SCHEME & SYLLABUS OF UNDERGRADUATE DEGREE COURSE

B. TECH.
COMPUTER SCIENCE & ENGINEERING
(CYBER SECURITY)

III YEAR
(V & VI Semester)

Effective for the students admitted in year 2021-22 and onwards
Approved by ……. academic council meeting held on …….

Teaching & Examination Scheme
B. Tech. (Computer Science & Engineering (Cyber Security))
3rd Year – V Semester
(Effective for the students admitted in year 2021-22 and onwards)

S. No.	Category	Course Code	Course Title	Hours			Exam Hours	Marks			Credit
				L	T	P		IA	ETE	Total	
	THEORY										
1	DC	5CY4-01	Operating Systems	3	-	-	3	30	70	100	**3**
2		5CY4-02	Computer Organization and Architecture	3	-	-	3	30	70	100	**3**
3		5CY4-03	Computer Networks	3	-	-	3	30	70	100	**3**
4		5CY4-04	Information Security Management	3	-	-	3	30	70	100	**3**
5		5CY4-05	Cryptography and Information Security	3	-	-	3	30	70	100	**3**
6	DE	5CY5-11	Smart Systems	2	-	-	3	30	70	100	**2**
		5CY5-12	Introduction to Data Science								
		5CY5-13	Distributed Systems								
7		5CY5-14	Cloud Computing	2	-	-	3	30	70	100	**2**
		5CY5-15	Introduction to Blockchain								
		5CY5-16	Data Mining and Warehousing								
Sub Total				**19**	**00**	**00**	**-**	**210**	**490**	**700**	**19**
PRACTICAL & SESSIONAL											
8	DC	5CY4-21	Computer Network Lab	-	-	2	-	60	40	100	**1**
9		5CY4-22	Cryptography and Information Security Lab	-	-	2	-	60	40	100	**1**
10		5CY4-23	Risk Analysis Lab	-	-	2	-	60	40	100	**1**
11	UI	5CY7-30	Industrial Training	-	-	1	-	60	40	100	**3**
12	CCA	5CY8-00	SODECA / Co-Curricular Activity	-	-	-	-	-	100	100	**1**
Sub Total				**00**	**00**	**07**	**-**	**240**	**260**	**500**	**7**
Total				**19**	**00**	**07**	**-**	**450**	**750**	**1200**	**26**

L = Lecture, **T** = Tutorial, **P** = Practical, **IA** = Internal Assessment, **ETE** = End Term Exam, **Cr** = Credits

Teaching & Examination Scheme
B. Tech. (Computer Science & Engineering (Cyber Security))
3rd Year – VI Semester
(Effective for the students admitted in year 2021-22 and onwards)

S. No.	Category	Course Code	Course Title	Hours			Exam Hours	Marks			Credit
				L	T	P		IA	ETE	Total	
	THEORY										
1	DC	6CY4-01	Compiler Design	3	-	-	3	30	70	100	**3**
2		6CY4-02	Design and Analysis of Algorithms	3	-	-	3	30	70	100	**3**
3		6CY4-03	Application and Network Security Fundamentals	3	-	-	3	30	70	100	**3**
4		6CY4-04	Network System Vulnerability Assessment	3	-	-	3	30	70	100	**3**
5		6CY4-05	Introduction to Cyber Crime, Law and Investigation	3	-	-	3	30	70	100	**3**
6	DE	6CY5-11	Internet of Things	2	-	-	3	30	70	100	**2**
		6CY5-12	Soft Computing and Evolutionary Algorithms								
		6CY5-13	Information Theory & Coding								
Sub Total				**17**	**00**	**00**		**180**	**420**	**600**	**17**
	PRACTICAL & SESSIONAL										
7	DC	6CY4-21	Design and Analysis of Algorithms Lab	-	-	2	-	60	40	100	**1**
8		6CY4-22	Network System Vulnerability Assessment Lab	-	-	2	-	60	40	100	**1**
9		6CY4-23	Application and Network Security Fundamentals Lab	-	-	2	-	60	40	100	**1**
10	UI	6CY7-50	Innovation and Design Thinking Hands-on Project	-	-	3	-	60	40	100	**2**
11	CCA	6CY8-00	SODECA / Co-Curricular Activity	-	-	-	-	-	100	100	**2**
Sub Total				**00**	**00**	**09**	**-**	**240**	**260**	**500**	**7**
Total				**17**	**00**	**09**	**-**	**420**	**680**	**1100**	**24**

L = Lecture, **T** = Tutorial, **P** = Practical, **IA**=Internal Assessment, **ETE**=End Term Exam, **Cr**=Credits

V Semester
B. Tech. (Computer Science & Engineering (Cyber Security))

5CY4-01: Operating Systems

Credit: 3	**Max. Marks: 100 (IA:30, ETE:70)**
3L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives: As a result of successfully completing this course, students will:

- Learn about how Operating System is Important for Computer System.
- Learn about different types of Operating Systems and their services.
- Learn different process scheduling algorithms and synchronization techniques to achieve better performance of a computer system.
- Learn about device and device management.
- Learn about the concept of memory management and virtual memory.
- Learn about the concept of file system.

Course Outcomes: Upon successful completion of the course the students will be able to

CO-1: Analyze basic concepts of operating systems and their structures.

CO-2: Analyze various issues related to inter-process communication like process synchronization and critical section.

CO-3: Synthesize the concepts of I/O management, file system implementation, scheduling, resource management and deadlocks.

CO-4: Interpret the issues and challenges of memory management.

CO-5: Understand protection and security issues related to the operating system.

S. No.	Contents	Hours
1	**Introduction to OS and Process Management:** Introduction to operating systems, operating system structure, system calls, Process concept, Operations on processes, cooperating processes, inter process communication, mutual exclusion, critical section problem, Synchronization hardware, wait and signal procedures, Semaphores, Classic problems of synchronization, critical regions, Monitors, process scheduling and algorithms, threads, multithreading. **CPU Scheduling**: Scheduling criteria, Scheduling algorithms, Multiple processor scheduling, Real time scheduling	**9**
2	**Memory Management:** Background, Swapping, Contiguous memory allocation, Paging, Segmentation, Segmentation with paging. Virtual Memory, Demand paging, Page replacement policies, Allocation of frames, Thrashing, case study.	**8**
3	**Deadlock and Device Management:** ***Deadlock:*** System model, Deadlock characterization, Methods for handling deadlocks, Deadlock prevention, Deadlock avoidance, Deadlock detection, Recovery from deadlock. ***Device management***: devices and their characteristics, device drivers, device handling, disk scheduling algorithms, Swap space management.	**9**
4	**File Systems and Its Implementation**: File System Interface, File concepts, Access methods, Directory structure, File system mounting, Directory implementation, Allocation methods, Free space management – efficiency and performance, recovery, log structured file systems	**7**
5	**Protection and Case Studies:** ***Protection***: Goals of protection, Principles of protection, Domain of protection, Access matrix, Implementation of access matrix, Access control, Revocation of access rights, file security, user authentication ***Case Study***: Linux Operating System Linux history; Design principles; Kernel modules;	**7**

	Process management; Scheduling; Memory management; File systems, Input and output; Inter-process communication, Case studies of Real Time and Mobile OS.	
Total		**40**

Suggested Books:

1. Silberschatz, Galvin, and Gagne, "Operating System Concepts", Wiley India Pvt Ltd.
2. Modern Operating Systems, Andrew S. Tanenbaum, Herbert Bos, Pearson Education India; Fourth edition 2016. ISBN-13:978- 9332575776
3. Operating Systems: Internals and Design Principles William Stallings, Pearson Education India; 7 edition (2013). ISBN-13: 978-9332518803
4. Gary Nutt, "Operating Systems", Third Edition, Pearson Education
5. Operating Systems: A Design-Oriented Approach, Charles Crowley, International edition, McGraw-Hill Education (ISE Editions). ISBN-13 978 0071144629

V Semester
B. Tech. (Computer Science & Engineering (Cyber Security))

5CY4-02: Computer Organization and Architecture

Credit: 3	**Max. Marks: 100 (IA:30, ETE:70)**
3L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:
As a result of successfully completing this course, students will:

- Learn the principles of computer organization and basic architectural concepts.
- Understand the basics of instructions sets and their impact on processor design.
- Demonstrate an understanding of the design of the functional units of a digital computer system.
- Evaluate cost performance and design trade-offs in designing and constructing a computer processor including memory.
- Design a pipeline for consistent execution of instructions with minimum hazards.
- Recognize and manipulate representations of numbers stored in digital computers.

Course Outcomes:
Upon successful completion of the course, students will be able to

CO-1: Study of the basic structure and operation of a digital computer system.

CO-2: Analysis of the design of arithmetic & logic unit and understanding of the fixed point and floating point arithmetic operations.

CO-3: Implementation of control unit techniques and the concept of Pipelining.

CO-4: Understanding the hierarchical memory system, cache memories and virtual memory.

CO-5: Understanding the different ways of communicating with I/O devices and standard I/O interfaces.

S. No.	Contents	Hours
1	**Introduction:** Objective, scope and outcome of the course.	**1**
2	**Register Transfer and Micro-operations**: Register Transfer Language (RTL), Bus and Memory Transfers, Arithmetic Micro-Operations, Logic Micro-Operations, Shift Micro-Operations, Arithmetic Logic Shift Unit (ALU).	**9**
3	**Basic Computer Organization and Design**: Instruction Codes, Computer Registers, Computer Instructions, Timing and Control, Instruction Cycle, Register-Reference and Memory- Reference Instructions, Input-Output and Interrupt, Design of Basic Computer.	**8**
4	**Central Processing Unit:** General Register Organization, Stack Organization, Instruction Format, Addressing Modes, Data Transfer and Manipulation, Program Control, Reduced Instruction Set Computer (RISC) and Complex Instruction Set Computer (CISC).	**8**
5	**Pipeline and Vector Processing**: Flynn's Taxonomy, Parallel Processing, Pipelining, Arithmetic Pipeline, Instruction Pipeline. **Computer Arithmetic**: Signed Magnitude Binary Numbers - Addition and Subtraction, Multiplication- Booth Multiplication Algorithm, Array Multiplier, Division Algorithm.	**8**
6	**Input-Output Organization**: Input-output Interface Modes of Transfer, Daisy Chaining Priority, Direct Memory Access (DMA), Input-Output Processor (IOP)- CPU-IOP Communication. **Memory Organization**: Memory Hierarchy, Main Memory, Auxiliary Memory, Associative Memory, Cache Memory, Virtual Memory.	**8**
	Total	**42**

Suggested Books:

1. M. Morris Mano, Computer System Architecture, Pearson
2. Carl Hamacher, Zvonko Vranesic, Safwat Zaky Computer Organization, McGraw-Hill, Fifth Edition, Reprint 2012
3. John P. Hayes, Computer Architecture and Organization, Tata McGraw Hill, Third Edition, 1998.
Reference books
4. William Stallings, Computer Organization and Architecture-Designing for Performance, Pearson Education, Seventh edition, 2006.
5. Behrooz Parahami, "Computer Architecture", Oxford University Press, Eighth Impression, 2011.
6. David A. Patterson and John L. Hennessy, "Computer Architecture-A Quantitative Approach", Elsevier, a division of reed India Private Limited, Fifth edition, 2012
7. Structured Computer Organization, Tannenbaum(PHI)

V Semester
B. Tech. (Computer Science & Engineering (Cyber Security))

5CY4-03: Computer Networks

Credit: 3	**Max. Marks: 100 (IA:30, ETE:70)**
3L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:
As a result of successfully completing this course, students will:

- Become familiar with layered communication architectures (OSI and TCP/IP models).
- Understand different services offered by various OSI and TCP/IP model layers.
- Understand the client/server model and key application layer protocols.
- Understand the concept of unreliable data transfer and its role in communication.
- Understand the concepts of reliable data transfer and how TCP implements these concepts.
- Know the principles of congestion control and trade-offs in fairness and efficiency.
- Understand the role and concept of routing in communication.
- Understand the basics of error detection, including parity, checksums, and CRC.
- Familiarize the student with current topics such as security, network management, sensor networks, and/or other topics.

Course Outcomes:
Upon successful completion of the course, students will be able to

CO-1: Understand basic computer network technology.

CO-2: Understand OSI and TCP/IP reference model and working of each layer of these reference models.

CO-3: Obtain the skills of subnetting and routing mechanisms.

CO-4: Address design and implementation aspects of various essential network protocols and its integration into network-based applications.

S. No.	Contents	Hours
1	**Introduction:** history and development of computer networks, networks topologies. Layering and protocols. OSI and TCP/IP Protocol Stacks, Basics of packet, circuit and virtual circuit switching. **Physical Layer:** Guided Transmission media: twisted pairs, coaxial cable, fiber optics, Wireless transmission.	**6**
2	**Data link layer:** Design issues, framing, Error detection and correction. Elementary data link protocols: simplex protocol, A simplex stop and wait protocol for an error-free channel, A simplex stop and wait protocol for noisy channel. Sliding Window protocols: A one-bit sliding window protocol, A protocol using Go-Back-N, A protocol using Selective Repeat, Example data link protocols. Medium Access sub layer: The channel allocation problem, Multiple access protocols: ALOHA, Carrier sense multiple access protocols, collision free protocols. Wireless LANs, Data link layer switching, Ethernet bridging.	**8**
3	**Network Layer:** Design issues, Routing algorithms, shortest path routing, Flooding, Hierarchical routing, Broadcast, Multicast, distance vector routing, link state routing, Congestion Control Algorithms, Quality of Service, Internetworking, Fragmentation, The Network layer in the internet, IP addressing, IPv4, IPv6. CIDR, NAT, Basics of IP support protocols (ARP, DHCP, ICMP)	**8**
4	**Transport Layer:** Transport Services, Elements of Transport protocols, Connection management, Error and Flow Control, Congestion Control, TCP and UDP protocols, Sockets.	**7**
5	**Application Layer**: Domain name system, Electronic Mail; the World Wide Web, HTTP, FTP, Streaming audio and video.	**7**

6.	**Current Topics Related to Computer Network**: Basic overview of the role and working of topic such as Software-defined Networks, Wireless Sensor Networks and Internet of Things, Cyber-physical systems	**6**
	Total	**42**

Suggested Books:

1. Computer Networks, Andrew S. Tanenbaum and David J Wetherall, 5th Edition. Pearson publication.
2. Computer Networking: A Top-Down Approach Featuring the Internet, James F Kurose and Keith W Ross. Pearson publication.
3. Computer Networking: A Top-Down Approach, Behrouz A. Forouzan, Firouz Mosharraf, TMH.
4. Data Communications and Networking – Behrouz A. Forouzan. 4th Edition TMH.
5. Computer Networks: A Systems Approach, 5th Ed., LL Peterson, BS Davie, Morgan-Kauffman, 2011.
6. Cryptography and Network Security, Principles and Practice, 5th Ed., W Stallings, Prentice-Hall, 2010
7. Internet of Things: A Hands-on Approach , by Arshdeep Bagha and Vijay Madisetti, Universities Press, 2015, ISBN: 9788173719547
8. Fundamentals of Cyber-Physical Systems - https://eprints.whiterose.ac.uk/173235/1/Chapter%201 .%20 Fundamentals%20of%20 Cyber-Physical %20Systems.pdf
9. Cyber-Physical Systems and Internet of Things - https://nvlpubs.nist.gov/nistpubs/SpecialPublications /NIST.SP.1900-202.pdf

V Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
5CY4-04: Information Security Management	
Credit: 3	**Max. Marks: 100 (IA:30, ETE:70)**
3L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:

As a result of successfully completing this course, students will:

- To learn threats and risks within context of the information security
- Explain the importance of Security Governance
- Describe various security Standards
- Learn Security management
- Learn Risk treatment methods.

Course Outcomes:

Upon successful completion of the course, students will be able to

CO-1: Understand basic security standards and framework

CO-2: Understand principles of security management

CO-3: Analyze and evaluate the cyber security risks.

CO-4: Understand the Risk assessment and mitigation method.

CO-5: Analyze and evaluate the information security needs of an organization

S. No.	Contents	Hours
1	**Introduction:** Objective, scope and outcome of the course.	**01**
2	**Information Security Standards:** Defining Cyberspace and Cybersecurity, Value of Standards, Good Practice for Information Security, ISO Suite of Information Security Standards, NIST Cybersecurity Framework and Security Documents, CIS Critical Security Controls for Effective Cyber Defense, COBIT-5 for Information Security, Payment Card Industry Data Security Standard, ITU-T Security Documents, Effective Cybersecurity	**08**
3	**Security Governance:** Security Governance and Security Management, Security Governance Principles and Desired Outcomes, Security Governance Components, Security Governance Evaluation, Security Governance	**07**
4	**Information Risk Assessment:** Risk Assessment Concepts, System Assessment Approaches, Asset Identification, Threat Identification, Control Identification, Vulnerability Identification, Consequences Identification, Risk Analysis, Risk Evaluation, Risk Treatment, Risk Assessment	**08**
5	**Security Management:** Security Management Function, Security Policy, Acceptable Use Policy, Security Management **Information Management:** Information Classification and Handling, Privacy, Document and Records Management, Sensitive Physical Information, Information Management	**08**
6	**People Management:** Human Resource Security, Security Awareness and Education, **Physical Asset Management:** Hardware Life Cycle Management, Office Equipment, Industrial Control Systems, Mobile Device Security, Physical Asset Management	**08**
	Total	**40**

Suggested Books:

1. Effective Cybersecurity: A Guide to Using Best Practices and Standards by William Stallings, August 2018, Addison-Wesley Professional, ISBN: 9780134772929

V Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
5CY4-05: Cryptography and Information Security	
Credit: 3	**Max. Marks: 100 (IA:30, ETE:70)**
3L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:

As a result of successfully completing this course, students will:

- Explain the objectives of information security.
- Explain the importance and application of each of confidentiality, integrity, authentication and availability.
- Describe public-key cryptosystem.
- Describe the enhancements made to IPv4 by IPSec.
- Discuss the fundamental ideas of public-key cryptography.
- Generate and distribute a PGP key pair and use the PGP package to send an encrypted email message.
- Discuss Web security and Firewalls.

Course Outcomes:

Upon successful completion of the course, students will be able to

CO-1: Understand basic cryptographic algorithms, message and web authentication and security issues.

CO-2: Understand Intrusions and intrusion detection

CO-3: Understand the basic categories of threats to computers and networks.

CO-4: Ability to identify information system requirements for both of them such as client and server.

CO-5: Understand the current legal issues towards information security.

S. No.	Contents	Hours
1	**Introduction:** Objective, scope and outcome of the course.	**01**
2	**Security Concepts:** Introduction, The need for security, Security approaches, Principles of security, Types of Security attacks, Security services, Security Mechanisms, A model for Network Security. **Cryptography Concepts and Techniques:** Introduction, plain text and cipher text, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography, steganography, key range and key size, possible types of attacks.	**07**
3	**Symmetric key Ciphers**: Block Cipher principles, DES, AES, Blowfish, RC5, IDEA, Block cipher operation, Stream ciphers, RC4. **Asymmetric key Ciphers:** Principles of public key cryptosystems, RSA algorithm, Elgamal Cryptography, Diffie-Hellman Key Exchange, Knapsack Algorithm.	**08**
4	**Cryptographic Hash Functions:** Message Authentication, Secure Hash Algorithm (SHA-512), **Message authentication codes:** Authentication requirements, HMAC, CMAC, Digital signatures, Elgamal Digital Signature Scheme. **Key Management and Distribution:** Symmetric Key Distribution Using Symmetric & Asymmetric Encryption, Distribution of Public Keys, Kerberos, X.509 Authentication Service, Public – Key Infrastructure.	**10**
5	**Transport-level Security**: Web security considerations, Secure Socket Layer and Transport Layer Security, HTTPS, Secure Shell (SSH). **Wireless Network Security:** Wireless Security, Mobile Device Security, IEEE 802.11 Wireless LAN, IEEE 802.11i Wireless LAN Security.	**08**
6	**E-Mail Security:** Pretty Good Privacy, S/MIME **IP Security:** IP Security overview, IP Security architecture, Authentication Header,	**08**

	Encapsulating security payload, Combining security associations, Internet Key Exchange **Case Studies on Cryptography and security:** Secure Multiparty Calculation, Virtual Elections, Single sign On, Secure Inter-branch Payment Transactions, Cross site Scripting Vulnerability	
	Total	**42**

Suggested Books:

1. Cryptography and Network Security - Principles and Practice: William Stallings, Pearson Education, 6th Edition.
2. Cryptography and Network Security: Atul Kahate, Mc Graw Hill, 3rd Edition.
3. Cryptography and Network Security: C K Shyamala, N Harini, Dr T R Padmanabhan, Wiley India, 1st Edition.
4. Cryptography and Network Security: Forouzan Mukhopadhyay, Mc Graw Hill, 3rd Edition.
5. Information Security, Principles, and Practice: Mark Stamp, Wiley India.
6. Principles of Computer Security: WM. Arthur Conklin, Greg White, TMH.
7. Introduction to Network Security: Neal Krawetz, CENGAGE Learning.
8. Network Security and Cryptography: Bernard Menezes, CENGAGE Learning.

V Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
5CY5-11: Smart Systems	
Credit: 2	**Max. Marks: 100 (IA:30, ETE:70)**
2L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:

As a result of successfully completing this course, students will:

- To introduce the fundamental concepts of MEMS based sensors and actuators.
- To acquaint the students with various materials and material properties for Microsystem designing.
- To provide comprehensive understanding of various micromachining techniques and expose the students to design, simulation and analysis software.

Course Outcomes:

Upon successful completion of the course, students will be able to

CO-1: Identify and understand the fundamental concepts and background of MEMS and Microsystems.

CO-2: Familiar with the basics of various sensors and actuators.

CO-3: Recognize and interpret various micromachining techniques and design, analysis and applications of various MEMS devices micromachining tools and techniques

CO-4: Incorporate simulation and micro-fabrication knowledge for developing various MEMS devices.

S. No.	Contents	Hours
1	Introduction to Sensor Devices, Piezoresistive pressure sensor, Piezoresistive Accelerometer, Capacitive Sensing, Accelerometer and Microphone, Resonant Sensor and Vibratory Gyroscope, Low-Power, Low Voltage Sensors Micro Electro Mechanical Systems Analysis and Design of MEMS Devices- Nano Sensors.	**5**
2	Interfacing Sensor Information and MCU Amplification and Signal Conditioning, Integrated Signal Conditioning, Digital conversion, MCU Control MCUs for Sensor Interface, Techniques and System Consideration, Sensor Integration.	**6**
3	Control Techniques and Standards Control of Sensors using - State Machines, Fuzzy Logic, Neural Networks, Adaptive Control. Control Application using - CISC, RISC, DSP Control and IEEE 1451 Standards.	**6**
4	Communication For Smart Sensors Wireless Data Communications- RF Sensing, Telemetry, Automotive Protocols, Industrial Networks Home Automation, MCU Protocols.	**6**
5	Packaging, Testing and Reliability Implications of Smart Sensors Semiconductor Packaging- Hybrid Packaging- Packaging for Monolithic Sensors- Reliability Implications Testing Smart Sensors- HVAC Sensor Chip	**5**
	Total	**28**

Suggested Books:

1. G. K. Ananthasuresh, K J Vinoy, S Gopalakrishnan, KN Bhatt, V K Aatre," Micro and Smart Systems: Technology and Modeling ", 2012, 1st ed., Wiley, New York.
2. Tai-Ran Hsu, “MEMS & Microsystem, Design and Manufacture”, 2017, 1st ed., McGraw Hill India, New Delhi.
3. Wolfgang Menz, Jürgen Mohr, Oliver Paul, "Microsystem Technology", 2011, 2nd ed., Wiley, New York.
4. Banks H.T. Smith R.C. and Wang Y. Smart, ‘Material Structures – Modeling, Estimation and Control’, 2011, 1st ed., John Wiley & Sons, NewYork.
5. Artificial Intelligence: A Modern Approach by S. Russell and P. Norvig, Prentice Hall.

V Semester
B. Tech. (Computer Science & Engineering (Cyber Security))

5CY5-12: Introduction to Data Science

Credit: 2	**Max. Marks: 100 (IA:30, ETE:70)**
2L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives: As a result of successfully completing this course, students will:

- To understand EDA, inference and regression techniques.
- Apply Matrix decomposition techniques to perform data analysis.
- Understand concepts and importance of data pre-processing techniques.
- Importance and application of Machine Learning Algorithms.
- Knowledge of acquiring data through web-scraping and data APIs

Course Outcomes: Upon successful completion of the course, students will be able to

CO-1: Utilize EDA, inference and regression techniques.
CO-2: Utilize Matrix decomposition techniques to perform data analysis.
CO-3: Apply data pre-processing techniques.
CO-4: Apply Basic Machine Learning Algorithms.
CO-5: Acquire data through web-scraping and data APIs.

S. No.	Contents	Hours
1	**Introduction:** Objective, scope and outcome of the course.	**1**
2	Introduction to data analysis: Introduction and importance of data science. Big Data Analytics, Business intelligence vs Big data, Current landscape of analytics, Exploratory Data Analysis (EDA), statistical measures, Basic tools (plots, graphs and summary statistics) of EDA, Data Analytics Lifecycle, Discovery, Data Visualization Principles of Data Visualization	**6**
3	Introductory hypothesis testing and statistical inference: Introduction to Hypothesis Testing, Central Limit Theorem, A/B testing. Identifying Potential Data Sources Linear regression - Introduction to simple linear regression, multiple linear regression, least squares principle, exploratory vs. inferential viewpoints, Model generalizability, cross validation, and using categorical variables in regression, logistic regression, Multiple correlation, Partial correlation	**5**
4	Linear Algebra Basics- Matrices to represent relations between data, Linear algebraic operations on matrices – Matrix decomposition: Singular Value Decomposition (SVD) and Principal Component Analysis (PCA).	**5**
5	Data Pre-processing and Feature Selection - Data cleaning - Data integration - Data Reduction - Data Transformation and Data Discretization, Feature Generation and Feature Selection, Feature Selection algorithms: Filters- Wrappers - Decision Trees - Random Forests	**6**
6	Basic Machine Learning Algorithms - Classifiers - Decision tree - Naive Bayes - k-Nearest Neighbors (k-NN), k-means – SVM Association Rule mining – Ensemble methods	**5**
	Total	**28**

Suggested Books:

1. Mining of Massive Datasets. v2.1, Jure Leskovek, Anand Rajaraman and Jefrey Ullman., Cambridge University Press. (2019)
2. Doing Data Science, Straight Talk From The Frontline, Cathy O'Neil and Rachel Schutt, O'Reilly
3. Python for Data Analysis: Data Wrangling with Pandas, NumPy, & IPython Wes McKinney, O'Reilly Media
4. Hands-On Machine Learning with Scikit-Learn and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems, Aurélien Géron, O'Reilly Media

V Semester
B. Tech. (Computer Science & Engineering (Cyber Security))

5CY5-13: Distributed Systems

Credit: 2	**Max. Marks: 100 (IA:30, ETE:70)**
2L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives: As a result of successfully completing this course, students will:

- To Understand hardware and software issues in modern distributed systems.
- To get knowledge in distributed architecture, naming, synchronization, consistency and replication, fault tolerance, security, and distributed file systems.
- To analyze the current popular distributed systems such as peer-to-peer (P2P) systems will also be analyzed.

Course Outcomes: Upon successful completion of the course, students will be able to

CO-1: To understand the foundations of distributed systems.

CO-2: To learn issues related to clock Synchronization and the need for global state in distributed systems.

CO-3: To learn distributed mutual exclusion and deadlock detection algorithms.

CO-4: To understand the significance of agreement, fault tolerance and recovery protocols in Distributed Systems.

CO-5: To learn the characteristics of peer-to-peer and distributed shared memory systems

S. No.	Contents	Hours
1	**Introduction:** Objective, scope and outcome of the course.	**1**
2	**Distributed Systems:** Features of distributed systems, nodes of a distributed system, Distributed computation paradigms, Model of distributed systems, Types of Operating systems: Centralized Operating System, Network Operating Systems, Distributed Operating Systems and Cooperative Autonomous Systems, design issues in distributed operating systems. Systems Concepts and Architectures: Goals, Transparency, Services, Architecture Models, Distributed Computing Environment (DCE).	**5**
3	**Theoretical issues in distributed systems:** Notions of time and state, states and events in a distributed system, time, clocks and event precedence, recording the state of distributed systems. **Concurrent Processes and Programming:** Processes and Threads, Graph Models for Process Representation, Client/Server Model, Time Services, Language Mechanisms for Synchronization.	**5**
4	**Distributed Process Scheduling:** A System Performance Model, Static Process Scheduling with Communication, Dynamic Load Sharing and Balancing, Distributed Process Implementation. Distributed File Systems: Transparencies and Characteristics of DFS, DFS Design and implementation, Transaction Service and Concurrency Control	**5**
5	**Distributed Shared Memory**: Non-Uniform Memory Access Architectures, Memory Consistency Models, Multiprocessor Cache Systems, Distributed Shared Memory, Implementation of DSM systems.	**6**
6	**Distributed Agreement:** Concept of Faults, failure and recovery, Replicated Data Management: concepts and issues, Database Techniques, Atomic Multicast, and Update Propagation. CORBA case study: Introduction, Architecture, CORBA RMI, CORBA Services.	**6**
	Total	**28**

Suggested Books:

1. Distributed Systems, Principles and Paradigms, 2nd edition by Andrew S. Tanenbaum and Maarteen Van Steen, Pearson Education, (ISBN-13: 978- 0132392273), 2013 IT-89
2. Distributed System: Concepts and Design, 5th edition by Coulouris, Dollimore, Kindberg,Pearson Ed, (ISBN-13: 978-0132143011), 2013

3. Distributed Algorithms: Principles, Algorithms, and Systems by A. D. Kshemkalyani and M. Singhal, (ISBN-13: 978-0521189842) , 2013

V Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
5CY5-14: Cloud Computing	
Credit: 2	**Max. Marks: 100 (IA:30, ETE:70)**
2L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:

As a result of successfully completing this course, students will:

- The fundamental ideas behind Cloud Computing, the evolution of the paradigm, its applicability; benefits
- The basic ideas and principles in data center design; cloud management techniques and cloud software deployment considerations;
- Different CPU, memory and I/O virtualization techniques in cloud

Course Outcomes:

Upon successful completion of the course, students will be able to

CO-1: Explain the core concepts of the cloud computing paradigm

CO-2: Discuss system, network and storage virtualization and outline their role in enabling the cloud computing system model.

CO-3: Understanding security architecture of cloud infrastructure

S. No.	Contents	Hours
1	**Introduction:** Objective, scope and outcome of the course.	**1**
2	**Cloud Computing:** Nutshell of cloud computing, Enabling Technology, Historical development, Vision, feature Characteristics and components of Cloud Computing. Challenges, Risks and Approaches of Migration into Cloud. Ethical Issue in Cloud Computing, Evaluating the Cloud's Business Impact and economics, Future of the cloud. Networking Support for Cloud Computing.	**5**
3	**Cloud Computing Architecture:** Cloud Reference Model, Layer and Types of Clouds, Services models, Data centre Design and interconnection Network, Architectural design of Compute and Storage Clouds. Cloud Programming and Software: Fractures of cloud programming, Parallel and distributed programming paradigms-Map Reduce, Hadoop, High level Language for Cloud. Programming of Google App engine	**6**
4	**Virtualization Technology:** Definition, Understanding and Benefits of Virtualization. Implementation Level of Virtualization, Virtualization Structure/Tools and Mechanisms, Hypervisor VMware, KVM, Xen. Virtualization of CPU, Memory, I/O Devices, Virtual Cluster and Resources Management, Virtualization of Server, Desktop, Network, and Virtualization of data-centre	**5**
5	**Securing the Cloud:** Cloud Information security fundamentals, Cloud security services, Design principles, Policy Implementation, Cloud Computing Security Challenges, Cloud Computing Security Architecture . Legal issues in cloud Computing.	**5**
6	**Data Security in Cloud:** Business Continuity and Disaster Recovery , Risk Mitigation , Understanding and Identification of Threats in Cloud, SLA-Service Level Agreements, Trust Management	**6**
	Total	**28**

Suggested Books:

1. Rajkumar Buyya, James Broberg, Andrzej M. Goscinski: "Cloud Computing: Principles and Paradigms", Wiley, 2011
2. Rajkumar Buyya, Christian Vecchiola, S Thamarai Selvi, Mastering Cloud Computing, Tata McGraw Hill, 2013
3. Barrie Sosinsky: "Cloud Computing Bible", Wiley-India, 2010

4. Ronald L. Krutz, Russell Dean Vines: "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley-India, 2010
5. Tim Mather, Subra Kumara swamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 2009.

V Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
5CY5-15: Introduction to Blockchain	
Credit: 2	**Max. Marks: 100 (IA:30, ETE:70)**
2L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:

As a result of successfully completing this course, students will:

- The students should be able to understand a broad overview of the essential concepts of blockchain technology.
- To familiarize students with Bitcoin protocol followed by the Ethereum protocol – to lay the foundation necessary for developing applications and programming.
- Students should be able to learn about different types of blockchain and consensus algorithms.

Course Outcomes:

Upon successful completion of the course, students will be able to

CO-1: To explain the basic notion of distributed systems.

CO-2: To use the working of an immutable distributed ledger and trust model that defines blockchain.

CO-3: To illustrate the essential components of a blockchain platform.

S. No.	Contents	Hours
1	**Introduction:** Objective, scope and outcome of the course.	**1**
2	Basics: The Double-Spend Problem, Byzantine Generals' Computing Problems, Public-Key Cryptography, Hashing, Distributed Systems, Distributed Consensus.	**5**
3	Technology Stack: Blockchain, Protocol, Currency. Bitcoin Blockchain: Structure, Operations, Features, Consensus Model, Incentive Model	**5**
4	Ethereum Blockchain: Smart Contracts, Ethereum Structure, Operations, Consensus Model, Incentive Model.	**5**
5	Tiers of Blockchain Technology: Blockchain 1.0, Blockchain 2.0, Blockchain 3.0, Types of Blockchain: Public Blockchain, Private Blockchain, Semi-Private Blockchain, Sidechains.	**6**
6	Types of Consensus Algorithms: Proof of Stake, Proof of Work, Delegated Proof of Stake, Proof Elapsed Time, Deposite-Based Consensus, Proof of Importance, Federated Consensus or Federated Byzantine Consensus, Practical Byzantine Fault Tolerance. Blockchain Use Case: Supply Chain Management.	**6**
Total		**28**

Suggested Books:

1. Kirankalyan Kulkarni, Essentials of Bitcoin and Blockchain, Packt Publishing.
2. Anshul Kaushik, Block Chain & Crypto Currencies, Khanna Publishing House.
3. Tiana Laurence, Blockchain for Dummies, 2nd Edition 2019, John Wiley & Sons.
4. Mastering Blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular Blockchain frameworks by Imran Bashir, Packt Publishing (2017).
5. Blockchain: Blueprint for a New Economy by Melanie Swan, Shroff Publisher O'Reilly Publisher Media; 1st edition (2015).

V Semester
B. Tech. (Computer Science & Engineering (Cyber Security))

5CY5-16: Data Mining and Warehousing

Credit: 2	**Max. Marks: 100 (IA:30, ETE:70)**
2L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:
As a result of successfully completing this course, students will:

- To introduce the fundamental processes data warehousing and major issues in data mining
- To impart the knowledge on various data mining concepts and techniques that can be applied to text mining, web mining etc.
- To develop the knowledge for application of data mining and social impacts of data mining.

Course Outcomes:
Upon successful completion of the course, students will be able to

CO-1: Interpret the contribution of data warehousing and data mining to the decision-support systems.

CO-2: Prepare the data needed for data mining using preprocessing techniques.

CO-3: Extract useful information from the labeled data using various classifiers.

CO-4: Compile unlabeled data into clusters applying various clustering algorithms.

CO-5: Discover interesting patterns from large amounts of data using Association Rule Mining

S. No.	Contents	Hours
1	**Introduction:** Objective, scope and outcome of the course.	**1**
2	**Introduction to Data Mining:** Introduction to data mining-Data mining functionalities-Steps in data mining process- Classification of data mining systems, Major issues in data mining. Data Wrangling and Preprocessing: Data Preprocessing: An overview-Data cleaning-Data transformation and Data discretization	**5**
3	**Predictive Modeling:** General approach to classification-Decision tree induction- Bayes classification methods- advanced classification methods: Bayesian belief networks Classification by Backpropagation- Support Vector Machines-Lazy learners	**6**
4	**Descriptive Modeling:** Types of data in cluster analysis-Partitioning methods- Hierarchical methods-Advanced cluster analysis: Probabilistic model-based clustering- Clustering high dimensional data-Outlier analysis	**5**
5	**Discovering Patterns and Rules:** Frequent Pattern Mining: Basic Concepts and a Road Map - Efficient and scalable frequent item set mining methods: Apriori algorithm, FP-Growth algorithm- Mining frequent item sets using vertical data format- Mining closed and max patterns Advanced Pattern Mining: Pattern Mining in Multilevel, Multidimensional Space	**5**
6	**Data Mining Trends and Research Frontiers:** Other methodologies of data mining: Web mining Temporal mining-Spatial mining-Statistical data mining- Visual and audio data mining- Data mining applications- Data mining and society: Ubiquitous and invisible data mining- Privacy, Security, and Social Impacts of data mining	**6**
	Total	**28**

Suggested Books:

1. Jiawei Han and Micheline Kamber, Data Mining: Concepts and Techniques, Morgan Kaufmann Publishers, third edition ,2013
2. Pang-Ning Tan, Michael Steinbach, Anuj Karpatne, Vipin Kumar, Introduction to Data Mining, second edition, Pearson, 2019
3. Ian. H. Witten, Eibe Frank and Mark. A. Hall, Data Mining: Practical Machine Learning Tools and Techniques, third edition , 2017

4. Alex Berson and Stephen J. Smith, Data Warehousing, Data Mining & OLAP, Tata McGraw Hill Edition, Tenth Reprint, 2008.
5. Hand, D., Mannila, H. and Smyth, P. Principles of Data Mining, MIT Press: Massachusetts third edition, Pearson, 2013

V Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
5CY4-21: Computer Network Lab	
Credit: 1	**Max. Marks: 100 (IA:60, ETE:40)**
0L+0T+ 2P	**End Term Exams: 2 Hours**

Course Objectives:
As a result of successfully completing this course, students will:

- To introduce the concepts of LAN, Network topologies
- To write client server based programs

Course Outcomes:

Upon successful completion of the course, students will be able to

CO-1: Understand fundamentals of networking

CO-2: Implementing server and client connections that facilitate the study of networking concepts and protocols.

S. No.	List of Experiments
1	Study of Different Type of LAN& Network Equipment.
2	Study and Verification of standard Network topologies i.e. Star, Bus, Ring etc.
3	LAN installations and Configurations.
4	Write a program to implement various types of error correcting techniques.
5	Write a program to implement various types of framing methods.
6	Write two programs in C: hello client and hello server a. The server listens for, and accepts, a single TCP connection; it reads all the data it can from that connection, and prints it to the screen; then it closes the connection b. The client connects to the server, sends the string “Hello, world!”, then closes the connection
7	Write an Echo Client and Echo server using TCP to estimate the round trip time from client to the server. The server should be such that it can accept multiple connections at any given time.
8	Repeat Exercises 6 & 7 for UDP.
9	Repeat Exercise 7 with multiplexed I/O operations.
10	Simulate Bellman-Ford Routing algorithm in NS2.
11	Analysis of packets using Wireshark, Network simulations

Suggested Books:

1. James F. Kurose, Computer networking: Atop-down approach featuring the internet, 6/E. Pearson Education India, 2005/2012
2. Ilya Grigori, High Performance Browser Networking: What every web developer should know about networking and web performance. “O’Reilly Media, Inc.", 2013.
3. Online Resources: Interactive animations, Video notes from Kurose and Ross 2012, Wire shark assignments, Presentation slides, interactive exercises from the following
4. link:http://wps.pearsoned.com/ecs_kurose_compnetw_6/216/55463/14198700.cw/

V Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
5CY4-22: Cryptography and Information Security Lab	
Credit: 1	**Max. Marks: 100 (IA:60, ETE:40)**
0L+0T+ 2P	**End Term Exams: 2 Hours**

Course Objectives:

As a result of successfully completing this course, students will:

- Explain the objectives of information security.
- Understand the importance and application of each of confidentiality, integrity, authentication and availability.
- Understand various cryptographic algorithms.

Course Outcomes:

Upon successful completion of the course, students will be able to

CO-1: Understand basic cryptographic algorithms.

CO-2: Understand message and web authentication.

CO-3: Understand various security issues.

CO-4: Identify information system requirements for both of them such as client and server.

CO-5: Understand the current legal issues towards information security.

S. No.	List of Experiments
1	Write a C program that contains a string (char pointer) with a value 'Hello world'. The program should XOR each character in this string with 0 and displays the result.
2	Write a C program that contains a string (char pointer) with a value 'Hello world'. The program should AND or and XOR each character in this string with 127 and display the result.
3	Write a Java program to perform encryption and decryption using the following algorithms a. Ceaser Cipher b. Substitution Cipher c. Hill Cipher
4	Write a C/JAVA program to implement the DES algorithm logic
5	Write a C/JAVA program to implement the Blowfish algorithm logic.
6	Write a C/JAVA program to implement the Rijndael algorithm logic.
7	Write the RC4 logic in Java Using Java cryptography; encrypt the text "Hello world" using Blowfish. Create your own key using Java key tool.
8	Write a Java program to implement RSA algorithm.
9	Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript.
10	Calculate the message digest of a text using the SHA-1 algorithm in JAVA.
11	Calculate the message digest of a text using the MD5 algorithm in JAVA.

Suggested Books:

1. Cryptography and Network Security - Principles and Practice: William Stallings, Pearson Education, 6th Edition.
2. Cryptography and Network Security: Atul Kahate, McGraw Hill, 3rd Edition.
3. Cryptography and Network Security: C K Shyamala, N Harini, Dr T R Padmanabhan, Wiley India, 1st Edition.
4. Cryptography and Network Security: Forouzan Mukhopadhyay, McGraw Hill, 3rd Edition.
5. Information Security, Principles, and Practice: Mark Stamp, Wiley India.
6. Principles of Computer Security: WM. Arthur Conklin, Greg White, TMH.
7. Introduction to Network Security: Neal Krawetz, CENGAGE Learning.
8. Network Security and Cryptography: Bernard Menezes, CENGAGE Learning.

V Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
5CY4-23: Risk Analysis Lab	
Credit: 1	**Max. Marks: 100 (IA:60, ETE:40)**
0L+0T+ 2P	**End Term Exams: 2 Hours**

Course Objectives:

As a result of successfully completing this course, students will:

- Understanding the attack surfaces, risk landscape.
- Explain the Risk Assessment Methods.
- Evaluate and select appropriate risk treatment options according to the combination of impacts and probabilities that the risk analysis has produced.

Course Outcomes:

Upon successful completion of the course, students will be able to

CO-1: Understand the principles of risk analysis and management and the purpose and benefits behind such activities.

CO-2: Learn risk, analysis, management, vulnerability, threats, actors, impact, risk matrix.

CO-3: Recognize the difference between vulnerabilities and threats.

CO-4: Classify and describe a number of different risk assessment/management methodologies.

CO-5: Identify and explain various threat sources and the impacts that their materialization may manifest.

S. No.	List of Experiments
1	**Case Study: Risk Assessment and Management Framework (Any One: OCTAVE-Allegro, OCTAVE-S, ISMS, any other)** **Identify and Prioritize Assets:** For each asset, gather the following information, as applicable: • Software • Hardware • Data • Interfaces • Users • Support personnel • Mission or purpose • Criticality • Functional requirements • IT security policies • IT security architecture • Network topology • Information storage protection • Information flow • Technical security controls • Physical security environment • Environmental security
2	**Identify Threats:** A threat is anything that could cause harm to your organization. While hackers and malware probably leap to mind, there are many other types of threats.

3	**Identify Vulnerabilities:** A vulnerability is a weakness that could enable a threat to harm your organization. Vulnerabilities can be identified through analysis, audit reports, the NIST vulnerability database, vendor data, information security test and evaluation (ST&E) procedures, penetration testing, and automated vulnerability scanning tools.Don't limit your thinking to software vulnerabilities; there are also physical and human vulnerabilities.
4	**Analyze Controls:** Analyze the controls that are either in place or in the planning stage to minimize or eliminate the probability that a threat will exploit vulnerability. Technical controls include encryption, intrusion detection mechanisms, and identification and authentication solutions. Nontechnical controls include security policies, administrative actions, and physical and environmental mechanisms. Both technical and nontechnical controls can further be classified as preventive or detective.
5	**Determine the Likelihood of an Incident:** Assess the probability that vulnerability might actually be exploited, taking into account the type of vulnerability, the capability and motivation of the threat source, and the existence and effectiveness of your controls. Rather than a numerical score, many organizations use the categories high, medium and low to assess the likelihood of an attack or other adverse event.
6	**Assess the Impact a Threat Could Have:** Analyze the impact that an incident would have on the asset that is lost or damaged, including the following factors: • The mission of the asset and any processes that depend upon it • The value of the asset to the organization • The sensitivity of the asset
7	**Prioritize the Information Security Risks:** For each threat/vulnerability pair, determine the level of risk to the IT system, based on the following: • The likelihood that the threat will exploit the vulnerability • The approximate cost of each of these occurrences • The adequacy of the existing or planned information system security controls for eliminating or reducing the risk A useful tool for estimating risk in this manner is the risk-level matrix.
8	**Recommend Controls:** Using the risk level as a basis, determine the actions needed to mitigate the risk. Here are some general guidelines for each level of risk: • High — A plan for corrective measures should be developed as soon as possible. • Medium — A plan for corrective measures should be developed within a reasonable period of time. • Low — The team must decide whether to accept the risk or implement corrective actions.
9	**Document the Results:** The final step in the risk assessment process is to develop a risk assessment report to support management in making appropriate decisions on budget, policies, procedures and so on. For each threat, the report should describe the corresponding vulnerabilities, the assets at risk, the impact to your IT infrastructure, the likelihood of occurrence and the control recommendations (In tabular Form).

Suggested Books:

1. JohnVeiga, Gary McGraw,"Building Secure Software: How to Avoid Security Problems the Right Way", Addison-Wesley Professional Computing Series, 2001
2. A.Refsdal, B. Solhaug, K. Stolen, " Cyber-Risk Management", Springer, 2015/Latest Edition.
3. E. Wheeler, "Security Risk Management", O'Reilly, 2011/Latest Edition.

4. R. Bentham, "Cyber Risk Management: Practical Strategies to Protect your Organization from Cyber Threats", Kogan Page, 2018/Latest Edition
5. C.J. Hodson, "Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls", Kogan Page, 2019/Latest Edition.

VI Semester
B. Tech. (Computer Science & Engineering (Cyber Security))

6CY4-01: Compiler Design

Credit: 3	**Max. Marks: 100 (IA:30, ETE:70)**
3L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:
As a result of successfully completing this course, students will:

- Familiar with basic ideas and the working of the compiler.
- Learn about syntax analysis.
- Learn about representation in the form of DAG.
- Learn about theory knowledge of Parsing, Code generation, and optimization.

Course Outcomes:
Upon successful completion of the course, students will be able to

CO-1: Acquire knowledge of different phases and passes of the compiler and use compiler tools like LEX and YACC.

CO-2: Understand the Top-Down and Bottom-up parsers and construction of LL, SLR, CLR, and LALR parsing tables.

CO-3: Acquire knowledge about runtime data structure, like symbol table organization and different techniques.

CO-4: Understand the target machine's run time environment, its instruction set for code generation, and techniques for code optimization.

S. No.	Contents	Hours
1	**Introduction:** Objective, scope, and outcome of the course. Compiler, Translator, Interpreter definition, Phase of compiler, Bootstrapping, Review of Finite automata lexical analyzer, Input, Recognition of tokens, Idea about LEX: A lexical analyzer generator, Error handling.	**6**
2	**Review of CFG Ambiguity of grammars:** Introduction to parsing. Top-down parsing, LL grammars & passers error handling of LL parser, Recursive descent parsing predictive parsers, Bottom-up parsing, Shift reduce parsing, LR parsers, Construction of SLR, Conical LR & LALR parsing tables, parsing with ambiguous grammar. Operator precedence parsing, Introduction of automatic parser generator: YACC error handling in LR parsers.	**10**
3	**Syntax-directed translation:** Construction of syntax trees, S-Attributed Definition, L-attributed definitions, Top-down translation. Intermediate code forms using postfix notation, DAG, Three address code, TAC for various control structures, Representing TAC using triples and quadruples, Boolean expression, and control structures.	**10**
4	**Runtime environments:** Storage allocation, Strategies, heap management, Activation records, Accessing local and non-local names in a block structured language, Parameters passing, Symbol table organization, Data structures used in symbol tables.	**8**
5	**Definition of basic block control flow graphs:** DAG representation of basic block, Advantages of DAG, Sources of optimization, Loop optimization, Loop invariant computation, Peephole optimization, Issues in the design of code generator, A simple code generator, Code generation from DAG. Machine Independent Optimization: Idea about global data flow analysis, constant propagation, liveness analysis, and common subexpression elimination.	**6**
	Total	**40**

Suggested Books:

1. Compilers: Principles, Techniques, and Tools, Second Edition, Alfred Aho, Monica Lam, Ravi Sethi, Jeffrey D. Ullman, January 2013. ISBN-978-9332518667.
2. Modern Compiler Implementation in Java. Andrew W Appel, Jens Paisberg. Cambridge University Press, January 2002. ISBN-978-0521820608
3. Modern Compiler Implementation in ML, Andrew W Appel, Cambridge University Press, December 1997. ISBN-0 521 58274 1
4. Modern Compiler Implementation in C, Andrew W Appel, Cambridge University Press, December 1997. ISBN 0-521-60765-5
5. Compiler Construction: Principles and Practice, 1st Edition, Kenneth C. Louden, Cengage Learning; 1 edition (January 24, 1997), ISBN-13: 978-0534939724
6. V Raghvan, " Principles of Compiler Design," McGraw-Hill, ISBN:9780070144712

VI Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
6CY4-02: Design and Analysis of Algorithms	
Credit: 3	**Max. Marks: 100 (IA:30, ETE:70)**
3L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:
As a result of successfully completing this course, students will:

- Able to analyze asymptotic runtime complexity of algorithms including formulating recurrence relations.
- Able to understand and design algorithms using greedy strategy, divide and conquer approach, dynamic programming.
- Demonstrate a familiarity with major algorithms and data structures and Synthesize efficient algorithms in common engineering design situations

Course Outcomes:
Upon successful completion of the course the students will be able to
CO-1: The ability of how to design an algorithm which solves the current problem in hand.
CO-2: To Write efficient algorithms for given problems.
CO-3: To focus on Deriving the complexities of any given algorithm.
CO-4: Learning the programming of various algorithms through assignments

S. No.	Contents	Hours
1	**Introduction**: Concept of algorithmic efficiency, run time analysis of algorithms, Asymptotic Notations. Growth of Functions, Master's Theorem,	**5**
2	**Searching and Sorting:** 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**
3	**Greedy Method:** Overview of the greedy paradigm examples of exact optimization solution: 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, Activity Selection Problem.	**8**
4	**Dynamic programming:** Principles of dynamic programming. Applications: Rod cutting problem, Floyd-Warshall algorithm for all pair shortest paths. Matrix multiplication, travelling salesman Problem, Longest Common sequence, Back tracking: Overview, 8-queen problem, and Knapsack problem, Traveling Salesman problem.	**7**
5	**Branch and bound:** LC searching Bounding, FIFO branch and bound, LC branch and bound application: 0/1 Knapsack problem	**6**
6	**Computational Complexity:** Polynomial Vs non-polynomial time complexity; NP-hard and NP-complete classes, examples: Circuit Satisfiablity, Vertex cover, Subset Sum problem, Randomized Algorithms, String Matching, NP-Hard and NP Completeness, Introduction to Approximation Algorithms,	**7**
Total		**40**

Suggested Books:

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
3. Sara Basse, A. V. Gelder, " Computer Algorithms," Addison Wesley
4. Aho ,Ullman "Principles of Algorithms "
5. S.K Basu- Design Methods and Analysis of Algorithms, 2nd Ed., PHI

VI Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
6CY4-03: Application and Network Security Fundamentals	
Credit: 3	**Max. Marks: 100 (IA:30, ETE:70)**
3L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:

As a result of successfully completing this course, students will:

- Identify security breaches in a computer network.
- Learn standard security tools to locate and fix security leaks in a computer network.
- Develop concept of security needed in communication of data through computers and networks along with various possible attacks.

Course Outcomes:

Upon successful completion of the course, students will be able to

CO-1: Understand cryptographic algorithms and protocols underlying network security applications.

CO-2: Understand various encryption mechanisms for secure transmission of data and management of key required for required for encryption.

CO-3: Develop concept of security needed in communication of data through computers and networks along with various possible attacks.

CO-4: Understand authentication requirements and various authentication mechanisms.

CO-5: Understand different Web security mechanisms

S. No.	Contents	Hours
1	**Introduction:** Objective, scope and outcome of the course.	**01**
2	**Basic Cyber Security Concepts:** Concepts of Confidentiality, Integrity and Availability; Threat Modeling, Overview of Security Models (OSI and TCP/IP Models), Cyber Security basic Terminologies	**07**
3	**Security Threats, Vulnerabilities & Attacks:** Network Protocols, Threat, Vulnerability and Attack, TCP Handshaking, Password Based, Address Based, Cryptographic Authentication. Passwords in distributed systems, on-line vs offline guessing, storing. Cryptographic Authentication: passwords as keys, protocols, KDC's Certification Revocation, Inter-domain, groups, delegation. Authentication of People: Verification techniques, passwords, length of passwords, password distribution, smart cards, biometrics.	**08**
4	**Application Security:** Introduction to Applications, Security for electronic commerce: SSL, SET, System security- intrusion detection, malicious software, firewalls. **Authentication Applications:** Kerberos, X.509 Authentication Service, **Electronic Mail Security:** Pretty Good Privacy, S/MIME. **IP Security:** IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations, Key Management. Kerberos V5: names, realms, delegation, forwarding and proxies, ticket lifetimes, revoking tickets, multiple Realms	**09**
5	**Network & Security Devices**: Network management security, security hardening guidelines for Network & security devices, Network vulnerability assessment phases, Device Auditing – Switch, Firewall, Router, Core-Switch. **Web Security:** Web Security Considerations, Secure Sockets Layer and Transport Layer Security, Secure Electronic Transaction.	**09**
6	**Security Policies and Handshake:** Digital Signatures, Authentication Protocols, Digital Signature Standard, security policy, high and low level policy, user issues, protocol problems, assumptions, shared secret protocols, public key protocols, mutual authentication,	**08**

	reflection attacks, use of timestamps, nonce and sequence numbers, session keys, one-and two-way public key based authentication.	
	Total	**42**

Suggested Books:

1. Stallings, W.,.Cryptography and Network Security: Principles and Practice, 3rd ed., Prentice Hall PTR.,2003.
2. Stallings, W. Network security Essentials: Applications and standards, Prentice Hall, 2000.
3. Cryptography and Network Security; McGraw Hill; Behrouz A Forouzan.
4. Atul Kahate, Cryptography and Network Security, McGraw Hill
5. Kaufman, c., Perlman, R., and Speciner, M., Network Security, Private Communication in a public world, 2nd ed., Prentice Hall PTR., 2002.

VI Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
6CY4-04: Network System Vulnerability Assessment	
Credit: 3	**Max. Marks: 100 (IA:30, ETE:70)**
3L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:

As a result of successfully completing this course, students will:

- Identify operating systems, server applications to widen the attack surface and perform vulnerability assessment activity and exploitation phase.
- Learn how vulnerability assessment can be carried out by means of automatic tools or manual investigation.
- Learn the web application attacks starting from information gathering to exploitation phases

Course Outcomes:

Upon successful completion of the course, students will be able to

CO-1: Understand the basic principles for information gathering and detecting vulnerabilities in the system.

CO-2: Understand testing the vulnerabilities and identifying threats.

CO-3: Determine the security threats and vulnerabilities in computer networks.

CO-4: Knowledge about the various attacks caused using the network and communication system

CO-5: Knowledge about the tools used for penetration testing.

S. No.	Contents	Hours
1	**Introduction:** Objective, scope and outcome of the course.	**01**
2	**Secure Coding:** Knowing Security Testing Methodology , Secure Development Life-cycle, Application Security Overview	**07**
3	**Vulnerabilities:** Injection, Broken Authentication And Session Management, Cross-Site Scripting (XSS), Insecure Direct Object Reference, Security Misconfiguration, Sensitive Data Exposure, Missing Function Level Access Control, Cross-Site Request Forgery (CSRF), Using Components With Know Vulnerabilities, Invalidated Redirects And Forwards	**08**
4	**Vulnerability Analysis of Application Protocols:** Testing for vulnerability web application and resources - Authentication Bypass with Insecure Cookie Handling - XSS Vulnerability - File inclusion vulnerability - Remote file Inclusion - Patching file Inclusions - Testing a website for SSI Injection.	**08**
5	**Wireless Network Vulnerability Analysis**: WLAN and its inherent insecurities Bypassing WLAN Authentication uncovering hidden SSIDs MAC Filters Bypassing open and shard authentication - Attacking the client caffe latte attack Deauthenticating the client cracking WEP with the hirte attack AP-less WPA cracking - Advanced WLAN Attacks Wireless eavesdropping using MITM session hijacking over wireless - WLAN Penetration Test Methodology	**09**
6	**Web Security Vulnerabilities:** Injection vulnerabilities, cross-Site scripting vulnerabilities, the rest of the OWASP Top Ten SQL Injection vulnerabilities, Cross-site scripting vulnerabilities. Vulnerability Analysis: Passive Analysis, Source Code Analysis, Binary Analysis.	**07**
	Total	**40**

Suggested Books:

1. Rafay Baloch, Ethical Hacking and Penetration Testing Guide, CRC Press, 2015. ISBN : 78-1-4822-3161-8.
2. Dr. Patrick Engebretson, The Basics of Hacking and Penetration Testing Ethical Hacking and Penetration Testing made easy , Syngress publications, Elsevier, 2013. ISBN :978-0-12-411644-3.

3. Andrew Whitaker and Daniel P. Newman, Penetration Testing and Network Defence The practical guide to simulating, detecting an responding to network attacks, Cisco Press, 2010. ISBN: 1-58705-208-3.
4. Vivek Ramachandran, BackTrack 5 Wireless Penetration Testing, Beginners guide Master bleeding edge wireless testing techniques with BackTrack 5, PACKT Publishing, 2011. ISBN 978-1-849515-58-0.
5. Mayor, K.K.Mookey, Jacopo Cervini, Fairuzan Roslan, Kevin Beaver, Metasploit Toolkit for Penetration Testing, Exploit Development and Vulnerability Research, Syngress publications, Elsevier, 2007. ISBN : 978-1-59749-074-0
6. Abhinav Singh, Metasploit Penetration Testing Cookbook, PACKT Publishing, 2012. ISBN 978-1-84951-742-3
7. Ken Dunham, Mobile Malware Attacks and Defence, Syngress Publisher 2009. ISBN: 978-1-59749-298-0
8. Pallapa Venkataram, Satish Babu, Wireless and Mobile Network Security, First Edition, Tata McGraw Hill, 2010.
9. Hakima Chaouchi, Maryline Laurent-Maknavicius, Wireless and Mobile Network Security Security Basics, Security in On-the-shelf and Emerging Technologies, Wiley, 2009
10. Tara M. Swaminathan and Charles R. Eldon, Wireless Security and Privacy- Best Practices and Design Techniques, Addison Wesley, 2002
11. Sullivan, Bryan, and Vincent Liu. Web Application Security, A Beginner's Guide. McGraw Hill Profe ssional, 2011.
12. Stuttard, Dafydd, and Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. John Wiley Sons, 2011

VI Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
6CY4-05: Introduction to Cyber Crime, Law and Investigation	
Credit: 3	**Max. Marks: 100 (IA:30, ETE:70)**
3L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives: As a result of successfully completing this course, students will:

- Explain about the various facets of cyber crimes.
- Explain the Intellectual Property issues in the cyber space and the growth and development of the law in this regard.
- Learn the cyber world and cyber law in general.

Course Outcomes:

Upon successful completion of the course, students will be able to

CO-1: Understand the need of cyber laws.

CO-2: Understand the various facets of cyber crimes.

CO-3: Understand regulation of cyber space at national and international level.

CO-4: Understand the Intellectual Property issues in the cyber space.

CO-5: Understand the problems arising out of online transactions and provoke them to find solutions

S. No.	Contents	Hours
1	**Introduction:** Objective, scope and outcome of the course.	**01**
2	**Cyber World:** An overview, The internet and online resources, Security of information, Digital signature.	**03**
3	**Cyber Law:** An Overview, Introduction about the cyber space, Regulation of cyber space – introducing cyber law, Scope of Cyber laws – e-commerce; online contracts; Need for cyber law in India, History of cyber law in India, Information Technology Act, 2000, Overview of other laws amended by the IT Act, 2000, National Policy on Information Technology 2012.	**09**
4	**Cyber Crimes:** Classification of cyber crimes, Distinction between cyber crime and conventional crimes, Reasons for commission of cyber crime, Cyber forensic, Cyber criminals and their objectives, Kinds of cyber crimes – cyber stalking; cyber pornography; forgery and fraud; crime related to IPRs; Cyber terrorism; computer vandalism etc.,	**09**
5	**Digital Signature** and Electronic signature, Digital Signature under the IT Act, 2000, E-Governance Attribution, Acknowledgement and Dispatch of Electronic Records, Certifying Authorities, Electronic Signature Certificates, Duties of Subscribers, Penalties and Offences, Intermediaries.	**09**
6	**Data Protection Law:** Data Protection Laws, Indian evidence act, Examiner of Electronic evidence, amendments introduced in Indian evidence act, Indian CERT, IT rules 2000, Ministerial Order on blocking of websites, Cyber laws in Global Prospective	**09**
	Total	**40**

Suggested Books:

1. Thomas R. Peltier, "Information Security policies and procedures: A Practitioner's Reference", 2nd Edition Prentice Hall, 2004
2. Jonathan Rosenoer, "Cyber law: the Law of the Internet", Springer-verlag, 1997
3. Matthew Richardson, Cyber Crime: Law and Practice, Second Edition, Wildy, Simmonds and Hill Publishing, 2019.
4. Prashant Mali, Cyber Law & Cyber Crimes Simplified, Fourth Edition, Snow White Publications, 2017.
5. Pavan Duggal, Textbook on Cyber Law, 2nd Edition, Universal Law Publishing, 2016.
6. Pavan Duggal, Indian Cyberlaw On Cyber Crimes.

VI Semester
B. Tech. (Computer Science & Engineering (Cyber Security))

6CY5-11: Internet of Things

Credit:2	**Max. Marks: 100 (IA:30, ETE:70)**
2L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:
As a result of successfully completing this course, students will:

- Able to Understand the fundamentals about IoT
- Able to Understand about IoT Access technologies
- Able to Understand the design methodology and different IoT hardware platforms.
- Able to Understand the basics of IoT Data Analytics and supporting services.
- Able to Understand about various IoT case studies and industrial applications.

Course Outcomes:
Upon successful completion of the course, students will be able to
CO-1: Understand the basics and Architecture of IoT
CO-2: Understand design methodology and hardware platforms involved in IoT
CO-3: Analyze the challenges in IoT based design and development
CO-4: Understand IOT Applications in Industrial & real world.

S. No.	Contents	Hours
1	Introduction: Objective, scope and outcome of the course.	**1**
2	Introduction to IoT: Definition and characteristics of IoT, Design of IOT: Physical design of IOT, Logical Design of IOT- Functional Blocks, communication models, communication APIs, IOT enabling Technologies- Wireless Sensor Networks, Cloud computing, big data analytics, embedded systems. IOT Levels and deployment templates.	**6**
3	IoT Hardware and Software: Sensor and actuator, Humidity sensors, Ultrasonic sensor, Temperature Sensor, Arduino, Raspberry Pi, LiteOS, RIoTOS, Contiki OS, Tiny OS.	**7**
4	Architecture and Reference Model: Introduction, Reference Model and architecture, Representational State Transfer (REST) architectural style, Uniform Resource Identifiers (URIs). Challenges in IoT- Design challenges, Development challenges, Security challenges, Other challenges.	**7**
5	IOT and M2M: M2M, Difference and similarities between IOT and M2M, Software defined networks, network function virtualization, difference between SDN and NFV for IoT. Case study of IoT Applications	**7**
	Total	**28**

Suggested Books:

1. IoT Fundamentals: Networking Technologies, Protocols and Use Cases for Internet of Things, David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton and Jerome Henry, Cisco Press, 2017
2. Internet of Things – A hands-on approach, Arshdeep Bahga, Vijay Madisetti, Universities Press, 2015
3. Internet of Things: Architecture, Design Principles And Applications, Rajkamal, McGraw Hill Higher Education
4. "From Machine-to-Machine to the Internet of Things Introduction to a New Age of Intelligence" Jan Höller, Vlasios Tsiatsis, Catherine Mulligan, Stamatis Karnouskos, Stefan Avesand, David Boyle, Elsevier, 2014.

VI Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
6CY5-12: Soft Computing and Evolutionary Algorithms	
Credit:2	**Max. Marks: 100 (IA:30, ETE:70)**
2L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives:

As a result of successfully completing this course, students will:

- Able to understand basics of Fuzzy Set
- Able to understand the concepts of the genetic algorithms.
- Able to understand the ide of the evolutionary algorithms.

Course Outcomes:

Upon successful completion of the course, students will be able to

CO-1: Comprehend the fuzzy logic and the concept of fuzziness involved in various systems and fuzzy set theory.

CO-2: Understand the concepts of fuzzy sets, knowledge representation using fuzzy rules, approximate reasoning, fuzzy inference systems, and fuzzy logic

CO-3: Describe with genetic algorithms and other random search procedures useful while seeking global optimum in self learning situations.

CO-4: Develop some familiarity with current research problems and research methods in Soft Computing Techniques

S. No.	Contents	Hours
1	**Introduction to Soft Computing**: Aims of Soft Computing-Foundations of Fuzzy Sets Theory-Basic Concepts and Properties of Fuzzy Sets- Elements of Fuzzy Mathematics-Fuzzy Relations-Fuzzy Logic	**5**
2	**Application of Fuzzy Sets**: Applications of Fuzzy Sets-Fuzzy Modeling – Fuzzy Decision Making-Pattern Analysis and Classification-Fuzzy Control Systems-Fuzzy Information Processing- Fuzzy Robotics.	**6**
3	**Genetic Algorithms**: Main Operators- Genetic Algorithm Based Optimization-Principle of Genetic Algorithm- Genetic Algorithm with Directed Mutation- Comparison of Conventional and Genetic Search Algorithms Issues of GA in practical implementation. Introduction to Particle swarm optimization-PSO operators-GA and PSO in engineering applications	**6**
4	**Neuro-Fuzzy Technology**: Fuzzy Neural Networks and their learning-Architecture of Neuro- Fuzzy Systems- Generation of Fuzzy Rules and membership functions - Fuzzification and Defuzzyfication in Neuro-Fuzzy Systems- Neuro-Fuzzy Identification - Neuro Fuzzy Control- Combination of Genetic Algorithm with Neural Networks- Combination of Genetic Algorithms and Fuzzy Logic-Neuro-Fuzzy and Genetic Approach in engineering applications.	**6**
5	**Basic Evolutionary Processes, EV**: A Simple Evolutionary System, Evolutionary Systems as Problem Solvers, A Historical Perspective, Canonical Evolutionary Algorithms - Evolutionary Programming, Evolution Strategies, A Unified View of Simple EAs- A Common Framework, Population Size	**5**
Total		**28**

Suggested Books:

1.An Introduction to Genetic Algorithm Melanic Mitchell (MIT Press)

2.Evolutionary Algorithm for Solving Multi-objective, Optimization Problems (2nd Edition), Collelo, Lament, Veldhnizer (Springer)

3.Fuzzy Logic with Engineering Applications Timothy J. Ross (Wiley)
4.Sivanandam, Deepa, " Principles of Soft Computing", Wiley
5.Jang J.S.R, Sun C.T. and Mizutani E, "Neuro-Fuzzy and Soft computing", Prentice Hall
6.Timothy J. Ross, "Fuzzy Logic with Engineering Applications", McGraw Hill

VI Semester
B. Tech. (Computer Science & Engineering (Cyber Security))

6CY5-13: Information Theory & Coding

Credit: 2	**Max. Marks: 100 (IA:30, ETE:70)**
2L+0T+ 0P	**End Term Exams: 3 Hours**

Course Objectives: As a result of successfully completing this course, students will:

- To understand information theoretic behavior of a communication system.
- To understand various source coding techniques for data compression.
- To understand various channel coding techniques and their capability.
- To Build and understanding of fundamental concepts of data communication and networking

Course Outcomes: Upon successful completion of the course, students will be able to

CO-1: Perform information theoretic analysis of communication system.

CO-2: Design a data compression scheme using suitable source coding technique.

CO-3: Design a channel coding scheme for a communication system.

CO-4: Understand and apply fundamental principles of data communication and networking.

CO-5: Apply flow and error control techniques in communication networks.

S. No.	Contents	Hours
1	Introduction: Objective, scope and outcome of the course	**1**
2	Introduction to information theory Uncertainty, Information and Entropy, Information measures for continuous random variables, source coding theorem. Discrete Memory less channels, Mutual information, Conditional entropy.	**5**
3	Source coding schemes for data compaction Prefix code, Huffman code, Shanon-Fane code &Hempel-Ziv coding channel capacity. Channel coding theorem. Shannon limit.	**5**
4	Linear Block Code Introduction to error connecting codes, coding & decoding of linear block code, minimum distance consideration, conversion of non-systematic form of matrices into systematic form.	**5**
5	Cyclic Code Code Algebra, Basic properties of Galois fields (GF) polynomial operations over Galois fields, generating cyclic code by generating polynomial, parity check polynomial. Encoder & decoder for cyclic codes.	**6**
6	Convolutional Code Convolutional encoders of different rates. Code Tree, Trllis and state diagram. Maximum likelihood decoding of convolutional code: The viterbi Algorithm fee distance of a convolutional code	**6**
	Total	**28**

Suggested Books:

1. J. A. Thomas and T. M. Cover: Elements of information theory, Wiley, 2006.
2. J. H. van Lint: Introduction to Coding Theory, Third Edition, Springer, 1998.
3. F. J. MacWilliams and N.J. Sloane: Theory of Error Correcting Codes, Parts I and II, North-Holland, Amsterdam, 1977.
4. D. Stinson: Combinatorial Designs: Constructions and Analysis, Springer, 2003
5. P. J. Cameron and J. H. van Lint: Designs, Graphs, Codes and their Links, Cambridge Univ.Press, 2010.
6. C. Fragouli and E. Soljanin: Network Coding Fundamentals, Now Publisher, 2007.
7. M. Medard and A. Sprintson, (editors): Network Coding – Fundamentals and Applications, Acadamic Press, 2012.
8. C. Fragouli, J. Le Boudec, J. Widmer: Network coding: An instant primer

VI Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
6CY4-21: Design and Analysis of Algorithms Lab	
Credit: 1	**Max. Marks: 100 (IA:60, ETE:40)**
0L+0T+ 2P	**End Term Exams: 2 Hours**

Course Objectives: As a result of successfully completing this course, students will:

- Able to understand a solid background in the design and analysis of the major classes of algorithms
- Able to develop their own versions for a given computational task and to compare and contrast their performance

Course Outcomes: Upon successful completion of the course, students will be able to

CO-1: Design algorithms using divide and conquer, greedy and dynamic programming.

CO-2: Execute sorting algorithms such as sorting, graph related and combinatorial algorithm in a high level language.

CO-3: Analyze the performance of merge sort and quick sort algorithms using divide and conquer technique.

CO-4: Apply the dynamic programming technique to solve real world problems such as knapsack and TSP

S. No.	List of Experiments
1	Sort a given set of elements using the Quicksort method and determine the time required to sort the elements. Repeat the experiment for different values of n, the number of elements in the list to be sorted and plot a graph of the time taken versus n. The elements can be read from a file or can be generated using the random number generator.
2	Implement a parallelized Merge Sort algorithm to sort a given set of elements and determine the time required to sort the elements. Repeat the experiment for different values of n, the number of elements in the list to be sorted and plot a graph of the time taken versus n. The elements can be read from a file or can be generated using the random number generator.
3	a. Obtain the Topological ordering of vertices in a given digraph. b. Compute the transitive closure of a given directed graph using Warshall's algorithm.
4	Implement 0/1 Knapsack problem using Dynamic Programming.
5	From a given vertex in a weighted connected graph, find shortest paths to other vertices using Dijkstra's algorithm.
6	Find Minimum Cost Spanning Tree of a given undirected graph using Kruskal's algorithm.
7	a. Print all the nodes reachable from a given starting node in a digraph using BFS method. b. Check whether a given graph is connected or not using DFS method.
8	Find Minimum Cost Spanning Tree of a given undirected graph using Prim's algorithm.

Suggested Books:

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
3. Sara Basse, A. V. Gelder, " Computer Algorithms," Addison Wesley
4. Aho ,Ullman "Principles of Algorithms "
5. S.K Basu- Design Methods and Analysis of Algorithms, 2nd Ed., PHI

VI Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
6CY4-22: Network System Vulnerability Assessment Lab	
Credit: 1	**Max. Marks: 100 (IA:60, ETE:40)**
0L+0T+ 2P	**End Term Exams: 2 Hours**

Course Objectives:
As a result of successfully completing this course, students will:

- Monitoring the network traffic and understand the host and services discovery
-

Course Outcomes:
Upon successful completion of the course, students will be able to

CO-1: Understand the system is susceptible to any known vulnerabilities.
CO-2: Learn to assigns severity levels to vulnerabilities.
CO-3: Design different types of vulnerabilities scanning
CO-4: Understand vulnerability tools
CO-5: Learn Security Frameworks

S. No.	List of Experiments
	Students are required to perform practical in PHP / Java or hand on practice on vulnerability tools
1	Security Frameworks 1. OWASP ESAPI Security 2. Java – Spring Security, JSR 303 validator
2	Scanning and its types(network, port and vulnerability scanning)
3	Nmap and live scanning on ports and networks NFS ,SMB ,SMTP enumeration
4	Netcat usage on TCP/UDP ports
5	Wireshark basics and capturing data
6	Vulnerability scanning overview
7	Different types of vulnerability scanning
8	Nessus installation and configuration
9	Vulnerability scanning with Nessus
10	Web application assessment with nikto & burp suite
11	Vulnerability analysis with Metasploit framework

Suggested Books:

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

VI Semester **B. Tech. (Computer Science & Engineering (Cyber Security))**	
6CY4-23: Application and Network Security Fundamentals Lab	
Credit: 1	**Max. Marks: 100 (IA:60, ETE:40)**
0L+0T+ 2P	**End Term Exams: 2 Hours**

Course Objectives:
As a result of successfully completing this course, students will:

- Find out various vulnerabilities in a network.
- Identify various internal attacks in a defined network.
- Learn techniques to secure network from external attacks

Course Outcomes:
Upon successful completion of the course, students will be able to

CO-1: Understand and differentiate among security threats.
CO-2: Understand the working of NMAP
CO-3: Understand the working of Wireshark
CO-4: Scan and analyze network dump in a network
CO-5: Understand the concepts of securing the network.

S. No.	List of Experiments
1	Reporting and analysing the network related threats using tools
2	Perform the following Scan using Wireshark and analyze your results (a)Analyze TCP session (b) Perform and analyze these scans (i) Start a Wireshark capture. Open a Windows-> command window and perform a Host Scan (using ICMP packets) on a neighbours machine using nmap –sP [neighbors ip address]. Stop the capture and filter the traffic for ARP and ICMP packets. (ii)Start a new Wireshark capture, and then perform a host scan (ICMP scan) on a system out with the subnet, such as nmap –sP scanme.nmap.org.(Stop the capture and filter the traffic for ARP and ICMP packets and Compare with previous results. (iii) Start a new Wireshark capture, and then perform a complete Port Scan (in this case a TCP SYN scan) and an Operating System Fingerprint on a neighbours machine using nmap –O [neighbours ip address] . The –O option should provide the OS running on the scanned machine. Stop the capture and filter for source address == your machines address if necessary.
3	To Analysis Network using Wireshark for (a)Traffic Monitoring (TCP slow down and HTTP slow down) (b) Packet Sniffing
4	Explore , execute and analysis traffic using TCP Dump and Net discover tools
5	To explore Shodan for (a) locating Boats and Ship Locations (b) Searching and capturing Live Cameras. (c) To Write a small NSE Script
6	To spoof IP address of your own system using Kali Linux

7	To sniff traffic using ARP Spoofing
8	To perform man in middle attack using DNS spoofing
9	Write and execute commands • To view routing Table • To view network statistics of a network • To view all routes • To update/modify/add/delete routes in a routing table
10	Configuring IPSec VPN Tunnel Mode using Packet Tracer
11	Decryption SSl/TLS Traffic using Wireshark

Suggested Books:

1. Ryan Russell, " Hack Proofing your network ", Wiley,2nd Edition,2002
2. Karen Scarf one, "Guide to Intrusion and prevention System", NIST Special Publication, 2nd Edition,2007

Learning best Scanning Tools:

- https://www.wireshark.org/
- https://www.tcpdump.org/
- https://www.tenable.com/
- https://nmap.org/

VI Semester B. Tech. (Computer Science & Engineering (Cyber Security))	
6CY7-50: Innovation and Design Thinking Hands-on Project	
Credit: 2	**Max. Marks: 100 (IA:60, ETE:40)**
0L+0T+3P	**Mode of evaluation: Report and presentation**

Course Objectives:

As a result of successfully completing this course, students will:

- Learn about the National Innovation and Startup Policy (NISP)of Govt. of India.
- Learn how to ideate, prototype and Iterate solutions.
- Learn about applying Design Thinking Tools and Approaches for Right Problem Identification and Solution Development.
- Learn about Business Plan Development.
- Learn about Legal Structures and Ethical Steps in Establishing Startups.
- Able to design and develop a Prototype.
- Students will be able to pitch their idea.
- Will be able to demonstrate their innovative and design thinking capabilities using mock-up models.

Course Outcomes:

Upon successful completion of the course, students will be able to

CO-1: learn about opportunities and challenges for startup and incubation.

CO-2: Students will be able to identify an Opportunity from a Problem using design thinking.

CO-3: Students will be able to frame Product and service ideas.

CO-4: Learn and implement Design Thinking Process.

CO-5: Students will be able to design and develop a Prototype.

CO-6: Students will be able to prepare documentation and pitch their idea.

exp. No.	Contents
1	National Innovation and Startup Policy (NISP) and Legal Structures and Ethical Steps in Establishing Startups, Generation and Management of IP at the Early Stage of Innovation and Startup Development, IPR and IPR policies.
2	Design Thinking, Process of Design Thinking, Empathy, Define, Ideate, Prototype, Testing.
3	Understanding Technology Readiness Level (TRL), Manufacturing Readiness Level (MRL) and Investment Readiness Level (IRL) Stages & Implications in Innovation Development
4	Capstone Project: Students in groups of 3 to 5 students must prepare a project idea using the design thinking process under the mentorship of the faculty members. Students must submit a capstone project report containing various ideas learned in experiments numbers 1-3 and their implementation or usage in the capstone project to the Institute Innovation Council (IIC) cell or Head of Department along with a presentation.

Assessment or Evaluation:

Students need to submit a capstone project report to the Institute Innovation Council (For the Institute having IIC cells) or the head of the department (For the Institute not having IIC cells) containing step by step approach to the project based on design thinking methodology along with the final presentation to IIC Cell (For the Institute having IIC cells) or Head of department (For the Institute not having IIC cells).

Suggested Books:

1. Idris Mootee, "Design Thinking for Strategic Innovation: What They Can't Teach You at Business or

Design School", John Wiley & Sons (2013).
2. Tim Brown, "Change by design", Harper Collins, 2009
3. "Design Thinking- The Guide Book" – Facilitated by the Royal Civil service Commission, Bhutan
4. The Lean Startup: How Constant Innovation Creates Radically Successful Businesses
5. Start With Why: How Great Leaders Inspire Every
6. National Innovation and Startup Policy 2019 for students and faculty of Higher Education Institutions (HEIs) https://mic.gov.in/assets/doc/startup_policy_2019.pdf
7. Tom Kelley, The Art of Innovation: Lessons in Creativity from IDEO, America's Leading Design Firm
8. Roger L. Martin , Design of Business: Why Design Thinking is the Next Competitive Advantage, Harvard Business Review Press
9. Online resource