementation Approach KragBrotby, Wiley A John Wiley & Sons, Inc., Publication

Reference Books:

1. Alan Calder, Steve G. Watkins, “Information Security Risk Management for ISO27001/ISO27002”,itgp, 2010.
2. Risk Management and Governance: Concepts, Guidelines and Applications:by Terje Aven and Ortwin Renn

21CY4281: Major Project

B.Tech. IV Year II Sem.

L	T	P	C
-	-	20	10