B. Tech. Cyber Security

I Year: First Semester

Teaching Scheme					Contact Hours/Week			Exam Duration (h)		Relative Weights (%)				
S. No.	**Subject Code**	**Course Title**	**Subject Area**	**Credit**	**L**	**T**	**P**	**Theory**	**Practical**	**CWS**	**PRS**	**MTE**	**ETE**	**PRE**
1	AM101	Mathematics-I	BSC	4	3	1	0	3	0	25	-	25	50	-
2	CO101	Programming Fundamentals	ESC	4	3	0	2	3	0	15	25	20	40	-
3	EC105	Digital Electronics	ESC	4	3	0	2	3	0	15	25	20	40	-
4	**CO103/CY101n**	**Computer Systems**	ESC	4	3	0	2	3	0	15	25	20	40	-
5	CY103 / IT103	Fundamentals of Web Design	SEC	2	1	0	2	0	3	-	50	-	-	50
6	AEC/VAC	AEC/VAC	AEC/VAC	2	2/1/0	0	0/2/4	3/3/0	0/2/3	25/15/0	0/25/50	25/20/0	50/40/0	0/0/50
Total				**20**										

I Year: Second Semester

1	AM102	Mathematics-II	BSC	4	3	1	0	3	0	25	-	25	50	-
2	AP102	Physics	BSC	4	3	0	2	3	0	15	25	20	40	-
3	**CY102**	**Data Structures**	ESC	4	3	1	0	3	0	25	-	25	50	-
4	CY104 / IT104	Object Oriented Programming	DCC	4	3	0	2	3	0	15	25	20	40	-
5	CY106	IT Workshop	SEC	2	1	0	2	0	3	-	50	-	-	50
6	AEC/VAC	AEC/VAC	AEC/VAC	2	2/1/0	0	0/2/4	3/3/0	0/2/3	25/15/0	0/25/50	25/20/0	50/40/0	0/0/50
Total				**20**										

B. Tech. Cyber Security

II Year: Third Semester

Teaching Scheme					Contact Hours/Week			Exam Duration (h)		Relative Weights (%)				
S. No.	**Subject Code**	**Course Title**	**Subject Area**	**Credit**	**L**	**T**	**P**	**Theory**	**Practical**	**CWS**	**PRS**	**MTE**	**ETE**	**PRE**
1	CY201	Micro-Processor and Controller	ESC	4	3	0	2	3	0	15	25	20	40	-
2	CY203	Introduction to Cyber Physical Systems	DCC	4	3	0	2	3	0	15	25	20	40	-
3	CY205	Fundamentals of Operating Systems	DCC	4	3	0	2	3	0	15	25	20	40	-
4	CY207	Computer Networks	DCC	4	3	0	2	3	0	15	25	20	40	-
5	CY209	Algorithm Design and Analysis	DCC	4	3	1	0	3	0	25	-	25	50	-
6	AEC/VAC	AEC/VAC	AEC/VAC	2	2/1/0	0	0/2/4	3/3/0	0/2/3	25/15/0	0/25/50	25/20/0	50/40/0	0/0/50
7	MS299	Community Engagement Course	Mandatory	2										
Total				**24**										

II Year: Fourth Semester

1	CY202	Network Security	ESC	4	3	0	2	3	0	15	25	20	40	-
2	CY204	System Security	DCC	4	3	0	2	3	0	15	25	20	40	-
3	CY206	Machine Learning	DCC	4	3	0	2	3	0	15	25	20	40	-
4	CY208	Secure Coding	DCC	4	3	1	0	3	0	25	-	25	50	-
5	CY210	Ethical Hacking	DCC	4	3	0	2	3	0	15	25	20	40	-
6	AEC/VAC	AEC/VAC	AEC/VAC	2	2/1/0	0	0/2/4	3/3/0	0/2/3	25/15/0	0/25/50	25/20/0	50/40/0	0/0/50
Total				**22**										

Additional 02 credits are to be earned from mandatory community engagement course in second year to fulfil the requirement of award of the four year B.Tech. Degree.

B. Tech. Cyber Security

III Year: Fifth Semester

Teaching Scheme					Contact Hours/Week			Exam Duration (h)		Relative Weights (%)				
S. No.	**Subject Code**	**Course Title**	**Subject Area**	**Credit**	**L**	**T**	**P**	**Theory**	**Practical**	**CWS**	**PRS**	**MTE**	**ETE**	**PRE**
1	CY301	Digital Forensics	DCC	4	3	0	2	3	0	15	25	20	40	-
2	CY303	Applied Cryptography	DCC	4	3	1	0	3	0	25	-	25	50	-
3	CY305	Web Application Security	DCC	4	3	0	2	3	0	15	25	20	40	-
4	HU301	Engineering Economics	SEC	3	3	1	0	3	0	25	-	25	50	-
5	CY3XX	Discipline Specific Elective Course - 1	DEC	4	3/3	0/1	2/0	3	0	15/25	25/0	20/25	40/50	-
6	GECXXX	Generic Elective Course - 1	GEC	4	3/3	0/1	2/0	3	0	15/25	25/0	20/25	40/50	-
Total				**23**										

III Year: Sixth Semester

1	CY302	Internet of Things and Security	DCC	4	3	0	2	3	0	15	25	20	40	-
2	CY304	Malware Analysis	DCC	4	3	0	2	3	0	15	25	20	40	-
3	MG302	Fundamentals of Management	SEC	3	3	1	0	3	0	25	-	25	50	-
4	CY3XX	Discipline Specific Elective Course - 2	DEC	4	3/3	0/1	2/0	3	0	15/25	25/0	20/25	40/50	-
5	CY3XX	Discipline Specific Elective Course - 3	DEC	4	3/3	0/1	2/0	3	0	15/25	25/0	20/25	40/50	-
6	GECXXX	Generic Elective Course - 2	GEC	4	3/3	0/1	2/0	3	0	15/25	25/0	20/25	40/50	-
Total				**23**										

B. Tech. Cyber Security

IV Year: Seventh Semester

Teaching Scheme					Contact Hours/Week			Exam Duration (h)		Relative Weights (%)				
S. No.	**Subject Code**	**Course Title**	**Subject Area**	**Credit**	**L**	**T**	**P**	**Theory**	**Practical**	**CWS**	**PRS**	**MTE**	**ETE**	**PRE**
1	CY401	B. Tech Project-I	DCC	4	-	-	-	-	-	-	40	-	-	60
2	CY403	Internship	DCC	2	-	-	-	-	-	-	40	-	-	60
3	CY4XX	Discipline Specific Elective Course - 4	DEC	4	3/3	0/1	2/0	3	0	15/25	25/0	20/25	40/50	-
4	CY4XX	Discipline Specific Elective Course - 5	DEC	4	3/3	0/1	2/0	3	0	15/25	25/0	20/25	40/50	-
5	GECXXX	Generic Elective Course - 3	GEC	4	3/3	0/1	2/0	3	0	15/25	25/0	20/25	40/50	-
6	VACXXX	Indian Knowledge System	VAC	Non Credit										
Total				**18**										

IV Year: Eight Semester

1	CY402	B. Tech Project-II	DCC	8	-	-	-	-	-	-	40	-	-	60
2	CY4XX	Discipline Specific Elective Course - 6	DEC	4	3/3	0/1	2/0	3	0	15/25	25/0	20/25	40/50	-
3	GECXXX	Generic Elective Course - 4	GEC	4	3/3	0/1	2/0	3	0	15/25	25/0	20/25	40/50	-
Total				**16**										

Cumulative Total	**166**	

B. Tech. Cyber Security

Discipline Specific Elective Courses

Discipline Specific Elective Course - 1 (Semester - 5)	
CY307	Deep Learning
CY309	Fundamentals of Blockchain
CY311	Penetration Testing
CY313	Quantum Computing
CY315	Windows Administration
CY317	Essentials of Generative AI & Prompt Engineering
CY319	Digital Image & Video Processing
CY321	Natural Language Processing
CY323	Computer Graphics for Virtual Reality
CY325	Mobile Application Development
CY327	Computer Controlled Systems
CY329	Multimodal Data Processing
CY331	Data Base Security & Access control
CY333	Windows Server Management
CY335	Ad hoc Mobile Security
CY337	High Performance Computing
CY339	Data Base Management

Discipline Specific Elective Course - 2 & 3 (Semester - 6)	
CY306	Pattern Recognition

Discipline Specific Elective Course - 4 & 5 (Semester - 7)	
CY405	Social Networks Analysis
CY407	Data Science & Big Data
CY409	Basics of Control Systems
CY411	Security and Privacy of CPS
CY413	Adversarial Machine Learning
CY415	Multimedia Forensics
CY417	Block chain Security & Performance
CY419	Block Chain & Fintech
CY421	Intrusion Detection and Information Warfare
CY423	Embedded Systems for IoT
CY425	Scientific and Engineering Data Visualization
CY427	Web Server Management
CY429	Data Warehousing and Data Mining
CY431	Steganography and Digital Watermarking
CY433	Smart Sensors for Healthcare
CY435	CPS for Internal and External Security
CY437	Game Theory
CY439	Information Theory and Coding
CY441	Grid and Cluster Computing
CY443	High-Speed Networks

Discipline Specific Elective Course - 6 (Semester - 8)	
CY404	Cluster Management

	CY308	Image Analysis		CY406	Hyper ledger and Fabric programming
	CY310	Blockchain Platform and Use Cases		CY408	Hardware Security
	CY312	Smart contracts and Solidity		CY410	IoT with Arduino, ESP, and Raspberry Pi
	CY314	Gen AI with cybersecurity		CY412	Mathematical Modelling and Computer-Aided Engineering
	CY316	Software Testing and Security Audit of CPS		CY414	Security Architecture
	CY318	Cyber Threat Intelligence		CY416	Cyber Laws
	CY320	Post Quantum Cryptography		CY418	Mobile VR and AI in Module
	CY322	Ubiquitous Sensing, Computing and Communication		CY420	CPS Assurance
	CY324	Concepts of Virtual and Augmented Reality		CY422	Cloud Security
	CY326	Linux Administration		CY424	Computer Vision
	CY328	Deep Learning Applications		CY426	Compliance Frameworks for Cyber Security
	CY330	Security Assessment & Risk Analysis		CY428	Edge and Fog Computing
	CY332	Human Computer Interactions		CY430	Cognitive Computing
	CY334	Data Analysis using open-source programming		CY432	Neuromorphic Computing
	CY336	Dependable Machine Learning		CY434	Optimization Techniques
	CY338	Embedded Systems		CY436	Pervasive and Ubiquitous Computing
	CY340	Real Time Operating Systems		CY438	Digital Twins
	CY342	Compiler Design		CY440	Robotics

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
EC105 Digital Electronics	**L**	**T**	**P**	**Basic Computer**
	3	**0**	**2**	

Course Objectives:

1. To provide the basic knowledge of gates, Number Systems and their Arithmetic, Computer Codes, digital logic families, SOP and POS simplifications.
2. Ability to design MSI/LSI circuits.
3. Gain Knowledge about the function of Flip-Flops, Counters, Registers.
4. Understanding the concepts of Sequential circuits.

S. NO	Course Outcomes (CO)
CO1	Ability to understand the fundamentals of digital systems.
CO2	Ability to apply learned fundamental to implement real systems that are useful for the society.
CO3	Ability to learn the basic concept of synthesis of combinational circuits.
CO4	Ability to learn the basic concept of synthesis of synchronous as well as asynchronous sequential circuits.

S. NO	Contents	Contact Hours
UNIT 1	Number Systems and Codes: Introduction to the positional number system, signed magnitude numbers, floating point numbers, binary arithmetic: addition, subtraction, multiplication and division, Base conversion, conversion formulas with examples, one's and two's compliment arithmetic, Computer codes – BCD codes, gray codes, excess-3 codes, parity checks, Hamming and alphanumeric codes.	**12**
UNIT 2	Combinational Logic Design: Introduction, standard representations for logical functions, Karnaugh map representation, simplification of logical functions using K- map, minimization of logical functions specified in minterms/maxterms or Truth Table, minimization of logical functions not specified in minterms/maxterms, Don't care conditions, design examples, Ex-or and Ex-nor simplification of K-maps, five and six-variable K-maps, QM method, MEV method,	**12**
UNIT 3	Introduction of multiplexers and their use in combinational logic design, demultiplexers /decoders and their use in combinational logic design, adders and their use as subtractors, digital comparators, parity generators/checkers, code converters, priority encoders, 7-segment decoder/driver.	**8**
UNIT 4	Synchronous Sequential Circuits and Asynchronous Sequential Circuits: Introduction, FSM model, memory elements and their excitation functions.	**10**

	Synthesis of synchronous sequential circuits, capabilities and limitation of FSM, state equivalence and minimization, simplification of incompletely specified machines, Fundamental mode circuits synthesis, state assignment, pulse mode circuits.	
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1.	R.P. Jain: Modern Digital Electronics, TMH Publications.	2009
2.	Z Kohavi: Switching and Finite Automata Theory, TMH Publications.	2009
3.	M.M. Mano: Digital Logic Design, PHI Publications.	2004
4.	Dr. B.R. Gupta: Digital Electronics, Katson Publications.	2012
5.	James W. Bignell& Robert Donovan: Digital Electronics, Cengage Learning Publications.	2013
6.	Sanjay Kumar Bose: Digital Systems, New Age International Publishers	2019

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY101 Computer Systems	**L**	**T**	**P**	**Basic Computer**
	3	**0**	**2**	

Course Objectives:

1. To provide foundational knowledge of computer hardware, software, and architecture.
2. To analyze security implications in system design and operations.
3. To develop skills in secure memory management, network protocols, and reverse engineering.
4. To explore emerging technologies like cloud computing and IoT with a security focus.

S. NO	Course Outcomes (CO)
CO1	Analyze computer architecture components and their security vulnerabilities.
CO2	Design secure systems using principles of digital logic and OS security.
CO3	Implement network security protocols and defend against common attacks.
CO4	Reverse-engineer malware and apply defensive strategies.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Computer Systems:** Overview of computer systems: Hardware, software, and firmware, Components: CPU, memory, storage, I/O devices, Evolution of computing systems and architectures, Role of computer systems in cybersecurity.	**10**
UNIT 2	**Digital Logic and Computer Architecture:** Basics of digital logic (gates, Boolean algebra), CPU architecture: Registers, ALU, control unit, Memory hierarchy: Cache, RAM, ROM, I/O systems and interrupts, Security implications of hardware design	**10**
UNIT 3	**Operating Systems and Security:** OS structure and kernel operations, Process management, threading, and scheduling, Memory and file system management, Security models: Access control, authentication, encryption, OS vulnerabilities and hardening techniques.	**8**
UNIT 4	**Computer Networks and Network Security:** Network fundamentals: Topologies, OSI/TCP/IP models; Protocols: HTTP, DNS, TCP, UDP, IP; Network security: Firewalls, VPNs, IDS/IPS; Common attacks: DDoS, MITM, phishing; Secure protocols: HTTPS, SSL/TLS, SSH.	**8**
UNIT 5	**Memory Management and Storage Systems:** Virtual memory, paging, and segmentation, Storage devices: HDD, SSD, RAID configurations, Data integrity and redundancy, Encryption: Full-disk encryption, secure deletion, Side-channel attacks on memory/storage	**6**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Computer Organization and Design (6th ed.), David A. Patterson, John L. Hennessy Morgan Kaufmann	2020
2	Operating System Concepts (10th ed.), Abraham Silberschatz, Peter B. Galvin, Greg Gagne, Wiley	2018
3	Computer Networking: A Top-Down Approach (8th ed.), James F. Kurose, Keith W. Ross Pearson	2020
4	Cybersecurity Essentials, Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short Sybex	2018

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY103 Fundamentals of Web Design	**L**	**T**	**P**	
	1	0	2	

Course Objectives: 1. Develop the skill & knowledge of Web page design.
2. Students will understand the knowhow and can function either as an entrepreneur or can take up jobs in the multimedia and Web site development studio and other information technology sectors

S. NO	Course Outcomes (CO)
CO1	Define the principle of Web page design
CO2	Visualize the basic concept of HTML.
CO3	Recognize the elements of HTML
CO4	Apply basics concept of CSS for styling the pages
CO5	Develop the concept of web publishing

S. NO	Contents	Contact Hours
UNIT 1	Introduction to Internet and HTML: WWW, Browser, URL, Web server, Web site, Domain Name, Basic principles involved in developing a web site, designing a web page, Page Layout, HTML Documents, Basic structure of an HTML document, Creating an HTML document, Mark up Tags, Heading-Paragraphs, Line Breaks, HTML Tags.	**9**
UNIT 2	Elements of HTML: Introduction, Working with Text, Working with Lists, Tables and Frames, Working with Hyperlinks, Images and Multimedia, Working with Forms and controls	**9**
UNIT 3	Introduction to Cascading Style Sheets: Concept of CSS, Creating Style Sheet, CSS Properties, CSS Styling, Working with block elements and objects, Working with Lists and Tables, CSS Id and Class, CSS Colour, Creating page Layout and Site Designs.	**9**
UNIT 4	Introduction to Web Publishing or Hosting: Creating the Web Site, Saving the site, working on the web site, creating web site structure, Creating Titles for web pages, Themes-Publishing web sites.	**9**
	TOTAL	**36**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	HTML 5 in simple steps, Kogent Learning Solutions Inc, Dreamtech Press	
2	Beginner's Guide to HTML, Michael Gabriel	
3	Beginning HTML, XHTML, CSS, and JavaScript, John Duckett, Wiley India	

4	Beginning CSS: Cascading Style Sheets for Web Design, Ian Pouncey, Richard York, Wiley India	

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY102 Data Structures	**L**	**T**	**P**	**Fundamentals of Programming**
	3	**0**	**2**	

Course Objective: 1) Design correct programs to solve problems.
2) Choose efficient data structures and apply them to solve problems.

S. NO	Course Outcomes (CO)
CO1	Ability to select the data structures that efficiently model the information in a problem.
CO2	Apply and implement stack and queue data structures using arrays, and solve problems involving expression evaluation, recursion, and priority queues.
CO3	Design and implement linked list data structures and perform operations such as insertion, deletion, traversal, and searching
CO4	Analyze and implement tree data structures and various operations on the tree.
CO5	Apply concepts of graph theory and file structures, including graph representations, traversal algorithms, shortest paths, spanning trees, hashing, and indexing techniques.

S. NO	Contents	Contact Hours
UNIT 1	Introduction: Introduction to Algorithmic, Complexity- Time-Space Trade off. Introduction to abstract data types, design, implementation and applications. Introduction to List data structure. Arrays and Strings: Representation of Arrays in Memory: one dimensional, Two dimensional and Multidimensional, Accessing of elements of array, performing operations like Insertion, Deletion. Sorting elements of arrays: Insertion Sort. Strings and String Operations. Searching: Linear Search, Binary search, Interpolation Search	**6**
UNIT 2	Stacks and Queues: Introduction to data structures like Stacks and Queues. Operations on Stacks and Queues, Array representation of Stacks , Applications of Stacks : recursion, Polish expression and their compilation conversion of infix expression to prefix and postfix expression, Operations of Queues, Representations of Queues Applications of Queues, Priority queues. .	**9**
UNIT 3	Linked Lists: Singly linked lists, Representation of linked list, Operations of Linked list such as Traversing, Insertion and Deletion, Searching, Applications of Linked List. Concepts of Circular linked list and Doubly linked list and their Applications. Stacks and Queues as linked list	**9**
UNIT 4	Trees: Basic Terminology, Binary Trees and their representation, binary search trees, various operations on Binary search trees like traversing, searching , Insertion and Deletion , Applications of Binary search Trees , Complete Binary trees, Extended binary trees. General trees, AVL trees, Threaded trees, B- trees, Red-Black Tree	**8**

UNIT 5	Graphs: Terminology and Representations, Graphs & Multi-graphs, Directed Graphs, Representation of graphs and their Transversal, Spanning trees, shortest path and Transitive Closure, Activity Networks, Topological Sort and Critical Paths, Strongly connected components, Bipartite Graphs. File Structure: File Organization, Indexing & Hashing, Hash Functions, Collision Resolution Techniques.	**10**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1.	Horowitz and Sahni, "Fundamentals of Data structures", Galgotia publications.	1999
2.	Tannenbaum, "Data Structures", PHI.	2007
3.	An introduction to data structures and application by Jean Paul Tremblay & Pal G. Sorenson (McGraw Hill).	2017
4.	Data Structures and Algorithms Made Easy by Narasimha Karumanchi, CareerMonk Publications	2016

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY104 Object-Oriented Programming	**L**	**T**	**P**	
	3	0	2	

Course Objectives: 1. To understand the basics of classes and objects.
2. To provide knowledge of Object-Oriented programming features.
3. To understand the concept of operator overloading and inheritance
4. To understand the concept of exception handling, Input-Output and File Operation

S. NO	Course Outcomes (CO)
CO1	To differentiate between structured and object-oriented programming
CO2	To apply the concepts of Constructor, destructor, friend functions and classes and dynamic objects
CO3	To investigate cases of operator overloading, inheritance and abstraction
CO4	To implement generic programming with templates
CO5	To investigate Byte code, casting and conversion and input-output
CO6	To explain access specifiers, polymorphism and STL

S. NO	Contents	Contact Hours
UNIT 1	Object oriented paradigm & C++ at a glance: Evolution of programming paradigm, structured versus object-oriented development, elements of object-oriented programming, Objects, classes, methods, popular OOP languages, software reuse. Classes and objects: Introduction, Class revisited, constant objects and constructor, static data members with constructors and destructors, constructor overloading, nested classes, objects as arguments, returning objects, friend functions and friend classes, constant parameters and member functions, static data and member functions.	**9**
UNIT 2	Dynamic objects: Introduction, pointers to objects, array of objects, pointers to object members, this pointer, self-referential classes Operator overloading and Inheritance: overloading of new and delete operators, conversion between objects and basic types, conversion between objects of different classes, overloading with friend functions, abstract classes, inheritance types, virtual base classes, virtual functions, pointer to derived class objects, and base class objects, pure virtual functions, virtual destructors	**10**
UNIT 3	Generic programming with templates: Introduction, function templates, overloaded function templates, class templates, inheritance of class template, class template containership, class template with overloaded operators	**7**
UNIT 4	Introduction to byte code, security and portability, Data Types, variables, operators, arrays, type conversion and casting, type promotion, Control statements, standard input-output, Designing Classes, constructors, methods, Access specifiers: public, private, protected, inheritance, packages and	**8**

	interfaces, Math, String, Vectors, and Array List classes, polymorphism: function and operator overloading, function overriding, abstract classes	
UNIT 5	Exception Handling: exception types, nested try-catch, throw, throws and finally, statements, Multithread Programming: thread creation, synchronization and priorities. Input-output and file operations: Java.io, stream classes, Byte streams, character streams, serialization.	**8**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Patrick Naughton, Herbert Schildt: "The Complete Reference: Java 2", 12th Edition, TMH.ISBN- 978-1260463415, McGraw Hill publisher, December 2021	2021
2	C Thomas Wu : "An Introduction to OO programming with Java", TMH, ISBN-10: 0073523305	
3	Balaguruswami, "Object oriented with C++", 8th Edition, TMH, 2020 ISBN 978-9389949186, McGraw Hill publisher, September 2020	2020
4	Budd, "Object Oriented Programming", Addison Wesley	
5	Mastering C++ K.R Venugopal Rajkumar, TMH.	

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY106 IT Workshop	**L**	**T**	**P**	**Fundamentals of IT**
	1	**0**	**2**	

Course Objectives:

1. Master foundational tools like Git, Docker, Kubernetes, and cloud platforms (AWS/Azure/GCP) to build scalable, cloud-native applications.
2. Gain hands-on experience with AI/ML, generative AI, IoT, blockchain, and quantum computing to solve real-world problems.
3. Design CI/CD pipelines, automate infrastructure, and deploy machine learning models in production environments.
4. Work in teams to integrate multiple technologies (e.g., IoT + AI + Cloud) in a capstone project, simulating industry workflows.

S. NO	Course Outcomes (CO)
CO1	Design and deploy serverless architectures using AWS Lambda/Azure Functions and automate cloud infrastructure with Terraform.
CO2	Build and fine-tune machine learning models (e.g., TensorFlow/PyTorch) and generative AI systems (e.g., GPT-4, LangChain) for domain-specific tasks.
CO3	Implement DevOps workflows by creating CI/CD pipelines (Jenkins/GitHub Actions) and managing containerized applications with Kubernetes.
CO4	Develop IoT solutions using edge devices (Raspberry Pi/Arduino) and deploy lightweight ML models for real-time data processing.
CO5	Create smart contracts and dApps on blockchain platforms (Ethereum/Hardhat) and explore Web3 use cases like NFTs.

S. NO	Contents	Contact Hours
UNIT 1	Basics of OS (Linux/Windows), CLI, and virtualization (Docker/WSL), Version control with Git & GitHub (collaborative workflows, CI/CD basics, Introduction to cloud-native development (VS Code, GitHub Codespaces).	**10**
UNIT 2	Introduction to Multi-cloud platforms (AWS, Azure, GCP): Compute, Storage, and DB services, Serverless computing (AWS Lambda, Azure Functions)., Infrastructure as Code (IaC) with Terraform.	**10**
UNIT 3	Introduction to CI/CD pipelines (Jenkins, GitLab CI), Container orchestration (Kubernetes, Docker Swarm), MLOps: Model deployment with MLflow/Kubeflow.	**8**
UNIT 4	Introduction to IoT protocols (MQTT, CoAP) and sensors (Raspberry Pi/Arduino), Edge AI: Deploying ML models on edge devices.	**8**
UNIT 5	Fundamental of Blockchain fundamentals (Ethereum, Solidity), Smart contracts and NFTs, Sustainable IT & Green Computing, AR/VR development (Unity, Unreal Engine), 5G/6G and network slicing.	**6**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1.	The Phoenix Project" (DevOps), "Hands-On Machine Learning" (Aurélien Géron).	2020
2.	Coursera's "AI for Everyone", edX's "Blockchain Fundamentals".	
3.	GitHub Open Source Projects, Stack Overflow, Hackathons	

List of Experiments:

1. Set up a Docker container for a Python app.
2. Collaborate on a GitHub repo with CI/CD using GitHub Actions.
3. Deploy a serverless API using AWS Lambda + API Gateway.
4. Automate cloud resource provisioning with Terraform.
5. Build a CI/CD pipeline for a microservice app.
6. Deploy a machine learning model using Kubernetes.
7. Create a smart home system with motion sensors and cloud integration.
8. Run a lightweight TensorFlow Lite model on Raspberry Pi.
9. Deploy a smart contract on Ethereum testnet.
10. Build a decentralized app (dApp) with Hardhat.

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY201 Micro-Processor and Controller	**L**	**T**	**P**	**Digital Electronics**
	3	**0**	**2**	

Course Objectives:

1. To understand microprocessor architecture and assembly language programming.
2. To analyze security vulnerabilities in hardware and firmware design.
3. To design secure embedded systems and IoT devices.
4. To implement secure communication protocols in microcontroller-based systems.

S. NO	Course Outcomes (CO)
CO1	Explain the architecture of microprocessors and microcontrollers. |.
CO2	Develop assembly-level programs and analyze security risks in low-level code.
CO3	Interface peripherals securely and mitigate hardware-level attacks.
CO4	Design secure embedded systems with encryption and authentication.
CO5	Evaluate IoT device vulnerabilities and apply hardware hardening techniques.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Microprocessors:** Evolution: 8085, 8086, x86, ARM architectures, Bus structure, registers, ALU, and control unit, Security flaws in legacy systems (e.g., Spectre/Meltdown)	**12**
UNIT 2	**Assembly Language Programming:** Instruction sets, addressing modes Interrupts, I/O programming, Vulnerabilities: Buffer overflows, code injection	**10**
UNIT 3	**Interfacing and Peripheral Devices:** Memory-mapped I/O, DMA, timers, Secure interfacing with sensors, displays, and communication modules, Hardware Trojans and side-channel attacks	**10**
UNIT 4	**Microcontrollers and Embedded Systems:** 8051, AVR, ARM Cortex architectures, Firmware security: Secure boot, OTA updates, Case study: IoT device security (e.g., Mirai botnet) | |	**10**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1.	The Intel Microprocessors (8th ed.), Barry B. Brey, Pearson	2009
2.	AVR Microcontroller and Embedded Systems, Muhammad Ali Mazidi, Pearson	2016

3.	Embedded Systems Security, David Kleidermacher, Elsevier	2012
4.	Hardware Security: A Hands-On Learning Approach Swarup Bhunia, Mark Tehranipoor, Morgan Kaufmann	2018

B.Tech. Information Technology (Cyber Security)

Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY203 Introduction to Cyber Physical Systems (CPS)	**L**	**T**	**P**	**Computer Systems**
	3	**0**	**2**	

Course Objectives:

1. To introduce the fundamentals of Cyber-Physical Systems (CPS) and their applications.
2. To analyze security vulnerabilities in CPS components (sensors, actuators, controllers).
3. To design secure architectures for industrial control systems (ICS), IoT, and smart grids.
4. To explore attack vectors like Stuxnet and mitigation strategies.

S. NO	**Course Outcomes (CO)**
CO1	Explain the architecture of CPS and their role in critical infrastructure.
CO2	Identify security threats in sensor networks, PLCs, and SCADA systems.
CO3	Implement secure communication protocols for CPS (e.g., Modbus, DNP3).
CO4	Apply intrusion detection and anomaly detection techniques in CPS.
CO5	Evaluate resilience strategies against cyber-physical attacks.

S. NO	**Contents**	**Contact Hours**
UNIT 1	**Introduction to CPS: Definition, components (sensors, actuators, controllers), Applications: Smart grids, healthcare, autonomous vehicles, Security challenges: Attack surfaces in CPS**	**9**
UNIT 2	**CPS Networking Protocols: Industrial protocols: Modbus, DNP3, OPC-UA, IoT protocols: MQTT, CoAP, LoRaWAN, Security flaws: Unencrypted traffic, protocol spoofing**	**9**
UNIT 3	**CPS Security Threats & Mitigation: Attack vectors: Stuxnet, Triton, ransomware, Cryptography for CPS: Lightweight algorithms, PKI, Intrusion detection systems (IDS) for CPS**	**9**
UNIT 4	**Secure CPS Architectures: Defense-in-depth for ICS/SCADA systems, Zero-trust architecture in CPS, Case study: Securing smart grids and water treatment plants**	**8**
UNIT 5	**Emerging Trends in CPS: AI/ML for anomaly detection in CPS, Blockchain for secure CPS data integrity, Post-quantum cryptography in CPS**	**7**
	TOTAL	**42**

REFERENCES

S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**

1.	Cyber-Physical Systems, Raj kumar, Dionisio de Niz, Addison-Wesley|	2016
2.	Introduction to Embedded Systems, Edward Ashford Lee, MIT Press |	2017
3.	Handbook of CPS Security, My T. Thai, Sajal K. Das, Springer |	2019
4.	AI for Cyber-Physical Systems, Alvaro Cardenas, Rakesh B. Bobba, CRC Press	2022

B.Tech. Information Technology (Cyber Security)

Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY205: Fundamentals of Operating Systems	**L**	**T**	**P**	Computer Organization and Architecture, Programming in C or C++, Data Structures and Algorithms
	3	**0**	**2**	

Course Objective: To provide foundational knowledge of operating system principles and mechanisms for managing hardware and software resources effectively.

S. NO	**Course Outcomes (CO)**
CO1	Describe the basic structure and functions of operating systems.
CO2	Explain and analyze process management, scheduling, and inter-process communication.
CO3	Understand memory management techniques and virtual memory concepts.
CO4	Analyze and apply file systems and I/O management strategies.
CO5	Evaluate concurrency, deadlock handling, and synchronization mechanisms.

S. NO	**Contents**	**Contact Hours**
UNIT 1	**Introduction to Operating Systems:** What is an Operating System, History and evolution of Operating Systems, Types of Operating Systems: Batch, Multitasking, Multiprogramming, Real-time, Distributed, Embedded, System components: Kernel, Shell, Command Interpreter, System Calls and Operating System Services, Structure of Operating Systems (Monolithic, Microkernel, Layered, Modular)	**8**
UNIT 2	**Process Management:** Process concept, PCB (Process Control Block), Process states and transitions, Threads and multithreading models, CPU Scheduling: FCFS, SJF, Priority, Round Robin, Multilevel Queue, Context switching and Dispatcher, Inter-Process Communication (IPC): Shared Memory, Message Passing, Process synchronization: Race conditions, Critical Section problem, Classical synchronization problems: Producer-consumer, Readers-writers, Dining Philosophers, Semaphores, Mutex, Monitors	**10**
UNIT 3	**Memory Management:** Basic memory management concepts, Contiguous memory allocation: First-fit, Best-fit, Worst-fit, Paging, Page tables, Inverted page tables, Segmentation and segmentation with paging, Virtual memory: Demand paging, Page fault, Page replacement algorithms (FIFO, LRU, Optimal), Thrashing and Working Set Model	**8**
UNIT 4	**File Systems and Storage Management:** File concept, File types, File operations, Directory structures: Single level, Two-level, Tree, Acyclic	**8**

	Graph, File allocation methods: Contiguous, Linked, Indexed, File access methods: Sequential and Direct, Disk scheduling algorithms: FCFS, SSTF, SCAN, C-SCAN, LOOK, C-LOOK, RAID levels and disk reliability	
UNIT 5	**Deadlocks, Security & Case Studies**: Deadlock characterization: Necessary conditions, Resource Allocation Graphs, Deadlock prevention, avoidance (Banker's Algorithm), detection, and recovery, Security and Protection mechanisms in OS, Case studies: Linux, Windows, or Android OS overview, Mini project or simulation (e.g., CPU scheduling, page replacement)	**8**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Abaham Silberschatz, Peter B. Galvin, and Greg Gagne, *Operating System Concepts*, Wiley	2017
2	Andrew S. Tanenbaum, *Modern Operating Systems*, Pearson	2014
3	William Stallings, *Operating Systems: Internals and Design Principles*, Pearson	2019
4	LINUX: THE COMPLETE REFERENCE, 6TH EDITION	2017

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY207: Computer Networks	**L**	**T**	**P**	**Operating systems, Algorithm Design and Analysis**
	3	**0**	**2**	

Course Objective: To understand design and application of layered architecture and protocols of computer networks

S. NO	Course Outcomes (CO)
CO1	Understand basic concepts, OSI reference model, services and role of each layer of OSI model and TCP/IP, networks devices and transmission media
CO2	Apply channel allocation, framing, error and flow control techniques.
CO3	Functions of Network Layer i.e. Logical addressing, subnetting & Routing Mechanism
CO4	Transport & Application Layer function i.e. Port addressing, Connection Management, Error control and Flow control mechanism.

S. NO	Contents	Contact Hours
UNIT 1	Introductory Concepts: Goals and applications of networks, Categories of networks, Organization of the Internet, ISP, Network structure and architecture (layering principles, services, protocols and standards), The OSI reference model, TCP/IP protocol suite, Network devices and components. Physical Layer	**8**

UNIT 2	Link layer: Framing, Error Detection and Correction, Flow control (Elementary Data Link Protocols, Sliding Window protocols). Medium Access Control and Local Area Networks: Channel allocation, Multiple access protocols, LAN standards, Link layer switches & bridges	**8**
UNIT 3	Network Layer: Point-to-point networks, Logical addressing, Basic internetworking (IP, CIDR, ARP, RARP, DHCP, ICMP), Routing, forwarding and delivery, Static and dynamic routing, Routing algorithms and protocols, Congestion control algorithms, IPv6.	**9**
UNIT 4	Transport Layer: Process-to-process delivery, Transport layer protocols (UDP and TCP), Multiplexing, Connection management, Flow control and retransmission, Window management, TCP Congestion control, Quality of service.	**9**
UNIT 5	Application Layer: Domain Name System, World Wide Web and Hyper Text Transfer Protocol, Electronic mail, File Transfer Protocol, Remote login, Network management, D	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Behrouz Forouzan, “Data Communication and Networking”, McGraw Hill	2021
2	Andrew Tanenbaum “Computer Networks”, Prentice Hall.	2018
3	William Stallings, “Data and Computer Communication”, Pearson.	2004
4	Kurose and Ross, “Computer Networking- A Top-Down Approach”, Pearson.	2012

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY209:ALGORITHM DESIGN AND ANALYSIS	**L**	**T**	**P**	**Data Structures**
	2	**1**	**0**	

Course Objective: To introduce the concept of algorithmic efficiency by analyzing various algorithms such as Searching, Sorting, Divide-and-Conquer algorithms and to know about Dynamic Programming techniques, Greedy Paradigm, Back Tracking, Branch and Bound, and Computational Complexity.

S. NO	Course Outcomes (CO)
CO1	Abilty to analyse and compare the runtime complexities of algorithms using various techniques.
CO2	Abilty to classify and solve problems using Divide and Conquer technique
CO3	Abilty to classify and solve problems using Dynamic Programming Techniques
CO4	Abilty to classify and solve problems using Greedy Paradigm
CO5	Abilty to identify and solve problems using Back-Tracking and Branch and Bound techniques
CO6	Abilty to learn NP-complete and NP-hard problems, and design approximate Solutions.

S. NO	Contents	Contact Hours
UNIT 1	Introduction: Concept of algorithmic efficiency, run time analysis of algorithms, Asymptotic Notations. Growth of Functions, Master's Theorem, Substitution method and Recursion Tree method.	**6**
UNIT 2	Divide and Conquer: Structure of divide-and-conquer algorithms; examples: binary search, quick sort, Strassen Matrix Multiplication; merge sort, heap sort and Analysis of divide and conquer run time recurrence relations.	**7**
UNIT 3	Dynamic programming: Principles of dynamic programming. Applications: Rod cutting problem, Matrix Chain multiplication, Longest Common subsequence, Travelling salesman Problem, and Floyd-Warshall algorithm for all pair shortest paths.	**8**
UNIT 4	Greedy Method: Overview of the greedy paradigm examples of exact optimization solution: Activity Selection Problem., minimum cost spanning tree, approximate solutions: Knapsack problem, Kruskal's algorithm and Prim's algorithm for finding Minimum cost Spanning Trees, Dijkstra's, and Bellman Ford Algorithm for finding Single source shortest paths, Huffman coding.	**8**

UNIT 5	Back tracking: Overview, 8-queen problem, and Knapsack problem, Traveling Salesman problem. Branch and bound: LC searching Bounding, FIFO branch and bound, LC branch and bound application: 0/1 Knapsack problem.	**7**
UNIT 6	Computational Complexity: Complexity measures, Polynomial Vs non-polynomial time complexity; NP-hard and NP-complete classes, examples: Circuit Satisfiability, Vertex cover, Subset Sum problem, Randomized Algorithms, String Matching, NP- Hard and NP-Completeness, Approximation Algorithms, Sorting Network, Matrix Operations, Polynomials and FFT, Number Theoretic Algorithms.	**6**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	T .H . Cormen, C . E . Leiserson, R .L . Rivest "Introduction to Algorithms", 3rd Ed., PHI.	2011(Reprint)
2	E. Horowitz, S. Sahni, and S. Rajsekaran, "Fundamentals of Computer Algorithms," Galgotia Publication	2010 (RePrint)
3	Sara Basse, A. V. Gelder, "Computer Algorithms: : Introduction to Design and Analysis" Addison Wesley, 3rd Edition, Pearson Education India	2002
4	Alfred V. Aho, John E. Hopcroft, Jeffrey D. Ullman "Design & Analysis of Computer Algorithms", 1e Paperback – 1 January 2002, Pearson Education India	2002/eighth impression

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY202: Network Security	**L**	**T**	**P**	**Computer Networks**
	3	**0**	**2**	

Course Objective: By the end of this session, students will be able to configure an IPsec VPN tunnel between two endpoints and analyze encrypted traffic using a network monitoring tool

S. NO	Course Outcomes (CO)
CO1	Analyze fundamental cybersecurity concepts, including security attacks, services, mechanisms, and cryptographic principles, and evaluate their role in securing network infrastructures.
CO2	**Implement** transport-level security protocols (TLS, HTTPS, SSH) and **assess** their effectiveness in protecting web-based and remote communication channels.
CO3	**Design** security solutions for wireless networks, email systems, and IP-based communications using standards such as IEEE 802.11i, S/MIME, SPF, and IPsec to mitigate vulnerabilities.
CO4	**Evaluate** cloud and IoT security risks, **apply** countermeasures, and **demonstrate** the use of open-source security modules to protect distributed and smart environments.

S. NO	Contents	Contact Hours
UNIT 1	Network Security Concepts: Cyber Security, Information Security and Network Security Concepts. The OSI Security Architecture, Security Attacks, Security Services, Security Mechanism, Cryptography, Network Security, Trust and Trustworthiness. Transport-level Security: Web Security Considerations, Transport Layer Security, HTTPS, Secure Shell (SSH).	**10**
UNIT 2	Wireless Network Security: Wireless security, Mobile Device Security, IEEE 802.11 Wireless Lan Overview, IEEE 802.11i wireless Lan Security. Electronic Mail Security: Internet Mail Architecture, Email formats, Email Threats and Comprehensive Email Security. S/MIME, DNSSEC, DNS-Based Authentication of Named Entities, Sender Policy Framework, Domain Keys identified mail, Domain-based Message Authentication, Reporting, and Conformance.	**11**
UNIT 3	IP Security : IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet key Exchange. Network End Point Security: Firewalls, Intrusion Detection System, Malicious Software, Distributed Denial of Service Attacks.	**11**
UNIT 4	Cloud Security: Cloud Computing, Cloud Security Concepts, Cloud Security Risks and Countermeasures, Cloud Security as a service, An Open -source Cloud Security Module. An open-Source Cloud	**10**

	Security Module. Internet of Things (IOT) Security: The Internet of Things, IOT Security Concepts and objectives, An open-Source IOT Security Module.	
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Edition, William Stallings Fifth. "Cryptography And Network Security."	2023
2	Campbell, Paul, Ben Calvert, and Steven Boswell. *Security+ guide to network security fundamentals*. Thomson Course Technology	2003
3	Malik, Saadat. "Network security principles and practices."	2003

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY204: System Security	**L**	**T**	**P**	**Computer Networks, Operating Systems**
	3	**0**	**2**	

Course Objective: To equip students with the skills to harden Linux and Windows operating systems against cyber threats by implementing security best practices, access controls, encryption, and monitoring techniques.

S. NO	Course Outcomes (CO)
CO1	Analyze security threats and apply fundamental hardening techniques to secure operating systems in virtual and physical environments.
CO2	Configure user authentication, access controls, and encryption to protect system integrity and confidentiality.
CO3	Implement network security measures, including firewalls and secure protocols, to defend against attacks.
CO4	Utilize advanced tools (SELinux, auditd, SIEM) for system monitoring, vulnerability assessment, and incident response.

S. NO	Contents	Contact Hours
UNIT 1	Introduction to OS Hardening and Security Fundamentals: Threat landscape: Attack vectors, vulnerabilities, and breaches, CIA triad (Confidentiality, Integrity, Availability), Virtualization for security: VirtualBox, VMware, cloud setups, Security news and updates (CVE, NIST, MITRE ATT&CK)	**8**
UNIT 2	User and Access Control Hardening: Risks of root/admin accounts and sudo best practices, Password policies: Complexity, aging, and lockout mechanismsnMulti-Factor Authentication (MFA) and passwordless auth Centralized user management (Active Directory, FreeIPA)	**9**
UNIT 3	Network and Firewall Security: Firewall systems: iptables, nftables, firewalld, UFW, Secure SSH configurations (disabling root login, protocol hardening), Encryption: GPG, LUKS, eCryptfs, OpenSSL/TLS, Network isolation and VLANs	**9**
UNIT 4	Advanced System Hardening: SELinux and AppArmor for Linux, Windows Defender Application Control (WDAC), Kernel hardening: sysctl, /proc, cgroups, namespaces, Auditing tools: auditd, OpenSCAP, Lynis	**8**
UNIT 5	Monitoring, Logging, and Incident Response: Log management: rsyslog, journald, SIEM (Security Onion) Intrusion Detection: Snort, Microsoft Defender for Endpoint Vulnerability scanning: Greenbone, Nikto Incident response and recovery	**8**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**

1	Tevault, Donald A. Mastering Linux Security and Hardening: A practical guide to protecting your Linux system from cyber attacks. Packt Publishing Ltd.	2023
2	Dunkerley, Mark, and Matt Tumbarello. Mastering Windows Security and Hardening: Secure and protect your Windows environment from intruders, malware attacks, and other cyber threats. Packt Publishing Ltd.	2020

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY206: Machine Learning	**L**	**T**	**P**	Probability, Statistics and Stochastic Processes, Linear Algebra
	3	**0**	**2**	

Course Objective: 1. To understand various key paradigms for machine learning approaches. 2. To familiarize with the mathematical and statistical techniques used in machine learning. 3. To understand and differentiate among various machine learning techniques.

S. NO	Course Outcomes (CO)
CO1	Understand the fundamental concepts and algorithms of machine learning
CO2	Develop a comprehensive understanding of fundamental machine learning concepts, algorithms, and techniques, including supervised and unsupervised learning, classification, regression, clustering, and dimensionality reduction.
CO3	Apply principles and algorithms to evaluate models generated from data
CO4	Learn to critically evaluate the performance of machine learning models using appropriate metrics
CO5	Develop the ability to identify and formulate problems suitable for machine learning solutions, design appropriate models, and interpret results in practical applications.

S. NO	Contents	Contact Hours
UNIT 1	Introduction to Machine Learning: Overview of different tasks: classification, regression, clustering, Concept of learning, Types of the Machine Learning, Data Table, Information System, Data Representation, diversity of data, Basic Linear Algebra and Probaboliy Theory, Optimization: Maximum likelihood, Expectation maximization, Gradient descent, Bias-Variance Tradeoff, Metrics to Evaluate Classification and Regression models	**14**
UNIT 2	Supervised Learning: Linear Regression, Logistic Regression, Baysian Decision Theory, Naïve Bayes, K-Nearest Neighbour, Support Vector Machine, Decision trees, Ensemble Classifier, Random Forest, Linear Classifiers and Kernels, Neural Networks, Deep Neural Network, Fundametals of Deep Learning: DNN, CNN.	**14**
UNIT 3	Unsupervised Learning: Clustering, Expectation Maximization, K-Mean Clustering, Hierarchical vs Partitional Clustering, Gaussian Mixture Model, Dimensionality Reduction, Feature Selection, PCA, factor analysis, manifold learning.	**14**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Introduction to Machine Learning, Alpaydin, E.,PHI Learning Pvt. Ltd.	2015

2	Machine Learning, Tom Mitchell, McGraw Hill	2017
3	Applied Machine Learning by M.Gopal|, McGraw Hill, ISBN: 978-9354601590	2021
4	Understanding Machine Learning: From Theory to Algorithms, 1st Edition,by Shai Shalev-Shwartz, Cambridge University Press	2015
5	Pattern Recognition and Machine Learning by Christopher Bishop, Springer Verlag	2006
6	Pattern Classification by Richard Duda, Wiley Publisher	2007

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY208: Secure Coding	**L**	**T**	**P**	**Programming Fundamentals**
	3	**1**	**0**	

Course Objective: ***To equip students with secure coding principles, vulnerability mitigation techniques, and best practices to develop resilient software against cyber threats.***

S. NO	Course Outcomes (CO)
CO1	Analyze security goals (confidentiality, integrity, availability, non-repudiation) and apply them in secure system design.
CO2	Implement secure coding principles (least privilege, defense-in-depth, fail-safe defaults) to mitigate common vulnerabilities.
CO3	Evaluate and defend against threats using STRIDE, attack trees, and threat modeling techniques.
CO4	Develop secure applications by preventing buffer overflows, SQL injection, XSS, and other code-based exploits.
CO5	Design authentication, authorization, and cryptographic mechanisms to ensure data security and accountability.

S. NO	Contents	Contact Hours
UNIT 1	Security Goals: Physical Security, Technological Security, Policies and Procedures, Authentication, Authorization, Confidentiality, Message/Data Integrity, Accountability, Availability, Non-repudiation Secure Systems Design: Understanding Threats, Designing-In Security, Convenience and Security, SimpleWebServer Code Example, Security in Software Requirements, Security by Obscurity, Open vs.Closed Source. Secure Design Principles: The Principle of Least Privilege, Defense-in-Depth, Diversity-in-Defense, Securing the Weakest Link, Fail-Safe Stance, Secure by Default, Simplicity, Usability. Worms and Other Malware	**8**
UNIT 2	Strategies for Threat Modeling: Brainstorming Your Threats, Structured Approaches to Threat Modeling, Models of Software. STRIDE: Understanding STRIDE and Why It's Useful, Spoofing Threats, Tampering Threats, Repudiation Threats, Information Disclosure Threats, Denial-of-Service Threats, Elevation of Privilege ThreatsSTRIDE Variants. Attack Trees: Working with Attack Trees, Representing a Tree, Example Attack Tree, Real Attack Trees	**8**
UNIT 3	Buffer Overflows: Anatomy of a Buffer Overflow, Safe String Libraries, StackGuard, Static Analysis Tools, Heap-Based Overflows, Format String Vulnerabilities, Integer Overflows, Pointer Subterfuge, Common memory management errors, Concurrency and common errors. File I/O: Interfaces, Access Control, identification, race condition, Mitigation Strategies. Client-State Manipulation: Pizza Delivery Web Site Example, Using HTTP POST Instead of GET, Cookies, JavaScript.	**9**

UNIT 4	SQL Injection: Attack Scenario, Whitelisting-Based Input Validation, Escaping, Second Order SQL Injection, Prepared Statements and Bind Variables, Mitigating the Impact of SQL Injection Attacks. Password Security: AStrawman Proposal, Hashing, Offline Dictionary Attacks, Salting, Online Dictionary Attacks, Additional Password Security Techniques. Cross-Domain Security in Web Applications: Interaction Between Web Pages from Different Domains, Attack Patterns, Preventing XSRF, Preventing XSSI, Preventing XSS	**9**
UNIT 5	Understanding Shellcode: An Overview of Shellcode, The Addressing Problem, The NULL Byte Problem, Implementing System Calls, System Call Numbers, Remote Shellcode, Local Shellcode, Writing Shellcode: Shellcode Examples, The Write System Call, execve Shellcode, Port-Binding Shellcode, Reverse Connection Shellcode, Socket Reusing Shellcode, Reusing File Descriptors, Encoding Shellcode, Reusing Program Variables, OS-Spanning Shellcode, Understanding Existing Shellcode.	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Seacord, Robert C. Secure Coding in C and C++. Addison-Wesley	2013
2	Kern, Christoph, Anita Kesavan, and Neil Daswani. *Foundations of security: what every programmer needs to know*. Apress	2007
3	Shostack, Adam. Threat modeling: Designing for security. John wiley & sons	2014
4	Foster, James C., Vitaly Osipov, and Nish Bhalla. Buffer overflow attacks. Syngress Publishing	2005

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY210: Ethical Hacking	**L**	**T**	**P**	**Computer Networks, Programming**
	3	**0**	**2**	

Course Objective: This course aims to equip students with a comprehensive understanding of security and ethical hacking principles, including reconnaissance, scanning, and password cracking techniques. Students will learn to identify and address vulnerabilities in web applications and wireless networks, using practical tools and methodologies to enhance their ability to secure systems and applications.

S. NO	Course Outcomes (CO)
CO1	Understand Security and Ethical Hacking: Grasp fundamental security principles, ethical hacking concepts, and key terminologies
CO2	Conduct Reconnaissance and Scanning: Perform footprinting and port scanning using relevant tools.
CO3	Analyze Cracking and Sniffing Techniques: Understand password cracking methods and sniffing techniques.
CO4	Secure Web Applications and Wireless Networks: Identify vulnerabilities in web applications and secure wireless networks.

S. NO	Contents	Contact Hours
UNIT 1	Ethical Hacking: Overview of Ethics, Overview of Ethical Hacking, Attack Modeling, Methodology of Ethical Hacking Networking Foundations: Communications Models, Topologies, Physical Networking, IP, TCP, UDP, Network Architectures, Cloud Computing. Security Foundations: The Triad, Information Assurance and Risk, Policies, Standards, and Procedures, Organizing Your Protections, Security Technology.	**8**
UNIT 2	Footprinting and Reconnaissance: Open Source Intelligence, Domain Name System, Passive Reconnaissance, Website Intelligence, Technology Intelligence. Scanning Networks: Ping Sweeps, Port Scanning, Vulnerability Scanning, Packet Crafting and Manipulation, Evasion Techniques, Protecting and Detecting.	**8**
UNIT 3	Enumeration: Service Enumeration, Remote Procedure Calls, Server Message Block, Simple Network Management Protocol, Simple Mail Transfer Protocol, Web-Based Enumeration System Hacking: Searching for Exploits, System Compromise, Gathering Passwords, Password Cracking, Client-Side Vulnerabilities, Living Off the Land, Fuzzing, Post Exploitation,	**9**
UNIT 4	Malware: Malware Types, Malware Analysis, Creating Malware, Malware Infrastructure, Antivirus Solutions, Persistence. Sniffing: Packet Capture, Detecting Sniffers, Packet Analysis, Spoofing Attacks Social Engineering: Physical Social Engineering, Phishing Attacks, Social Engineering for Social Networking, Website Attacks, Wireless Social	**9**

	Engineering, Automating Social Engineering	
UNIT 5	Wireless Security: Wi-Fi, Bluetooth, Mobile Devices Attack and Defense: Web Application Attacks, Denial-of-Service Attacks, Application Exploitation, Lateral Movement, Defense in Depth/Defense in Breadth, Defensible Network Architecture	**8**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Messier, Ric. *CEH V10 certified ethical hacker study guide*. John Wiley & Sons.	2019
2	"Network Seuciryt and Ethical Hacking", Rajat Khare, Luniver Press ISBN:978- 1-905986-00-2	2006
3	Thomas Mathew, "Ethical Hacking", OSB publishers ISBN: 0972936211	2003
4	Ramachandran V, BackTrack 5 Wireless Penetration Testing Beginner's Guide (3rd ed.). Packt Publishing, ISBN: 9781849515580	2011

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY301: Digital Forensics	**L**	**T**	**P**	
	3	**0**	**0**	

Course Objective:

S. NO	Course Outcomes (CO)
CO1	Explain the concept of Cybercrimes and summarize the legal frameworks of different types of Cybercrimes.
CO2	Demonstrate the different forms of digital forensic investigation and its life cycle.
CO3	Make use of various digital forensic tools in real-time scenarios for investigation procedures
CO4	Examine network logs, cache, cookie, history recorded in web browsers, file systems of Windows, Linux, and Mac operating systems.
CO5	Analyze email crime, dark web, and static and malware code.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Digital Forensics:** Fundamentals of Digital Forensics,Digital Evidence, Forensic Readiness, Roles and Responsibilities of a Forensic Investigator, Legal Compliance in Computer Forensics, Commercial and open source tools for digital forensics, Setting up Kali Linux for digital forensics process, Anti-forensic tools.	**05**
UNIT 2	**Computer Forensic Investigation Process:** Forensic Investigation Process and its Importance, Pre-investigation, Investigation Phase, Post-investigation Phase, Indian IT Act 2000, IT Amendment Act 2008 and Indian Evidence Act	**07**
UNIT 3	**Understanding File systems and Storage media**: Understanding Hard Disks and File Systems, Different Types of Disk Drives and their Characteristics, Logical Structure of a Disk, Booting Process of Windows, Linux, and Mac Operating Systems, File Systems of Windows, Linux, and Mac Operating Systems, File System Examination	**08**
UNIT 4	**Incident Response and Data Acquisition:** Data Acquisition and Duplication, Data Acquisition Fundamentals, Types of Data Acquisition, Data Acquisition Format, Data Acquisition Methodology, Data imaging and hashing, Evidence Acquisition and Preservation with DC3DDand Guymager, File	**06**
UNIT 5	**Operating System Forensics:** Windows Forensics, Volatile and Non-Volatile Information, Windows Memory and Registry Analysis, Cache, Cookie, and History Recorded in Web Browsers, Windows Files and Metadata, Linux and Mac Forensics, Volatile and Non-Volatile Data in Linux, Analyze File system Images Using The Sleuth Kit, Memory Forensics, Mac Forensics.	**06**
UNIT 6	**Network Forensics**: Network Forensics Fundamentals, Event Correlation Concepts and Types, Identify Indicators of Compromise (IoCs) from Network Logs, Investigate Network Traffic, Network and Internet Capture	**10**

	Analysis with Xplico **Malware Forensics**: Malware, its Components and Distribution Methods, Malware Forensics Fundamentals and Recognize Types of Malware, Analysis, Static Malware Analysis, Analyze Suspicious Word Documents, Dynamic Malware Analysis	
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics by John Sammons, Syngress; 2nd edition	2014
2	Shiva V.N. Parasaram, “Digital Forensics With Kali Linux”, Packet publishing	2017
3	Brian Carrier, " File System Forensic Analysis", Person Education	2005
4	Cybercrime and Digital Forensics: An Introduction by Thomas J. Holt , Adam M. Bossler, Kathryn C. SeigfriedSpellar, Routledge; 2nd edition	2017
5.	Digital Forensics and Incident Response: A practical guide to deploying digital forensic techniques in response to cyber security incidents by Gerard Johansen, Packt Publishing Limited	2017

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY303 Applied Cryptography	**L**	**T**	**P**	**Computer Networks, Network Security, Data Structures**
	3	**1**	**0**	

Course Objective: Students will be able to implement a secure communication protocol using AES for encryption, RSA for key exchange, and SHA-3 for integrity checks in a hands-on lab environment

S. NO	Course Outcomes (CO)
CO1	**Analyze and apply fundamental number-theoretic concepts** (divisibility, modular arithmetic, primality testing, Chinese Remainder Theorem) **to design and evaluate cryptographic algorithms.**
CO2	**Implement and assess symmetric encryption techniques** (DES, AES, block cipher modes) **and public-key cryptosystems** (RSA, Diffie-Hellman, ECC) **for secure data transmission.**
CO3	Evaluate cryptographic hash functions (SHA, SHA-3), message authentication codes (MACs), and digital signatures (DSA, ECDSA) for ensuring data integrity and authenticity.
CO4	**Design secure key management schemes** (PKI, X.509 certificates, key distribution) **and apply best practices for cryptographic implementations in real-world systems.**

S. NO	Contents	Contact Hours
UNIT 1	Introduction to Number Theory: Divisibility and Division Algorithm, The Euclidean Algorithm, Modular Arithmetic, Prime Numbers, Fermat's and Euler Theorems, Testing for Primality, The Chinese Remainder Theorem, Discrete Logarithms Classical Encryption Techniques: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques Block Cipher and the Data Encryption Standards: Traditional Block Cipher Structures, The Data Encryption Standards, A DES Example, The Strength of DES, Block Cipher Design Principles.	**9**
UNIT 2	Finite Fields: Groups, Rings, Fields, polynomial Arithmetic, Finite Field Forms. Advanced Encryption Standards: AES Structures, AES Transformation Functions, AES Key Expansion, AES Example, AES Implementation. Block Cipher Operations: Multiple Encryption, Triple DES, Electronic CodeBook, Cipher Block Channing Mode, cipher feedback mode, output feedback mode, counter mode, xts-aes mode for block-oriented storage devices, format-preserving encryption	**8**
UNIT 3	Public Key Cryptography and RSA: Principles of Public-Key Cryptosystems, The RSA Algorithm, Deffie-Hellman Key Exchange, Elgamal Cryptographic System, Elliptic Curve Arithmetic, Elliptic Curve Cryptography.	**8**
UNIT 4	Cryptographic Hash Functions: Applications of Cryptographic Hash Functions, Two Simple Hash Functions, Requirements and Security, Secure Hash Algorithm (SHA), SHA-3, Message Authentication Codes: Message Authentication Requirements, Message Authentication Functions, Requirements of Message Authentication	**9**

	Codes, Security of MACs, MACs based on hash functions, MACs based on Block Ciphers, Authentication Encryption, Key Wrappings, Pseudorandom Number Generators using Hash Functions and MACs.	
UNIT 5	Digital Signatures: ElGamal Digital signature Scheme, Schorr Digital signature Scheme, NIST Digital signature Algorithm, Elliptic Curve Digital signature Algorithm, RSA-PSS Digital signature Algorithm Cryptographic Key Management and Distribution: Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Distribution of Public Keys, X.509 Certificates, Public-Key Infrastructure.	**8**
	TOTAL	**42**

REFERENCES

S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Edition, William Stallings Fifth. "Cryptography And Network Security."	2023
2	Katz, Jonathan, and Yehuda Lindell. *Introduction to modern cryptography: principles and protocols*. Chapman and hall/CRC	2007
3	Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC press.	2018

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY305: Web Application Security	**L**	**T**	**P**	**Fundamentals of Web Development, Programming, Computer Networks**
	3	**0**	**2**	

Course Objective:

S. NO	Course Outcomes (CO)
CO1	**Identify and Exploit Common Web Vulnerabilities**
CO2	**Conduct Comprehensive Web Reconnaissance**
CO3	**Assess and Secure Application Architecture**
CO4	**Execute Ethical Hacking Workflows**

S. NO	Contents	Contact Hours
UNIT 1	Introduction to Web Application Reconnaissance: Information Gathering, Web Application Mapping The Structure of a Modern Web Application: Modern Versus Legacy Web Applications, REST APIs, JavaScript Object Notation, JavaScript, SPA Frameworks, Authentication and Authorization Systems, Web Servers, Server-Side Databases, Client-Side Data Stores, GraphQL, Version Control Systems, CDN/Cache. Finding Subdomains: Multiple Applications per Domain, The Browser's Built-In Network Analysis Tools, Taking Advantage of Public Records, Zone Transfer Attacks, Brute Forcing Subdomains, Dictionary Attacks	**8**
UNIT 2	API Analysis: Endpoint Discovery, Authentication Mechanisms, Endpoint Shapes Identifying Third-Party Dependencies: Detecting Client-Side Frameworks, Detecting Server-Side Frameworks Identifying Weak Points in Application Architecture : Secure Versus Insecure Architecture Signals, Multiple Layers of Security, Adoption and Reinvention Introduction to Hacking Web Applications: The Hacker's Mindset, Applied Recon.	**9**
UNIT 3	Cross-Site Scripting: XSS Discovery and Exploitation, Stored XSS, Reflected XSS, DOM-Based XSS, Mutation-Based XSS, Bypassing Filters, XSS Sinks and Sources Cross-Site Request Forgery: Query Parameter Tampering, Alternate GET Payloads, CSRF Against POST Endpoints, Bypassing CSRF Defenses, Header Validation, Token Pools, Weak Tokens, Content Types, Regex Filter Bypasses, Iframe Payloads, AJAX Payloads, Zero Interaction Forms XML External Entity: XXE Fundamentals, Direct XXE, Indirect XXE, Out-of-Band Data Exfiltration, Account Takeover Workflow Injection: SQL Injection, Code Injection, Command Injection, Injection Data Exfiltration Techniques, Bypassing Common Defenses	**9**

UNIT 4	Denial of Service: Regex DoS, Logical DoS Vulnerabilities, Distributed DoS, Advanced DoS. Attacking Data and Objects: Mass Assignment, Insecure Direct Object Reference, Serialization Attacks. Client-Side Attacks: Methods of Attacking a Browser Client, Advantages of Client-Side Attacks, Prototype Pollution Attacks, Clickjacking Attacks, Tabnabbing and Reverse Tabnabbing Exploiting Third-Party Dependencies: Methods of Integration, Package Managers, Common Vulnerabilities and Exposures Database. Business Logic Vulnerabilities: Custom Math Vulnerabilities, Programmed Side Effects, Quasi-Cash Attacks, Vulnerable Standards and Conventions, Exploiting Business Logic Vulnerabilities.	**8**
UNIT 5	Securing Modern Web Applications: Defensive Software Architecture, Comprehensive Code Reviews, Vulnerability Discovery, Vulnerability Analysis, Vulnerability Management, Regression Testing, Mitigation Strategies, Applied Recon and Offense Techniques. Secure Application Architecture: Analyzing Feature Requirements, Authentication and Authorization, PII and Financial Data, Search Engines, Zero Trust Architecture. Secure Application Configuration: Content Security Policy, Cross-Origin Resource Sharing, Headers, Cookies, Framing and Sandboxing.	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Hoffman, Andrew. Web application security. " O'Reilly Media, Inc.".	2024
2	Sullivan, Bryan, and Vincent Liu. Web Application Security, A Beginner's Guide. McGraw Hill Profe ssional.	2011
3	Stuttard, Dafydd, and Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. John Wiley Sons.	2011

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY307: Deep Learning	**L**	**T**	**P**	**Machine Learning**
	3	0/1	2/0	

Course Objective: The primary objective of a deep learning course for undergraduate students is to equip them with a solid foundation in the theory and practical application of deep learning techniques.

S. NO	Course Outcomes (CO)
CO1	Demonstrate a clear understanding of the fundamental concepts of deep learning, including neural networks, activation functions, loss functions, and optimization techniques.
CO2	Design, implement, and train basic neural network architectures, including feedforward networks, convolutional neural networks (CNNs), and recurrent neural networks (RNNs) using modern deep learning frameworks like TensorFlow or PyTorch.
CO3	Apply deep learning techniques to solve complex problems in various domains such as image classification, object detection, natural language processing, and time-series prediction.
CO4	Explore and implement advanced deep learning techniques such as transfer learning, generative adversarial networks (GANs), attention mechanisms, and transformers to address cutting-edge research and industry challenges.

S. NO	Contents	Contact Hours
UNIT 1	Overview of Artificial Intelligence, Machine Learning, and Deep Learning, History and evolution of deep learning, Applications of deep learning, Perceptron and multi-layer perceptron, Activation functions, Loss functions and their significance, Gradient Descent and Backpropagation, Neural Networks: Deep vs Shallow Networks, Training Deep Networks: Vanishing and Exploding Gradients, Techniques to mitigate gradient issues (Batch Normalization, Gradient Clipping), Optimization algorithms (SGD, Adam, RMSprop), Regularization techniques (L2, Dropout), and Weight Initialization	**16**
UNIT 2	Convolutional Neural Networks, and their significance in image processing, Convolution operations and feature maps. Pooling layers, CNN architectures: LeNet, AlexNet, VGG, ResNet, Inception, Transfer learning and fine-tuning pre-trained models, Object detection and segmentation (YOLO, SSD, Mask RCNN), Introduction to Generative Adversarial Networks, Autoencoder. Variational Autoencoders.	**14**
UNIT 3	Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, Gated Recurrent Unit (GRU), Attention Mechanisms and Transformers, Sequence-to-sequence models with attention, and applications in natural language processing.	**12**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Deep Learning by Ian Goodfellow , Yoshua Bengio , and Aaron Courville, MIT Press (https://www.deeplearningbook.org/)	2016
2	Deep Learning: Foundations and Concepts by Christopher M. Bishop and Hugh Bishop, Springer	2023
3	Introduction to Deep Learning by Eugene Charniak, MIT Press	2019
4	Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow" by Aurélien Géron	2022

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY309: Fundamentals of Blockchain Technology	**L**	**T**	**P**	
	3	0/1	2/0	

Course Objectives: This course provides a comprehensive introduction to blockchain technology, covering its fundamental concepts, key platforms, and cryptographic solutions. Students will explore security, privacy, scalability, and interoperability challenges, along with the consensus protocols that maintain blockchain integrity. By the end of the course, students will be prepared to understand and apply blockchain technology in various real-world scenarios.

S. NO	Course Outcomes (CO)
CO1	To understand the fundamentals of blockchain technology.
CO2	To acquire the knowledge on various blockchain platforms.
CO3	To study the Cryptographic Solution in Blockchain and understand their security and privacy issues.
CO4	To study the various consensus protocols used in the blockchain technology.
CO5	To understand the scalability, interoperability issues and their proposed solutions in current scenarios.

S. NO	Contents	Contact Hours
UNIT 1	Introduction: Decentralised System: Difference between centralised, decentralised and distributed system, Introduction and need of decentralised ledger system. Blockchain Technology: Introduction of blockchain, Architecture of Blockchain, detailed knowledge of Block Structure, Working of Blockchain, main barrier to blockchain adoption, use-case of blockchain in various fields.	**8**
UNIT 2	Blockchain Platform: Introduction of Public/permissionless, Private/Permissioned Ethereum: Basics, Ethereum clients, Wallets, Tokens, Oracles, Ethereum Virtual Machine, Smart Contract, Introduction to Solidity	**8**
UNIT 3	Cryptography: Public key cryptography, Digital Signature, Hashing, SHA256, AES, RSA, Security and privacy: Issues in blockchain, attacks on Blockchains – such as Sybil attacks, selfish mining, 51% attacks, Smart Contract Vulnerability, Hard fork/ soft Fork, Mitigatation Techniques.	**8**
UNIT 4	Consensus: Foundation od Consensus, Classical Consensus, Nakamoto Consensus, Ethereum Merge, Blockchain Selfish Mining, Proof based consensus: PoW, Pos, PoA, PoET, Voting Based Consensus: Paxos, RAFT, PBFT	**10**
UNIT 5	Scalability and Interoperability: Addressing the Issue of Scalability and Interoperability, Blockchain scalability solutions: Layer 1, Layer 2, Various Off-chain Storage.	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Mastering Blockchain: Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3, 4th Edition "imran bashir", Packt Publishing	2023
2	Mastering Ethereum: Building Smart Contracts and DApps by Andreas M. Antonopoulos and Gavin Wood, Shroff/O'Reilly	2018
3	Mastering Bitcoin: Programming the Open Blockchain (Second Edition) "Andreas Antonopoulos", O'Reilly Media	2017

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY311: Penetration Testing	**L**	**T**	**P**	**Introduction to Software Engineering**
	3	**0/1**	**2/0**	

Course Objective: To provide students with a comprehensive understanding of the fundamental principles and techniques in penetration testing, including vulnerability assessment, information gathering, network scanning etc.

S. NO	Course Outcomes (CO)
CO1	Explain key concepts in penetration testing and cybersecurity.
CO2	Perform vulnerability assessment using standard tools.
CO3	Design and execute penetration tests.
CO4	Interpret test results and propose mitigation strategies.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Penetration Testing:** Definition and Purpose of Penetration Testing, Ethical Hacking and Legal Issues, Phases of Penetration Testing, Reconnaissance and Information Gathering Techniques.	**8**
UNIT 2	**Scanning and Vulnerability Analysis:** Scanning Networks and Systems, Vulnerability Identification Tools (e.g., Nmap, Nessus), Exploiting Common Vulnerabilities, Reporting and Documentation.	**8**
UNIT 3	**System Hacking and Exploitation:** Password Cracking and Privilege Escalation, Malware, Trojans, and Backdoors, Exploit Frameworks (e.g., Metasploit), Real-World Case Studies.	**9**
UNIT 4	**Web and Network Security Testing:** Attacking Web Applications (SQLi, XSS, CSRF), Testing Network Services and Wireless Security, Security in Cloud and IoT Environments, Penetration Testing Standards (OWASP, PTES).	**9**
UNIT 5	**Reporting and Mitigation Strategies:** understanding Test Reports and Presenting Findings, Recommendations for Security Enhancements, Incident Response Planning, Ethical Responsibilities and Best Practices.	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Georgia Weidman, "Penetration Testing: A Hands-On Introduction to Hacking"	2014
2	Patrick Engebretson, "The Basics of Hacking and Penetration Testing"	2011
3	Allen, J. (2017). *Advanced Penetration Testing: Hacking the World's Most Secure Networks*. Indianapolis: Wiley.	2017

4	Shimonski, R. J. (2019). *The Art of Penetration Testing: A Guide to Ethical Hacking and Cybersecurity*. New York: McGraw-Hill Education.	2019

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY313: Quantum Computing	**L**	**T**	**P**	**Mathematics: linear algebra, probability, complex numbers, Algorithms, data structure, programming language, electronics**
	3	**1/0**	**0 /2**	

Course Objective:

S. NO	**Course Outcomes (CO)**
CO1	Understand the Fundamental Principles of Quantum Mechanics and Computing
CO2	Develop Proficiency in Quantum Algorithms and Circuit Design
CO3	Explore Quantum Information Theory and Its Applications
CO4	Evaluate Quantum Hardware Technologies and Address Implementation Challenges

S. NO	**Contents**	**Contact Hours**
UNIT 1	Introduction to Quantum Computing: Basics of Quantum Mechanics, Quantum states, superposition, and entanglement. Quantum measurement and operators. Quantum Computation Overview Comparison with classical computing. Quantum vs. classical bits (qubits). Quantum Gates and Circuits Quantum Gates : Single-qubit gates: Pauli-X, Pauli-Y, Pauli-Z, Hadamard, Phase, and T-gates. Multi-qubit gates: CNOT, Toffoli, SWAP. Quantum Circuits	**10**
UNIT 2	Quantum Algorithms: Basic Algorithms Deutsch-Josza algorithm. Grover's algorithm for unstructured search. Shor's Algorithm, Quantum factorization and implications for cryptography. Quantum Fourier Transform (QFT) Applications in quantum algorithms.	**8**
UNIT 3	Quantum Information Theory: Quantum Entanglement Bell states, EPR pairs, and teleportation. Quantum Error Correction Error correction codes: Shor code, Steane code. Quantum Cryptography Quantum key distribution (e.g., BB84 protocol).	**8**

UNIT 4	Quantum Simulation and Optimization Quantum Simulators Simulating quantum systems with quantum computers. Quantum Optimization Algorithms Variational Quantum Eigensolver (VQE), Quantum Approximate Optimization Algorithm (QAOA).	**8**
UNIT 5	Practical Quantum Computing Quantum Programming Languages Qiskit, QuTiP, Cirq, and others. Quantum Computing Frameworks IBM Quantum Experience, Google Quantum AI, Microsoft Quantum Development Kit.	**8**
	TOTAL	**42**

REFERENCES

S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Quantum Computation and Quantum Information" by Michael A. Nielsen and Isaac L. Chuang (2000)	2000
2	Quantum Computing: An Applied Approach" by Jack D. Hidary (2021)	2021
3	Quantum Computation and Quantum Information: 10th Anniversary Edition" by Michael A. Nielsen and Isaac L. Chuang (2010)	2010
4	Quantum Computing: A Gentle Introduction" by Yasir A. Abbas (2021)	2021

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY315: Windows Administration	**L**	**T**	**P**	Basic knowledge of Operating Systems and Networking
	3	**0/1**	**2/0**	

Course Objective: This course provides in-depth knowledge and practical skills for administering Microsoft Windows servers, including installation, configuration, security, networking, user and group management, and cloud/virtualization integration. It also introduces students to ethical considerations and security vulnerabilities in Windows environments.

S. NO	Course Outcomes (CO)
CO1	**Explain the core roles and responsibilities of a Windows system administrator.**
CO2	**Perform installation and configuration of Windows Server 2016 and 2019.**
CO3	**Administer user accounts, Active Directory, and group policies effectively.**
CO4	**Implement security, data sharing, and virtualization concepts in Window environments.**

S. NO	Contents	Contact Hours
UNIT 1	Introduction to System Administration & Windows Server Environment: System Administrator roles in enterprise networks, Understanding Windows Server architecture and editions, Exploring administrative tools: Server Manager, MMC, PowerShell, Overview of network services and Active Directory, Windows Server GUI vs. Core installations	**7**
UNIT 2	Installation, Configuration & Basic Management: Installing Windows Server 2016/2019: GUI and Server Core, Server configuration, time zone, IP, computer name, Roles and Features using Server Manager and PowerShell, Windows updates, remote desktop, licensing, Basic command-line tools and scripts for automation	**8**
UNIT 3	Active Directory and User Management: Installing and Configuring Windows 2016 Active Directory, Creating, Managing, and Restoring User Accounts and AD Objects, Group Policy Objects (GPO): design, application, and troubleshooting, Password policies and security settings	**9**
UNIT 4	File System, Storage, and Network Services: File system structure and NTFS permissions, File sharing, DFS, quotas, and disk management, Configuring DHCP, DNS, and IP addressing, Network policies and firewall settings, Introduction to auditing and event logs	**9**
UNIT 5	Virtualization, Security & Administration Tools :Introduction to Hyper-V and virtual switches, Server monitoring, backup and restore strategies, Administrative security practices: UAC, BitLocker, role delegation, Windows Remote Management (WinRM) and remote PowerShell, Overview of system vulnerabilities and patch management	**9**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Tom Carpenter, Microsoft Windows Server Administration Essentials, Sybex	2016
2	William R. Stanek , Windows Server 2016: The Administrator's Reference, Microsoft Press	2017
3	Craig Zacker, *Exam Ref 70-740 Installation, Storage and Compute with Windows Server 2016*, Microsoft Press	2017
4	Darril Gibson, *Windows Server 2019 & PowerShell All-in-One For Dummies*, Wiley	2019

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY317: ESSENTIALS OF GENERATIVE AI & PROMPT ENGINEERING	**L**	**T**	**P**	**Probability theory, Machine learning**
	3	**1/0**	**0/2**	

Course Objective: 1. To introduce the fundamental concepts and techniques of Generative AI.
2. To explore various generative models and their applications in real-world scenarios.
3. To develop skills in designing, training, and evaluating generative models.
4. To explore advanced prompting strategies for generative models.

S. NO	Course Outcomes (CO)
CO1	Ability to explain the principles and architectures of generative models.
CO2	Ability to implement and train generative models such as GANs, VAEs, and GPT-based models like LLMs.
CO3	Ability to apply Generative AI techniques to solve real-world problems in areas like image synthesis, data augmentation, and text & speech generation.
CO4	Ability to apply optimal prompting strategies for generative models

S. NO	Contents	Contact Hours
UNIT 1	Introduction to Generative AI: Overview of Generative AI and its applications; Key concepts: Latent spaces, probability distributions, and sampling, Comparison between discriminative and generative models, Ethical considerations in Generative AI	**8**
UNIT 2	Foundations of Generative Models: Autoregressive models: RNNs, LSTMs, and Transformers, Variational Autoencoders (VAEs): Architecture, training, and applications, Flow-based models: Normalizing flows and their use cases, Evaluation metrics for generative models: Inception Score, FID, etc.	**8**
UNIT 3	Generative Adversarial Networks (GANs): GAN architecture: Generator and Discriminator, Training GANs: Challenges and techniques (e.g., mode collapse, Wasserstein GANs), Applications of GANs: Image synthesis, style transfer, and data augmentation.	**6**
UNIT 4	Applications of Generative AI: Text generation: GPT models such as Large Language Models (LLMs) and their applications, Intelligent chatbots–ChatGPT. Image generation: DALL·E, Stable Diffusion, and MidJourney. Audio, speech and video generation: WaveNet, DeepMind's VQ-VAE.	**8**
UNIT 5	Significance of prompt engineering for optimizing generative AI, Zero-shot versus fine-tuned LLMs, Examples of prompts for different use cases, Prompt engineering strategies, Vector database. Retrieval Augmented Generation (RAG): Principles, Architecture and Implementation,	**12**

	Constructing RAG chatbot using LangChain. Designing a prompt + RAG workflow, Advanced prompting strategies like chain of thought and ReAct styles. Prompt evaluation frameworks and metrics. Prompt safety- Hallucination risks.	
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Generative Deep Learning: Teaching Machines to Paint, Write, Compose, and Play by David Foster	2022
2	GANs in Action: Deep Learning with Generative Adversarial Networks by Jakub Langr and Vladimir Bok	2019
3	Generative AI with Python and TensorFlow 2 by Babcock and Bali	2021
4	Deep Learning by Ian Goodfellow, Yoshua Bengio, and Aaron Courville (Chapter on Generative Models)	2016
5	The Art of Prompt Engineering with ChatGPT by Nathan Hunter	2023
6	Prompt Engineering for Generative AI by James Phoenix and Mike Taylor (O'Reilly)	2024
7	Hands-on RAG development by Steven Hay	2024

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY319: Digital Image and Video Processing	**L**	**T**	**P**	Basic knowledge of signals and systems, linear algebra
	3	**0/1**	**2/0**	

Course Objectives: This course aims to introduce the fundamentals of digital image and video processing. Students will gain knowledge in image acquisition, enhancement, compression, segmentation, and representation. The course also covers video processing techniques including motion estimation and video compression.

S. NO	Course Outcomes (CO)
CO1	Understand the fundamentals of image formation, acquisition, and sampling.
CO2	Apply image enhancement and restoration techniques.
CO3	Analyze and implement image segmentation and representation methods.
CO4	Understand the principles of video processing and motion estimation.
CO5	Apply image and video compression techniques in cybersecurity contexts.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Digital Image Processing**: Elements of visual perception, image sensing and acquisition, sampling and quantization, image file formats, basic operations on images.	**8**
UNIT 2	**Image Enhancement and Restoration**: Spatial domain methods – contrast stretching, histogram equalization, smoothing and sharpening filters; frequency domain filtering, noise models, restoration techniques using inverse and Wiener filtering.	**8**
UNIT 3	**Image Segmentation and Representation**: Edge detection, thresholding, region-based segmentation, morphological operations, representation and description: boundary descriptors, regional descriptors.	**8**
UNIT 4	**Video Processing and Motion Estimation**: Basics of video signals, temporal sampling, motion models, optical flow, block matching algorithms, camera motion estimation, applications in surveillance and forensics.	**10**
UNIT 5	**Image and Video Compression**: Fundamentals of compression, JPEG and JPEG2000 for image compression, video compression standards – MPEG, H.264, HEVC; applications in secure transmission and storage.	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Digital Image Processing by Rafael C. Gonzalez and Richard E. Woods, Pearson Education	2018
2	Digital Video Processing by A. Murat Tekalp, Pearson	2015

3	Image and Video Processing in the Compressed Domain by Naoya Mori, Springer	2022
4	Handbook of Image and Video Processing by Alan C. Bovik, Academic Press	2005

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY321: NATURAL LANGUAGE PROCESSING	**L**	**T**	**P**	**Probability and statistics, Machine learning**
	3	**1/0**	**0/2**	

Course Objective: 1. To familiarize with basic text pre-processing steps and pattern matching using regular expressions
2. To design grammar based text parsing systems.
3. To understand, design and implement machine learning based text classification and text generation systems.

S. NO	Course Outcomes (CO)
CO1	Ability to understand and implement text pre-processing techniques and pattern matching using regular expressions.
CO2	Ability to implement Bag-of-Words models for feature extraction and machine learning for text classification.
CO3	Ability to analyze the use of word senses and word embeddings with sequence learning using LSTM or transformer.
CO4	Ability to execute syntactic parsing of sentences for a given grammar and probabilistic inferencing.
CO5	Ability to design and implement text generation models using Language modelling and encoder- decoder models.
CO6	Ability to describe real-world applications of Natural Language Processing and Natural Language Generation.

S. NO	Contents	Contact Hours
UNIT 1	Introduction: The study of Language, Introduction to NLP and various terms related to NLP- morphology, syntax, semantics, pragmatics, discourse, ambiguity. Regular Expression, Finite State Automata.	**6**
UNIT 2	Text representation and classification: Pre-processing: Tokenization, Lemmatization, Stemming. Frequency Based Methods: Bag-of-Words features, 1-hot encoding, TF, TF-IDF, Machine learning classifiers. Sequence Based Methods: Word Embeddings, LSTM/Transformer.	**8**
UNIT 3	Lexical Semantics: Word Senses, WordNet, SentiWordNet, Synsets, Hypernyms, Hyponyms, Meronyms, Holonyms, Word Sense Disambiguation, Word Similarity, Semantic Role Labelling.	**8**
UNIT 4	Natural language generation: Probabilistic Context-Free Grammars, Syntactic Parsing, Part-of-speech-tagging, Probabilistic Language Processing, N-gram language modelling for text generation. Encoder-decoder LSTM/Transformer models for sequence-to-sequence learning, Attention mechanism.	**12**
UNIT 5	Advanced techniques: Large Language Models, Machine Translation, Man-Machine Interfaces, Natural language Question-Answering Systems, Text summarization models, Information Retrieval.	**8**

	TOTAL	42

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	D. Jurafsky, J. H. Martin, Speech and Language Processing, 2/e, Pearson Education.	2013
2	James Allen, Natural Language Understanding, 2/e, Pearson Education.	2003
3	S. Bird, E. Klein, E. Loper, "Natural Language Processing with Python", O'Reilly.	2009
4	Manning and Schutze, "Foundation of Statistical Natural Language Processing", MIT press.	1999
5	U. Kamath, J. Liu, J. Whitaker, "Deep learning for NLP and speech recognition", Springer.	2019
6	D. Rothman, "Transformers for Natural Language Processing", Packt publishing.	2021

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY323: Computer Graphics for Virtual Reality	**L**	**T**	**P**	**Computer Graphics**
	3	**1/0**	**0/2**	

Course Objective: This course introduces graphics systems, their components and algorithms, 3D graphics principles, and the process of mapping world coordinates to device coordinates through clipping and projections.

S. NO	Course Outcomes (CO)
CO1	To list the basic concepts used in computer graphics.
CO2	To implement various algorithms to scan, convert the basic geometrical primitives, transformations, Area filling, and clipping.
CO3	To define the fundamentals of animation, virtual reality, and its related technologies.
CO4	To design an application with the principles of virtual reality.

S. NO	Contents	Contact Hours
UNIT 1	Graphics system and models: applications of computer graphics, graphics system, physical and synthetic images, imaging systems, graphics architectures.	**4**
UNIT 2	Geometric objects and transformations: scalars, points and vectors, three-dimensional primitives, coordinate systems and frames, frames in OpenGL, matrix and vector classes, modelling a colored cube, affine transformations - translation, rotation and scaling, transformations in homogeneous coordinates, concatenation of transformations, transformation matrices in OpenGL, interfaces to 3D applications, quaternion. Vertices to fragments: basic implementation strategies, four major tasks, clipping - line clipping, polygon clipping, clipping of other primitives, clipping in three dimensions, polygon rasterization, hidden-surface removal, antialiasing, display considerations.	**10**
UNIT 3	Lighting and shading: light and matter, light sources, the Phong reflection model, computation of vectors, polygonal shading, approximation of a sphere by recursive subdivision, specifying lighting parameters, implementing a lighting model, shading of the sphere model, per-fragment lighting, global illumination. Hierarchical modelling: symbols and instances, hierarchical models, a robot arm, trees and traversal, use of tree data structures, other tree structures, scene graphs, open scene graph	**9**
UNIT 4	Discrete techniques: buffers - digital images - writing into buffers - mapping methods - texture mapping - texture mapping in OpenGL - texture generation - environment maps - reflection map - bump mapping - compositing techniques - sampling and aliasing. Advanced rendering: going beyond pipeline rendering - ray tracing - building a simple ray tracer - the rendering equation - radiosity - Renderman - parallel rendering - volume rendering - Isosurfaces and marching cubes -	**10**

	mesh simplification - direct volume rendering - image-based rendering.	
UNIT 5	Fractals: modelling - Sierpinski Gasket - coastline problem - fractal geometry - fractal dimension - recursively defined curves - Koch curves - c curves - dragons - space filling curves - turtle graphics - grammar based models - Graftals - volumetric examples - kmidpoint subdivision - fractal Brownian motion - fractal mountains - iteration in the complex plane - Mandelbrot set. Virtual reality modelling language: introduction, exploring and building a world, building object, lighting, sound and complex shapes, animation and user interaction, colors, normals and textures, nodes references. Special applications: stereo display programming, multiport display systems, multi-screen display system, fly mode navigation, walk through navigation, virtual track ball navigation.	**9**
	TOTAL	**42**

REFERENCES

S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Donald Hearn and M. Pauline Baker, “Computer Graphics C Version”, 2nd Edition, Pearson Education.	2002
2	James D. Foley, Andries van Dam, Steven K Feiner, John F. Hughes, “Computer Graphics Principles and Practice in C”, 2nd Edition, Pearson Publication.	1995
3	Rajesh K. Maurya, “Computer Graphics”, 3rd Edition, Wiley India Publication.	2016
4	Interactive Computer Graphics: A Top-Down Approach Using OpenGL (4th Edition)	2005

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY325: Mobile Application Development	**L**	**T**	**P**	**Programming Fundamentals, Web Application Security**
	2	**0/1**	**2/0**	

Course Objective: To enable students to develop secure mobile applications for Android and iOS platforms, focusing on secure coding, testing, and mitigation of mobile-specific threats, with practical exposure suitable for mid-level expertise.

S. NO	Course Outcomes (CO)
CO1	Understand mobile application security principles and threat landscapes.
CO2	Develop secure mobile applications using platform-specific security features.
CO3	Perform security testing and hardening of mobile applications.
CO4	Implement advanced mobile security measures, including API and biometric security.

S. NO	Contents	Contact Hours
UNIT 1	**Mobile Application Security Fundamentals**- Mobile app ecosystems: Android, iOS- Threat landscape: Malware, phishing, data leaks- Security models: Android permissions, iOS sandboxing- OWASP Mobile Top 10	8
UNIT 2	**Secure Coding Practices**- Secure coding: Input validation, secure storage- Android: SecureIntents, content providers- iOS: Keychain, App Transport Security- Tools: Android Studio, Xcode	9
UNIT 3	**Mobile Application Testing**- Static and dynamic analysis: MobSF, Drozer- Penetration testing: Burp Suite, Frida- Runtime protection: RASP, app shielding- Secure session management	8
UNIT 4	**Application Hardening Techniques**- Code obfuscation and anti-reverse engineering- Secure storage: Encrypted databases- Secure communication: TLS pinning- Handling third-party libraries	9
UNIT 5	**Advanced Mobile Security Topics**- Mobile API security: REST, GraphQL- Biometric authentication: Fingerprint, face recognition- Emerging threats: 5G, edge computing- Secure app distribution	8
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Six, J. *Mobile Application Security*. McGraw-Hill.	2022
2	Chell, D., & Erasmus, T. *The Mobile Application Hacker's Handbook*. Wiley.	2020
3	OWASP. *OWASP Mobile Security Testing Guide*. OWASP Foundation.	2023

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY327: Computer Controlled Systems	**L**	**T**	**P**	**Basic Control Systems, Digital Electronics**
	3	**0/1**	**2/0**	

Course Objective: This course equips students with theoretical foundations and hands-on skills to design and implement computer-based control systems. It emphasizes sensors, actuators, control algorithms, real-time operation, data acquisition, discretization, and embedded controllers using modern tools like MATLAB/Simulink.

S. NO	Course Outcomes (CO)
CO1	**Understand the fundamental components of a computer-controlled system, including sensors, actuators, and converters.**
CO2	**Analyze and model real-time digital control systems considering discretization, sampling, and quantization.**
CO3	**Design and simulate digital controllers using MATLAB/SIMULINK.**
CO4	**Implement and evaluate embedded control systems using real-time hardware platforms.**

S. NO	Contents	Contact Hours
UNIT 1	Fundamentals of Computer-Controlled Systems: Overview of computer control applications: household, automotive, industrial, aerospace, Concepts of feedback and feedforward control in digital environments, Structure of computer-controlled systems: controllers, sensors, actuators, Closed-loop vs open-loop systems; benefits of automation, Introduction to sampled-data control systems	**7**
UNIT 2	Instrumentation and Signal Conditioning: Measurement concepts: accuracy, precision, resolution, and error analysis, Electrical and optical sensors: thermocouples, LVDTs, photodiodes, strain gauges Digital sensors and signal transmission: counters, encoders, trigger circuits, A/D and D/A conversion: operation, resolution, interfacing techniques, Signal conditioning and noise mitigation strategies	**8**
UNIT 3	Discrete-Time Control and Real-Time Constraints: Sampling theory, anti-aliasing filters, and zero-order hold models, Real-time systems, interrupts, event scheduling, timing diagrams, Quantization effects and error sources in digital systems, Introduction to real-time operating systems (RTOS) and system latencies	**9**
UNIT 4	Embedded Platforms and Software for Control: Embedded controllers microcontrollers, PC104, and industrial platforms, Development tools: MATLAB/Simulink, xPC Target, auto-code generation, Host-target architecture and communication protocols (RS232, GPIB, Ethernet),Building standalone applications for control environments	**9**
UNIT 5	Control Design and Emerging Applications: Design and tuning of digital PID controllers and discrete control strategies, Discrete system modelling, state-space, transfer functions, discretization, Modern control topics,smart sensors, distributed control, FPGAs, Project-based simulations,virtual heat	**9**

	exchanger, water tank, inverted pendulum	
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Computer Control of Processes, M. Chidambaram, Alpha Science Intl. Ltd	2002
2	Digital Control of Dynamic Systems, Franklin, Powell, Workman, Ellis-Kagle Press	2006
3	3. Digital Control Systems: Analysis and Design, C.L. Phillips & H.T. Nagle, Prentice Hall	2007
4	4. Computer-Controlled Systems: Theory and Design, K.J. Åström & B. Wittenmark, Prentice Hall	1997

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY329: Multimodal Data Processing	**L**	**T**	**P**	**Machine Learning**
	3	**1/0**	**0/2**	

Course Objective: To Understand the fundamentals of Multimodal data, text processing techniques and language models

S. NO	Course Outcomes (CO)
CO1	Identify and explain the idea of multimodal data processing along with its applications in text processing
CO2	Locate and describe various terminologies in Speech processing
CO3	Interpret and analyze different digital image and video processing approaches.
CO4	Demonstrate the need of Conventional multi-modal learning and co-learning.

S. NO	Contents	Contact Hours
UNIT 1	Introduction: Introduction to Multimodal data and applications, Multimodal Representation: two broad approaches, Joint and Coordinated. Challenges of multimodal data, Data collection & cleaning. Text Processing: Text normalization, Lemmatization, Morphology, Sub word tokenization; Text processing and statistics: TFIDF, BM-25, Zipf's law, Hipf's law; Language models and smoothing techniques; Vector space models.	**8**
UNIT 2	**Speech Processing**: Speech production and perception, Acoustic and articulatory phonetics; Short- term analysis: Need and windowing, Energy, Zero-crossing rate, Autocorrelation function, Fourier transform, Spectrogram; Short-term synthesis: Overlap-add method; Cepstrum analysis: Basis and development, mel-cepstrum.	**6**
UNIT 3	Digital Image and Video Processing: Point processing, Neighborhood processing, Enhancement, Edge detection, Segmentation, Feature descriptors, Restoration, Morphological operations, Image transforms, Spatial and temporal data handling	**6**
UNIT 4	Multi-modal learning and associated challenges: Applications and challenges from fusing two or more modalities such as vision, language, audio, graphs, biomedical signals, Development of shallow and deep networks for multimodal learning.	**8**
UNIT 5	Multi-modal processing and learning with applications: Image captioning, visual questioning answering system, automatic commentary generation, cognitive state estimation, recommendation system. Other Modalities: Biomedical signals, and Conventional multi-modal learning, co-learning etc.	**8**

	TOTAL	42

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	R. C. Gonzalez, R. E. Woods, “Digital Image Processing”, Pearson, Prentice- Hall, 4th Edition	2017
2	R. Klette, “Concise Computer Vision: An Introduction into Theory and Algorithms”, Springer, Latest Edition	2014
3	L. R. Rabiner, R. W. Schafer, “Introduction to Digital Speech Processing”, Now Publishers Inc, Latest Edition	2007

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY331: Database Security & Access Control	**L**	**T**	**P**	Database Management
	3	**0/1**	**2/0**	

Course Objectives: To provide fundamentals of database security. Various access control techniques mechanisms were introduced along with application areas of access control techniques.

S. NO	Course Outcomes (CO)
CO1	Understand and implement classical models and algorithms.
CO2	Analyze the data, identify the problems, and choose the relevant models and algorithms to apply.
CO3	Assess the strengths and weaknesses of various access control models and to analyze their behaviour.
CO4	Analyze and implement Smart Card security procedures.
CO5	Assess the strengths and weaknesses of various access control models in cloud based architecture.

S. NO	Contents	Contact Hours
UNIT 1	Introduction to Access Control, Purpose and fundamentals of access control.	**7**
UNIT 2	Policies of Access Control, Models of Access Control, and Mechanisms, Discretionary Access Control (DAC), Non- Discretionary Access Control, Mandatory Access Control (MAC). Capabilities and Limitations of Access Control Mechanisms: Access Control List (ACL) and Limitations, Capability List and Limitations	**8**
UNIT 3	Role-Based Access Control (RBAC) and Limitations, Core RBAC, Hierarchical RBAC, Statically Constrained RBAC, Dynamically Constrained RBAC, Limitations of RBAC. Comparing RBAC to DAC and MAC Access Control policy, Integrating RBAC with enterprise IT infrastructures: RBAC for WFMSs, RBAC for UNIX and JAVA environments.	**10**
UNIT 4	Smart Card based Information Security, Smart card operating system-fundamentals, design and implantation principles, memory organization, smart card files, file management. PPS Security techniques- user identification, smart card security, quality assurance and testing, smart card life cycle-5 phases, smart card terminals	**8**
UNIT 5	Cloud Data Security: Recent trends in Database security and access control mechanisms. Cloud Data Audit: Intro, Audit, Best Practice, Key management, Cloud Key Management Audit.	**9**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Role Based Access Control: David F. Ferraiolo, D. Richard Kuhn, Ramaswamy Chandramouli.	2007
2	http://www.smartcard.co.uk/tutorials/sct-itsc.pdf : Smart Card Tutorial.	___
3	Advanced System Security Topics, https://www.coursera.org/lecture/advanced-system-security-topics/role-based-access-control-rbac-bYvzS.	____

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY333: Windows Server Management	**L**	**T**	**P**	Basic knowledge of Operating Systems and Networking
	3	**0/1**	**2/0**	

Course Objective: This course aims to equip students with the skills to install, configure, and manage Windows Server environments effectively. Emphasis is placed on network infrastructure services, secure remote access, disaster recovery planning, performance monitoring, and virtualization techniques.

S. NO	Course Outcomes (CO)
CO1	**Install and maintain Windows Server environments.**
CO2	**Manage Active Directory and Group Policy.**
CO3	**Configure network services (DNS, DHCP, VPN).**
CO4	**Design and implement backup/disaster recovery solutions.**

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Windows Server Management:** Overview of Windows Server editions and features, Installation options: Server Core vs. Desktop Experience, Introduction to Windows Admin Center and PowerShell, Licensing and activation methods.	8
UNIT 2	**Active Directory and Identity Services:** Deploying and configuring Active Directory Domain Services (AD DS), Managing users, groups, and organizational units, Implementing Group Policy Objects (GPOs), Overview of Active Directory Certificate Services (AD CS).	8
UNIT 3	**Network Infrastructure Services:** Deploying and managing DHCP services, Configuring and administering DNS servers, Implementing IP Address Management (IPAM), Integrating network services with Active Directory, Troubleshooting network infrastructure issues	8
UNIT 4	**Remote Access and Disaster Recovery:** Implementing Remote Access Services (RAS) and VPNs, Configuring Network Policy Server (NPS) for authentication, Setting up Always On VPN for persistent connections, Developing and executing disaster recovery plans, Performing system backups and restorations	9
UNIT 5	**Monitoring, Security, and Virtualization:** Monitoring server performance using built-in tools, Implementing security measures and role-based access control, Utilizing Windows Defender and firewall configurations, Deploying and managing Hyper-V virtual machines,Ensuring high availability through failover clustering	9
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Michael Palmer, *Hands-On Microsoft® Windows® Server 2016*, 2nd Ed.; Cengage. ISBN 9781305078628	2016
2	Jason Eckert, *Hands-On Microsoft® Windows Server 2019*, 3rd Ed.; Cengage. ISBN 9780357436158	2019
3	Darril Gibson, *Microsoft Windows Server Administration Fundamentals*; Microsoft Press. ISBN 9781118016862	2017
4	Darril Gibson, *Windows Server 2019 & PowerShell All-in-One For Dummies*, Wiley	2019

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
	L	**T**	**P**	
CY335: Ad hoc Mobile Security	**3**	**0/1**	**2/0**	Basic understanding of Computer Networks, Familiarity with TCP/IP protocols, Knowledge of Operating Systems concepts

Course Objective: This course provides an understanding of the current topics in Mobile Ad Hoc Networks (MANETs) and Wireless Sensor Networks (WSNs) from both industry and research perspectives. Students will learn the principles distinguishing MANETs from infrastructure-based networks, comprehend proactive routing protocols and their impact on data transmission delay and bandwidth consumption, and analyze various routing algorithms to evaluate their performance.

S. NO	Course Outcomes (CO)
CO1	**Explain the fundamental principles and challenges of MANETs.**
CO2	**Analyze and compare various MAC and routing protocols used in MANETs.**
CO3	**Evaluate transport layer protocols and identify security threats and solutions in MANETs.**
CO4	**Apply knowledge of MANETs to real-world applications and emerging technologies.**

S. NO	Contents	Contact Hours
UNIT 1	Introduction to Ad Hoc Networks:Definition, characteristics, and applications of ad hoc networks, Differences between infrastructure-based and ad hoc networks, Challenges in MANETs: dynamic topology, limited bandwidth, energy constraints, Mobility models	**8**
UNIT 2	Medium Access Control (MAC) Protocols :Design issues and goals for MAC protocols in MANETs, Classification, contention-based, contention-free, hybrid protocols, Examples: IEEE 802.11, MACA, MACAW, S-MAC, Performance metrics and comparison of MAC protocols	**7**
UNIT 3	Routing Protocols: Routing challenges in MANETs, Proactive routing protocols: DSDV, OLSR, Reactive routing protocols,Hybrid routing protocols: ZRP, Routing metrics: hop count, delay, bandwidth	**9**
UNIT 4	Transport Layer and Security Issues: Transport layer challenges in MANETs, TCP over MANETs: issues and enhancements, Security threats: eavesdropping, spoofing, denial of service, Security mechanisms: encryption, authentication, secure routing protocols	**9**
UNIT 5	Applications and Advanced Topics: Applications, military, disaster recovery, vehicular networks, Integration with Wireless Sensor Networks (WSNs), Quality of Service (QoS) in MANETs, Simulation tools: NS-2, NS-3, OMNeT++, Emerging trends: Internet of Things (IoT), UAV networks	**9**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	C. Siva Ram Murthy and B. S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*, Pearson Education	2004
2	Charles E. Perkins, *Ad Hoc Networking*, Addison-Wesley	2001
3	Stefano Basagni, Marco Conti, Silvia Giordano, and Ivan Stojmenovic, *Mobile Ad Hoc Networking: Cutting Edge Directions*, Wiley-IEEE Press	2004
4	Subir Kumar Sarkar, T.G. Basavaraju, and C. Puttamadappa, *Ad Hoc Mobile Wireless Networks: Principles, Protocols, and Applications*, Auerbach Publications	2008

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY337: High Performance Computing	**L**	**T**	**P**	**Operating systems, Algorithm Design and Analysis**
	3	**0/2**	**1/0**	

Course Objective: To understand design and application of advanced computer architectures and parallel algorithms to achieve high performance computing

S. NO	**Course Outcomes (CO)**
CO1	Understand basic concepts, advanced computer architectures, parallel algorithms

CO2	Apply priciples of Memory Hierarchies, Multi core Processors
CO3	Parallel Programming involving Revealing concurrency
CO4	Compare high performance methods with Achieving Measuring performance

S. NO	Contents	Contact Hours
UNIT 1	Introduction to advanced computer architectures, parallel algorithms, parallel languages, and performance oriented computing, discussing about the key characteristics of highend computing architectures.	**8**
UNIT 2	Introduction to Computational Science and Engineering Applications, their characteristics and requirements,Review of Computational Complexity, Performance: metrics and measurements, Granularity and Partitioning, temporal/spatial/stream/kernel, Basic methods for parallel programming, Real-world case studies which are drawn from multiscale, multidiscipline applications.	**8**
UNIT 3	Memory Hierarchies, Multi core Processors, Homogeneous and Heterogeneous, Sharedmemory Symmetric Multiprocessors, Vector Computers, Distributed Memory Computers, Supercomputers and Petascale Systems, Application Accelerators/ Reconfigurable Computing, Novel computers: Stream, multithreaded, and purposebuilt	**9**
UNIT 4	Parallel Programming involving Revealing concurrency in applications ,Task and Functional parallelism, Task Scheduling, Synchronization Methods, Parallel Primitives (collective operations), SPMD Programming (threads, OpenMP, MPI), I/O and File Systems, Parallel Matlabs (Parallel Matlab, StarP, Matlab MPI) Partitioning Global Address Space (PGAS) languages (UPC, Titanium, Global Arrays).	**9**
UNIT 5	Discussion about high performance methods with Achieving Measuring performance, Identifying performance bottlenecks, Restructuring applications for deep memory hierarchies, Partitioning applications for heterogeneous resources, Using existing libraries, tools, and framework.	**8**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Introduction to Parallel Computing, Ananth Grama, Anshul Gupta, George Karypis, and Vipin Kumar, 2nd edition, AddisonWelsey, 2003.	2021
2	Petascale Computing: Algorithms and Applications, David A. Bader (Ed.), Chapman & Hall/CRC Computational Science Series, 2007	2018
3	Chuck helebuyck, Programming PIC microcontrollers with PIC basic.	2004
4	Grama, A. Gupta, G. Karypis, V. Kumar, An Introduction to Parallel Computing, Design and Analysis of Algorithms: 2/e, AddisonWesley,2003	2012

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY339: Database Management	**L**	**T**	**P**	-
	3	**0/1**	**2/0**	

Course Objectives: 1. To understand the concepts of database management system and its applications, data modeling, database design, and query languages.
2. To understand different files structures, transaction management, concurrency control, database recovery, query processing and optimization.

S. NO	Course Outcomes (CO)
CO1	Analyse database system architecture and develop conceptual data models using the ER model.
CO2	Apply relational data model concepts and perform queries using relational algebra, calculus, and SQL.
CO3	Design normalized databases using functional, multivalued, and join dependencies.
CO4	Analyze file organization and indexing techniques, and understand transaction processing and recovery.
CO5	Implement concurrency control techniques and understand protocols used in database systems.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction:** Database system concepts and its architecture, Data models schema and instances, Data independence and database language and interface, Data definition languages, DML. Overall database structure.Data modeling using Entity Relationship Model: E.R. model concept, notation for ER diagrams mapping constraints, Keys, concept of super key, candidate key, primary key generalizations, Aggregation, reducing ER diagrams to tables, extended ER model.	**9**
UNIT 2	**Relational Data Model and Language:** Relational data model concepts, integrity constraints, Keys domain constraints, referential integrity, assertions, triggers, foreign key relational algebra, relational calculus, domain and tuple calculus, SQL data definition queries and updates in SQL.	**9**
UNIT 3	**Data Base Design:** Functional dependencies, normal forms, 1NF, 2NF, 3NF and BCNF, multi-valued dependencies fourth normal form, join dependencies and fifth normal form. Inclusion dependencies, lossless join decompositions, normalization using FD, MVD and JDs, alternatives approaches to database design	**8**
UNIT 4	**File Organization, Indexing and Hashing:** Overview of file organization techniques, Indexing and Hashing- Basic concepts, Static Hashing, Dynamic Hashing, Ordered indices, Multi-level indexes, B-Tree index files, B+- Tree index files, Buffer management **Transaction processing concepts:** Transaction processing system, schedule and recoverability, Testing of serializability, Serializability	**8**

	of schedules, conflict & view serializable schedule, recovery from transaction failures, deadlock handling.	
UNIT 5	**Concurrency Control Techniques**: Locking Techniques for concurrency control, time stamping protocols for concurrency control, concurrency control in distributed systems. multiple granularities and multi-version schemes.	**8**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Elmasri, Navathe,"Fundamentals of Database systems", Addision Wesley	2019
2	Korth, Silbertz, Sudarshan,"Data base concepts", McGraw-Hill.	2021
3	Ramakrishna, Gehkre, "Database Management System", McGraw-Hill	2002
4	Date C.J.,"An Introduction to Database systems"	2006

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY302: Internet of Things and Security	**L**	**T**	**P**	**Computer Networks and Security**
	3	**0**	**2**	

Course Objectives:

1. To introduce IoT architecture, components, and communication protocols.
2. To analyze security vulnerabilities in IoT devices, networks, and data.
3. To implement secure IoT systems using encryption, authentication, and access control.
4. To explore advanced topics like blockchain and AI for IoT security.

S. NO	**Course Outcomes (CO)**
CO1	Explain IoT architecture, protocols, and applications.
CO2	Identify vulnerabilities in IoT devices and communication channels.
CO3	Design secure IoT systems with encryption and access control.
CO4	Implement intrusion detection and anomaly mitigation in IoT networks.
CO5	Evaluate emerging technologies (e.g., blockchain, AI) for IoT security.

S. NO	**Contents**	**Contact Hours**
UNIT 1	Fundamentals of IoT: IoT architecture: Sensors, actuators, cloud, edge, Communication protocols: MQTT, CoAP, HTTP, LoRaWAN, IoT applications: Smart homes, healthcare, Industry 4.0, Security challenges: Attack surfaces in IoT ecosystems	10
UNIT 2	IoT Communication & Network Security: Secure protocols: DTLS, TLS, Zigbee Security, Vulnerabilities: Man-in-the-middle (MITM), DDoS, Securing wireless networks: Wi-Fi, Bluetooth, RFID, Case study: Mirai botnet attack analysis | |	10
UNIT 3	IoT Device & Firmware Security: Hardware security: TPM, secure boot, hardware roots of trust, Firmware vulnerabilities: Reverse engineering, OTA update risks, Secure coding practices for embedded systems, Case study: Jeep Cherokee hack (2015)	**8**
UNIT 4	IoT Data Security & Privacy: Data encryption: AES, RSA, lightweight cryptography, Privacy concerns: GDPR compliance, data anonymization, Secure cloud storage and edge computing, Anomaly detection using machine learning	**8**
UNIT 5	**Advanced IoT Security & Emerging Trends: Blockchain for IoT: Decentralized trust, smart contracts, AI/ML for threat detection and predictive security, Post-quantum cryptography in IoT, Ethical hacking and penetration testing for IoT**	**6**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
	IoT Security: Advances in Authentication, Madhusanka Liyanage, Wiley	2020
	Practical Internet of Things Security, Brian Russell, Drew Van Duren, Packt	2018
	Security and Privacy in the Internet of Things, Ali Ismail Awad, Wiley	2021
	Blockchain and Machine Learning for IoT Security, Mohammad Reza Khalifeh, Springer	2022

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY304: Malware Analysis	**L**	**T**	**P**	**Computer Networks**
	3	**0**	**2**	

Course Objective: After learning the course the students will be able to:

- Learn to analyze various malicious file types
- Learn to build and utilize a sandbox environment for malware analysis
- Apply various tools to Identify the vulnerabilities and to perform Malware analysis
- Apply malware classification and functionality & anti-reverse engineering techniques

S. NO	Course Outcomes (CO)
CO1	Learn to analyze various malicious file types
CO2	Learn to build and utilize a sandbox environment for malware analysis
CO3	Apply various tools to Identify the vulnerabilities and to perform Malware analysis
CO4	Apply malware classification and functionality & anti-reverse engineering techniques

S. NO	Contents	Contact Hours
UNIT 1	**Malware Analysis Fundamentals:** Assembling a toolkit for effective malware analysis, examining static properties of suspicious programs, performing behavioral analysis of malicious Windows executable, performing static and dynamic code analysis of malicious Windows executables, interacting with malware in a lab to derive additional behavioral characteristics.	08
UNIT 2	**Malicious Web and Document Files:** Interacting with malicious websites to assess the nature of their threats, Deobfuscating malicious JavaScript using debuggers and interpreters, analyzing suspicious PDF files, examining malicious Microsoft Office documents, including files with macros, Analyzing malicious RTF document files	10
UNIT 3	**Reversing Malicious Code:** Understanding core x86 assembly concepts to perform malicious code analysis, Identifying key assembly logic structures with a disassembler, following program control flow to understand decision points during execution, recognizing common malware characteristics at the Windows API level (registry manipulation, key logging, HTTP communications, droppers), Extending assembly knowledge to include x64 code analysis	09
UNIT 4	**In-Depth Malware Analysis:** Recognizing packed malware, Getting started with unpacking, using debuggers for dumping packed malware from memory, analyzing multi-technology and file-less malware, Code injection and API hooking, Using memory forensics for malware analysis	07
UNIT 5	**Examining Self-Defending Malware:** How malware detects debuggers and protects embedded data, unpacking malicious software that employs process	08

	hollowing, Bypassing the attempts by malware to detect and evade the analysis toolkit, Handling code misdirection techniques, including SEH and TLS Callbacks, unpacking malicious executable by anticipating the packer's actions	
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Practical Malware Analysis The Hands-on guide to Dissecting Malicious Software	2012
2	Jamie Butler and Greg Hoglund, “Rootkits: Subverting the Windows Kernel”, Addison-Wesley	2005
3	Dang, Gazet and Bachaalany, “Practical Reverse Engineering”,Wiley	2014
4	Reverend Bill Blunden, “The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System” Second Edition,Jones& Bartlett	2013

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY306: PATTERN RECOGNITION	**L**	**T**	**P**	**Linear algebra, Probability theory**
	3	**1/0**	**0/2**	

Course Objective: To equip with basic mathematical and statistical techniques commonly used in pattern recognition. Also provide with an adequate background on probability theory, statistics, and optimization theory to tackle a wide spectrum of engineering problems.

S. NO	**Course Outcomes (CO)**
CO1	Ability to apply the knowledge of mathematics and probability theory for obtaining solutions in pattern recognition domain
CO2	Ability to apply various algorithms for pattern recognition
CO3	Ability to apply pattern recognition concepts for solving real life problems
CO4	Ability to carry out implementation of algorithms using different simulation tools

S. NO	**Contents**	**Contact Hours**
UNIT 1	Introduction to Pattern Recognition: Feature Detection, Classification, Review of Probability Theory, Conditional Probability and Bayes Rule, Random Vectors, Expectation, Correlation, Covariance, Review of Linear Algebra, Basics of Estimation theory, Decision Boundaries, Decision region / Metric spaces/ distances.	**10**
UNIT 2	Classification: Bayes decision rule, Error probability, Normal Distribution, Discriminant functions, Decision surfaces, K-NN Classifier, Single Layer Perceptron, Multi-Layer Perceptron, Training set, test set; standardization and normalization.	**8**
UNIT 3	Clustering: Basics of Clustering; similarity / dissimilarity measures; clustering criteria, Different distance functions and similarity measures, Minimum within cluster distance criterion, K-means algorithm, K-medoids, DBSCAN, Data sets - Visualization; Unique Clustering, No existence of clusters.	**8**
UNIT 4	Feature selection: Problem statement and Uses; Algorithms - Branch and bound algorithm, sequential forward / backward selection algorithms, (l,r) algorithm; Probabilistic separability based criterion functions, interclass distance based criterion functions.	**8**
UNIT 5	Feature extraction: PCA, Structural PR, SVMs, FCM, Soft-computing and Neuro-fuzzy techniques, and real-life examples.	**8**
	TOTAL	**42**

REFERENCES

S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	R. O. Duda, P. Hart, D. Stork, Pattern Classification, 2nd Ed. Wiley, ISBN:	2000

	9780-471-05669-0.,2000	
2	Bishop, C. M., Pattern Recognition and Machine Learning. Springer, ISBN 978-0- 387-31073-2,2007	2007
3	Bishop, C. M., Neural Networks for Pattern Recognition, Oxford University Press, ISBN-13: 978-0198538646,1995	1995
4	Theodoridis, S. and Koutroumbas, K., Pattern Recognition, 4th Ed. Academic Press, ISBN :9781597492720.,2008	2008

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY308: Image Analysis	**L**	**T**	**P**	**Basic Math, Basic C**
	3	**0/1**	**2/0**	

Course Objective: 1) To provide students with a comprehensive understanding of the fundamental principles and techniques in image analysis, including image acquisition, preprocessing, enhancement, segmentation, feature extraction, morphological operations, pattern recognition, object detection, and image classification.

S. NO	Course Outcomes (CO)
CO1	Demonstrate understanding of core image processing operations.
CO2	Apply various filters and transformations for image enhancement.
CO3	Implement segmentation and object detection methods.
CO4	Analyze images using statistical and machine learning-based techniques.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Image Analysis:** Digital Image Fundamentals, Image Acquisition and Sampling, Pixel Relationships and Color Models, Applications of Image Analysis in Engineering.	**8**
UNIT 2	**Image Enhancement and Filtering:** Histogram Processing, Spatial and Frequency Domain Filtering, Noise Reduction Techniques, Image Smoothing and Sharpening.	**9**
UNIT 3	**Image Segmentation:** Thresholding and Region-Based Segmentation, Edge Detection Techniques (Sobel, Canny, etc.), Watershed and Morphological Approaches, Clustering Techniques (K-means, Mean Shift).	**9**
UNIT 4	**Feature Extraction and Pattern Recognition:** Texture and Shape Features, Principal Component Analysis (PCA), Classification Techniques (SVM, k-NN), Basics of Convolutional Neural Networks (CNNs) for image classification and object detection.	**8**
UNIT 5	**Understanding Applications and Projects:** Medical Image Analysis, Remote Sensing and Satellite Image Analysis, Biometric Systems (Face, Fingerprint Recognition), Real-Time Implementation using OpenCV, MATLAB, or Python.	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Rafael C. Gonzalez and Richard E. Woods, *Digital Image Processing*, Pearson Education.	2018
2	Anil K. Jain, *Fundamentals of Digital Image Processing*, Prentice Hall.	1989

3	Milan Sonka, Vaclav Hlavac, and Roger Boyle, *Image Processing, Analysis, and Machine Vision*, Cengage Learning.	2017
4	Mark Nixon and Alberto S. Aguado, *Feature Extraction and Image Processing for Computer Vision*, Academic Press.	2019

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY310: Blockchain Platform and Use Cases	**L**	**T**	**P**	Data Structures & Networks
	3	**1/0**	**0/2**	

Course Objective: Provide students with a comprehensive understanding of blockchain architectures, development platforms, and their real-world applications.

S. NO	Course Outcomes (CO)
CO1	Describe the core components and consensus mechanisms of blockchain systems.
CO2	Analyze and compare major blockchain platforms including Bitcoin, Ethereum, and Hyperledger.
CO3	Develop and deploy smart contracts and decentralized applications on public and permissioned ledgers.
CO4	Evaluate blockchain use cases in various domains, addressing security, privacy, and scalability challenges.

S. NO	Contents	Contact Hours
UNIT 1	Evolution of distributed ledger technology, blockchain architecture fundamentals, block structure and header fields, transaction lifecycle and validation process, cryptographic hash functions and Merkle tree construction, digital signature schemes, consensus mechanism taxonomy (PoW, PoS, DPoS), public versus private versus permissioned blockchains.	**8**
UNIT 2	Bitcoin protocol internals and UTXO model, Ethereum account model versus UTXO, gas model and transaction fees, Ethereum Virtual Machine architecture and bytecode execution, Hyperledger Fabric architecture including membership service provider and ordering service, permissioned consensus algorithms (RAFT, PBFT), performance benchmarking and throughput analysis, interoperability challenges	**10**
UNIT 3	Solidity language syntax and data types, contract functions and modifiers, events and logging, smart contract design patterns and security best practices (reentrancy guard, access control), development toolchain (Remix IDE, Truffle, Hardhat), deploying to public and private testnets, front-end integration using Web3.js and Ethers.js, gas optimization strategies	**8**
UNIT 4	Supply chain provenance implementations, decentralized finance primitives (lending, borrowing, decentralized exchanges), stablecoin design mechanisms (collateralized, algorithmic), on-chain and off-chain oracle integration, decentralized identity management solutions, governance through decentralized autonomous organizations (DAOs), non-fungible token standards (ERC-721, ERC-1155)	**8**
UNIT 5	Common attack vectors and mitigation (51% attacks, double-spend, eclipse attacks), smart contract vulnerabilities (reentrancy, integer overflow/underflow), cryptographic privacy techniques (zero-knowledge proofs, ring signatures, mixers), scalability solutions (sharding, state channels, sidechains), Layer-2 protocols (Lightning Network, Plasma, Rollups), regulatory, legal, and compliance considerations	**8**

	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Andreas M. Antonopoulos & Gavin Wood, *Mastering Ethereum: Building Smart Contracts and DApps*, O'Reilly Media	2018
2	Imran Bashir, *Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained*, Packt Publishing	2017
3	Daniel Drescher, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, Apress	2017
4	Melanie Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly Media	2015

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY312: Smart Contracts and Solidity	**L**	**T**	**P**	**Data Structures & Networks**
	3	**1/0**	**0/2**	

Course Objective: Enable students to design, implement, test, and deploy secure smart contracts using the Solidity language on Ethereum-compatible platforms.

S. NO	Course Outcomes (CO)
CO1	Explain the architecture of Ethereum and the role of smart contracts in decentralized applications.
CO2	Write, compile, and deploy Solidity contracts using standard development tools and frameworks.
CO3	Integrate smart contracts with web front-ends using Web3.js or Ethers.js libraries.
CO4	Identify, analyze, and mitigate common security vulnerabilities in smart contracts.

S. NO	Contents	Contact Hours
UNIT 1	Overview of Ethereum blockchain and smart contract concepts, Ethereum accounts and transaction lifecycle, gas model and fee calculation, contract ABI and bytecode structure, development environments such as Remix IDE and VS Code plugins, introduction to Truffle and Hardhat toolchains	**8**
UNIT 2	Solidity data types and variables, functions and visibility specifiers, control structures (if/else, loops), arrays and mappings, structs and enums, events and logging mechanisms, error handling with require/assert/revert, contract compilation and ABI generation	**10**
UNIT 3	Contract inheritance and interfaces, library usage and deployable libraries, function modifiers and fallback/receive functions, payable functions and Ether transfers, design patterns (Ownable, Proxy, Pull-over-Push), contract upgradeability techniques, gas optimization strategies	**8**
UNIT 4	Local blockchain networks with Ganache, writing unit tests in JavaScript/TypeScript using Mocha/Chai, script-based deployment with Truffle and Hardhat, front-end integration using Web3.js and Ethers.js, debugging and transaction tracing, working with public testnets (Ropsten, Rinkeby)	**8**
UNIT 5	Common smart contract vulnerabilities (reentrancy, integer overflow/underflow, front-running), analysis tools (MythX, Slither), secure coding best practices, role of formal verification, security audit workflows, emerging topics in DeFi security and on-chain governance	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint

1	Chris Dannen, *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*, Addison-Wesley Professional	2017
2	Ritesh Modi, *Solidity Programming Essentials*, Packt Publishing	2018
3	Andreas M. Antonopoulos & Gavin Wood, *Mastering Ethereum: Building Smart Contracts and DApps*, O'Reilly Media	2018
4	Roberto Infante, *Building Ethereum DApps: Decentralized Applications on the Ethereum Blockchain*, Packt Publishing	2020

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY314: GEN AI WITH CYBERSECURITY	**L**	**T**	**P**	**Probability theory, Machine learning**
	3	**1/0**	**0/2**	

Course Objective: To explore the utility of Generative AI (Gen AI) in the field of cybersecurity, specifically for applications of threat detection and mitigation. Also explored are the vulnerabilities of Gen AI models and ethical practices to be followed while using Gen AI.

S. NO	Course Outcomes (CO)
CO1	Ability to explain the principle and working of generative AI models.
CO2	Ability to implement generative AI models for automation of tasks in cybersecurity.
CO3	Ability to implement generative AI models for detection of threats and anomalies.
CO4	Ability to build a resilient Gen AI program following ethical digital practices.

S. NO	Contents	Contact Hours
UNIT 1	Introduction to Generative AI: Overview of Generative AI (Gen AI) and its applications; Key concepts: Latent spaces, probability distributions, and sampling, Comparison between discriminative and generative models, Large Language Models (LLMs).	**10**
UNIT 2	Exploring use cases of Gen AI for cybersecurity domain: Automation of tasks, threat detection, identifying potential attacks, and improving incident response. Application of Gen AI to data security, model security, application-level security.	**10**
UNIT 3	Use of Gen AI to create models for normal and anomalous network behavior and user behavior, Case studies of cyber threats, Applications of Gen AI in real-time analytics for detecting anomalies and potential attacks in real-time.	**12**
UNIT 4	Security threats posed by Gen AI, misuse of Gen AI for creating attacks such as phishing emails, mitigating attacks using Gen AI. Vulnerabilities of Gen AI models, Ethical AI practices for secure digital environment.	**10**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Generative Deep Learning: Teaching Machines to Paint, Write, Compose, and Play by David Foster	2022
2	Generative AI with Python and TensorFlow 2 by Babcock and Bali	2021
3	Generative AI and its impact on cybersecurity by Nednur	2024
4	Generative AI security by Huang, Wang, Goertzl, Li, Wright	2024
5	Generative AI: Phishing and Cybersecurity metrics by Ravindra Das	2025

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY316: Software Testing and Security Audit of CPS	**L**	**T**	**P**	**Introduction to Cyber Physical Systems, Software Engineering**
	3	**0/1**	**2/0**	

Course Objective: To equip students with the knowledge and skills to perform software testing and security audits for cyber-physical systems, focusing on identifying vulnerabilities, ensuring system integrity, and validating security controls in critical CPS applications.

S. NO	Course Outcomes (CO)
CO1	Understand the principles and methodologies of software testing and security auditing for CPS.
CO2	Apply testing techniques to evaluate the functionality and security of CPS software.
CO3	Conduct security audits to identify vulnerabilities and ensure compliance in CPS.
CO4	Analyze emerging trends in CPS testing and auditing, including AI-driven approaches.

S. NO	Contents	Contact Hours
UNIT 1	**Fundamentals of CPS Software Testing and Auditing**- Overview of CPS software: Components, architecture- Importance of testing and auditing in CPS- Testing methodologies: Black-box, white-box, grey-box- Security audit frameworks: NIST SP 800-115, ISO/IEC 27007	8
UNIT 2	**Software Testing Techniques for CPS**- Functional testing: Unit, integration, system testing- Non-functional testing: Performance, reliability, safety- Model-based testing for CPS: Simulink, Stateflow- Testing real-time constraints in CPS	9
UNIT 3	**Security Testing and Vulnerability Assessment**- Penetration testing for CPS- Fuzz testing and fault injection- Static and dynamic analysis: SAST, DAST tools- Vulnerability scanning: OWASP ZAP, Nessus- Threat modeling for CPS software	8
UNIT 4	**Security Auditing and Compliance**- Audit planning and execution: Risk-based auditing- CPS security standards: IEC 62443, NIST SP 800-82- Compliance auditing: GDPR, HIPAA for CPS- Audit reporting and remediation strategies	9
UNIT 5	**Advanced Trends in CPS Testing and Auditing**- AI-driven testing: Automated test case generation- Testing for autonomous CPS: Drones, self-driving cars- Blockchain for audit trail integrity- Case studies: CPS security breaches and lessons learned	8
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint

1	Myers, G. J., Sandler, C., & Badgett, T. *The Art of Software Testing*. Wiley.	2011
2	NIST. *SP 800-115: Technical Guide to Information Security Testing and Assessment*. NIST.	2008

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY318: Cyber Threat Intelligence	**L**	**T**	**P**	**Computer Networks, Operating Systems**
	3	**0/1**	**2/0**	

Course Objective: To understand cyber threat intelligence's principles and processes and analyze different threat actor tactics, techniques, and procedures (TTPs). To use CTI tools and frameworks to build threat profiles and to develop reporting and communication skills in CTI context.

S. NO	Course Outcomes (CO)
CO1	Explain the fundamentals and importance of cyber threat intelligence.
CO2	Identify and analyze cyber threat actors and their attack strategies.
CO3	Collect, process, and analyze cyber threat data effectively.
CO4	Use appropriate tools and frameworks to assess and respond to threats.
CO5	Produce actionable intelligence reports and understand legal implications.

S. NO	Contents	Contact Hours
UNIT 1	Introduction to Cyber Threat Intelligence, Overview of cybersecurity and threat landscape, Importance of threat intelligence, Types of cyber threat intelligence (strategic, operational, tactical, technical), Intelligence life cycle	**8**
UNIT 2	Threat Actors and Attack Lifecycle, Cyber threat actors: nation-states, hacktivists, insiders, cybercriminals, Cyber kill chain, MITRE ATT&CK frame work, Case studies of real-world attack	**9**
UNIT 3	Collection and Analysis of Threat Data, Threat data sources (OSINT, HUMINT, SIGINT, etc.), Indicators of Compromise (IOCs), Tactics, Techniques, Procedures (TTPs), Threat intelligence platforms (TIPs)	**8**
UNIT 4	Tools and Technologies for CTI, Open-source and commercial CTI tools, Malware analysis basics, Sandboxing, honeypots, SIEM integration, Threat feeds and API	**8**
UNIT 5	Reporting, Sharing, and Legal Considerations, Writing effective threat intelligence reports, Intelligence sharing frameworks (ISACs, STIX/TAXII), Ethics and legal issues in CTI, Privacy, attribution, and policy concerns	**9**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Eric Hutchins, Michael Cloppert, and Rohan Amin, 'Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains', 2011	2011
2	Scott J. Roberts and Rebekah Brown, 'Intelligence-Driven Incident Response', O'Reilly Media, 2017	2017

3	Steven Adair et al., 'APT1: Exposing One of China's Cyber Espionage Units', Mandiant Report, 2013	2013
4	John Robertson et al., 'Cyber Threat Intelligence', SANS Institute Reading Room, 2020	2020

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY320: Post Quantum Cryptography	**L**	**T**	**P**	Basics of Cryptography, Linear Algebra, Number Theory
	3	**1/0**	**0/2**	

Course Objective: To provide students with a comprehensive understanding of the fundamental principles and techniques in post-quantum cryptography, including threats from quantum computers to classical cryptographic systems, quantum-resistant algorithms, implementation and evaluation of post-quantum schemes, and secure system.

S. NO	Course Outcomes (CO)
CO1	Explain the principles of quantum computing and its impact on classical cryptography.
CO2	Distinguish between various post-quantum cryptographic approaches.
CO3	Implement lattice-based and code-based cryptographic protocols.
CO4	Evaluate quantum-resistant algorithms for practical use.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Quantum Threats and Classical Cryptography Review:** Fundamentals of Classical Cryptography (RSA, ECC, AES, Hashes), Overview of Quantum Computing: Qubits, Superposition, Entanglement, Quantum Algorithms: Shor's Algorithm and Grover's Algorithm, Quantum Threat to RSA, ECC, and Symmetric Cryptography.	**7**
UNIT 2	**Introduction to Post-Quantum Cryptography:** Need for Post-Quantum Cryptography, NIST PQC Standardization Project, Security Assumptions and Hardness Problems, Categories of PQC: Lattice, Code, Multivariate, Hash-Based, Isogeny-Based.	**7**
UNIT 3	**Lattice-Based Cryptography:** Lattices and Hard Problems: SVP, CVP, LWE, Ring-LWE, NTRU and NTRUEncrypt, LWE-based Public Key Encryption, Signature Schemes: Dilithium, Falcon, Security and Efficiency Analysis.	**10**
UNIT 4	**Code-Based and Multivariate Cryptography:** Code-Based Cryptography: McEliece Cryptosystem, BIKE, HQC, Multivariate Polynomial Cryptography: MQ Problem, Multivariate Signature Schemes (Rainbow, UOV), Practical Implementations and Limitations.	**10**
UNIT 5	**Hash-Based and Isogeny-Based Cryptography:** Hash-Based Signatures: Merkle Trees, SPHINCS+, Stateless and Stateful Signature Schemes, Isogeny-Based Cryptography: SIDH, SIKE, Hybrid Schemes and PQC in TLS.	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	**Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009).** *Post-Quantum Cryptography*. Springer.	2009
2	**Paar, C., & Pelzl, J. (2009).** *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer.	2024
3	**Chen, L., et al. (2016).** *Report on Post-Quantum Cryptography*. NISTIR 8105.	2016
4	**Mosca, M. (2021).** *Quantum Threat Timeline Report*. Global Risk Institute.	2021

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY322: Ubiquitous Sensing, Computing and Communication	**L**	**T**	**P**	**Operating systems, Algorithm Design and Analysis**
	3	**0/1**	**2/0**	

Course Objective: • Basic introduction of all the elements of IoT-Mechanical, Electronics/sensor platform, Wireless and wireline protocols, Mobile to Electronics integration, Mobile to enterprise integration.
• To have an understanding of basics of open source/commercial electronics platform for IoT.
• To have an understanding of basics of open source /commercial enterprise cloud platform for IoT.

S. NO	Course Outcomes (CO)
CO1	Understand basic concepts, OSI reference model, services and role of each layer of OSI model and TCP/IP, networks devices and transmission media
CO2	Apply channel allocation, framing, error and flow control techniques.
CO3	Functions of Network Layer i.e. Logical addressing, subnetting & Routing Mechanism
CO4	Transport & Application Layer function i.e. Port addressing, Connection Management, Error control and Flow control mechanism.

S. NO	Contents	Contact Hours
UNIT 1	Introduction, Overview, Challenges in IoT, Networking Basics of IoT, NFC, Wireless LAN.	**8**
UNIT 2	Location in ubiquitous computing: Personal assistants, Location aware computing, Location tracking, Architecture, Location based service and applications, Location based social networks (LBSN), LBSN Recommendation.	**8**
UNIT 3	Privacy and security in ubiquitous computing, Energy constraints in ubiquitous computing. Wearable computing, Glass and Augmented Reality, Eye-Tracking, Digital Pen and Paper, Mobile social networking & crowd sensing, Event based social network.	**9**

UNIT 4	Mobile affective computing: Human Activity and Emotion Sensing, Health Apps, Mobile p2p computing, Smart Homes and Intelligent Buildings, Mobile HCI, Cloud centric IoT, Open challenges, Architecture, Energy Efficiency, Participatory sensing, Protocols, QoS, QoE.	**9**
UNIT 5	IoT and data analytics IoT and Data Management, Data cleaning and processing, Data storage models. Search techniques, Deep Web, Semantic sensor web, Semantic Web Data Management, Searching in IoT. Real-time and Big Data Analytics for The Internet of Things, Heterogeneous Data Processing, High-dimensional Data Processing, Parallel and Distributed Data Processing.	**8**
	TOTAL	**42**

REFERENCES

S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	1. N. Jeyanthi, Ajith Abraham, Hamid Mcheick, "Ubiquitous Computing and Computing Security of IoT".	2021
2	2. John Krumm, Ubiquitous Computing Fundamentals, CRC Press.	2018
3	3. Dirk Slama, "Enterprise IoT", Shroff Publisher/O'Reilly Publisher	2004

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY324: Concepts of Virtual and Augmented Reality	**L**	**T**	**P**	**None**
	3	**1/0**	**0/2**	

Course Objective: This course is designed to give historical and modern overviews and perspectives on virtual reality. It describes the fundamentals of sensation, perception, technical and engineering aspects of virtual reality systems.

S. NO	Course Outcomes (CO)
CO1	Describe how VR systems work and list the applications of VR.
CO2	Understand the design and implementation of the hardware that enables VR systems to be built.
CO3	Understand the system of human vision and its implications on perception and rendering.
CO4	Explain the concepts of motion and tracking in VR systems.
CO5	Describe the importance of interaction and audio in VR systems.

S. NO	Contents	Contact Hours
UNIT 1	Virtual reality and virtual environments: the historical development of VR, scientific landmarks, computer graphics, real-time computer graphics, virtual environments, requirements for VR, benefits of virtual reality. Hardware technologies for 3D user interfaces: visual displays, auditory displays, haptic displays, and choosing output devices for 3D user interfaces.	**9**
UNIT 2	3D user interface input hardware: input device characteristics, desktop input devices, tracking devices, 3d mice, special-purpose input devices, direct human input, home-brewed input devices, choosing input devices for 3D interfaces. Software technologies: database - world space, world coordinate, world environment, objects - geometry, position/orientation, hierarchy, bounding volume, scripts and other attributes, VR environment - VR database, tessellated data, LODs, Cullers and Occluders, lights and cameras, scripts, interaction - simple, feedback, graphical user interface, control panel, 2D controls, hardware controls, room / stage / area descriptions, world authoring and playback, VR toolkits, available software in the market.	**14**
UNIT 3	3D interaction techniques: 3D manipulation tasks, manipulation techniques and input devices, interaction techniques for 3D manipulation, design guidelines – 3D travel tasks, travel techniques, design guidelines - theoretical foundations of wayfinding, user centered wayfinding support, environment centered wayfinding support, evaluating wayfinding aids, design guidelines - system control, classification, graphical menus, voice commands, Gestrual commands, tools, mutimodal system control techniques, design guidelines, case study: mixing system control methods, symbolic input tasks, symbolic input techniques, design guidelines, beyond text and number entry.	**8**
UNIT 4	Designing and developing 3D user interfaces: strategies for designing and developing guidelines and evaluation. Advances in 3D user interfaces: 3D	**7**

	user interfaces for the real world, AR interfaces as 3D data browsers, 3D augmented reality interfaces, augmented surfaces and tangible interfaces, agents in AR, transitional AR-VR interfaces - the future of 3D user interfaces, questions of 3D UI technology, 3d interaction techniques, 3d UI design and development, 3D UI evaluation and other issues.	
UNIT 5	Virtual reality applications: engineering, architecture, education, medicine, entertainment, science, training.	**4**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Virtual Reality, Steven M. LaValle, Cambridge University Press..	2016
2	Understanding Virtual Reality: Interface, Application and Design, William R Sherman and Alan B Craig, (The Morgan Kaufmann Series in Computer Graphics)". Morgan Kaufmann Publishers, San Francisco.	2002
3	Developing Virtual Reality Applications: Foundations of Effective Design, Alan B Craig, William R Sherman and Jeffrey D Will, Morgan Kaufmann.	2009
4	Paul Mealy, Virtual & Augmented Reality for Dummies, John Wiley & Sons.	
5	Doug A Bowman, Ernest Kuijff, Joseph J LaViola, Jr and Ivan Poupyrev, "3D User Interfaces, Theory and Practice", Addison Wesley, USA	2011

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY326: Linux Administrator	**L**	**T**	**P**	**None**
	3	**0/1**	**2/0**	

Course Objective: Master Linux command-line operations, file system management, and essential system tools across distributions.
Operate and troubleshoot Linux servers in networked environments, integrating and administering core services and ensuring system security.

S. NO	Course Outcomes (CO)
CO1	Work confidently in the Linux environment and automate tasks using shell scripts.
CO2	Implement Linux utilities and system calls for file and process management.
CO3	Develop and debug systems and network programs using C and shell scripting.
CO4	Administer Linux servers, configure network services, and ensure system security.
CO5	Troubleshoot and resolve issues in Linux system and network administration

S. NO	Contents	Contact Hours
UNIT 1	**Linux Utilities and Shell Programming:** File handling utilities, file permissions, process utilities, disk utilities, networking commands, filters, text processing, backup utilities, sed and awk scripting, shell programming with bash (pipes, redirection, variables, control structures, functions, debugging).	**8**
UNIT 2	**Files and Directories:** File concepts, types, filesystem structure, inodes, kernel support, system calls for file I/O (open, read, write, etc.), file status, locking, permissions, ownership, links (hard/soft), directory management (mkdir, rmdir, chdir), directory scanning.	**7**
UNIT 3	**Processes and Signals:** Process concepts, program memory layout, environment variables, process control (fork, exec, wait, exit), process groups, sessions, threads vs processes, signals (generation, handling, kernel support, kill, alarm, pause, sleep)	**8**
UNIT 4	**Interprocess Communication (IPC):** IPC on single and multiple systems, unnamed and named pipes (FIFOs), message queues, semaphores, file locking, popen/pclose, client/server examples. **Shared Memory and Sockets:** Shared memory support and APIs, socket programming (Berkeley sockets, address structures, connection-oriented/connectionless protocols), client/server models, socket options, IPC mechanism comparison.	**10**
UNIT 5	**Linux Server Administration & Networking:** Linux distributions, software management, user/group management, boot/shutdown, file systems, kernel compilation, TCP/IP, firewall (Netfilter), system/network security, DNS, FTP, Apache, SMTP, POP/IMAP, SSH, OpenLDAP, Samba, Kerberos, NFS, DFS, NIS, DHCP, MySQL, LAMP, VPN, file/email/chat servers.	**9**

	TOTAL	42

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Linux Administration: A Beginner's Guide, Wale Soyinka, 7th Ed., McGraw-Hill.	2016.
2	Ubuntu Server Guide, Ubuntu Documentation Team.	2016
3	Mastering Ubuntu Server, Jay LaCroix, PACKT Publisher.	2016
4	W. Richard. Stevens, Advanced Programming in the UNIX Environment, 3rd edition, Pearson Education, New Delhi, India	2005

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY328 Deep Learning Applications	**L**	**T**	**P**	Fundamentals of Deep Learning
	3	**1/0**	**0/2**	

Course Objective: Provide students with practical knowledge to apply deep learning techniques across diverse real-world domains.

S. NO	Course Outcomes (CO)
CO1	Design and implement end-to-end deep learning solutions for tasks in vision, language, and audio.
CO2	Evaluate and select appropriate neural architectures based on application requirements and performance metrics.
CO3	Integrate data preprocessing, model training, and deployment workflows using modern DL frameworks.
CO4	Assess challenges of interpretability, scalability, and ethical considerations in deep learning applications.

S. NO	Contents	Contact Hours
UNIT 1	Overview of deep learning application pipeline, data collection and preprocessing techniques, framework ecosystems such as TensorFlow and PyTorch, transfer learning and fine-tuning methodologies, experiment tracking and model versioning, hyperparameter tuning strategies	**8**
UNIT 2	Image classification and feature extraction, object detection and localization, semantic and instance segmentation, facial recognition and verification systems, video analytics for action recognition and anomaly detection, real-time inference on edge devices	**10**
UNIT 3	Text classification and sentiment analysis, sequence-to-sequence models for machine translation, text generation with RNNs and transformer architectures, question-answering systems and chatbots, contextual embeddings using BERT and GPT families	**8**
UNIT 4	Automatic speech recognition workflows, text-to-speech synthesis techniques, acoustic scene and emotion classification, music generation and enhancement, time-series forecasting with LSTM and temporal convolutional networks	**8**
UNIT 5	Generative adversarial networks for image and data synthesis, reinforcement learning for robotics and game AI, recommendation systems with deep embeddings, multimodal learning combining vision and language, ethics and fairness in deployed systems	**8**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**

1	Ian Goodfellow, Yoshua Bengio & Aaron Courville, *Deep Learning*, MIT Press	2016
2	François Chollet, *Deep Learning with Python*, Manning Publications	2017
3	Aurélien Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow*, O'Reilly Media	2019
4	Gökhan Tur & Rezvan Rahimi, *Deep Learning for NLP and Speech Recognition*, Springer	2019

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
Cy330: Security Assessment & Risk Analysis	**L**	**T**	**P**	**Computer Security**
	3	**0/1**	**2/0**	

Course Objectives:

1. To understand risk management frameworks and methodologies.
2. To identify vulnerabilities and assess threats in organizational systems.
3. To apply qualitative and quantitative risk analysis techniques.
4. To design mitigation strategies and compliance-driven risk management plans.
5. To evaluate legal, regulatory, and ethical aspects of risk assessment.

S. NO	**Course Outcomes (CO)**
CO1	Analyze organizational risks using frameworks like NIST RMF and ISO 27005.
CO2	Conduct vulnerability assessments using tools like Nessus and Metasploit.
CO3	Quantify risks using metrics (ALE, SLE, CVSS) and prioritize mitigation.
CO4	Develop compliance reports for standards like GDPR, HIPAA, and PCI-DSS.
CO5	Design incident response plans aligned with risk tolerance and business objectives.

S. NO	**Contents**	**Contact Hours**
UNIT 1	Fundamentals of Security Risk Management: Risk vs. threat vs. vulnerability, Frameworks: NIST RMF, ISO 27005, FAIR, Risk appetite, tolerance, and governance, Role of CISO and risk management teams	**10**
UNIT 2	Threat Identification & Vulnerability Assessment: Threat modeling methodologies (STRIDE, DREAD), Vulnerability scanning tools: Nessus, Qualys, OpenVAS, Penetration testing phases and reporting, Case study: SolarWinds breach analysis	**10**
UNIT 3	Risk Analysis & Quantification: Qualitative vs. quantitative risk analysis, Metrics: ALE, SLE, ARO, CVSS scoring, Scenario analysis and Monte Carlo simulations, Risk heat maps and prioritization matrices	**8**
UNIT 4	Compliance & Legal Aspects of Risk Management: Standards: GDPR, HIPAA, PCI-DSS, SOX, Auditing frameworks: COBIT, SOC 2, Legal implications of data breaches, Ethical considerations in risk disclosure	**8**
UNIT 5	**Risk Mitigation & Incident Response: Mitigation strategies: Avoidance, transfer, acceptance, Business continuity planning (BCP) and disaster recovery (DRP), Incident response lifecycle (NIST SP 800-61), Case study: Equifax breach response**	**6**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1.	Security Risk Assessment, Douglas Landoll, CRC Press	2020
2.	Threat Modeling: Designing for Security, Adam Shostack, Wiley	2014
3.	Risk Management Framework, James Broad, Syngress	2019
4.	NIST SP 800-30 Guide for Conducting Risk Assessments, NIST	2012
5.	PCI DSS: A Practical Guide, Brian Honan, IT Governance	2017

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY332: Human-Computer Interactions	**L**	**T**	**P**	
	3	**1/0**	**0/2**	

Course Objective: To provide a theoretical and practical understanding of human-machine interaction (HMI) design, including concepts of user centered and design thinking, usability, interfaces, rapid prototyping, and evaluation.

S. NO	Course Outcomes (CO)
CO1	Students would be able to evaluate user interfaces with human participants;;
CO2	To apply cognitive walkthroughs to simulate a user's experience of an interface
CO3	To be able to break a graphical user interface (GUI) activity sequence into the component actions
CO4	To be able to choose an appropriate interaction design for a given need; and, be able to implement simple GUIs.

S. NO	Contents	Contact Hours
UNIT 1	Introduction to HCI: goals in HCI; importance of design for usability; usability goals and metrics; historical perspective: machinery, computers, PCs and GUIs, and the Internet; different types of users; usability guidelines, principles, and theories of attention, perception, memory, and decision making.	**8**
UNIT 2	User experience and design: Different methods and frameworks of design; tools, practices, and patterns of design; social impact analysis; task decomposition; cognitive walkthroughs; expert reviews and heuristics; heuristic evaluation; guidelines of usability; active use evaluation; motion and time studies; GOMS keystroke-level models; human-study methodologies and techniques; survey and interview instruments; metaphors; storyboards; acceptance tests; ethical issues; design cases.	**12**
UNIT 3	Interaction Design: Direct manipulation; 2D devices and 3D interfaces; teleoperation and presence; augmented and virtual augmented reality; certain design patterns; fluid navigation; speech recognition and production; human language technology; traditional command languages; models of collaboration and contexts; deciding the appropriate interaction design.	**10**
UNIT 4	Design choices: Choices for user experience (animation, color, error handling, etc.); timing of user experience (system response time influence); help menus; information search; data types and data visualizations; grand challenges and future interfaces.	**12**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Ben Shneiderman, Catherine Plaisant, Maxine Cohen, Steven Jacobs, Niklas Elmqvist, and Nicholas Diakopoulos, Designing the User Interface: Strategies for Effective Human Computer Interaction, 6th Edition, Pearson, USA, 2016	2016
2	Dan R. Olsen Jr., Building Interactive Systems: Principles for Human-Computer Interaction, Cengage, 2010.	2010
3	Jeff Johnson, Designing with the Mind in Mind: Simple Guide to Understanding User Interface Design Guidelines, 3rd edition, Morgan Kaufmann, 2020.	2020

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY334: Data Science using Open Source Programming	**L**	**T**	**P**	Python Programming
	3	**0/1**	**2/0**	

Course Objective: 1. To gain technical skills for applying data science concepts to real-world applications.
2. To execute various data science processes including data wrangling, data exploration, and data visualization using Python.
3. To explore various packages and libraries in Python for data preprocessing, analysis, and visualization.

S. NO	Course Outcomes (CO)
CO1	Ability to apply data preprocessing and transformation techniques.
CO2	Ability to understand and implement different data visualization techniques.
CO3	Ability to understand and execute different data exploration techniques.
CO4	Ability to implement different real-world applications of data science.

S. NO	Contents	Contact Hours
UNIT 1	Mathematical Computing with Python (NumPy):Working with NumPy Arrays, Data Types, Array Creation, Indexing and Slicing, Numerical Operations on Arrays, Array Functions, Data Processing using Arrays, Loading and Saving Data, Saving an Array, Loading an Array, Numpy Random Numbers	**8**
UNIT 2	Data Manipulation with Pandas: Data Wrangling, Data Exploration, Cleaning Data, Filtering, Merging Data, Reshaping Data, Data Aggregation, Reading and Writing Files, Loading and Saving Data with Pandas	**8**
UNIT 3	Exploratory Data Analysis: Data exploration for univariate data. Outlier detection techniques. Descriptive statistics (mean, standard deviation etc.) for data exploration. Correlation statistics for data exploration. Data exploration for multivariate data.	**10**
UNIT 4	Data Visualization in Python, Understanding Data Visualization, Creating different Visualization like Bar Charts, Line Plot, Area Plots, Histograms, Pie Charts, Box Plots, Scatter Plots, Time Series plots, Figures and Subplots, Plotting Functions with Pandas, Use of multivariate visualization tools such as bar charts, bar plots, heat maps, bubble charts, run charts, and scatter plots.	**10**
UNIT 5	Descriptive Statistics, Basic of Grouping, ANOVA, Correlation, Polynomial Regression and Pipelines, R-squared and MSE for In-Sample Evaluation, Prediction and Decision Making.	**6**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Introducing data science, Davy Cielen, Arno D.B. Meysman, Mohamed Ali, 1st ed., Manning publications.	2016
2	The data science handbook, Field Cady, John Wiley & sons.	2017
3	Joshua N. Milligan, Learning Tableau 2020: Create effective data visualizations, build interactive visual analytics and transform your organization, Packt Publishing Limited, 4th/Latest Edition (2020).	2020
4	Wes McKinney, Python for Data Analysis: Data Wrangling with Pandas, NumPy, and IPython, O'Reilly Media, 2017	2017

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY336: Dependable Machine Learning	**L**	**T**	**P**	Fundamentals of Machine Learning
	3	**1/0**	**0/2**	

Course Objective: Equip students with the principles and practices needed to build, evaluate, and maintain trustworthy and reliable machine learning systems.

S. NO	Course Outcomes (CO)
CO1	Define key concepts of dependability in machine learning, including robustness, reliability, and interpretability.
CO2	Analyze adversarial vulnerabilities and apply defense techniques to improve model robustness.
CO3	Implement uncertainty quantification and calibration methods to assess model confidence.
CO4	Apply explainability, fairness, and monitoring frameworks to ensure ethical and dependable ML deployments.

S. NO	Contents	Contact Hours
UNIT 1	Definitions and taxonomy of dependable ML, reliability versus robustness versus safety, threat models and adversarial risk, trustworthiness metrics, overview of explainability and fairness, case studies of high-impact ML failures	**8**
UNIT 2	Adversarial attack methods (FGSM, PGD, CW), adversarial training and certified defenses, gradient masking pitfalls, randomized smoothing, provable robustness techniques, evaluation of robustness benchmarks	**10**
UNIT 3	Uncertainty quantification techniques including Bayesian neural networks, Monte Carlo dropout, deep ensembles and variational inference, calibration metrics (ECE, reliability diagrams), rejection and out-of-distribution detection methods	**8**
UNIT 4	Model interpretability methods: feature importance, LIME and SHAP explanations, saliency maps for vision models, counterfactual and prototype explanations, model-agnostic versus model-specific approaches, toolkits and libraries for explainability	**8**
UNIT 5	Fairness and bias detection metrics, differential privacy and data anonymization, continuous monitoring and drift detection, ML lifecycle governance and MLOps practices, ethical considerations and regulatory frameworks, guidelines for safe deployment and incident response	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Christoph Molnar, *Interpretable Machine Learning: A Guide for Making*	2019

	Black Box Models Explainable, Leanpub	
2	Clarence Chio & David Freeman, *Machine Learning and Security: Protecting Systems with Data and Algorithms*, O'Reilly Media	2018
3	Emmanuel Ameisen, *Building Machine Learning Powered Applications: Going from Idea to Product*, O'Reilly Media	2020
4	Kevin P. Murphy, *Probabilistic Machine Learning: An Introduction*, MIT Press	2022

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY338: Embedded Systems	**L**	**T**	**P**	
	3	**1/0**	**0/2**	

Course Objective:• To make students know the basic concept and architecture of embedded systems.
• Different design platforms used for an embedded system for IoT applications.
• To have knowledge about the IoT enabled technology.

S. NO	Course Outcomes (CO)
CO1	Introduction to significance of autonomus components and robotics
CO2	Study field transmitters
CO3	Compare Final control elements and accessories:
CO4	Understand Components of Industrial Robot

S. NO	Contents	Contact Hours
UNIT 1	Purpose and requirement specification, IoT level specification, Functional view specification, Operational view specification, Device and component integration, Pillars of Embedded IoT and Physical Devices: The internet of devices.	**8**
UNIT 2	Design of Embedded Systems: Common Sensors, Actuators, Embedded Processors, Memory Architectures, Software architecture.	**8**
UNIT 3	Inputs and Outputs: Digital Inputs and Outputs, Digital Inputs, Digital Outputs, BusIn, BusOut, and BusInOut, Analog Inputs and Outputs, Analog Inputs, Analog Outputs, Pulse Width Modulation (PWM), Accelerometer and Magnetometer, SD Card, Local File System (LPC1768).	**9**
UNIT 4	IoT Enabling Technologies: Communications, RFID and NFC (Near-Field Communication), Bluetooth Low Energy (BLE), LiFi, 6LowPAN, ZigBee, Z-Wave, LoRa, Protocols, HTTP, WebSocket, MQTT, CoAP, XMPP, Node-RED, Platforms, IBM Watson IoT—Bluemix, Eclipse IoT, AWS IoT, Microsoft Azure IoT Suite, Google Cloud IoT, ThingWorx, GE Predix, Xively, macchina.io, Carriots.	**9**

UNIT 5	Web of Things and Cloud of Things: Web of Things versus Internet of Things, Two Pillars of the Web, Architecture Standardization for WoT, Platform Middleware for WoT, Cloud of Things. IoT Physical Servers, Cloud Offerings and IoT Case Studies: Introduction to Cloud Storage Models, Communication API.	**8**
		8
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	1. RMD Sundaram Shriram K Vasudevan, Abhishek S Nagarajan, Internet of Things, John Wiley and Sons.	2023
2	2. Klaus Elk, “Embedded Software for the IoT”.	2024
3	3. Perry Xiao, “Designing Embedded Systems and the Internet of Things (IoT) with the ARM Mbed”.	2022
4	4. Elizabeth Gootman et. al, “Designing Connected Products”, Shroff Publisher/O’Reilly Publisher.	2023

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY340: Real Time Operating Systems	**L**	**T**	**P**	**Fundamentals of Operating Systems**
	3	**1/0**	**0/2**	

Course Objective: Enable students to understand, design, and evaluate operating system mechanisms tailored for real-time and embedded applications.

S. NO	Course Outcomes (CO)
CO1	Explain the distinguishing characteristics and classifications of real-time systems and their timing constraints.
CO2	Analyze and apply both static-priority and dynamic-priority scheduling algorithms to meet task deadlines.
CO3	Design synchronization and resource-sharing protocols to avoid priority inversion and ensure predictability.
CO4	Evaluate RTOS architectures and services, performing schedulability analysis and performance assessment for real-time applications.

S. NO	Contents	Contact Hours
UNIT 1	Definitions and classifications of real-time systems, characteristics of hard versus soft real-time, task types (periodic, aperiodic, sporadic), timing constraints and deadlines, real-time versus general-purpose OS trade-offs, representative real-world use cases in embedded and industrial domains	**8**
UNIT 2	Static-priority scheduling fundamentals, rate monotonic and deadline monotonic policies, utilization bounds and response-time analysis, dynamic-priority scheduling with earliest deadline first, scheduling aperiodic and sporadic tasks, handling scheduling overheads and context-switch costs	**10**
UNIT 3	Priority inversion and its impact, priority inheritance and priority ceiling protocols, mutual exclusion mechanisms in RTOS, semaphore versus spinlock trade-offs, interrupt handling strategies, deadlock avoidance techniques for real-time environments	**8**
UNIT 4	RTOS services and kernel architecture, task creation and management, inter-task communication (message queues, mailboxes), timers and clock management, memory allocation and fragmentation issues, device I/O and driver models, case studies of VxWorks, FreeRTOS, and RTLinux architectures	**8**
UNIT 5	Schedulability analysis techniques and tools, performance metrics (latency, jitter, throughput), mode changes and aperiodic server algorithms (polling server, sporadic server), fault tolerance and recovery in RTOS, real-time middleware frameworks, emerging trends in real-time IoT and virtualization	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	C. M. Krishna & Kang G. Shin, *Real-Time Systems*, McGraw Hill Education	2018
2	Jane W. S. Liu, *Real-Time Systems*, Pearson	2012
3	Giorgio C. Buttazzo, *Hard Real-Time Computing Systems: Predictable Scheduling Algorithms and Applications*, Springer	2011
4	Phillip A. Laplante, *Real-Time Systems Design and Analysis*, Springer	2012

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY342: COMPILER DESIGN	**L**	**T**	**P**	**Principles of computing**
	3	**0 /1**	**2/0**	

Course Objective: 1. To familiarize with the basic concepts of compiler design such as parsing and code optimization.
2.To design and implement different phases of a compiler.
3. To execute IR and target code generation and optimization.

S. NO	Course Outcomes (CO)
CO1	Ability to understand and describe the phases of a compiler
CO2	Ability to design and implement lexical analyzer
CO3	Ability to design and implement top-down or LL parsers
CO4	Ability to design and implement bottom-up or LR parsers
CO5	Ability to translate various expressions and statements.
CO6	Ability to execute IR and target code generation and optimization

S. NO	Contents	Contact Hours
UNIT 1	Introduction: Compiler flowchart - Phases of a compiler. Data Structure for Symbol Tables, representing scope information. Run time allocation: Stack versus Heap management.	**6**
UNIT 2	Lexical analysis: Input buffers and sentinels, Tokens and lexemes, Lexical categories, Implementation of Lexical Analyzer for an input string using regular expressions and NFA, Thompson algorithm, Subset construction, Automatic Lexical Analyzer Generator - Lex.	**8**
UNIT 3	Syntax analysis: Formal Grammars and their application to Syntax Analysis, BNF Notation, Derivation and Parse Trees, Top down parsing- elimination of left recursion, left factoring, recursive descent parsers, predictive parsers or LL(k) parsers. Bottom up parsing- LR Parsers, the canonical collection of LR(0) items, constructing SLR Parsing Tables, canonical LR Parsing tables and LALR parsing tables, An Automatic Parser Generator - YACC. Error detection and error recovery schemes.	**10**
UNIT 4	Syntax Directed Translation: Syntax Directed Definition (SDD), L-attributed and S-attributed SDD, Parse Trees, Annotated parse tree and Abstract Syntax Tree (AST), Syntax directed Translation Schemes, Postfix notation, Desktop calculator, Semantic analysis, Translation of Assignment Statements, Boolean expressions, Control Statements, Array references , Procedure Calls, Declarations and Case statements.	**8**
UNIT 5	Code generation and optimization: Three address code or IR code, Storage structures for IR code: Quadruple, Triple and Indirect Triple. Syntax directed translation for IR code generation. IR code optimization using Directed Acyclic Graph (DAG), Loop optimization, Global data flow analysis. Target code generation and optimization.	**10**

	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Aho, Lam, Sethi and Ullman, “Compilers: Principles, Techniques and Tools”, Second edition, Pearson Education.	2013
2	D.M.Dhamdhere, “Compiler Construction – Principles & Practice”, Macmillan, India.	2000
3	A. Appel, "Applied Intelligence for Medical Image Analysis", Cambridge university press.	2004
4	K.C. Loude, "Compiler construction: Principles and Practice", Course Technology Inc	1997
5	K.D. Cooper and L. Torczon, "Engineering a compiler", 3rd ed., Morgan Kaufmann.	2023

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY405: Social Network Analysis	**L**	**T**	**P**	Basic Programming Knowledge (Python), Discrete Mathematics (Graph theory), Data Structures and Algorithms, Introductory course in Probability/Statistics
	3	**0/1**	**2/0**	

Course Objective: To introduce students to the fundamental concepts, models, and analytical techniques used in studying and understanding social networks**.**

S. NO	Course Outcomes (CO)
CO1	Understand the key concepts and characteristics of social networks.
CO2	Apply graph theory and network metrics to analyze social structures.
CO3	Model real-world social networks and identify influential nodes and communities.
CO4	Utilize tools and algorithms to perform social network analysis on datasets
CO5	interpret and communicate insights from network data for decision-making

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Social Network Analysis:** Overview and history of social networks, Applications of social network analysis in various domains (Sociology, Marketing, Epidemiology, etc.), Basic concepts: Nodes, edges, degree, adjacency matrix, Types of networks: Directed vs Undirected, Weighted vs Unweighted, One-mode vs Two-mode, Key terminology: Ego networks, dyads, triads, cliques	**8**
UNIT 2	**Mathematical Foundations and Graph Theory:** Graph theory basics: paths, walks, cycles, connectivity, Types of graphs: Trees, bipartite graphs, small-world and scale-free networks, Network properties: Diameter, density, clustering coefficient, Hands-on: NetworkX basics in Python or Gephi introduction	**9**
UNIT 3	**Network Models and Community Detection:** Random graph models: Erdős–Rényi, Watts-Strogatz, Barabási–Albert, Homophily, preferential attachment, Community detection algorithms: Girvan-Newman, Louvain method, Modularity and quality of community detection, Case Study: Detecting communities in real social networks	**9**
UNIT 4	**Diffusion, Influence, and Link Prediction**: Information diffusion and cascade models, Influence maximization in networks, Threshold and independent cascade models, Link prediction algorithms and similarity metrics, Application: Viral marketing and influence analysis	**8**
UNIT 5	**Practical Applications and Tools:** Social media network analysis (Facebook, Twitter, LinkedIn), Analyzing hashtag and retweet networks, Ethics and privacy in social network analysis, Hands-on projects using tools: NetworkX, Gephi, SNAP, Neo4j, Mini-project / case study presentation	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Stanley Wasserman and Katherine Faust, *Social Network Analysis: Methods and Applications*, Cambridge University Press	1994
2	David Easley and Jon Kleinberg, *Networks, Crowds, and Markets*, Cambridge University Press	2010
3	Matthew O. Jackson, *Social and Economic Networks*, Princeton University Press	2010
4	Tutorials and documentation for NetworkX, Gephi	

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY407: Data Science & Big Data	**L**	**T**	**P**	Probability, Statistics, Linear Algebra
	3	**0/1**	**2/0**	

Course Objective: To familiarize with different types of data distributions, data preprocessing techniques, and big data analytics for processing and storing huge volumes of data.

S. NO	Course Outcomes (CO)
CO1	Ability to identify different types of data and data distributions.
CO2	Ability to understand and apply data preprocessing and data transformation techniques.
CO3	Ability to understand and explain the principles and applications of distributed file systems in big data systems.
CO4	Ability to configure Hadoop environment and execute Hadoop commands for large-scale data processing.
CO5	To understand working and commands of Hdoop.

S. NO	Contents	Contact Hours
UNIT 1	Introduction to data science: Basics of Probability & Statistics (Random Variables, Bayes's Theorem, Normal distribution, Central Limit Theorem). Defining data science, Recognizing different types of data, Data distributions. Data acquisition and data storage.	**9**
UNIT 2	Data pre-processing: Missing data problem, Outlier definition. Data cleaning, Data transformation or data wrangling procedures such as merging, ordering and aggregating	**8**
UNIT 3	Introduction – distributed file system – Big Data and its importance, Four Vs, Drivers for Big data, Big data analytics, Big data applications. Algorithms using map reduce.	**8**
UNIT 4	Big Data – Apache Hadoop & Hadoop EcoSystem – Moving Data in and out of Hadoop – Understanding inputs and outputs of MapReduce - Data Serialization.	**8**
UNIT 5	Hadoop Architecture, Hadoop Storage: HDFS, Common Hadoop Shell commands , Anatomy of File Write and Read, NameNode, Secondary NameNode, and DataNode, Hadoop MapReduce paradigm, Map and Reduce tasks, Job, Task trackers - Cluster Setup – SSH & Hadoop Configuration – HDFS Administering –Monitoring & Maintenance.	**9**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Data science from scratch, Joel Grus, 2nd ed., O'Reilly Media.	2019
2	Doing data science: Straight talk from the frontline, Cathy O'Neil, Rachel Scutt, O'Reilly Media.	2013
3	Python data science handbook, Jake VanderPlas, 2nd ed., O'Reilly Media.	2016
4	Introducing data science, Davy Cielen, Arno D.B. Meysman, Mohamed Ali, 1st ed., Manning publications.	2016
5	B. Lublinsky, K. T. Smith and A.Yakubovich, "Professional Hadoop Solutions", Wiley, ISBN: 9788126551071, 2015.	2015
6	T. White, "HADOOP: The definitive Guide" , O Reilly 2012.	2012
7	C. Eaton and D.deroos et al., "Understanding Big data ", McGraw Hill, 2012	2012

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY409: Basics of Control Systems	**L**	**T**	**P**	**Mathematics for Cyber Security, Introduction to Cyber Physical Systems**
	3	**0/1**	**2/0**	

Course Objective: To provide students with a comprehensive understanding of control system principles and their application in cyber-physical systems, focusing on system modeling, stability analysis, and control design for secure and reliable operation.

S. NO	Course Outcomes (CO)
CO1	Understand the fundamental concepts of control systems and their role in CPS.
CO2	Model and analyze dynamic systems using mathematical tools.
CO3	Design and evaluate control strategies for CPS stability and performance.
CO4	Apply control system principles to secure and optimize CPS applications.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Control Systems**- Definition and components of control systems- Open-loop vs. closed-loop control- Control systems in CPS: Examples (smart grids, robotics)- Basic control system terminology: Feedback, error, gain	8
UNIT 2	**System Modeling and Representation**- Differential equations and transfer functions- Block diagrams and signal flow graphs- State-space representation- Modeling CPS: Mechanical, electrical, and hybrid systems	9
UNIT 3	**Time and Frequency Domain Analysis**- Time response: Transient and steady-state analysis- Stability analysis: Routh-Hurwitz criterion- Frequency response: Bode and Nyquist plots- Root locus techniques	8
UNIT 4	**Control System Design**- PID controllers: Design and tuning- Compensator design: Lead, lag, lead-lag- Digital control systems: Z-transform, discrete-time systems- Control design for CPS: Robustness and performance	9
UNIT 5	**Control Systems in CPS Security**- Security challenges in control systems: Stuxnet case study- Secure control design: Fault detection and isolation- Resilience in control systems: Redundancy, fail-safe mechanisms- Emerging trends: AI-based control optimization	8
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Nise, N. S. *Control Systems Engineering*. Wiley.	2020
2	Dorf, R. C., & Bishop, R. H. *Modern Control Systems*. Pearson.	2016
3	Franklin, G. F., Powell, J. D., & Emami-Naeini, A. *Feedback Control of*	2019

	Dynamic Systems. Pearson.	

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY411: Security and Privacy of CPS	**L**	**T**	**P**	**Introduction to Cyber Physical Systems, Applied Cryptography**
	3	**0/1**	**2/0**	

Course Objective: To enable final-year students to design and implement security and privacy mechanisms for cyber-physical systems, addressing threats, ensuring data protection, and complying with regulatory standards in critical CPS applications.

S. NO	Course Outcomes (CO)
CO1	Understand security and privacy challenges in CPS environments.
CO2	Implement cryptographic and access control mechanisms for CPS security.
CO3	Design privacy-preserving techniques for CPS data handling.
CO4	Evaluate advanced security and privacy solutions for CPS in emerging technologies.

S. NO	Contents	Contact Hours
UNIT 1	**Fundamentals of CPS Security and Privacy**- CPS architecture and security requirements- Threat models: Physical, cyber, insider threats- Privacy concerns in CPS: Data leakage, user tracking- Standards: NIST SP 800-82, IEC 62443	8
UNIT 2	**Cryptographic Mechanisms for CPS**- Lightweight cryptography: AES, SPECK, SIMON- Secure communication: TLS, DTLS for CPS- Key management: PKI, TPM-based solutions- Homomorphic encryption for CPS data	9
UNIT 3	**Access Control and Authentication**- Role-based and attribute-based access control- Authentication mechanisms: MFA, biometrics- Zero-trust architecture for CPS- Secure device identity: X.509 certificates	8
UNIT 4	**Privacy-Preserving Techniques**- Differential privacy in CPS data analytics- Anonymization and data minimization- Privacy impact assessments (PIA) for CPS- Compliance: GDPR, CCPA, HIPAA for CPS	9
UNIT 5	**Advanced Security and Privacy Trends**- Blockchain for CPS: Secure data sharing- AI-driven security: Anomaly detection, threat prediction- 5G and IoT privacy challenges- Case studies: CPS privacy breaches	8
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Weerakkody, S., Ozel, O., Mo, Y., & Sinopoli, B. *Resilient Control in Cyber-Physical Systems*. Wiley.	2019
2	Dwork, C., & Roth, A. *The Algorithmic Foundations of Differential Privacy*.	2014

	Now Publishers.	

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY413: Adversarial Machine Learning	**L**	**T**	**P**	Fundamentals of Machine Learning
	3	**1/0**	**0/2**	

Course Objective: Equip students with the theory and practice needed to understand, generate, and defend against adversarial attacks on machine learning models.

S. NO	Course Outcomes (CO)
CO1	Describe the threat models, attack surfaces, and taxonomy of adversarial attacks in ML.
CO2	Craft and evaluate common evasion and poisoning attacks against supervised models.
CO3	Implement and compare defensive strategies including empirical and certified robustness methods.
CO4	Apply adversarial techniques and defenses in domains such as computer vision, NLP, and federated learning.

S. NO	Contents	Contact Hours
UNIT 1	Introduction to adversarial machine learning including definitions and motivations, threat models and attacker capabilities, taxonomy of adversarial attacks covering evasion versus poisoning, formulation of adversarial examples with norm constraints, evaluation metrics for robustness	**8**
UNIT 2	Evasion attacks on classifiers and neural networks including FGSM, PGD, DeepFool, CW method, black-box and transferability attacks, decision-based and score-based attack strategies, adaptive attacks and gradient-free optimization	**10**
UNIT 3	Empirical defenses such as adversarial training, defensive distillation, input transformations and feature squeezing, certified defenses including randomized smoothing and convex relaxation, pitfalls like gradient masking, benchmarking robustness on standard datasets	**8**
UNIT 4	Data-poisoning and backdoor attacks including label flipping, clean-label poisoning, gradient matching methods, backdoor trigger design and detection, data sanitization and robust learning algorithms, differential privacy as a defense mechanism	**8**
UNIT 5	Adversarial robustness beyond vision: attacks and defenses in NLP and speech, adversarial reinforcement learning, federated learning vulnerabilities and secure aggregation, certified robustness for structured data, emerging research challenges and future directions	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Battista Biggio & Fabio Roli (eds.), *Adversarial Machine Learning*,	2018

	Springer	
2	Clarence Chio & David Freeman, *Machine Learning and Security: Protecting Systems with Data and Algorithms*, O'Reilly Media	2018
3	Rohan Chopra, *Hands-On Adversarial Machine Learning with Python*, Packt Publishing	2019
4	Yevgeniy Vorobeychik & Murat Kantarcioglu (eds.), *Adversarial Machine Learning*, Morgan & Claypool Publishers	2020

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY415: Multimedia Forensics	**L**	**T**	**P**	Digital Forensics and Image Processing
	3	**1/0**	**0/2**	

Course Objective: The course aims to provide a comprehensive understanding of forensic techniques for analyzing multimedia data including images, videos, and audio. It covers the principles of detecting tampering, source identification, and authenticity validation using state-of-the-art algorithms and tools.

S. NO	Course Outcomes (CO)
CO1	Understand fundamental principles and challenges of multimedia forensics.
CO2	Apply forensic techniques for detecting digital media tampering.
CO3	Analyze multimedia data for source identification and authentication.
CO4	Utilize open-source tools and software for forensic analysis of images, audio, and video.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Multimedia Forensics**: Overview of digital forensics, types of digital media, characteristics of multimedia files, forensic challenges in multimedia.	**8**
UNIT 2	**Image Forensics**: Image acquisition and compression, photo manipulation detection, copy-move and splicing detection, JPEG artifacts, sensor pattern noise, PRNU-based source identification.	**9**
UNIT 3	**Video Forensics**: Video encoding and formats, frame-level analysis, video tampering techniques, detection of frame insertion/deletion, double compression analysis.	**9**
UNIT 4	**Audio Forensics**: Basics of audio signal processing, audio compression formats, forgery detection in audio, speaker verification, steganography and watermarking in audio.	**8**
UNIT 5	**Tools, Techniques, and Case Studies**: Overview of forensic tools (Amped Authenticate, FotoForensics, Triage tools), real-world case studies, legal and ethical issues in multimedia forensics.	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	H. Farid, *Photo Forensics*, MIT Press	2013
2	A. Piva, *Multimedia Forensics and Security*, Springer	2016
3	S. Lyu, *Digital Image Forensics*, Cambridge University Press	2020

4	T. Böhme, M. Kirchner, *Multimedia Forensics – Principles and Practice*, Springer	2021

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY417: Block chain Security & Performance	**L**	**T**	**P**	Blockchain Platform and Use Cases
	3	**1/0**	**0/2**	

Course Objective:

S. NO	**Course Outcomes (CO)**
CO1	Equip students with the knowledge to assess and enhance the security and performance of blockchain systems.
CO2	Evaluate consensus-level attacks and defense mechanisms in proof-based systems.
CO3	Apply techniques for securing smart contracts and mitigating on-chain risks.
CO4	Measure and optimize blockchain performance through scalability and benchmarking strategies.

S. NO	**Contents**	**Contact Hours**
UNIT 1	Cryptographic primitives in blockchains, threat models and security properties, adversary capabilities and attack surfaces, permissionless versus permissioned security assumptions, regulatory and compliance considerations	**8**
UNIT 2	Consensus-level attacks and defenses including 51% attacks, selfish mining, nothing-at-stake issues, long-range forks, hybrid consensus protocols, network partition and eclipse attacks, mitigation via checkpointing and finality gadgets	**10**
UNIT 3	Smart contract vulnerabilities such as reentrancy, integer overflow/underflow, front-running and denial-of-service, attack case studies, static and dynamic analysis tools, formal verification approaches, security testing frameworks	**8**
UNIT 4	P2P network security and privacy challenges, eclipse and Sybil attacks, DDoS protection mechanisms, transaction propagation optimizations, privacy techniques including mixers and zero-knowledge proofs	**8**
UNIT 5	Performance metrics for throughput and latency, scalability solutions such as sharding and sidechains, Layer-2 protocols (state channels, rollups), benchmarking methodologies, trade-offs between security and performance	**8**
	TOTAL	**42**

REFERENCES

S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**

1	Imran Bashir, *Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained*, Packt Publishing	2017
2	Andreas M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*, O'Reilly Media	2017
3	Daniel Drescher, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*, Apress	2017
4	Andreas M. Antonopoulos & Gavin Wood, *Mastering Ethereum: Building Smart Contracts and DApps*, O'Reilly Media	2018

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY419: Block Chain & Fintech	**L**	**T**	**P**	**Blockchain Platform and Use Cases**
	3	**1/0**	**0/2**	

Course Objective: Introduce students to the convergence of blockchain technology and financial services, enabling design and evaluation of blockchain-based fintech solutions.

S. NO	Course Outcomes (CO)
CO1	Describe key fintech concepts and the role of blockchain in modern financial ecosystems.
CO2	Analyze blockchain-driven payment, remittance, and asset-tokenization platforms.
CO3	Design and prototype decentralized finance (DeFi) applications and digital asset offerings.
CO4	Assess regulatory, security, and performance considerations in blockchain-enabled financial services.

S. NO	Contents	Contact Hours
UNIT 1	Evolution of financial technology ecosystem, key fintech services (payments, lending, wealth management, insurtech), blockchain fundamentals and distributed ledger properties, decentralization and trust models, smart contracts in finance, comparison of blockchain versus traditional financial ledgers	**8**
UNIT 2	Blockchain-based payment systems and digital wallets, cross-border remittance and settlement solutions, stablecoin architectures (fiat-backed, crypto-collateralized, algorithmic), central bank digital currencies overview, peer-to-peer lending and crowdfunding platforms, KYC/AML frameworks in blockchain fintech	**10**
UNIT 3	Decentralized finance primitives: lending and borrowing protocols, decentralized exchanges and automated market makers, yield farming and liquidity mining, derivatives and synthetic assets, on-chain governance and voting mechanisms, risk management strategies in DeFi	**8**
UNIT 4	Tokenization of real-world assets and security tokens, initial coin offerings (ICOs) and security token offerings (STOs), regulatory compliance and legal considerations for tokenized securities, digital identity solutions in fintech, custody and settlement infrastructures for digital assets	**8**
UNIT 5	Security and privacy challenges in blockchain fintech, cryptographic privacy techniques and audit frameworks, scalability and throughput optimization for high-volume transactions, integration with legacy banking systems and APIs, performance benchmarking methodologies, emerging trends in Open Banking and API-driven finance	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Alex Tapscott & Don Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World*, Portfolio Penguin	2016
2	Bernardo Nicoletti, *The Future of FinTech: Integrating Finance and Technology in Financial Services*, Palgrave Macmillan	2017
3	Paolo Sironi, *FinTech Innovation: From Robo-Advisors to Goal-Based Investing and Gamification*, Wiley	2016
4	Dirk A. Zetzsche, Ross P. Buckley & Douglas W. Arner, *The Rise of FinTech: Risks and Opportunities for the Financial Sector*, Cambridge University Press	2020

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY421: Intrusion Detection and Information Warfare	**L**	**T**	**P**	**Basic of cyber security and Cryptography**
	3	**0/1**	**2/0**	

Course Objective: To provide students with a comprehensive understanding of the fundamental principles and techniques in cyber intrusion detection and information warfare, including types of cyber intrusions, detection mechanisms, IDS configuration and management.

S. NO	Course Outcomes (CO)
CO1	Analyze intrusion detection techniques and systems.
CO2	Identify and assess cyber threats and vulnerabilities.
CO3	Implement IDS and respond to attacks.
CO4	Understand key strategies in information warfare.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Intrusion Detection:** Overview of Information Security, Types of Intrusions and Attack Vectors, Intrusion Detection Systems: NIDS vs HIDS, Signature-based vs Anomaly-based Detection.	**8**
UNIT 2	**IDS Architecture and Implementation:** Components of IDS, Snort and Suricata IDS Tools, Placement of IDS in Network, Logging, Alerts and Response Mechanisms.	**8**
UNIT 3	**Intrusion Prevention and Response:** Intrusion Prevention Systems (IPS), Real-Time Attack Detection, Incident Response Planning, Case Studies of IDS Applications.	**9**
UNIT 4	**Information Warfare Concepts:** Definition and Evolution of Information Warfare, Cyber Espionage, Cyber Terrorism, and Cyber Conflicts, Psychological Operations and Disinformation Campaigns, Role of Governments and Cyber Armies.	**9**
UNIT 5	**Legal, Ethical and Strategic Issues:** Cyber Laws and Regulations in India, Digital Forensics and Evidence Handling, Ethical Hacking and Professional Conduct, National and Global Security Frameworks.	**8**
	TOTAL	**42**

REFERENCES

S. No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Northcutt, S. & Novak, J. (2002). *Network Intrusion Detection*. New Riders Publishing.	2002
2	Bace, R. (2000). *Intrusion Detection*. Macmillan Technical Publishing.	2000

3	Andress, J. (2014). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Syngress.	2014
4	Vacca, J. R. (2009). *Computer and Information Security Handbook*. Elsevier.	2009

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY423: Embedded Systems for IoT	**L**	**T**	**P**	**Micro-Processor and Controller, Internet of Things and Security**
	3	**0/1**	**2/0**	

Course Objective: To prepare students to design and secure embedded systems for IoT applications, addressing resource constraints, secure communication, and advanced IoT security challenges, with hands-on practice.

S. NO	Course Outcomes (CO)
CO1	Understand embedded systems and IoT architectures and security challenges.
CO2	Design secure embedded systems with lightweight cryptography.
CO3	Implement IoT device security, including authentication and OTA updates.
CO4	Evaluate advanced IoT security solutions, including blockchain and AI.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Embedded Systems and IoT**- Embedded systems: Microcontrollers, sensors- IoT architecture: Device, gateway, cloud- Protocols: MQTT, CoAP, HTTP/REST- Security challenges: Resource constraints	8
UNIT 2	**Secure Embedded System Design**- Secure boot and firmware integrity- Lightweight cryptography: AES, ChaCha- Secure communication: DTLS, TLS for IoT- Embedded OS: FreeRTOS, Zephyr	9
UNIT 3	**IoT Device Security**- Device authentication: X.509, TPM attestation- Secure OTA updates: Code signing- Physical security: Tamper resistance- Standards: NIST IR 8259, ETSI EN 303 645	8
UNIT 4	**IoT Network Security**- Network protocols: 6LoWPAN, Zigbee- Intrusion detection for IoT networks- Secure gateways and edge devices- Network segmentation for IoT	9
UNIT 5	**Advanced IoT Security Trends**- Blockchain for IoT: Decentralized identity- AI-based security: Anomaly detection- 5G-enabled IoT security- Case studies: Mirai, IoT botnets	8
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Marwedel, P. *Embedded System Design: Embedded Systems Foundations of Cyber-Physical Systems, and the Internet of Things*.	2021

	Springer.	
2	Molloy, D. *Exploring Raspberry Pi: Interfacing to the Real World with Embedded Linux*. Wiley.	2020
3	Russell, B., & Van Duren, D. *Practical Internet of Things Security*. Packt Publishing.	2019

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY425: Scientific and Engineering Data Visualization	**L**	**T**	**P**	**Programming, Statistics and Visualization**
	3	**0/1**	**2/0**	

Course Objective: Purpose of this course is to introduce data science techniques to enhance the decision-making strategies through analysis, interpretation, and management of data. It also aims to provide overview of different data visualization techniques for efficient and effective data representation.

S. NO	Course Outcomes (CO)
CO1	Identify the data types, the relationship between data, and the visualization techniques for data.
CO2	To be able to apply the concept of probability, sampling, distribution, and estimation in solving real time problems.
CO3	To be able to implement various data visualization techniques and draw basic and advanced graphics shapes using SVG and Canvas.
CO4	Apply appropriate data visualization techniques on multiple data files and draw different charts.
CO5	Identify the data types, the relationship between data, and the visualization techniques for data.

S. NO	Contents	Contact Hours
UNIT 1	Introduction to Business Analytics:Why Analytics, Business Analytics: The Science of Data-Driven Decision Making, Descriptive Analytics, Predictive Analytics, Prescriptive Analytics, Big Data Analytics, Web and Social Media Analytics. Types of Data Measurement Scales, Percentile, Decile and Quartile, Measures of Variation, Measures of Shape − Skewness and Kurtosis.	**08**
UNIT 2	Introduction to Probability: Introduction to Probability Theory, Probability Theory – Terminology, Fundamental Concepts in Probability – Axioms of Probability, Application of Simple Probability, Bayes' Theorem, Random Variables, Probability Mass Function (PMF) and Cumulative Distribution Function (CDF) of a Discrete Random Variable, Binomial Distribution, Poisson Distribution, Geometric Distribution, Probability Density Function (PDF) and Cumulative Distribution Function (CDF) of a Continuous Random Variable, Uniform Distribution, Exponential Distribution, Chi-Square Distribution, Student's t- Distribution, F-Distribution.	**10**
UNIT 3	Introduction to Sampling, Population Parameters and Sample Statistic, Sampling, Probabilistic Sampling, Non-Probabilistic Sampling, Sampling Distribution, Central Limit Theorem (CLT),Introduction to Data Visualization: Acquiring and Visualizing Data, Simultaneous acquisition and visualization, Applications of Data Visualization, Keys factors of Data Visualization (Control of Presentation, Faster and Better JavaScript processing, Rise of HTML5, Lowering the implementation Bar) Exploring the Visual Data Spectrum: charting Primitives (Data Points, Line Charts, Bar Charts, Pie Charts, Area Charts), Exploring	**08**

	advanced Visualizations (Candlestick Charts, Bubble Charts, Surface Charts, Map Charts, Infographics). Making use of HTML5 CANVAS, Integrating SVG	
UNIT 4	Tabular Data Visualization: Tables: Reading Data from Standard text files (.txt, .csv, XML), Outputting Basic Table Data (Building a table, Using Semantic Table, Configuring the columns), Assuring Maximum readability (Styling your table, Increasing readability, Adding dynamic Highlighting), Including computations, Using data tables library.	**08**
UNIT 5	Visualizing data Programmatically: Creating HTML5 CANVAS Charts (HTML5 Canvas basics, A Simple Column Chart, Animations), Starting with Google charts (Google Charts API Basics, A Basic bar chart, A basic Pie chart).	**08**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	U.Dinesh Kumar, Business Analytics, Wiley, Indi	2021
2	V.K. Jain, Data Science & Analytics, Khanna Book Publishing, New Delhi	2018
3	Data Science For Dummies by Lillian Pierson, Jake Porwa	2017
4	Jon Raasch, Graham Murray, Vadim Ogievetsky, Joseph Lowery, "JavaScript and jQuery for Data Analysis and Visualization", WROX	2014
5	Ben Fry, "Visualizing data: Exploring and explaining data with the processing environment", O'Reilly, 2008.	2008

B.Tech. Information Technology (Cyber Security)

Course code: Course Title	**Course Structure**			**Pre-Requisite**
C427: Web Server Management	**L**	**T**	**P**	**Web Application Security, Network Security**
	3	**0/1**	**2/0**	

Course Objective: To train students in managing and securing web servers against advanced threats, focusing on secure configuration, attack mitigation, and modern cloud and containerized environments, with practical skills.

S. NO	**Course Outcomes (CO)**
CO1	Understand web server security principles and threat landscapes.
CO2	Configure secure web servers with SSL/TLS and WAFs.
CO3	Mitigate web server attacks through patching and session security.
CO4	Implement advanced security for cloud and containerized web servers.

S. NO	Contents	Contact Hours
UNIT 1	**Web Server Security Fundamentals**- Web server architecture: Apache, Nginx, IIS- Threats: DDoS, SQL injection, XSS- Standards: OWASP Top 10, CIS Benchmarks- Hardening principles: Least privilege	8
UNIT 2	**Secure Configuration**- Secure installation: File permissions, roles- SSL/TLS: Certificates, HSTS- Web Application Firewalls: ModSecurity- Logging and monitoring setup	9
UNIT 3	**Attack Mitigation Techniques**- Common attacks: Command injection, session hijacking- Input sanitization and secure session management- Patching: CVEs, automated updates- Backup and recovery strategies	8
UNIT 4	**Cloud and Container Security**- Cloud web servers: AWS, Azure, GCP- Container security: Docker, Kubernetes- Orchestration security: Pod security policies- Serverless architecture security	9
UNIT 5	**Advanced Web Server Security Trends**- API security: Rate limiting, gateways- Web3 and decentralized hosting- AI-driven threat detection- Compliance: PCI-DSS, SOC 2	8
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Garber, L., & Kocher, P. *Web Security, Privacy & Commerce*. O'Reilly Media.	2021
2	Stuttard, D., & Pinto, M. *The Web Application Hacker's Handbook*. Wiley.	2023

B.Tech. Information Technology (Cyber Security)

Course code: Course Title	Course Structure			Pre-Requisite
CY429: DATA WAREHOUSING AND DATA MINING	**L**	**T**	**P**	**Probability theory, Database management systems**
	3	**1/0**	**0/2**	

Course Objective: 1. To familiarize with the concepts of data mining, data storage, data pipeline and data integration.
2.To analyze data using classification, clustering, feature selection, association rule mining and itemset mining.
3. To understand and explore data warehousing architectures and data lakes

S. NO	Course Outcomes (CO)
CO1	Ability to understand and describe data mining, data storage, data pipeline and data integration concepts.

CO2	Ability to understand and implement classification and clustering algorithms for analyzing linearly and non-linearly separable data.
CO3	Ability to understand and implement feature selection algorithms for data reduction.
CO4	Ability to understand and explore patterns and dependencies in data using association-rule mining and itemset-mining.
CO5	Ability to understand, explore and describe data warehousing architectures and data lakes.

S. NO	**Contents**	**Contact Hours**
UNIT 1	Advanced data analytics and machine learning: Cluster Analysis, Types of Data in Cluster Analysis, Partitioning methods, Hierarchical Methods. Classification techniques for linearly separable and non-linearly separable data- Linear Discriminant Analysis and Support Vector Machine. Feature Ranking and Feature Selection Algorithms.	**10**
UNIT 2	Frequent itemset mining and association rule mining: Associations and correlations- basic concepts, efficient and scalable frequent item sets mining methods, mining various kinds of association rules, constraint-based association mining	**8**
UNIT 3	Introduction to data engineering: Storing data, Data loading, Data transformation, Data structures, SQL and NoSQL databases, Database normalization, Data cubes, Snowflake scheme, Data warehouses, Data lakes, Data Marts, Metadata in Data Warehouse, Data pipeline, Data integration- Extract, Transform, and Load (ETL) processes for integrating data from multiple sources.	**8**
UNIT 4	Data warehousing: Planning Your Data Warehouse, The Data Warehouse Project, Architectural Components: Understanding Data Warehouse Architecture, Infrastructure Supporting Architecture, Collection of Tools. Indexing the data warehouse, performance enhancement techniques.	**8**
UNIT 5	Data design and data preparation: From Requirements to Data Design, The STAR Schema, STAR Schema Keys, Advantages of the STAR Schema. Data modeling for data warehouses. Scalable data engineering solutions - handling massive datasets. Online Analytical Processing models, Online Transaction Processing models.	**8**
	TOTAL	**42**

REFERENCES

S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Data Mining: Concepts and Techniques, Jiawei Han, Micheline Kamber and Jian Pei, 3rd ed., Morgan Kaufmann	2022
2	Mining Introductory and Advanced Topics, M.H. Dunham, Pearson Education.	2002
3	Data mining, Pieter Adriaans, Pearson Education.	1996
4	Data warehousing in the real world for building decision support systems, Sam Anahory, Pearson Education.	1997

5	The Data Warehouse Lifecycle toolkit, Ralph Kimball, John Wiley.	1996
6	Oracle8 data warehousing, Michael Corey, Tata McGraw Hill.	1998
7	Data Warehousing Fundamentals, Paulraj Ponniah, John Wiley.	2001

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY431: Steganography and Digital Watermarking	**L**	**T**	**P**	
	3	**0/1**	**2/0**	

Course Objective: 1) To provide students with a fundamental understanding of steganography and digital watermarking, including data hiding techniques, algorithm evaluation, and practical implementation using software tools.

S. NO	Course Outcomes (CO)
CO1	Describe the theoretical foundations of steganography and watermarking.
CO2	Apply classical and modern data hiding techniques.
CO3	Evaluate the performance and security of embedding methods.
CO4	Design secure and robust information hiding schemes.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Information Hiding:** Overview of Information Security, Steganography vs Cryptography vs Watermarking, Applications and Challenges, Historical Background and Evolution.	**8**
UNIT 2	**Steganography Techniques:** Types of Steganography (Text, Image, Audio, Video), Spatial Domain Techniques (LSB Insertion), Frequency Domain Techniques (DCT, DWT), Steganalysis and Attacks.	**8**
UNIT 3	**Digital Watermarking:** Fundamentals of Digital Watermarking, Perceptual Models and Robustness, Invisible vs Visible Watermarking, Fragile and Robust Watermarking.	**8**
UNIT 4	**Algorithms and Implementations:** Algorithms: Patchwork, Spread Spectrum, Quantization Index Modulation, Use of Tools and Libraries (OpenStego, MATLAB, Python Libraries), Evaluation Metrics: PSNR, NC, BER, Security Analysis.	**9**
UNIT 5	**Legal, Ethical, and Research Perspectives:** Legal Issues in Digital Media Protection, Ethical Use of Steganography, Case Studies and Research Trends, Intellectual Property Rights and DRM.	**9**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Katzenbeisser, S., & Petitcolas, F. A. (2000). *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House.	2000
2	Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2007). *Digital Watermarking and Steganography* (2nd ed.). Morgan Kaufmann.	2007
3	Johnson, N. F., Duric, Z., & Jajodia, S. (2001). *Information Hiding:	2001

	Steganography and Watermarking - Attacks and Countermeasures*. Springer.	

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY433 Smart Sensors for Healthcare	**L**	**T**	**P**	**IOT**
	3	**1/0**	**0/2**	

Course Objective:

S. NO	Course Outcomes (CO)
CO1	To understand the fundamental principles of smart sensors and their role in healthcare monitoring systems.
CO2	To explore various types of biomedical sensors and their applications in physiological signal acquisition
CO3	To integrate sensor data with communication systems for IoT-enabled healthcare solutions.
CO4	To evaluate the design and implementation of wearable and remote health monitoring devices.

S. NO	Contents	Contact Hours
UNIT 1	UNIT 1 Introduction to Smart Sensors and Healthcare Applications: - Need for smart sensing in healthcare - Overview of sensor-based health monitoring systems - Classification and characteristics of smart sensors - Recent trends in healthcare sensor technology	**9**
UNIT 2	UNIT 2 Physiological Signal Acquisition and Sensors: - Bio-potential electrodes: ECG, EMG, EEG sensors - Temperature, blood pressure, pulse oximetry, and respiration sensors - Biochemical and optical sensors - Design considerations for biomedical sensors	**10**
UNIT 3	UNIT 3 Sensor Signal Conditioning and Processing: - Signal filtering and amplification - A/D and D/A conversion - Wireless transmission of sensor data - Embedded systems and microcontrollers in smart sensing	**10**
UNIT 4	UNIT 4 Integration with IoT and Communication Protocols: - IoT architecture for healthcare - Sensor networks and data aggregation - Communication technologies: Bluetooth, Zigbee, Wi-Fi, LoRa - Security and privacy issues in medical data	**7**
UNIT 5	UNIT 5 Wearables and Remote Health Monitoring:	**6**

	- Design of wearable sensor systems - Case studies: smart watches, glucose monitors, fitness trackers - Energy management and power optimization - Future trends: AI in sensor-based diagnostics	
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Rangaraj M. Rangayyan, Biomedical Signal Analysis, Wiley-IEEE Press (2015)	2015
2	John G. Webster, Bioinstrumentation, Wiley (2009)	2009
3	Edward Sazonov and Michael R. Neuman, Wearable Sensors:Fundamentals, Implementation and Applications, Academic Press (2020)	2020
4	Waltenegus Dargie, Christian Poellabauer, Fundamentals of Wireless Sensor Networks: Theory and Practice, Wiley (2010)	2010
5	Yang Xiao, Body Area Networks and Implications for Healthcare Systems, IGI Global (2011)	2011

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY435: CPS for Internal and External Security	**L**	**T**	**P**	**Introduction to Cyber Physical Systems, System Security**
	3	**0/1**	**2/0**	

Course Objective: To equip students with expertise in securing cyber-physical systems against internal and external threats, focusing on insider threat mitigation, perimeter security, and advanced techniques for critical infrastructure protection.

S. NO	Course Outcomes (CO)
CO1	Understand CPS security frameworks and threat models.
CO2	Implement internal security measures, including insider threat detection.
CO3	Design external security solutions with zero-trust and incident response.
CO4	Evaluate advanced CPS security for critical infrastructure and emerging tech.

S. NO	Contents	Contact Hours
UNIT 1	**CPS Security Fundamentals**- CPS components: Controllers, networks- Internal vs. external threats- Security frameworks: NIST CPS, IEC 62443- Threat modeling: STRIDE, attack surfaces	8
UNIT 2	**Internal Security Mechanisms**- Insider threats: RBAC, behavior monitoring- Data security: Encryption, integrity checks- Network segmentation: Micro-segmentation- Anomaly detection: ML-based approaches	9
UNIT 3	**External Security Measures**- External threats: Malware, APTs- Perimeter security: Firewalls, IDS/IPS- Secure remote access: Zero-trust, MFA- Incident response: Containment, recovery	8
UNIT 4	**Critical Infrastructure Protection**- CPS in critical sectors: Energy, healthcare- Supply chain security: Vendor risk management- Resilience: Redundancy, failover systems- Case studies: Stuxnet, grid attacks	9
UNIT 5	**Advanced CPS Security Trends**- Blockchain for CPS: Decentralized trust- 5G-enabled CPS security- Quantum-resistant security for CPS- AI-driven threat detection	8
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Song, D., & Shi, E. *Cyber-Physical Systems Security*. Springer.	2020

2	Rajkumar, R., & Lee, I. *Cyber-Physical Systems: Foundations, Principles, and Applications*. Academic Press.	2022
3	Wolf, M., & Serpanos, D. *Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems*. Springer.	2019

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY437 Game Theory	**L**	**T**	**P**	Basic Probability and Linear Algebra (or equivalent)
	3	**0/1**	**2/0**	

Course Objective:

·To introduce students to the fundamental concepts of game theory.
· To equip students with the tools to analyze strategic interactions between rational agents.
· To apply game theory to problems in cyber security and related fields.
· To develop logical thinking and problem-solving skills in strategic settings.

S. NO	Course Outcomes (CO)
CO1	Understand and apply the basic concepts of game theory, including players, strategies, and payoffs.
CO2	Analyze and solve various types of games, such as static and dynamic games, with complete and incomplete information.
CO3	Apply game theory concepts to model and analyze strategic interactions in cyber security scenarios.
CO4	Evaluate and compare different solution concepts, such as Nash equilibrium and subgame perfect equilibrium.

S. NO	Contents	Contact Hours
UNIT 1	Introduction to Game Theory: What is Game Theory? , Basic concepts: players, strategies, payoffs, rationality. Examples of games: Prisoner's Dilemma, Battle of the Sexes, Matching Pennies, Types of games: cooperative vs. non-cooperative, static vs. dynamic, complete vs. incomplete information.	**8**
UNIT 2	Static Games with Complete Information: Normal form representation of games. Dominant strategies and iterated elimination of dominated strategies. Nash equilibrium: definition, existence, and uniqueness. Applications: Cournot and Bertrand competition, public goods.	**10**
UNIT 3	Dynamic Games with Complete Information: Extensive form representation of games. Subgame perfect equilibrium. Backward induction. Applications: Stackelberg competition, bargaining games.	**8**
UNIT 4	Static Games with Incomplete Information: Bayesian games: players' types and beliefs. Bayesian Nash equilibrium. Mechanism design: auctions. Applications: Cyber security auctions, intrusion detection games.	**8**
UNIT 5	Dynamic Games with Incomplete Information: Perfect Bayesian equilibrium. Signaling games. Applications to Cyber Security: Network security games, Security investment strategies, Adversarial machine learning, Cryptography and game theory.	**8**

	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	“Game Theory: Analysis of Conflict” by Roger B. Myerson, Harvard University Press	1991
2	“Game Theory and Mechanism Design” by Vijay Krishna, Academic Press	2002
3	"Algorithmic Game Theory" by Noam Nisan, Tim Roughgarden, Eva Tardos, and Vijay V. Vazirani, Cambridge University Press	2007
4	“Strategy: An Introduction to Game Theory” by Joel Watson, W.W. Norton & Company	2013

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY439 Information Theory and Coding	**L**	**T**	**P**	Probability Theory, Linear Algebra
	3	**0/1**	**2/0**	

Course Objective:

1. To introduce the fundamental concepts of information theory and coding.
2. To equip students with the mathematical tools for analyzing and quantifying information.
3. To enable students to understand and design efficient coding schemes for data compression and error correction.
4. To explore applications of information theory and coding in cyber security.

S. NO	Course Outcomes (CO)
CO1	Understand the fundamental concepts of information theory, including entropy, mutual information, and channel capacity.
CO2	Apply source coding techniques for data compression, including Huffman coding and arithmetic coding.
CO3	Apply channel coding techniques for error detection and correction, including linear block codes and convolutional codes.
CO4	Analyze the performance of different coding schemes and their applications in cyber security.

S. NO	Contents	Contact Hours
UNIT 1	Introduction to Information Theory: Entropy, Joint Entropy, and Conditional Entropy, Mutual Information and its properties, Kullback-Leibler Divergence, Relationship between entropy and mutual information, Information Rate, Channel Capacity, Redundancy	**8**
UNIT 2	Source Coding: Source coding theorem, Lossless compression: Huffman coding, Arithmetic coding, Lempel-Ziv-Welch (LZW) coding, Lossy compression: Quantization, Rate-distortion theory, Applications of source coding	**8**
UNIT 3	Channel Coding: Channel coding theorem, Linear Block Codes: Generator and parity-check matrices, encoding and decoding, Standard array and syndrome decoding, Hamming codes, Cyclic codes	**8**
UNIT 4	Convolutional Codes: Convolutional code representation: Code rate, constraint length, Encoding and decoding of convolutional codes: Viterbi algorithm, Applications of convolutional codes, Turbo Codes	**8**
UNIT 5	Information Theory and Coding in Cyber Security: Applications of information theory in cryptography, Error correction for secure communication, Information-theoretic security, Coding for data integrity and authentication, Steganography and watermarking	**10**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Thomas M. Cover and Joy A. Thomas, "Elements of Information Theory," Wiley	2006
2	Shu Lin and Daniel J. Costello Jr., "Error Control Coding," Pearson Education	2004
3	Ron Roth, "Introduction to Coding Theory", Cambridge University Press	2006
4	Raymond W. Yeung, "Information Theory and Network Coding," Springer	2008

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY441 Grid and Cluster Computing	**L**	**T**	**P**	**Operating Systems, Computer Networks**
	3	**0/1**	**2/0**	

Course Objective: 1. To understand and use the theory and basic applications on Grid, cluster and especially cloud computing.
2. Acquire the main skills and abilities to work with scalable systems that allow solving large problems by dividing them into parallel subproblems or by dividing the input data and processing it in parallel bulks.

S. NO	Course Outcomes (CO)
CO1	Analyse the role of clusters and Compare it with other computing Technologies
CO2	Analyse the performance of cluster computing, models, hardware & networks simulations
CO3	Design and implement clustering system
CO4	Design and implement Grid computing applications with grid Standards

S. NO	Contents	Contact Hours
UNIT 1	**Introduction** The Data Centre, the Grid and the Distributed / High Performance Computing, Cluster Computing and Grid Computing, Metacomputing – the Precursor of Grid Computing, Scientific, Business and e-Governance Grids, Web Services and Grid Computing, Business Computing and the Grid – a Potential Win – win Situation, e-Governance and the Grid. **Technologies and Architectures for Grid Computing** Clustering and Grid Computing, Issues in Data Grids, Key Functional Requirements in Grid Computing, Standards for Grid Computing, Recent Technological Trends in Large Data Grids **World Wide Grid Computing Activities, Organizations and Projects** Standard Origanizations, Organizations Developing Grid Computing Tool Kits, Framework, and Middleware, Grid Projects and Organizations Building and Using Grid Based Solutions, Commercial Organizations Building and Using Grid Based Solutions.	**12**
UNIT 2	**Web Services and the Service Oriented Architecture (SOA)** History and Background, Service Oriented Architecture, How a Web Service Works, SOAP and WSDL, Description, Creating Web Services, Server Side. **OGSA and WSRF** OGSA for Resource Distribution, Stateful Web Services in OGSA, WSRF (Web Services Resource Framework), Resource Approach to Stateful Services, WSRF Specification. **Globus Toolkit** History of Globus Toolkit, Versions of Globus Toolkit, Applications of GT4-Cases, GT4-Approaches and Benefits, Infrastructure Management, Monitoring and Discovery, Security, Data, Choreography and Coordination, Main Features of GT4 Functionality – a Summary, GT4 Architecture, GT4	**12**

	Command Line Programs, GT4 Containers **The Grid and the Databases** Issues in Database Integration with the Grid, The Requirements of a Grid-enabled Database, Storage Request Broker (SRB), How to Integrate the Databases with the Grid?, The Architecture of OGSA-DAI for Offering Grid Database Services	
UNIT 3	**What is Cluster Computing?** Approaches to Parallel Computing, How to Achieve Low Cost Parallel Computing through Clusters, Definition and Architecture of a Cluster, What is the Functionality a Cluster can Offer? Categories of Clusters **Cluster Middleware : An Introduction** Levels and Layers of Single System Image (SSI), Cluster Middleware Design Objectives, Resource Management and Scheduling, Cluster Programming Environment and Tools **Early Cluster Architectures and High Throughput Computing Clusters** Early Cluster Architectures, High Throughput Computing Clusters, Condor. **Networking, Protocols & I/O for Clusters** Networks and Inter-connection/Switching Devices, Design Issues in Interconnection Networking/Switching, Design Architecture-General Principles and Trade-offs, HiPPI, ATM (Asynchronous Transmission Mode), Myrinet, Memory Channel (MC), Gigabit Ethernet	**10**
UNIT 4	**Setting Up and Administering a Cluster** How to Set Up a Simple Cluster?, Design Considerations for the Front End of a Cluster, Setting Up Nodes, Clusters of Clusters or Metaclusters, System Monitoring, Directory Services Inside the Clusters & DCE, Global Clocks Sync, Administering Heterogeneous Clusters **Cluster Technology for High Availability** Highly Available Clusters, High Availability Parallel Computing, Mission Critical (or Business Critical or Business Continuity) Applications, Types of Failures and Errors, Cluster Architectures and Configurations for High Availability, Faults and Error Detection, Failure Recovery, Failover/Recovery Clusters **Load Sharing and Load Balancing** Load Sharing and Load Balancing, Strategies for Load Balancing, Modelling Parameters **Distributed Shared Memory** Issues in DSM, Write Synchroni- zation for Data Consistency, Double Faulting, Application/Type Specific Consistency, Issues in Network Performance in DSM	**8**
	TOTAL	**42**

REFERENCES

S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Jankiram, “Grid Computing Models : A Research Monograph”, TMH	(2005)
2	C.S.R.Prabhu – “Grid and Cluster Computing”-PHI Chapters: 1 to 13, 16, 17.	(2008)
3	High Performance Cluster Computing: Architectures and Systems (Volume - 1) 01 Edition, Rajkumar Buyya , Pearson	(2014)

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY433: High Speed Networks	**L**	**T**	**P**	**Computer Networks**
	3	**1/0**	**0/2**	

Course Objective: To understand design and application of architechture and protocols of high speed computer networks

S. NO	Course Outcomes (CO)
CO1	Understand concept of High Speed networks with Asynchronous transfer mode
CO2	Comprehend various Congestion And Traffic Management algorithms and Queuing Analysis-
CO3	Compare Integrated and differentiated network services
CO4	Learn Internetworking and Inter-domain Routing,

S. NO	Contents	Contact Hours
UNIT 1	High Speed networks: Asynchronous transfer mode – ATM Protocol Architecture,ATM logical Connection, ATM Cell – ATM Service Categories – AAL, High Speed LANs:Fast Ethernet, Gigabit Ethernet, Fiber Channel – Wireless LANs: applications,requirements – Architecture of 802.11	**9**
UNIT 2	Congestion And Traffic Management: Queuing Analysis- Queuing Models – Single Server Queues – Effects of Congestion –Congestion Control – Traffic Management – Congestion Control in Packet SwitchingNetworks	**8**
UNIT 3	TCP And ATM Congestion Control : TCP Flow control – TCP Congestion Control – Retransmission – Timer Management – Exponential RTO backoff – KARN's Algorithm – Window management – Performance ofTCP over ATM. Traffic and Congestion control in ATM – Requirements – Attributes –Traffic Management Frame work, Traffic Control – ABR traffic Management – ABR ratecontrol, RM cell formats, ABR Capacity allocations – GFR traffic management	**8**

UNIT 4	Integrated and differential services integrated services architecture - approach, components, servicesqueuing discipline, fq, ps, brfq, gps, wfq - random early detection, differentiated services	**8**
UNIT 5	Protocols for qos support rsvp - goals & characteristics, data flow, rsvp operations, protocol mechanisms - multiprotocol label switching - operations, label stacking, protocol details - rtp - protocol architecture, data transfer protocol, rtcp.	**9**
UNIT 6	Internetworking: Inter-domain Routing, BGP, IPv6, Multicast Routing Protocols, Applications and Other Networking Technologies: RTP, RTSP, SIP, VoIP, Security Systems, SSH, PGP, TLS, IPSEC, DDoS AttackStacking, Protocol details - RTP - Protocol Architecture, Data Transfer Protocol, RTCP.	**8**
	TOTAL	**42**

REFERENCES

S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	HIGH SPEED NETWORKS AND INTERNET, 2nd edition, 2002 by William Stallings, Pearson Education, (ISBN-13: 9788177585698), 2002	2002
2	HIGH PERFORMANCE COMMUNICATION NETWORKS, 2nd edition, 2001, by Warland & Pravin Varaiya, Jean Hardcourt Asia Pvt. Ltd (ISBN-978-1-55860-574- 9), 2001	2001
3	MPLS and VPN architecture by Irvan Pepelnjk,Jin Guichard and Jeff Apcar, Cisco Press, Volume 1 and 2 ,2003 (ISBN-13: 061-9472143230), 2003	2003
4	Behrouz A. Forouzan, Data Communications and Networking, Fourth Ed., Tata McGraw Hill, (ISBN-0072967757), 2007	2007

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY404: Cluster Management	**L**	**T**	**P**	**Operating System**
	3	**0/1**	**2/0**	

Course Objective: This course aims to provide students with an in-depth understanding of cluster computing architecture, its components, fault tolerance, system dependability, load balancing algorithms, and advanced scheduling techniques. It prepares students to manage cluster setups and apply efficient resource management in high-performance computing environments.

S. NO	Course Outcomes (CO)
CO1	Understand the architecture of a cluster computer and its components.
CO2	Know the setup of the cluster and its administration.
CO3	Analyze dependability trade-offs and the limits of computer system dependability.
CO4	Gain knowledge in sources of faults and their prevention, and impacts.
CO5	Analyse load sharing and balancing algorithms and their performance.

S. NO	Contents	Contact Hours
UNIT 1	Introduction to Cluster Computing, Scalable Parallel Computer Architectures, Low Cost Parallel Computing, Cluster Computer and its Architecture, Classifications, Components for Clusters.	**8**
UNIT 2	Network Services, Cluster Middleware and Single System Image, Resource Management and Scheduling, Programming Environments and Tools, Applications, Representative Cluster Systems, Cluster of SMPs.	**8**
UNIT 3	Cluster Setup and its Administration: Setting up the Cluster, Security, System Monitoring and System Tuning, Constructing Scalable Services: Environment, Resource Sharing, Locality, Prototype Implementation and Extension.	**8**
UNIT 4	Dependable Clustered Computing: Dependable Parallel Computing, Critical Computing, Dependability, Cluster Architectures, Detecting and Masking Faults and Recovering from Faults, High Throughput Computing Cluster: Condor.	**9**
UNIT 5	Process Scheduling, Load Sharing and Balancing, Job and Resource Management Systems, Scheduling Parallel Jobs on Clusters, Fault Tolerance by Means of Checkpointing and Integration, Parallel Program Scheduling Techniques.	**9**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	R. Buyya, "High Performance Cluster Computing: Architectures and	2007

	Systems", Vol. 1	
2	I. Koren and C. M. Krishna, “Fault Tolerant System”, Morgen Kauffman	2007

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY406: Hyperledger and Fabric Programming	**L**	**T**	**P**	**Blockchain, DSA, Networking basics**
	3	**1/0**	**2/0**	

Course Objective:	
S. NO	**Course Outcomes (CO)**
CO1	To understand the fundamentals of blockchain technology and the architecture of Hyperledger Fabric.
CO2	To set up and configure a Fabric network, including peers, orderers, MSPs, channels, and endorsement policies.
CO3	To develop, package, and deploy chaincode (smart contracts) in Go and JavaScript (Node.js).
CO4	To build client applications and DApps using Fabric SDKs and leverage advanced Fabric features (private data, CouchDB, events).

S. NO	**Contents**	**Contact Hours**
UNIT 1	Introduction to Blockchain & Hyperledger: - Blockchain basics: blocks, transactions, consensus - Permissioned vs. permissionless networks - Overview of Hyperledger projects and use-cases - Why Hyperledger Fabric?	**10**
UNIT 2	UNIT 2 Hyperledger Fabric Architecture: - Components: peers, orderers, CAs, clients - Ledger (world state) and state database (LevelDB/CouchDB) - Membership Service Provider (MSP) and identities - Transaction flow & endorsement	**8**
UNIT 3	UNIT 3 Environment Setup & Network Deployment: - Prerequisites: Docker, Docker Compose, Go/Node.js, CLI tools - Fabric binaries and sample networks (test-network/BYFN) - Creating and joining channels - Configuring channel policies and updates	**8**
UNIT 4	UNIT 4 Chaincode Development: - Data modeling with key–value pairs - Writing chaincode in Go and JavaScript (Node.js) - Packaging, installing, approving, and committing chaincode (lifecycle v2.x) - Query vs. invoke transactions	**8**
UNIT 5	UNIT 5 Advanced Features & DApp Development: - Private Data Collections and CouchDB rich queries - Chaincode events and event listeners	**8**

	- Fabric SDK: Go and Node.js gateways, wallets - Building a simple end-to-end DApp (demo)	
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Nitin Gaur et al., Hands-On Blockchain with Hyperledger, Packt Publishing	(2019)
2	Ashwani Kumar et al., Mastering Hyperledger Fabric, Packt Publishing (2020)	2020
3	Xun Wang, Hyperledger Fabric in Action, Manning Publications (2021)	2021
4	Brandon Byrne, Blockchain by Example, Packt Publishing (2018)	2018
5	Fabian Vogelsteller & Gavin Wood, Introducing Ethereum and Solidity, Manning Publications (2018)	2018
6	Hyperledger Fabric Documentation, The Linux Foundation (online)	-
7	Arun Suhag, Blockchain Quick Reference, Apress (2019)	2019
8	Richard Caetano, Hyperledger Cookbook, Packt Publishing (2021)	2021

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY408 Hardware Security	**L**	**T**	**P**	**Applied Cryptography, Micro-Processor and Controller**
	3	**0/1**	**2/0**	

Course Objective: To equip students with advanced knowledge and skills to design, analyze, and secure hardware systems against physical and logical attacks, focusing on secure architectures, threat mitigation, and emerging hardware security trends.

S. NO	Course Outcomes (CO)
CO1	Understand hardware security principles, threats, and primitives.
CO2	Design secure hardware systems using secure boot and trusted environments.
CO3	Analyze and mitigate hardware attack vectors like side-channel attacks and trojans.
CO4	Apply advanced hardware security techniques for post-quantum and AI-driven systems.

S. NO	Contents	Contact Hours
UNIT 1	**Fundamentals of Hardware Security**- Role of hardware security in CPS and IoT- Threat models: Physical, logical, supply chain- Security primitives: PUFs, TRNGs- Case studies: Spectre, Meltdown	8
UNIT 2	**Secure Hardware Design Principles**- Secure boot and firmware integrity- Hardware Description Languages: Verilog, VHDL for security- Trusted Platform Module (TPM), Hardware Security Modules (HSM)- Secure memory: Intel SGX, encrypted memory	9
UNIT 3	**Hardware Attack Vectors**- Side-channel attacks: Power, EM, timing- Physical attacks: Fault injection, reverse engineering- Hardware trojans: Detection and prevention- Supply chain vulnerabilities	8
UNIT 4	**Countermeasures and Verification**- Differential power analysis (DPA) resistance- Tamper-proofing and obfuscation techniques- Formal verification of security properties- Hardware security testing tools	9
UNIT 5	**Emerging Trends in Hardware Security**- Post-quantum cryptography: Lattice, hash-based- Hardware acceleration for cryptographic algorithms- AI hardware security: Neural accelerators- Quantum computing threats to hardware	8
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Tehranipoor, M., & Wang, C. (Eds.). *Introduction to Hardware Security and Trust*. Springer.	2020
2	Bhunia, S., & Tehranipoor, M. *Hardware Security: A Hands-on Learning Approach*. Morgan Kaufmann.	2018
3	Rostami, M., Koushanfar, F., & Karri, R. *Hardware Security Primitives: Design and Applications*. Wiley.	2023

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY410: IoT with Arduino, ESP, and Raspberry Pi	**L**	**T**	**P**	**Computer Networks**
	3	**1/0**	**0/2**	

Course Objective: • To give students hands-on experience using different IoT architectures.
• To provide skills for interfacing sensors and actuators with different IoT architectures.
• To develop skills on data collection and logging in the cloud.

S. NO	Course Outcomes (CO)
CO1	Understand concepts in Cluster based distributed computing Hardware technologies
CO2	Learn Programming Models and Paradigms
CO3	Compare Grid Computing: Grids and Grid Technologies, Programming models and Parallelization Techniques
CO4	Study Data Management Application

S. NO	Contents	Contact Hours
UNIT 1	IoT- introduction and its components, IoT building blocks, Sensors and Actuators, IoT Devices, IoT boards (Arduino Uno, ESP 8266-12E Node MCU, and Raspberry Pi 3).	**8**
UNIT 2	Arduino Uno – getting started with the Uno boards, blink program, connection of sensors to the Uno board, reading values of sensors from the Uno board, interrupts. Case study: Temperature/Humidity Control; Case Study: Sending values Temperature/Humidity values to the Internet via GSM module.	**9**
UNIT 3	ESP 8266-12E Node MCU – getting started with the ESP board, Micropython and Esplorer IDE, Flushing the ESP8266 board with micropython, connecting sensors to the ESP board, Connecting ESP board to WiFi, Interfacing ESP with the Cloud (REST API-GET, POST, MQTT), interrupts, comparison of ESP 32 board with the ESP 8266 board. Case Study: Switching light on /off remotely. Case Study: Voice-based Home Automation for switching lights on/off (Android phone – Google Assistant (Assistant <-> IFTTT), MQTT (ESP <-> IFTTT), ESP 8266 <-> Lights).	**9**

UNIT 4	Raspberry Pi 3 - Rpi3 introduction and installing the Raspbian Stretch OS, Headless - Computer and Rpi3 configuration to connect through SSH via Ethernet, Headless - connecting Rpi3 remotely without Ethernet cable via SSH, IP address, Rpi 3 - Testing the GPIO pins through Scripts.	**8**
UNIT 5	Raspberry pi3 interfacing with Sensor DHT11, Raspberry pi3 python library install and reading sensor feed, 'Plug and play ' type cloud platform overview for integration to IOT devices, 'Plug and play' cloud platform for integration to IOT device - actuator (LED), Plug and play platform - Custom widget (DHT11-Sensor) integration through Python. New - Raspeberry Pi 4 Vs Raspberry Pi3 Mobel B Comparison, LoRawan /LPWAN – Overview.	**8**
		8
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Rao, M. (2018). Internet of Things with Raspberry Pi 3: Leverage the power of Raspberry Pi 3 and JavaScript to build exciting IoT projects. Packt Publishing Ltd	2008
2	Baichtal, J. (2013). Arduino for beginners: essential skills every maker needs. Pearson Education.	2005
3	Schwartz, M. (2016). Internet of Things with ESP8266. Packt Publishing Ltd.	2009
4	Richardson, M., & Wallace, S. (2012). Getting started with raspberry PI. " O'Reilly Publisher Media, Inc."	2008

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY412: Mathematical Modelling and Computer-Aided Engineering	**L**	**T**	**P**	**Engineering Mathematics**
	3	**0/1**	**2/0**	

Course Objective:

- Students should be able to formulate, analyze, and apply mathematical models.
- Students should be able to understand the necessary mathematical abstraction to solve problems.

S. NO	Course Outcomes (CO)
CO1	To describe the basics of partial differential equations and numerical methods.
CO2	To understand the methods of finite element methods.
CO3	Design and validate technological solutions to defined problems and communicate clearly and effectively for the practical application of their work.
CO4	Formulate relevant research problems; conduct experimental and/or analytical studies, and analyze results with modern mathematical/scientific methods and the use of software tools.

S. NO	Contents	Contact Hours
UNIT 1	Introduction: problems in engineering-structural - fluid flow and heat transfer with their relevance in product development - examples - need for computer aided engineering. Partial differential equations: elliptic, parabolic and hyperbolic - physical significance - solution techniques. Numerical methods to solve PDEs: central differences, Crank-Nicolson and ADI methods - examples - stability and error of numerical schemes.	**12**
UNIT 2	Variational calculus: introduction, solutions selected differential equations by Variational methods, Rayleigh - Ritz method - introduction to finite element method.	**6**
UNIT 3	Finite element method: concepts, nodes, elements, connectivity, coordinate systems, shape functions, stiffness matrix, global stiffness matrix, Isoparametri elements solution methods – examples- use of software.	**8**
UNIT 4	Fluid flow: introduction to computational fluid dynamics (finite difference, finite element techniques) - formulation of fluid flow problems (simple cases only) - NavierStokes equation - solution techniques - examples, solution of fluid flow problems using software.	**6**
UNIT 5	Heat transfer: derivation of energy equation in general form - solutions using numerical methods (finite difference and finite element techniques), solutions using FEA and CFD techniques for conductive and convective heat transfer problems. Introduction to multi-physics problems: electrophoresis, electro-osmosis, lab-on – chip used in biotechnology use of software.	**10**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Reddy J N, "An Introduction to the Finite Element Method", Tata McGraw Hill, 4th edition.	2020
2	Singerasu S Rao, "The Finite Element Method in Engineering", Butterworth Heinemann, 6th Edition.	2017
3	Curtis F Gerald Patrick O Wheatley, "Applied Numerical Analysis", Pearson, 7th edition.	2006
4	Muralidhar K and Sundararajan T, "Computational Fluid Flow and Heat Transfer", Narosa Publications, 2nd edition.	2014

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY414: Security Architecture	**L**	**T**	**P**	**Network Security, Applied Cryptography**
	3	**0/1**	**2/0**	

Course Objective: To enable students to design and implement robust security architectures for networks, systems, and applications, integrating advanced threat modeling, secure design principles, and resilience strategies for complex cyber environments.

S. NO	Course Outcomes (CO)
CO1	Understand security architecture frameworks and threat modeling techniques.
CO2	Design secure network architectures using zero-trust principles.
CO3	Implement secure system and application architectures with advanced IAM.
CO4	Evaluate advanced security architectures for CPS, blockchain, and AI systems.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Security Architecture**- Scope and principles of security architecture- Security models: Bell-LaPadula, Biba- Standards: NIST SP 800-53, ISO/IEC 27001- Threat modeling: STRIDE, DREAD	8
UNIT 2	**Network Security Architecture**- Secure network design: DMZ, VLANs- Zero-trust architecture principles- Secure protocols: TLS, IPsec, DNSSEC- Software-defined networking (SDN) security	9
UNIT 3	**System and Application Security**- OS security: SELinux, sandboxing- Secure SDLC: OWASP, secure coding practices- Cloud security: Microservices, shared responsibility- Identity and Access Management: OAuth, SAML	8
UNIT 4	**Resilience and Monitoring**- Intrusion detection and prevention systems- Security Information and Event Management (SIEM)- Disaster recovery and redundancy- Real-time threat monitoring	9
UNIT 5	**Advanced Security Architecture Trends**- CPS and IIoT security architectures- Blockchain-based security frameworks- AI-driven security: Threat prediction, anomaly detection- Regulatory compliance: GDPR, CCPA	8
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Schoenfield, B. S. *Securing Systems: Applied Security Architecture*	2021

	and Threat Models. CRC Press.	
2	Merkow, M. S., & Raghavan, L. *Secure and Resilient Software Development*. Auerbach Publications.	2020
3	NIST. *Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations*. NIST.	2020

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY416: Cyber Laws	**L**	**T**	**P**	
	3	**1**	**0**	

Course Objective: This course introduces the students to the concepts of information security and different type of attacks in the cyber space. The course also introduces countermeasures to mitigate attacks and different existing cyber laws.

S. NO	Course Outcomes (CO)
CO1	Learn, structure, mechanics and evolution of various crime threats.
CO2	Learn to protect information systems from external attacks by developing skills in enterprise security, wireless security and computer forensics.
CO3	Analyse the risks involved while sharing their information in cyber space and numerous related solutions like sending protected and digitally signed documents
CO4	Insights of ethical hacking and usage of password cracking tools
CO5	Get an overview of different ciphers used for encryption and decryption.

S. NO	Contents	Contact Hours
UNIT 1	**Definitions:** Protection, Security, risk, threat, vulnerability, exploit, attack, confidentiality, integrity, availability, non-repudiation, authentication, authorization, codes, plain text, encryption, decryption, cipher text, key, ciphers, Symmetric and asymmetric cryptography, Public key, private key, Crypt analysis,, Cyber forensics. Substitution cipher (Caesar), Transposition cipher (Rail-Fence).	**09**
UNIT 2	Risk analysis, process, key principles of conventional computer security, security policies, data protection, access control, internal vs external threat, security assurance, passwords, access control, computer forensics and incident response.	**07**
UNIT 3	CYBER ATTACKS (definitions and examples): Denial-of-service attacks, Man-in-themiddle attack, Phishing, spoofing and spam attacks, Drive-by attack, Password attack, SQL injection attack, Cross-site scripting attack, Eavesdropping attack, Birthday attack, Malware attacks, Social Engineering attacks	**09**
UNIT 4	Brief Introduction of handling the attacks described in UNIT 3. Firewalls, logging and intrusion detection systems, e-mail security, security issues in operating systems, ethics of hacking and cracking.	**06**
UNIT 5	Definitions: Digital Signature and Electronic Signature, Digital Certificate I. [Section 43] Penalty and compensation for damage to computer etc. II. [Section 65] Tampering with computer source documents III. [Section 66A] Punishment for sending offensive messages through communication service etc.	**08**

	IV. [Section 66B] Punishment for dishonestly receiving stolen computer resource or communication device V. [Section 66C] Punishment for identity theft VI. [Section 66D] Punishment for cheating by impersonation by using computer resource VII. [Section 66E] Punishment for violation of privacy VIII. [Section 66F] Punishment for cyber terrorism IX. [Section 67] Punishment for publishing or transmitting obscene material in electronic form X. [Section 67A] Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form XI. [Section 67B] Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form XII. [Section 72] Breach of confidentiality and privacy	
UNIT 6	Brief introduction of IT infrastructure in India, National agencies handling IT.	**03**
	TOTAL	**42**

REFERENCES

S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Merkow, M., & Breithaupt, J.(2005) Information Security Principles and Practices. 5th edition. Prentice Hall.	2005
2	Snyder, G.F. (2010). Network Security, Cengage Learning.	2010
3	Whitman, M. E. & Mattord, H. J. (2017) Principles of Information Security. 6th edition. Cengage Learning.	2017
4	Basta, A., & Halton, W., (2010) Computer Security: Concepts, Issues and Implementation, Cengage Learning India.	2010

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
Cy418: Mobile VR and AI in Moduley	**L**	**T**	**P**	**None**
	3	**1/0**	**0/2**	

Course Objective:

- To give students hands-on exposure to mobile virtual reality in Moduley.
- To give students experience with basic AI algorithms in virtual reality.
- To provide students with the fundamentals of game design in virtual reality

S. NO	Course Outcomes (CO)
CO1	To learn to code for game development in Moduley C#
CO2	To understand the fundamentals of game design.
CO3	To learn to use AI algorithms (A*, IL, and RL) in Moduley-ML
CO4	Analyze challenges, limitations, and future trends in mobile VR and AI .

S. NO	Contents	Contact Hours
UNIT 1	Introduction to Moduley, Moduley Editor, Moving a Cube, Lights, Particle Systems, Applying Physics, and Moduley Asset Store, C# Coding Introduction, Variables, Methods, If Blocks, Loops, Hello Mammoth, User Interaction in Moduley, Inputs Introduction Preview, Key Presses, Moving a Player, Jumping, Moving Forward, Cycling Cameras, Prefabs Introduction, What are Prefabs?, Instantiating Objects, Random Angles, Destroying Objects, Explosion Effects, Adding Explosion Effects.	**12**
UNIT 2	Developing a Pathfinding Game, How to Set Up a Project, Node, String Map, A* Algorithm Setup, A* Algorithm Loop, Auxiliary Methods, Finishing the Algorithm, Importing 2D Assets, Building a Level, From Console to Visual, Adding Tanks, Identifying Nodes, Moving the Tank, Visually Moving Tank, Smooth Movement, Smooth Rotation, Ordering Tank to Move, Speeding up Player, Spawning Logic, Crate Visuals, Adding Crates to Valid Positions, Collecting Crates, Score Counting, Game Interface, Starting the Game, Game Over Screen, Scoring, Sounds.	**7**
UNIT 3	VR Introduction - Moduley, Activating VR, Building a Castle, Camera Changing Position, Lowering Castle Doors, Triggering Events Interface, Blender, Download and Install Blender, Introduction & Customizing Settings, Controlling Blender Camera, Emulate Numpad Camera, Manipulating Objects, Common Tools, Mirroring 1 Side of Object. Case Study: Flappy bird Moduley game, First person shooter game, Kart Moduley game.	**7**
UNIT 4	Introduction to Moduley-ML, Why Machine Learning, different kinds of learnings, Neural Networks (NNs), Training a NN, Optimizer, Convolutional layers, Transfer learning, Imitation learning in Moduley, Training the kart in kart game via IL, Testing the drive	**6**

UNIT 5	Introduction to Reinforcement Learning in Moduley-ML, Reinforcement Learning, Initial state, training a policy, The PPO algorithm, Evolutional Strategies, Reward, training a kart in the kart game with RL, Tensor board analysis, Testing results.	**10**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Linowes, J., & Schoen, M. .Cardboard VR Projects for Android. Packt Publishing Ltd.	2016
2	Lanham, M., Hands-On Deep Learning for Games: Leverage the power of neural networks and reinforcement learning to build intelligent games. Packt Publishing Ltd.	2019
3	3. Aversa, D., Kyaw, A. S., & Peters, C. (2018). Moduley Artificial Intelligence Programming: Add powerful, believable, and fun AI entities in your game with the power of Moduley 2018! Packt Publishing Ltd.	
4		

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY420: CPS Assurance	**L**	**T**	**P**	**Introduction to Cyber Physical Systems, Applied Cryptography**
	3	**0/1**	**2/0**	

Course Objective: To provide students with advanced techniques for assuring the security, safety, and reliability of cyber-physical systems, focusing on formal methods, testing, and compliance for critical applications.

S. NO	Course Outcomes (CO)
CO1	Understand CPS assurance frameworks and risk assessment methodologies.
CO2	Apply security assurance techniques, including formal verification and testing.
CO3	Ensure CPS safety and reliability using standards and fault tolerance.
CO4	Address advanced CPS assurance challenges in autonomous and AI-driven systems.

S. NO	Contents	Contact Hours
UNIT 1	**Fundamentals of CPS Assurance**- CPS overview: Sensors, actuators, networks- Assurance concepts: Security, safety, reliability- Frameworks: NIST CPS Framework, IEC 62443- Risk assessment: Safety-security trade-offs	8
UNIT 2	**Security Assurance Techniques**- Vulnerability assessment and penetration testing- Formal methods: Model checking, theorem proving- Runtime monitoring and anomaly detection- Assurance cases: Goal Structuring Notation	9
UNIT 3	**Safety Assurance in CPS**- Safety standards: ISO 26262, DO-178C- Safety analysis: FMEA, FTA- Human-in-the-loop assurance- Certification processes	8
UNIT 4	**Reliability and Fault Tolerance**- Dependability metrics: Availability, MTBF- Fault tolerance: Redundancy, failover mechanisms- Resilient design for CPS- Testing for reliability	9
UNIT 5	**Emerging CPS Assurance Trends**- Assurance for autonomous systems: Drones, AVs- 5G and IoT-enabled CPS assurance- AI assurance: Trustworthy AI frameworks- Regulatory compliance: GDPR, CCPA	8
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Lee, E. A., & Seshia, S. A. *Introduction to Cyber-Physical Systems*.	2022

	MIT Press.	
2	Baheti, R., & Gill, H. *Cyber-Physical Systems: Assurance and Resilience*. Springer.	2021
3	Alur, R. *Principles of Cyber-Physical Systems*. MIT Press.	2019

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY422: Cloud Security	**L**	**T**	**P**	**Cloud Computing**
	3	**0/1**	**2/0**	

Course Objective:	
S. NO	**Course Outcomes (CO)**
CO1	Understand the basic components of cloud & Security in the cloud.
CO2	Illustrate the Infrastructure Security, Data Security, storage, and security management in the cloud.
CO3	Understand the concepts of Identity and Access Management.
CO4	Apply security architectures that assure secure isolation of physical and logical infrastructures.

S. NO	**Contents**	**Contact Hours**
UNIT 1	Fundamentals of Cloud Computing and Architectural Characteristics- Cloud Computing Architectural- Cloud deployment models: Public, Private, Community, and Hybrid models. Scope of Control: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)- Cloud Computing Roles Risks, Cloud Architecture, Virtualization in Cloud, Cloud Data Centre, SLA, Cloud Applications.	**8**
UNIT 2	Cloud Security Challenges, Cloud Information Security Objectives, Cloud Security Services, Secure Cloud Software Requirements, Cloud Security Policy Implementation, Infrastructure Security, Data Security and Storage, Privacy in Cloud.	**8**
UNIT 3	Threats and Vulnerabilities to Infrastructure, Data, and Access Control; Risk Management and Risk Assessment in Cloud, Cloud Service Provider Risks, Virtualization Security Management in the Cloud, Trusted Cloud Computing, Identity Management and Access Control.	**9**
UNIT 4	Cloud Computing and Business Continuity Planning/Disaster Recovery, Cloud Audit and Compliance: Internal Policy Compliance, Regulatory/External Compliance, Cloud Security Alliance.	**8**
UNIT 5	Standards for Security: SAML OAuth, OpenID, SSL/TLS, Encrypting Data and Key Management, Creating a Cloud Security Strategy, The Future of Security in Cloud Computing. What Is Privacy, What Is the Data Life Cycle, What Are the Key Privacy Concerns in the Cloud, Who Is Responsible for Protecting Privacy,	**9**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**

1	Ronald L. Krutz, Russell Dean Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing.	2010
2	Tim Mather, Subra Kumaraswamy, and Shahed Latif, "Cloud Security and Privacy", O'Reilly Media, Inc.	2009
3	John Rittinghouse, James Ransome, "Cloud Computing" CRC Press; 1 edition [ISBN:1439806802].	2009

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY424 Computer Vision	**L**	**T**	**P**	Basic of Linear Algebra and Programming
	3	**0/1**	**2/0**	

Course Objective: To introduce fundamentals of computer vision so that students will understand to program a computer for understanding a scene or features in an image development.

S. NO	Course Outcomes (CO)
CO1	To describe Image Formation Models, Monocular imaging system, Orthographic & Perspective projections
CO2	To evaluate applications of 2D/3D Vision Filters, Binary Images, Features and Edge Detection
CO3	To describe Image Processing and Feature Extraction concepts
CO4	To analyze motion Estimation, Regularization theory, Optical computation, Stereo Vision
CO5	To investigate Shape Representation Segmentation, Deformable curves and surfaces
CO6	To explain about Object recognition, describe Hough transforms and other simple object recognition methods

S. NO	Contents	Contact Hours
UNIT 1	Image Formation Models: Monocular imaging system, Orthographic & &Perspective Projection, Cameras – lenses, projections, sensors, Radiometry –Measuring Light, light and surfaces Representation – color spaces, Camera model and Camera calibration, Binocular imaging systems, Sources, Shadows and Shading.	**8**
UNIT 2	2D/3D Vision: Filters, Binary Images, Features, Edge Detection, Texture, Shape, Segmentation, Clustering, Model Fitting, Probabilistic, 3D Vision: Multiview geometry, Stereo, Shape from X, 3D data	**6**
UNIT 3	Image Processing and Feature Extraction: Image representations (continuous and discrete), Linear Filters, Texture, Edge detection.	**6**
UNIT 4	Motion Estimation: Regularization theory, Optical computation, Stereo Vision, Motion estimation, Structure from motion.	**8**
UNIT 5	Shape Representation and Segmentation: Deformable curves and surfaces, Snakes and active contours, Level set representations, Fourier and wavelet descriptors, Medial representations, Multi- resolution	**8**

	analysis.	
UNIT6	Object recognition: Hough transforms and other simple object recognition methods, Shape correspondence and shape matching, Principal component analysis, Shape priors for recognition.	**6**
	TOTAL	**42**

REFERENCES

S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Computer Vision: A Modern Approach by D. A. Forsyth and J. Ponce, Prentice Hall, 2003/2011	2011
2	Computer Vision by Linda Shapiro and George Stockman, Prentice-Hall, 2001	2001
3	Robot Vision, by B. K. P. Horn, McGraw-Hill., 1986	1986
4	Richard Hartley and Andrew Zisserman, Multiple View Geometry in Computer Vision, Second Edition, Cambridge University Press, March 2004	2004

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY426: Compliance Frameworks for Cyber Security	**L**	**T**	**P**	**Basics of Cyber Security**
	3	**1/0**	**0/2**	

Course Objective: To understand the role of compliance in cyber security and to study major international and national compliance frameworks. Analyzing laws and regulations governing data protection and applying compliance best practices for risk management are also important.

S. NO	Course Outcomes (CO)
CO1	Understand the importance of cyber security compliance.
CO2	Apply major compliance frameworks to real-world systems.
CO3	Interpret global and local data protection laws.
CO4	Conduct audits and document compliance requirements.
CO5	Recommend strategies for enterprise compliance.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Cyber Security Compliance:** Concept of cyber security compliance, Need for compliance frameworks, Governance, Risk and Compliance (GRC), Compliance vs security vs privacy.	**8**
UNIT 2	**International Compliance Frameworks:** ISO/IEC 27001, NIST Cybersecurity Framework, COBIT and ITIL, PCI-DSS (Payment Card Industry Data Security Standard)	**8**
UNIT 3	**Data Protection Laws and Regulations:** General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA) Gramm-Leach-Bliley Act (GLBA), Children's Online Privacy Protection Act (COPPA)	**9**
UNIT 4	**Indian Cyber Laws and Compliance:** Information Technology Act 2000 (Amendments), CERT-IN Guidelines, Data Protection Bill (latest draft), SEBI, RBI Guidelines	**9**
UNIT 5	**Compliance Implementation and Auditing:** Risk assessment and compliance auditing, Developing security policies and SOPs, Role of compliance officer and DPO, Compliance reporting and documentation	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Peltier, Thomas R., "Information Security Policies, Procedures, and Standards: guidelines for effective information security management", CRC Press, 2016.	2016

2	Kohnke, Anne, et al., "Cybersecurity Essentials", Springer, 2021	2021
3	Paul Rohmeyer and Jennifer Bayuk, "Financial Cybersecurity Risk Management", Springer, 2018	2018
4	Krutz, Ronald L., and Russell Dean Vines, "The CISSP Prep Guide: Mastering the Ten Domains of Computer.	2020

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY428: Edge and Fog Computing	**L**	**T**	**P**	Computer Networks, Cloud Computing, IoT
	3	**1/0**	**0/2**	

Course Objective:

S. NO	**Course Outcomes (CO)**
CO1	Understand the fundamental concepts of Edge and Fog Computing and how they differ from Cloud Computing.
CO2	Analyze architectures and communication protocols used in Edge and Fog environments.
CO3	Design IoT-based systems leveraging Edge and Fog Computing for low-latency and bandwidth-efficient processing.
CO4	Evaluate the security, privacy, and performance issues in Edge and Fog Computing systems.

S. NO	**Contents**	**Contact Hours**
UNIT 1	Introduction to Edge and Fog Computing: Concepts, architecture, need for Edge and Fog Computing in IoT systems. Comparison with Cloud Computing. Use cases and application domains.	**8**
UNIT 2	UNIT 2 Edge and Fog Computing Architectures: Architecture models, components, and service models. Fog nodes, Edge gateways, communication models. Middleware platforms for Edge/Fog Computing.	**10**
UNIT 3	Data Management and Analytics: Data preprocessing and analytics at the Edge. Real-time data stream processing frameworks. Resource management and orchestration.	**8**
UNIT 4	Protocols and Communication: IoT and edge communication protocols (MQTT, CoAP, 6LoWPAN). Data flow, message queue systems, containerization (Docker, Kubernetes).	**8**
UNIT 5	Security and Challenges: Security and privacy in Edge and Fog Computing. Authentication, access control, trust models. Challenges and future research directions.	**8**
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**

1	Rajkumar Buyya and Satish Narayana Srirama, "Fog and Edge Computing: Principles and Paradigms", Wiley (2019)	2019
2	Meikang Qiu, "Edge Computing: Models, Technologies and Applications", Springer (2021)	2021
3	F. Bonomi et al., "Fog Computing and Its Role in the Internet of Things", MCC Workshop on Mobile Cloud Computing (2012)	2012
4	Pethuru Raj and Anupama C. Raman, "The Internet of Things: Enabling Technologies, Platforms, and Use Cases", CRC Press (2017)	2017

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY430: Cognitive Computing	**L**	**T**	**P**	Fundamentals of Artificial Intelligence and Machine Learning
	3	**1/0**	**0/2**	

Course Objective: Provide students with a solid grounding in the principles, architectures, and applications of cognitive computing systems that emulate human thought processes.

S. NO	Course Outcomes (CO)
CO1	Explain the foundations of cognitive computing including models of human cognition and knowledge representation.
CO2	Apply machine learning and deep learning techniques within cognitive architectures to solve real-world problems.
CO3	Design and implement end-to-end natural language and multimodal perception pipelines.
CO4	Critically evaluate the ethical, interpretability, and scalability challenges of cognitive computing systems.

S. NO	Contents	Contact Hours
UNIT 1	Introduction to cognitive computing field, models of human cognition and mental architectures (SOAR, ACT-R), knowledge representation techniques including semantic networks and ontologies, symbolic versus subsymbolic approaches, overview of cognitive applications	**8**
UNIT 2	Machine learning foundations for cognition, supervised and unsupervised learning algorithms, reinforcement learning basics, neural network architectures for pattern recognition, feature extraction and dimensionality reduction	**10**
UNIT 3	Natural language processing and understanding, language modeling and embeddings, parsing and semantic analysis, speech recognition and synthesis, question-answering systems and dialog management	**8**
UNIT 4	Multimodal perception and reasoning, computer vision techniques for image and video understanding, sensor data fusion, probabilistic reasoning with Bayesian networks, fuzzy logic systems	**8**
UNIT 5	Cognitive agents and human–computer interaction, chatbot and virtual assistant design, knowledge discovery and mining, explainable AI and interpretability methods, ethical considerations and bias mitigation, emerging trends in neuromorphic computing	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach*, Pearson	2020

2	Judith Hurwitz, Marcia Kaufman & Adrian Bowles, *Cognitive Computing: Theory and Applications*, CRC Press	2017
3	Natarajan Meghanathan & Sriram Chandrasekaran, *Cognitive Computing Concepts in Big Data*, Springer	2018
4	Rajendra Akerkar, *Cognitive Computing*, CRC Press	2020

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY432: Neuromorphic computing	**L**	**T**	**P**	**Electronics, sensors, deep learning, computer vision**
	3	**1 /0**	**0/2**	

Course Objective:

S. NO	Course Outcomes (CO)
CO1	Understand the Biological Foundations of Neuromorphic Computing
CO2	Design and Analyze Neuromorphic Hardware Architectures
CO3	Implement and Evaluate Neuromorphic Algorithms for Real-World Applications
CO4	Apply Simulation Tools to Model and Test Neuromorphic Systems

S. NO	Contents	Contact Hours
UNIT 1	Introduction to Neuromorphic Computing: Foundations of Neuroscience, Neurons and Synapses, Biological neuron structure and function. Synaptic plasticity, Hebbian learning. Neural Networks, Structure and function of biological neural networks.Information processing in the brain. Spiking Neural Networks (SNNs) Neuron models: integrate-and-fire, Hodgkin-Huxley. Temporal encoding and spike-timing-dependent plasticity (STDP).	**8**
UNIT 2	Neuromorphic Hardware and Neuromorphic Processors: Overview of neuromorphic chips (e.g., IBM TrueNorth, Intel Loihi). Design principles and architecture of neuromorphic hardware. Analog and Digital Circuits, Analog VLSI for neuromorphic systems. Mixed-signal circuits, CMOS technology in neuromorphic design. Memristors and Emerging Devices, Memristor theory and applications in neuromorphic systems.	**10**
UNIT 3	Neuromorphic Algorithms Learning Algorithms: Supervised, unsupervised, and reinforcement learning in SNNs. STDP, spike-based learning rules. Pattern Recognition and Sensory Processing, Neuromorphic approaches to vision, auditory, and tactile processing, Neuromorphic Control Systems	**8**
UNIT 4	Simulation Tools and Software Simulation Platforms: NEURON, NEST, BindsNET, and other neuromorphic simulators. Programming Models Programming frameworks for neuromorphic hardware (e.g., PyNN, Lava). Toolchains for Neuromorphic Design CAD tools for neuromorphic VLSI design. Integration of hardware and software in neuromorphic systems.	**8**
UNIT 5	Neuromorphic System Design System-Level Design: Architectures of large-scale neuromorphic systems. Network-on-Chip (NoC) for neuromorphic systems. Integration with Sensors and Actuators Interface design for neuromorphic sensors (e.g., dynamic vision sensors). Real-time neuromorphic processing for robotics and IoT.	**8**

	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Neuromorphic Engineering: From Neural Systems to Brain-Like Circuits" by Elisabetta Chicca, Giacomo Indiveri, and Stefan J. Thorpe (2021)	2021
2	Introduction to Neuromorphic Computing" by S. Rajasekaran and G. A. Vijayalakshmi Pai (2021)	2021
3	Learning in Energy-Efficient Neuromorphic Computing: Algorithm, Architecture, and System" by Qingwei Li, Yiran Chen, and Yuan Xie (2020)	2020
4	Brain-Inspired Computing: The Next Revolution in Computational Neuroscience" by Anup Basu (2017)	2017

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY434: Optimization Techniques	**L**	**T**	**P**	**Calculus, Linear Algebra, Data Structures & Algorithms**
	3	**1/0**	**0/2**	

Course Objective: Enable students to formulate and solve a variety of optimization problems using classical and modern algorithmic techniques.

S. NO	Course Outcomes (CO)
CO1	Formulate engineering and computer-science problems as mathematical optimization models.
CO2	Analyze convexity and duality properties to assess solution existence and optimality.
CO3	Implement and compare classical algorithms for linear, nonlinear, and integer optimization.
CO4	Apply metaheuristic methods to complex and multi-objective optimization scenarios.

S. NO	Contents	Contact Hours
UNIT 1	Introduction to optimization problem classification, objective functions and constraint types, feasible region and optimality concepts, convex sets and convex functions overview, role of gradient and Hessian in search methods, examples from engineering and computer science.	**8**
UNIT 2	Linear programming model formulation and standard form conversion, graphical method for two-variable LP, simplex algorithm mechanics and tableau operations, duality theory and economic interpretation, sensitivity and post-optimality analysis, network flow and transportation problem formulations	**10**
UNIT 3	Unconstrained optimization methods including steepest descent and Newton's method, convergence properties and rate analysis, constrained optimization via Lagrange multipliers and Karush–Kuhn–Tucker conditions, penalty and barrier function approaches, trust-region concepts	**8**
UNIT 4	Integer programming formulations for combinatorial problems, branch-and-bound framework and node-selection strategies, cutting plane methods and Gomory cuts, mixed-integer programming techniques, dynamic programming principles and applications to knapsack and shortest-path problems	**8**
UNIT 5	Metaheuristic algorithm principles, genetic algorithms and encoding schemes, particle swarm optimization fundamentals, simulated annealing and temperature schedules, ant colony optimization basics, multi-objective optimization and Pareto-front concepts, hybrid and memetic algorithm strategies	**8**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Singiresu S. Rao, *Engineering Optimization: Theory and Practice*, Wiley	2018
2	Hamdy A. Taha, *Operations Research: An Introduction*, Pearson	2017
3	Dimitri P. Bertsekas, *Nonlinear Programming*, Athena Scientific	1999
4	El-Ghazali Talbi, *Metaheuristics: From Design to Implementation*, Wiley	2009

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY436: Pervasive and Ubiquitous Computing	**L**	**T**	**P**	**Mobile Networks, Sensors, Networks, Security**
	3	**1/0**	**0/2**	

Course Objective:

S. NO	Course Outcomes (CO)
CO1	Understand the Core Concepts and Technologies of Pervasive and Ubiquitous Computing
CO2	Design and Develop Context-Aware Ubiquitous Systems
CO3	Address Security and Privacy Challenges in Ubiquitous Environments
CO4	Explore and Apply Emerging Trends in Pervasive Computing

S. NO	Contents	Contact Hours
UNIT 1	Introduction to Pervasive and Ubiquitous Computing: Definition and concepts of pervasive and ubiquitous computing. Evolution from traditional computing to pervasive environments. Key characteristics: invisibility, context-awareness, and adaptive behavior.	**7**
UNIT 2	Enabling Technologies: Wireless Communication Wi-Fi, Bluetooth, Zigbee, RFID, and NFC. Mobile and sensor networks. Embedded Systems Microcontrollers, embedded operating systems. Internet of Things (IoT) devices and platforms. Context-Aware Computing Sensors and context acquisition. Context modeling and reasoning.	**10**
UNIT 3	Human-Computer Interaction (HCI): Natural User Interfaces (NUIs) Touch, gesture, voice recognition. Wearable Computing Wearable devices and their interaction models. Augmented Reality (AR) Integration of AR in ubiquitous systems.	**11**
UNIT 4	Middleware for Ubiquitous Computing Middleware Architectures and Service-oriented architecture (SOA): Event-driven and agent-based middleware. Resource Management Context-aware resource allocation. Power management in pervasive environments. Security and Privacy: Challenges in Pervasive Computing , Authentication, data privacy, and access control. Privacy-Preserving Techniques	**11**
UNIT 5	Applications of Pervasive Computing Smart Homes and Buildings Automation, energy management, and security systems. Healthcare Wearable health monitors, remote patient monitoring. Smart Cities Transportation systems, environmental monitoring. Retail and Marketing Location-based services, personalized advertising.	**6**

	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	Pervasive Computing: Technology and Architecture of Mobile Internet Applications" by Uwe Hansmann, Lothar Merk, Martin S. Nicklous, and Thomas Stober (2003)	2003
2	Ubiquitous Computing Fundamentals" edited by John Krumm (2010)	2010
3	"Pervasive Computing: Concepts, Technologies, and Applications" by Minyi Guo, Jingyu Zhou, Feilong Tang, and Yao Shen (2016)	2016
4	Security and Privacy in Ubiquitous Computing by Stefan Poslad (2009)	2009

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY438: Digital Twins	**L**	**T**	**P**	**IOT**
	3	**1/0**	**0/2**	

Course Objective: To understand the fundamental principles of Digital Twin technology and explore architecture, modelling, and simulation techniques. To integrate Digital Twins with IoT, AI, and cloud computing. To evaluate the application of Digital Twins in various industries.

S. NO	Course Outcomes (CO)
CO1	Understand the foundational concepts of Digital Twins and their ecosystem.
CO2	Design Digital Twin architectures for real-time systems.
CO3	Apply modeling and simulation tools to develop virtual models.
CO4	Integrate AI, IoT, and cloud platforms for data-driven insights.
CO5	Evaluate Digital Twin applications in various sectors.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to Digital Twins:** Definition and evolution of Digital Twins, Key components: physical entity, virtual model, and data connection, Difference between simulation and Digital Twin, Use cases in manufacturing, healthcare, smart cities	**9**
UNIT 2	**Digital Twin Architecture and Technologies**: Digital Twin Reference Models, System architecture (physical + cyber layer), Data integration, sensors, and real-time monitoring, IoT platforms supporting Digital Twins.	**8**
UNIT 3	**Modelling and Simulation Techniques:** 3D modeling, CAD tools, and BIM, Physics-based vs data-driven models- Simulation tools (e.g., ANSYS, Simulink), Model validation and calibration.	**8**
UNIT 4	**Integration with AI, Cloud, and Edge Computing:** AI for predictive analytics in Digital Twins, Cloud architecture and data storage, Edge computing for real-time decisions, Cybersecurity and data privacy considerations.	**8**
UNIT 5	**Applications and Case Studies:** Industry 4.0 and Digital Manufacturing, Smart cities and infrastructure monitoring, Healthcare and personalized medicine, Case studies (GE, Siemens, NASA, etc.	**9**
	TOTAL	**42**

REFERENCES

S.No.	Name of Books/Authors/Publishers	Year of Publication / Reprint
1	Michael Grieves and John Vickers, "Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior	2021
2	Rajiv Pandey et al., "Digital Twin Technologies and Smart Cities", Springer, 2021	2021

3	Evgeni Gousev et al., "Digital Twin Development and Deployment on the Cloud", Springer, 2020	2020
4	Andreas Tolk, "Engineering Principles of Combat Modeling and Distributed Simulation", Wiley, 2012	2012

B.Tech. Information Technology (Cyber Security)				
Course code: Course Title	**Course Structure**			**Pre-Requisite**
CY440: Robotics	**L**	**T**	**P**	
	3	**1/0**	**0/2**	

Course Objective:

S. NO	Course Outcomes (CO)
CO1	To express his views as per terminologies related to Robotics technology.
CO2	To apply logic for selection of robotic sub systems and systems.
CO3	To analyse basics of principals of robot system integration.
CO4	To understand ways to update knowledge in the required area of robotic technology.

S. NO	Contents	Contact Hours
UNIT 1	**Introduction to robotics :** Brief History, Basic Concepts of Robotics such as Definition , Three laws, Elements of Robotic Systems i.e. Robot anatomy, DOF, Misunderstood devices etc., Classification of Robotic systems on the basis of various parameters such as work volume, type of drive, etc., Associated parameters i.e. resolution, accuracy, repeatability, dexterity, compliance, RCC device etc., Introduction to Principles & Strategies of Automation, Types & Levels of Automations, Need of automation, Industrial applications of robot.	**10**
UNIT 2	Grippers **and Sensors for Robotics:** Grippers for Robotics - Types of Grippers, Guidelines for design for robotic gripper, Force analysis for various basic gripper system. Sensors for Robots - Types of Sensors used in Robotics, Classification and applications of sensors, Characteristics of sensing devices, Selections of sensors. Need for sensors and vision system in the working and control of a robot.	**8**
UNIT 3	**Drives and Control for Robotics:** Drive - Types of Drives, Types of transmission systems, Actuators and its selection while designing a robot system. Control Systems: Types of Controllers, Introduction to closed loop control	**8**
UNIT 4	**Programming and Languages for Robotics**: Robot Programming: Methods of robot programming, WAIT, SIGNAL and DELAY commands, subroutines, Programming Languages: Generations of Robotic Languages, Introduction to various types such as VAL, RAIL, AML, Python, ROS etc., Development of languages since WAVE till ROS.	**8**
UNIT 5	**Related Topics in Robotics:** Socio-Economic aspect of robotisation.	**8**

	Economical aspects for robot design, Safety for robot and standards, Introduction to Artificial Intelligence, AI techniques, Need and application of AI, New trends & recent updates in robotics.	
	TOTAL	**42**

REFERENCES		
S.No.	**Name of Books/Authors/Publishers**	**Year of Publication / Reprint**
1	S. K. Saha, Introduction to Robotics 2e, TATA McGraw Hills Education (2014)	2014
2	Asitava Ghoshal, Robotics: Fundamental concepts and analysis, Oxford University Press (2006)	2006
3	Dilip Kumar Pratihar, Fundamentals of Robotics, Narosa Publishing House, (2019)	2019
4	R. K. Mittal, I. J. Nagrath, Robotics and Control, TATA McGraw Hill Publishing Co Ltd, New Delhi (2003)	2003
5	S. B. Niku, Introduction to Robotics – Analysis, Contro, Applications, 3rd edition, John Wiley & Sons Ltd., (2020)	2020
6	J. Angeles, Fundamentals of Robotic Mechanical Systems Theory Methods and Algorithms, Springer (1997)	1997
7	Mikell Groover, Mitchell Weiss, Roger N. Nagel, Nicholas Odrey, Ashish Dutta, Industrial Robotics 2nd edition, SIE, McGraw Hill Education (India) Pvt Ltd (2012)	2012
8	R. D. Klafter, Thomas A. Chmielewski, and Mechael Negin, Robotic Engineering – An Integrated Approach, EEE, Prentice Hall India, Pearson Education Inc. (2009)	2009