5th Semester (Third Year)-NEP 2020

Course Title: Fundamentals of Cryptography										
Semester	V	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PCC6	3	1	-	4	10	15	50	-	-
Course Code	23BTCYL301									
Teaching Mode	Offline	4 Hrs			Total	75			-	
Duration of ESE	3:00 Hr					75				

Course Objectives	Understanding of the basic concepts of Cryptography
	To understand the techniques of Classical Cryptosystems
	To understand concepts of Symmetric cryptography
	To understand concepts of Asymmetric cryptography
	To Provide students with a comprehensive overview of Message Authentication Code and Hash Functions
Course Outcomes	CO1: To elaborate the role of cryptography & its fundamentals
	CO2: To apply various cryptography techniques
	CO3: To apply concepts of Symmetric cryptography
	CO4 : To apply concepts of Asymmetric cryptography
	CO5 : TO analyze MAC and Hash Codes

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes													
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO 2
CO1	**2**	**2**	**3**										**3**	
CO2		**2**												**2**
CO3		**3**											**1**	
CO4			**3**	**3**										**2**
CO5	**3**			**3**										

Course Contents:

Unit	Contents	Hours
I	**Introduction to Cryptography:** Introduction to Cryptography, History of Cryptography ,Shannon's Description of a Conventional Cryptosystem, Statistical Description of a Plaintext Source, Problems, Attacks, services, mechanisms, security attacks, security services, a model for internetwork security, encryption model, steganography.	8
II	**Classical Cryptosystems :** Caesar, Simple Substitution, Caesar Cipher, .Playfair ,Simple Substitution Cryptanalysis by The Method of a Probable Word .VigenèreCryptosystem ,Kasiski's Method, Transpositions, Rail Fence The One-Time Pad Transposition, Rotor Machines. INTRODUCTION TO NUMBER THEORY: Prime Numbers, Fermat's and Euler's Theorem, Testing for Primality, The Chinese Remainder Theorem, Discrete logarithms,	8
III	PUBLIC KEY CRYPTOGRAPHY AND RSA: Principles Public key crypto Systems, Diffie Hellman Key Exchange, the RSA algorithm, Key Management, , Elliptic Curve Arithmetic, Elliptic Curve Cryptography. MESSAGE AUTHENTICATION AND HASH FUNCTIONS: Authentication Requirement, Authentication Function, Message Authentication Code, Hash Function, Security of Hash Function and MACs. HASH AND MAC ALGORITHM: Secure Hash Algorithm, Whirlpool, HMAC, CMAC. DIGITAL SIGNATURE: Digital Signature, Authentication Protocol, Digital Signature Standard.	8
IV	AUTHENTICATION APPLICATION: Kerberos, X.509 Authentication Service, Public Key Infrastructure. Dictionary Attack, Biometric System EMAIL SECURITY: Pretty Good Privacy (PGP) and S/MIME. IP SECURITY: Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.	8
V	WEB SECURITY: Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET), Intruders, Viruses and related threats. FIREWALL: Firewall Design principles, Trusted Systems. Malicious Logic: Types of Malicious Logic: Virus, Worm, Trojan Horse, Zombies, Denial of Service Attacks, Intrusion, Intruders and their types, Intrusion Detection System	8

Text Books	1.	a) . "Cryptography and Network Security: Principles and Practice" by William Stallings (1st ed. 1995, latest ed. 2020).
On line TL Material	1.	1. nptel.ac.in/courses/106105031 (IIT K) 2. https://nptel.ac.in/courses/106105031/39 3. https://nptel.ac.in/courses/106106129 4. https://onlinecourses.nptel.ac.in/noc18_cs24 5. https://onlinecourses.nptel.ac.in/noc22_cs03/preview 6. https://archive.nptel.ac.in/courses/106/106/106106221/

Cyber Laws and Ethics

Course Title:	**Cyber Laws and Ethics**									
Semester	V	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PCC7	3Hrs.	-	-	3	10	15	50	-	-
Course Code	23BTCYL302									
Teaching Mode	Classroom	3Hrs			Total	75				
Duration of ESE	3Hrs.									

Course Objectives	1. Gain foundational knowledge of cyber law and its application within the Indian legal system
	2. Understand the integration of the Bhartiya Nyaya Sanhita and its influence on cyber law
	3. Familiarize with cybercrime sections and punishments under the current Indian framework
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1: Understanding Cyber Law and its Impact on the Indian Legal System
	CO2: Identification of Cybercrimes and Legal Consequences
	CO3: Identify Critical Analysis of Cyber Ethics in Digital Environments
	CO4: Understand Application of Intellectual Property Laws in Cyberspace
	CO5: Understand Comprehension of E-Governance, Digital Contracts, and Cyber security Frameworks

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	**Program Outcomes and Program Specific Outcomes**													
	PO 1	**PO 2**	**PO 3**	**PO 4**	**PO 5**	**PO 6**	**PO 7**	**PO 8**	**PO 9**	**PO 10**	**PO 11**	**PO 12**	**PS O 1**	**PS O 2**
CO1								2				2	1	
CO2								3				2	1	
CO3								3				2	3	
CO4								2				3		1
CO5								1				2		1

Course Contents:

Unit	Contents	Hours
I	**Cyber Ethics and Ethical Issues in Cyberspace:** **1. Importance of Cyber Ethics:** Definition of **Cyber Ethics**: The moral and ethical principles governing online behaviour, Ethical concerns in cyberspace: data privacy, intellectual property, and online content regulation. **2. Ethical Challenges in Emerging Technologies:** Exploring the ethical challenges posed by AI, data analysis in digital transactions, Digital Privacy: Ethical implications of surveillance, tracking, and data harvesting. **3. Ethical Codes and Regulations:** The role of the Indian Computer Emergency Response Team (CERT-In) in promoting cyber ethics. BNS Ethical Considerations	8Hrs.
II	**Introduction to Cyber Laws and the Bhartiya Nyaya Sanhita:** **1. Overview of Cyber Law in India:** Introduction to Cyber Law and its significance in the Indian legal system, Bhartiya Nyaya Sanhita (BNS): How the BNS impacts legal frameworks for cyberspace, Key cyber laws in India, including the Information Technology Act, 2000, and its amendments. **2. Legal Provisions under IT Act and Punishments:** Detailed examination of Section 66, Section 67, Section 43A, and other BNS sections, Punishments: Legal consequences of cybercrimes under the BNS framework (e.g., hacking, cyber-stalking, identity theft). **3. Overview of Indian Cyber Jurisprudence:** Evolution of cyber jurisprudence in India with notable **case studies.**	8Hrs.
III	**Cybercrime and Punishments:** **1. Types of Cybercrimes: Hacking and Cyber-terrorism**: Legal definitions, case studies, and punishments under Section 66 of the IT Act and related sections of BNS, Cyberbullying: Legal responses and ethical challenges, Identity Theft and Phishing. **2. Cybercrime Investigation and Law Enforcement:** Role of law enforcement in investigating cybercrimes, Tools and technologies used for cybercrime prevention, **Case studies**	7Hrs.
IV	**Intellectual Property Rights in Cyberspace:** **1. Copyright and Trademarks in the Digital World: Copyright Protection**: Legal protections for digital content, software, and online media under Indian copyright law, **Trademarks**: Legal issues related to domain names, cybersquatting, and the use of trademarks in cyberspace. **2. Software Piracy and Patent Issues:** Legal consequences of software piracy and digital piracy under the **Bhartiya Nyaya Sanhita**, Patent law issues in the context of digital inventions and technology. **3. Intellectual Property Disputes in Cyberspace:** Case studies	8Hrs.
V	**E-Governance, Digital Contracts, and Legal Frameworks:** **1. Legal Recognition of Electronic Records: E-Governance in India**: Legal framework for the recognition of electronic documents and records under the **Indian Evidence Act, 1872**. **2. Cybersecurity and the Role of Certifying Authorities:** The role of **Certifying Authorities** (CAs) in securing digital records and authentication, India's cybersecurity initiatives and the establishment of the **Cyber Appellate Tribunal.** **Case studies** .	8Hrs.

Text Books	1.	"Cyber Law and E-Commerce" by S. S. Gulshan A comprehensive guide on cyber laws, including case studies and legal principles applied in India
	2.	"Information Technology Act 2000: Law and Practice" by Dr. Gaurav Agrawal A detailed study of the IT Act, with sections on amendments, challenges, and judicial interpretations
	3.	"Bhartiya Nyaya Sanhita" (Updated 2024 Edition) The latest provisions, amendments, and punishments under the Bhartiya Nyaya Sanhita, specifically addressing issues in cyber law and ethics.
Reference Books	1.	"Cyber Law in India" by P.K. Agarwal In-depth analysis of cyber law in India, including its evolution, challenges, and judicial pronouncements.
	2.	"Ethics of Artificial Intelligence and Robotics" by Vincent C. Müller Discusses ethical issues surrounding emerging technologies such as AI and its implications on cyber law.
	3.	"Principles of Cyber Security and Digital Law" by Gurpreet KaurFocuses on the interplay between cybersecurity, digital laws, and ethical principles in cyberspace
On line TL Material	1.	**Primer on New Criminal Laws (NCL)** **By Dr. Neeraj Tiwari | National Law University** **https://onlinecourses.swayam2.ac.in/cec25_lw03/preview**
	2	**Introduction to Cyber Law** **By Alison** **https://alison.com/course/introduction-to-cyber-law**

Introduction to Penetration Testing

Course Title: **Introduction to Penetration Testing**										
Semester	V	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PCC8	2 Hrs	NA	2 Hrs	3	10	15	50	25	-
Course Code	23BYCYL303/ 23BYCYP303									
Teaching Mode	Offline	4 Hrs			Total	75			25	
Duration of ESE	3 Hrs					100				

Course Objectives	To understand how intruders escalate privileges.
	To understand Intrusion Detection, Policy Creation, Social Engineering, Buffer Overflows and different types of Attacks and their protection mechanisms
	To learn about penetration testing.
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1: Understand the concept of penetration testing.
	CO2: To apply technique of reconnaissance.
	CO3: Evaluate exploitation and elaborate the technology.
	CO4: Understanding post exploitation maintaining access.
	CO5: Apply and execute the penetration test.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	**Program Outcomes and Program Specific Outcomes**														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO3
CO1	**3**	**3**	**2**	**2**	**2**	**2**	**1**	**2**	**2**	**2**	**1**	**2**	**2**	**2**	**1**
CO2	**3**	**3**	**2**	**2**	**2**	**2**	**1**	**2**	**1**	**1**	**1**	**3**	**2**	**2**	**2**
CO3	**3**	**3**	**3**	**2**	**2**	**2**	**1**	**3**	**1**	**2**	**2**	**2**	**2**	**3**	**3**
CO4	**3**	**3**	**3**	**3**	**3**	**2**	**1**	**2**	**2**	**1**	**2**	**2**	**2**	**2**	**3**
CO5	**3**	**3**	**3**	**3**	**3**	**2**	**1**	**1**	**3**	**3**	**3**	**3**	**3**	**3**	**3**

Course Contents:

Unit	Contents	Hours
I	**INTRODUCTION TO PENETRATION TESTING:** Introduction - Terminologies - Categories of Penetration Testing - Phases of Penetration Test -Penetration Testing Reports - Information Gathering Techniques - Active, Passive and Sources of Information Gathering - Approaches and Tools- Traceroutes, Neotrace, Whatweb, Netcraft, Xcode Exploit Scanner and NSlookup. Host discovery - Scanning for open ports and services.	4
II	**RECONNAISSANCE:** Reconnaissance: HTTrack: Website Copier- Google Directives: Practicing Your Google-Fu.- The Harvester: Discovering and Leveraging E-mail Addresses, Fierce and Other Tools to Extract Information from DNS.-Extracting Information from E-mail Servers.-Threat Agent: Attack of the Drones.-Sifting through the Intel to Finding Attackable Targets.	4
III	**EXPLOITATION:** Medusa: Gaining Access to Remote Services - Metasploit: Hacking Hugh Jackman Style - John the Ripper: King of the Password Crackers - Password Resetting: The Building and the Wrecking Ball - Wireshark: Sniffing Network Traffic - Wireshark: Sniffing Network Traffic.- Armitage: Breaking Out the M-60.	4
IV	**POST EXPLOITATION AND MAINTAINING ACCESS:** Netcat: The Swiss Army Knife - Cryptcat: Netcat's Cryptic Cousin - Rootkits - Hacker Defender: It is Not What You Think - Detecting and Defending Against Rootkits - Meterpreter: The Hammer that Turns Everything into a Nail	4
V	**APPLYING THE PENETRATION TEST** Writing the Penetration Testing Report - You Do Not Have to Go Home but You Cannot Stay Here - Where Do I Go from Here? - Wrap Up -The Circle of Life	4

Text Books	1.	Weidman, Georgia. Penetration testing: a hands-on introduction to hacking / Georgia Weidman. IN 2014.
E--Books	1.	https://www.scribd.com/book/470612770/Penetration-Testing
Reference Books	1.	Sean -Philip oriyano "penetration testing essentials", Released December 2016 Publisher(s): Sybex ISBN: 9781119235309
	2.	Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy", Syngress Basics Series – Elsevier, August 4, 2011.
	3.	Philip L. Wylie "The Pentester Blueprint" SBN-139781119684305 Publisher:Wiley
online TL Material	1.	https://www.youtube.com/watch?v=q-ZrX41cIOA

PRACTICAL LIST

Course Name: Introduction to Penetration Testing [UNDIP309]

Course Outcome:

CO1: Understand the concept of penetration testing.
CO2: To apply technique of reconnaissance.
CO3: Evaluate exploitation and elaborate the technology.
CO4: Understanding post exploitation maintaining access.
CO5: Apply and execute the penetration test.

Practical No.	List of Practical	COs
01	**Introduction to Penetration Testing**: To identify and install Virtual machines and Operating Systems used in Penetration Testing	CO1
02	**Monitoring Network Traffic**: To analyze and capture network traffic to identify patterns, detect anomalies and assess overall network performance and security.	CO1
03	**Host & Services Discovery using Nmap**: To identify active hosts and the services they are running within a network using Nmap, enabling a comprehensive understanding of the network environment.	CO2
04	**Vulnerability Scanning using OpenVAS**: To perform a systematic assessment of networked systems using OpenVAS to identify potential vulnerabilities that could be exploited by attackers.	CO2
05	**Internal Penetration Testing:** To perform a thorough internal penetration test that systematically assesses the security of the organization's network infrastructure by mapping network resources, scanning for vulnerabilities, exploiting known weaknesses and demonstrating attack techniques, including credential sniffing and poisoning attacks, in order to identify and mitigate potential	CO3
06	**External Penetration Testing:** To conduct a comprehensive external penetration test aimed at evaluating the security of the organization's external infrastructure by assessing vulnerabilities, mapping the network topology, gathering IP and domain registry information, and examining the implementation of IPv6, ultimately identifying potential entry points and recommending measures to strengthen defenses against external threats.	CO3
07	**Different Types of Vulnerability Scanning:** To explore and compare various vulnerability scanning techniques and tools, assessing their effectiveness in identifying and prioritizing security risks.	CO4
08	**Vulnerability Scanning with Nessus:** To utilize Nessus for comprehensive vulnerability scanning, identifying security weaknesses in systems and providing recommendations for remediation.	CO4
09	**Web Application Assessment with Nikto Suite:** To evaluate web applications for security vulnerabilities using Nikto, identifying issues such as misconfigurations and common vulnerabilities in web applications.	CO5
10	**Web Application Assessment with Burp Suite:** To evaluate web applications for security vulnerabilities using Burp, identifying issues such as misconfigurations and common vulnerabilities in web applications.	CO5
Practical Beyond Syllabus (Open Ended)		
11	Install and Implement various commands Wireshark on Linux	CO3
12	Case study on: PTES Framework (Penetration Testing Methodologies and Standards)	CO5

Course Title: Ethical Hacking-PE1										
Semester	V	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	E-I	3	-	2	4	10	15	50	25	-
Course Code	23BTCYLXXXX									
Teaching Mode	Offline	5 Hrs			Total	75			25	
Duration of ESE	3 Hrs					100				

Course Objectives	1. To understand how intruders escalate privileges.
	2 To understand Intrusion Detection, Policy Creation, Social Engineering, Buffer Overflows and different types of Attacks and their protection mechanisms
	3. To learn about ethical laws and tests
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1- Understand the legal and ethical requirements related to ethical hacking.
	CO2 – Identifying how to access an environment using foot-printing.
	CO3 - Apply Data Security in various environment.
	CO4 - Creating Network Protection System & Hacking Web Servers.
	CO5 - Analyze the tools for conducting ethical hacking.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	**Program Outcomes**												**Program Specific Outcomes**		
	PO 1	**PO 2**	**PO 3**	**PO 4**	**PO 5**	**PO 6**	**PO 7**	**PO 8**	**PO 9**	**PO10**	**PO 11**	**PO 12**	**PSO 1**	**PSO 2**	**PSO3**
CO1	2	2	2			2		2	1	2			2	3	2
CO2			2								2		2	2	2
CO3	2			3			2		2				1	2	2
CO4				2					2		2		1	2	2
CO5	2				2								2	2	3

Course Contents:

Unit	Contents	Hours
I	**INTRODUCTION TO ETHICAL HACKING:** Ethical Hacking Definition, difference between hacking and ethical hacking. Vulnerability, Attack Vector. Five stages of hacking: Reconnaissance (Survey), Probing, Actual attack, maintaining presence, Covering attack tracks, Introduction to OWASP top 10 vulnerabilities.	6
II	**SCANNING AND SYSTEM HACKING: Port Scanning, Network Scanning, Vulnerability Scanning, NMAP Scanning tool, OS Fingerprinting** **System Hacking: Password cracking techniques, Key loggers, Escalating privileges, URL Hiding Files, Sniffers & SQL Injection: Active and passive sniffing, ARP Poisoning, Session Hijacking, DNS Spoofing, Conduct SQL Injection attack, Counter measures. Study of open source scanning tools.**	7
III	**DATA SECURITY: Physical Security –** Attacks and Protection, Steganography – Methods, Attacks and Measures, Cryptography – Methods and Types of Attacks, Wireless Hacking, Windows Hacking, Linux Hacking.	5
IV	**NETWORK PROTECTION SYSTEM & HACKING WEB SERVERS:** Routers, Firewall & Honeypots, IDS & IPS, Web Filtering, Vulnerability, Penetration Testing, Session Hijacking, Web Server, SQL Injection, Cross Site Scripting, Exploit Writing, Buffer Overflow, Reverse Engineering, Email Hacking, Incident Handling & Response, Bluetooth Hacking, Mobiles Phone Hacking.	7
V	HACKING ENVIRONMENT DAMN VULNERABLE WEB APPLICATION (DVWA) Installation and configuration of DVWA environment. Virtual box installation, Installation of Kali Linux within virtual box. Kali Linux penetration testing and ethical hacking tools. What is TOR? How can you use it to protect your anonymity online? Social Engineering: Phases of an attack, Common targets, Common sources of information. Web Servers and applications: Common attacks and flaws, Current tools.	7

Text Books	1.	Michael T. Simpson, Kent Backman, James E. "Corley, Hands-On Ethical Hacking and Network Defense", Second Edition, CENGAGE Learning, 2010.
Reference Books		**Steven DeFino, Barry Kaufman, Nick Valenteen, "Official Certified Ethical Hacker Review Guide", CENGAGE Learning, 2009-11-01.**
	2.	Patrick Engebretson, "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy", Syngress Basics Series – Elsevier, August 4, 2011

Practical No.	Experiment Name
1	Study and Demonstration of the Five Stages of Hacking
2	Introduction to OWASP Top 10 vulnerabilities
3	To perform port scanning on a target system to identify open ports and services using Nmap, and understand the role of port scanning in ethical hacking and network reconnaissance.
4	To perform network scanning using tools like **Nmap** and **Netdiscover** to identify live hosts, open ports, and network services within a target network.
5	To perform vulnerability scanning on a target system or web application using tools like **Nikto** and **Nessus**, and analyze discovered vulnerabilities.
6	To study and implement basic cryptographic techniques
7	To study and apply **steganography techniques** to hide and extract information within digital media (images, audio files, etc.) using common tools.
8	To understand and implement a honeypot in a network for detecting and analyzing unauthorized access attempts.
9	To understand and exploit Cross-Site Scripting (XSS) vulnerabilities in a web application
10	To understand the concept of Session Hijacking

Program Electives

Course Title: AI for IoT Applications										
Semester	V	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PE-I	3	-	2	4	10	15	50	25	-
Course Code										
Teaching Mode	Offline	5 Hrs			Total	75			25	
Duration of ESE	3 Hrs					100				

Course Objectives	1. To equip students with an understanding of how Artificial Intelligence (AI) and Machine Learning (ML) can be integrated into Internet of Things (IoT) applications
	2 To explore the principles, methods, and tools for implementing AI-based solutions in IoT environments.
	3. The students will be proficient in applying AI techniques to enhance the functionality of IoT systems
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1- Grasp the role of AI in enhancing IoT functionality.
	CO2 - Apply machine learning algorithms to process IoT data
	CO3 - Apply AI-based data analytics to real-time IoT systems.
	CO4 - Understand and implement deep learning techniques in IoT applications.
	CO5 - Understand the ethical and regulatory challenges of integrating AI into IoT applications.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	**Program Outcomes and Program Specific Outcomes**													
	PO 1	**PO 2**	**PO 3**	**PO 4**	**PO 5**	**PO 6**	**PO 7**	**PO 8**	**PO9**	**PO10**	**PO11**	**PO12**	**PSO 1**	**PSO 2**
CO1		2											2	
CO2			2										2	
CO3				3									1	
CO4				2									1	
CO5					2									2

Course Contents:

Unit	Contents	Hours
I	**Introduction to IoT and AI** Overview of Internet of Things (IoT): Architecture, Components, and Applications, Introduction to Artificial Intelligence (AI): History, Scope, and AI vs ML, Role of AI in IoT: Data Analysis, Decision Making, and Predictive Models, IoT-AI Integration: Challenges and Opportunities	6
II	Machine Learning Techniques for IoT Data Supervised and Unsupervised Learning Algorithms, Regression, Classification, Clustering, and Dimensionality Reduction, Data Preprocessing for IoT Sensor Data,	6
III	**AI-based Data Analytics and Predictive Modelling** Data Analytics: From Data Acquisition to Visualization, Time Series Forecasting for IoT: Techniques and Applications, Predictive Maintenance in IoT Systems, Anomaly Detection in IoT Data Streams	8
IV	**Deep Learning and Edge AI** Applying Deep Learning to IoT: Object Recognition, Sensor Fusion, Convolutional Neural Networks (CNN) for Image Processing in IoT, Recurrent Neural Networks (RNN) for IoT Time Series Data, Edge AI and Edge Computing in IoT Systems, Lightweight machine learning Models eg. MobileNet, SqueezeNet, TinyML Models.	8
V	Security, Privacy, and Ethical Considerations in AI for IoT Security and Privacy Issues in IoT Systems, Securing AI in IoT: Approaches for Data Encryption and Authentication, Ethical Implications of AI in IoT: Bias, Transparency, and Accountability, Blockchain for IoT Security, AI for Threat Detection in IoT Networks, Regulations and Standards for AI-enabled IoT Systems **Case study absed on IOT Application**	8

Text Books	1.	**Artificial Intelligence: A Modern Approach** -by Russell/Norvig (Author) Publisher-Pearson Education Edition-4, Publication Date-31 May 2022
	2	**Confluence of AI and IoT : Marriage Made in Heaven** -by Vinay Solanki (Author) Publisher-Notion Press, Publication Date-30 December 2022
Reference Books	1.	**AI for Everyone: A Beginner's Handbook for Artificial Intelligence (AI) -by Saptarsi Goswami (Author) Publisher-Pearson Education-Publication Date-23 May 2024**
	2.	**The Today and Future of WSN, AI, and IOT** by Dr.Chandrakant (Author), Dr Suresh (Author) ,ISBN-13-978-9389845167, Publication Date-1 January 2020

Sr.no	Name of Experiments
1	Assemble a basic IoT device using a microcontroller (e.g., Raspberry Pi or Arduino) and connect it to the cloud.
2	Implement a basic AI decision tree for an IoT-based home automation system.
3	Use Scikit-learn or TensorFlow to implement regression and classification for IoT sensor data.
4	Create visualizations of IoT sensor data and predictions using Python libraries like Matplotlib.
5	Develop a simple predictive maintenance model using time series forecasting for an industrial IoT scenario.
6	Design a small-scale smart healthcare monitoring system leveraging predictive analytics.
7	Apply convolutional neural networks (CNNs) for IoT-based image recognition (e.g., detecting objects using a smart camera).
8	Use RNNs for time series data, such as predicting weather patterns from IoT sensors.
9	OPEN ENDED Practical 1
10	OPEN ENDED Practical 2

Course Title: High Performance Computing (Elective)										
Semester	V	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	E-I	3	-	1	4	10	15	50	25	-
Course Code										
Teaching Mode	Offline	5 Hrs			Total	75			25	
Duration of ESE	3 Hr					100				

Course Objectives	To understand different parallel programming models
	To analyze the performance and modeling of parallel programs
	To illustrate the various techniques to parallelize the algorithm
	To implement parallel communication operations
	To discriminate CUDA Architecture and its components.
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1:**Understand** various Parallel Paradigm
	CO2: **Design and Develop** an efficient parallel algorithm to solve given problem.
	CO3: **Illustrate** data communication operations on various parallel architecture
	CO4: **Analyze** and measure performance of modern parallel computing systems
	CO5: **Apply** CUDA architecture for parallel programming

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	1											2	
CO2	2	1					1						1	
CO3	2	1	3	2									2	
CO4	1	2	3									1		3
CO5	1	2	3									1		3

SYLLABUS:

MODULE	DETAILS	HOURS
I	**Introduction to Parallel Computing:** Motivating Parallelism, **Modern Processor:** Stored- program computer architecture, General-purpose Cache-based Microprocessor architecture. **Parallel Programming Platforms:** Implicit Parallelism, Dichotomy of Parallel Computing Platforms, Physical Organization of Parallel Platforms, Communication Costs in Parallel Machines. Levels of parallelism, **Models:** SIMD, MIMD, SIMT, SPMD, Data Flow Models, Demand-driven Computation, **Architectures:** N-wide superscalar architectures, multi-core, multi-threaded.	**9**
II	**Parallel Algorithm Design :** Global System for Mobile Communications (GSM) architecture , Mobile Station, Base Station System, Switching subsystem, Security, Data Services, HSCSD, GPRS - GPRS system and protocol architecture 2.3 UTRAN, UMTS core network; Improvements on Core Network, 802.11 Architecture 802.11a, 802.11b standard	**8**
III	**Parallel Communication** : **Basic Communication:** One-to-All Broadcast, All-to-One Reduction, All-to-All Broadcast and Reduction, All-Reduce and Prefix-Sum Operations, Collective **Communication using MPI:** Scatter, Gather, Broadcast, Blocking and non blocking MPI, All-to-All Personalized Communication, Circular Shift, Improving the speed of some communication operations	**8**
IV	**Analytical Modeling of Parallel Programs** Sources of Overhead in Parallel Programs, **Performance Measures and Analysis:** Amdahl's and Gustafson's Laws, Speedup Factor and Efficiency, Cost and Utilization, Execution Rate and Redundancy, The Effect of Granularity on Performance, Scalability of Parallel Systems, Minimum Execution Time and Minimum Cost, Optimal Execution Time, Asymptotic Analysis of Parallel Programs. **Matrix Computation:** Matrix-Vector Multiplication, Matrix-Matrix Multiplication	**9**
V	**CUDA Architecture** : **Introduction to GPU:** Introduction to GPU Architecture overview, Introduction to CUDA C-CUDA programming model, write and launch a CUDA kernel, Handling Errors, CUDA memory model, Manage communication and synchronization, Parallel programming in CUDA- C.	**7**
	TOTAL HOURS	**41**

T/R	BOOK TITLE/AUTHORS/PUBLICATION
Text Books	**1.** Ananth Grama, Anshul Gupta, George Karypis, and Vipin Kumar, "Introduction to Parallel Computing", 2nd edition, Addison-Wesley, 2003, ISBN: 0-201-64865-2 **2.** Seyed H. Roosta, ―Parallel Processing and Parallel Algorithms Theory and Computation‖, Springer-Verlag 2000 ,ISBN 978-1-4612-7048-5 ISBN 978-1-4612-1220-1 **3.** John Cheng, Max Grossman, and Ty McKercher, ―Professional CUDA C Programming‖, John Wiley &
Reference Books	**1.** Kai Hwang,, "Scalable Parallel Computing", McGraw Hill 1998. **2.** George S. Almasi and Alan Gottlieb, "Highly Parallel Computing", The Benjamin and Cummings Pub. Co., Inc **3.** Jason sanders, Edward Kandrot, ―CUDA by Example‖, Addison-Wesley, ISBN-13: 978- 0-13-138768-3 **4.** Pacheco, Peter S., ―An Introduction to Parallel Programming‖, Morgan Kaufmann Publishers ISBN 978-0-12-374260-5
e-Books	**e Books :** 1.http://prdrklaina.weebly.com/uploads/5/7/7/3/5773421/introduction_to_high_performance_computing_for_scientists_and_engineers.pdf 2. https://www.vssut.ac.in/lecture_notes/lecture1428643084.pdf
Online Learning Material	**NPTEL/YouTube video lecture link** ● https://nptel.ac.in/courses/106108055 ● https://www.digimat.in/nptel/courses/video/106104120/L01.html

List of Practical's

Subject: High Performance Computing (Elective)

Semester: V

Sr.No.	List of Practical's
1	Design and implement Parallel Breadth First Search and Depth First Search based on existing algorithm using Open MP. Use a Tree or an undirected graph for BFS and DFS
2	Write a program to implement Parallel Bubble Sort. Use existing algorithm and measures the performance of sequential and Parallel algorithm.
3	Implement Min, Max, Sum and Average operations using Parallel Reduction
4	Write a CUDA Program for : 1.Addition of two large vectors
5	Write a CUDA Program for: 1. Matrix Multiplication using CUDA
6	Implement HPC application for AI/ML domain
7	Mini Project: Evaluate performance enhancement of parallel Quicksort Algorithm using MPI
8	Mini Project: Implement Huffman Encoding on GPU
9	Mini Project: Implement Parallelization of Database Query optimization
10	Mini Project: Implement Non-Serial Polyadic Dynamic Programming with GPU Parallelization

MD-3

Course Title: Computer Security										
Semester	V	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	MDM3	3	-	2	4	10	15	50	25	-
Course Code	23BTCYL XXX 23BTCYP XXX									
Teaching Mode	Offline	5 Hrs			Total	75			25	
Duration of ESE	3 Hr					100				

Course Objectives	Understanding of the basic concepts of Computer Security
	To understand the techniques of Networks security
	To understand concepts of Web security
	To understand concepts of Server Security
	To Provide students with a comprehensive overview of Disaster Recovery and Fault Tolerance.
Course Outcomes	**CO1:** Apply basic concepts of Computer Security
	CO2: Analyze the techniques of Networks security
	CO3: Remember the concepts of Web security
	CO4: Apply the concepts of Server Security
	CO5: Evaluate the concepts in Disaster Recovery and Fault Tolerance.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	**3**	**2**	**0**	**1**	**2**	**1**	**0**	**2**	**0**	**1**	**0**	**2**	**3**	**2**	**1**
CO2	**2**	**3**	**2**	**2**	**3**	**1**	**0**	**2**	**0**	**1**	**1**	**2**	**1**	**3**	**1**
CO3	**2**	**2**	**1**	**1**	**2**	**1**	**0**	**1**	**0**	**1**	**0**	**2**	**3**	**2**	**1**
CO4	**3**	**2**	**2**	**2**	**3**	**1**	**0**	**2**	**0**	**1**	**1**	**2**	**2**	**3**	**2**
CO5	**2**	**3**	**2**	**3**	**2**	**1**	**0**	**2**	**1**	**2**	**2**	**3**	**2**	**2**	**3**

Course Contents:

Unit	Contents	Hours
I	**Introduction to computer security** Overview of Computer Security Concepts and Foundations Threats, Attacks, and Assets .**Computer Security Technology and Principles** User Identification and Authentication Access Control Database and Cloud Security Malicious Software Denial-of-Service Attacks Intrusion Detection **Firewalls:** Types of Firewalls, design principles, trusted systems, Honeypots.	6
II	**Networks security practice:** E-mail security: pretty Good privacy, S/MIME. **IP security:** overview, architecture, authentication header, encapsulating security payload, combining security associations, key management. Intrusion Prevention Systems(IPS), Secure N/2 Design and Architecture	6
III	**Web security:** Requirements, secure electronic transaction, networks management security. System Security: Intruders, viruses and worms, Web Browser Security - Email Security Firewall VPN - Transport Layer Security (TLS) Handshake Protocol Alert Message Protocol Chan	10
IV	**Server Security:** Server Roles and Security Server Roles and Baselines - Securing Network Infrastructure Servers DNS. DHCP, WINS, Remote Access Servers, NAT servers, RTO (Recovery Time Objective) and RPO (Recovery Point Objective), BCB and BIA. Domain Controllers – Securing File and Print Servers -Securing Application Servers	6
V	**Disaster Recovery and Fault Tolerance** Planning for the Worst -Creating a Backup Strategy -Designing for Fault Tolerance Antivirus **Privacy rules:** Access, data backup and type of data backup, test security systems and processes. Mobile/Cloud security issues and challenges in futuristic web security applications. Load balancers, Byte Streams Checksums - Custom Check-sums - Cryptographic Hashes Advanced Signatures - Fuzzy Hashing - Graph-Based Hashes for Executable Files	10

Text Books	1.	1 Computer System Security: Basic Concepts and Solved Exercises (Computer and Communiaction Sciences) Hardcover – Illustrated, 13 July 2007by Gildas Avoine (Author), Philippe Oechslin (Author), & 1 More 2. Computer System and Network Security Edited By Eric A. Fisch, Gregory B. White ISBN 9781138583085Published August 10, 1995 by CRC Press310 PagesCopyright Year 1996
E--Books	1.	https://www.researchgate.net/publication/220117871_Security_of_Computer_Systems_and_Networks_Book_Preview

Practical No.	Topic to be covered
1	**Practical No 1** Study of steps to protect your personal computer system by creating User Accounts with Passwords and types of User Accounts for safety and security.
2	**Practical No 2** Study the steps to protect a Microsoft Word Document of different version with different operating system
3	**Practical No 3** Study the steps to remove Passwords from Microsoft Word
4	**Practical No 4** Study various methods of protecting and securing databases.
5	**Practical No 5** Study “How to make strong passwords” and “passwords cracking techniques”.
6	**Practical No 6** Study of different wireless network components and features of any one of the Mobile Security Apps.
7	**Practical No 7** Study of the features of firewall in providing network security and to set Firewall Security in windows.
8	**Practical No 8** Steps to ensure Security of any one web browser (Mozilla Firefox/Google Chrome)
9	**Practical No 9** Study of different types of vulnerabilities for hacking a websites / Web Applications.
10	**Practical No 10** Analysis the Security Vulnerabilities of E-commerce services.
11	**Practical No 11** Open Ended Practical: Analysis the Security Vulnerabilities of E-mail services.

Open Electives-III

Course Title: Principles of Cryptography										
Semester	V	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	ODD	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	OE3	2	-	-	2	10	15	50	-	-
Course Code	23BTCYL308									
Teaching Mode	Offline	2 Hrs			Total	75			-	
Duration of ESE	3 Hr					75				

Course Objectives	To understand the techniques of Classical Cryptosystems
	To understand concepts of Symmetric cryptography
	To understand concepts of Asymmetric cryptography
	To Provide students with a comprehensive overview of Message Authentication Code and Hash Functions
Course Outcomes	CO1: Elaborate the role of cryptography & its fundamentals
	CO2: Apply various cryptography techniques
	CO3: Understand concepts of Symmetric cryptography
	CO4 : Understand concepts of Asymmetric cryptography
	CO5 : Analyze MAC and Hash algorithms

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	
CO1	**2**	**2**	**3**										**3**		
CO2		**2**												**2**	
CO3		**3**											**1**		
CO4			**3**	**3**										**3**	
CO5	**3**			**3**											

Course Contents:

Unit	Contents	Hours
I	**Introduction to Cryptography:** Introduction to, Terminology, History of Cryptography ,Shannon's Description of a Conventional Cryptosystem, Statistical Description of a Plaintext Source, Problems, Attacks, services, mechanisms, security attacks, security services.	4
II	**Classical Cryptosystems :** Caesar, Simple Substitution, Caesar Cipher, .Playfair ,Simple Substitution Cryptanalysis by The Method of a Probable Word .Vigenère Cryptosystem ,Kasiski's Method, Transpositions, Rail Fence The One-Time Pad Transposition.	4
III	**Introduction to Symmetric cryptography:** Symmetric cryptography, algorithms under symmetric cryptography.Block Ciphers Some General Principles Some Block Cipher ModesCodebook Mode Cipher Block Chaining Cipher Feedback Mode DES DES ,Triple DES and IDEA .	5
IV	**Introduction to Asymmetric cryptography:** Asymmetric cryptography, algorithms under asymmetric cryptography, placement of encryption function, traffic confidentiality, key distribution, Public key cryptography, Chinese remainder theorem, discrete logarithms.	4
V	**Message Authentication and Hash Functions** Authentication requirements, functions, codes, security of hash function & MACs. Hash & MAC algorithms. Digital signatures & authentication protocols.	3

Text Books	1.	a)Cryptography and networks security principles & practice by William Stallings (Pearson Education prentice Hall b) FUNDAMENTALS OF CRYPTOLOGY KLUWER ACADEMIC PUBLISHERS By Henk C.A. van Tilborg Eindhoven University of Technology The Netherlands
E--Books	1.	Cryptography and networks security principles & practice by William Stallings (Pearson Education prentice Hall

6th Sem as per NEP

Course Title: **Principles of Algorithm Design**										
Semester	VI	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	Even	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PCC9	3 Hrs.	-	2 Hrs.	4	10	15	50	25	25
Course Code	-									
Teaching Mode	Offline	5 Hrs.			Total	75			50	
Duration of ESE	3 Hrs.					125				

Course Objectives	This course introduces students the general idea of analysis and design of Algorithms while making them aware of basic methods of algorithm analysis and design.
	It is also aimed at developing skills to solve real life applications which involve algorithm development
	The course also provides career opportunities in analysis, design and optimization technique in algorithms
Course Outcomes	CO1: Recall basic concepts of algorithm in analysis and Design of algorithms.
	CO2: Examine Recurrence relations, solutions of recurrence of searching sorting methods
	CO3: Apply Greedy methods used for analysis and Design of Algorithm
	CO4: Analyze Dynamic Programming concepts in designing algorithm
	CO5: Evaluate advanced techniques and tools available for algorithm analysis and development

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO 1	PSO 2
CO1	--	3	--	--	--	--	--	--	--	--	--	--	2	--
CO2	--	--	3	--	--	--	--	--	--	--	--	--	1	--
CO3	--	--	--	3	--	--	--	--	--	--	--	--	2	--
CO4	--	--	3	--	--	--	--	--	--	--	--	--	2	--
CO5	--	--	3	--	--	--	--	--	--	--	--	--	2	--

Course Contents:

Unit	Contents	Hours
I	**Unit – I: Mathematical foundations & Asymptotic notations** summation of arithmetic and geometric series, n, n2,, Complexity calculation of various standard functions, Principles of designing algorithms, ,Asymptotic notations of analysis of algorithms, analyzing control structures, worst case and average case analysis, Iterative Algorithm analysis	9
II	**Unit – II: Divide and Conquer Method** Recurrence relations, solutions of recurrence relations using technique of Characteristic equation and generating functions Divide and conquer basic strategy, matrix operation, Strassens matrix multiplication, binary search, quick sort, merge sort.	8
III	**Unit – III: Greedy Method** Greedy method – basic strategy, application to job sequencing with deadlines problem, minimum cost spanning trees, single source shortest path, Huffman Coding, Prim's Algorithm, Kruskal's Algorithm, Dijkstra's Algorithm	8
IV	**Unit IV: Dynamic Programming** Dynamic Programming basic strategy, multistage graphs, all pairs shortest path, single source shortest paths, optimal binary search trees, traveling salesman, Knapsack, sum of subset problems	8
V	**Unit V: Traversal and Search Techniques** Basic Traversal and Search Techniques, breadth first search and depth first Search, Backtracking basic strategy, 8-Queen's problem, graph coloring, Hamiltonian cycles , NP-HARD AND NP-COMPLETE PROBLEMS: Basic concepts, non-deterministic algorithms, NP-hard and NP-complete classes.	9

Text Books	1.	Thomas H. Cormenet. al. "Introduction to Algorithms", Prentice Hall of India.
	2.	Design & Analysis of Computer Algorithms by Aho,. Horowitz, Sahani, Rajsekharam, Pearson education
Reference Books	1.	"Computer Algorithms", Galgotia Publications Pvt. Ltd. Brassard, Bratley, "Fundamentals of Algorithms", Prentice Hall
	2.	Computer Algorithms: Introduction to Design and analysis, 3rd Edition, By Sara Baase & A. V. Gelder Pearson Education.
On-line TL Material	1.	NPTEL course on Design and Analysis of Algorithms: https://www.class-central.com/course/nptel-design-and-analysis-of- algorithms-3984

Sr. No	Title of Practical	Hrs. Allotted	Relevance to CO
1	To Implement and analyze time complexity of Searching Algorithm.	2	CO1
2	To Implement and analyze time complexity of Sorting Algorithm.	2	CO1
3	To Implement and analyze time complexity of algorithm using Divide and Conquer Technique.	2	CO2
4	To Implement and analyze time complexity of Greedy Algorithm.	2	CO2
5	Implement Prim's algorithm using an adjacency matrix or list.	**2**	**CO3**
6	**Case Study:** Conference Room Booking System A company has multiple meeting requests. Design a system that selects the maximum number of meetings without time	**2**	**CO3**
7	To implement and analyze time complexity of Single source shortest path Algorithm.	2	CO4
8	To implement and analyze time complexity of All pair shortest path Algorithm.	2	CO4
9	To implement and analyze time complexity of Graph Traversing Algorithm.	2	CO5
10	Open-Source Practical	2	CO5

Course Title: **Data Analytics**										
Semester	VI	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	Even	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	PCC9	3	-	2	4	10	15	50	25	25
Course Code	-									
Teaching Mode	Offline	5 Hrs			Total	75			50	
Duration of ESE	3 Hrs.					125				

Course Objectives	To perform descriptive statistics on the given dataset
	To perform inferential statistics on the given dataset
	Apply linear regression and logistic regression and perform data visualization on the given dataset.
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1: Generate the dataset and perform Descriptive Statistics
	CO2: Evaluate the dataset and perform an Inferential Statistics
	CO3: Apply regression Analysis on the given dataset
	CO4: Create an interactive data visualization
	CO5: Recite the various learning techniques to derive case study

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	**Program Outcomes and Program Specific Outcomes**														
	PO1	PO 2	PO3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO1	PSO 2	PSO3
CO1	**3**			**2**		**2**				**2**			**2**		**1**
CO2	**3**							**2**					**2**		**2**
CO3			**3**				**2**		**3**		**2**		**3**	**1**	
CO4			**3**						**2**		**1**			**3**	**2**
CO5					**3**					**2**				**2**	**2**

Course Contents:

Unit	Contents	Hours
I	Data Analytics: Introduction to Analytics, Introduction to Tools and Environment, Application of Modeling in Business, Databases and Types of Data and variables, Data Modeling Techniques, Missing Imputations etc. Need for Business Modeling.	8
II	Descriptive statistics, data preparation. Exploratory Data Analysis data summarization, data distribution. Visualizing numerical data - graphing systems, measures of central tendency and dispersion – correlation - transforming data - exploring categorical variables.	8
III	Regression: linear regression simple linear regression, multiple & Polynomial regression, Sparse model. Supervised Learning: First step, learning curves, training validation and test. Learning models generalities, support vector machines, decision trees and random forest.	9
IV	Unsupervised learning, clustering, similarity and distances, quality measures of clustering, case study.	5
V	Classification and Prediction Issues Regarding Classification and Prediction, Classification by Decision Tree Induction, Bayesian Classification, and Classification Methods, Prediction, Classifier Accuracy.	8

Text Books	1.	Data Analytics: The Complete Beginner's Guide: the Black Book,Byron Francis, CreateSpace Independent Publishing Platform, 2016
	2.	Gupta S. C., & Kapoor V. K., Fundamental of Mathematical Statistics, Sultan Chand & Sons, 2018.
	3.	Teetor P, R cookbook: Proven recipes for data analysis, statistics, and graphics, O' Reilly Media Inc., 2011.
E--Books	1.	Fundamentals of Mathematical Statistics, Gupta SC, Kapoor V.K.. Publisher: Sultan Chand & Sons. Publishing Year: 2020. http://dcpehvpm.org/E-Content/Stat/FUNDAMENTAL%20OF%20MATHEMATICAL%20STATISTICS-S%20C%20GUPTA%20&%20V%20K%20KAPOOR.pdf
Reference Books	1.	Joel Grus , Data Science from Scratch First Principles with Python, O'Reilly Media, 2016

Data Analytics

List of Practical

Sr. No.	Name of Experiments
1	Loading dataset and visualizing data
2	Producing descriptive statistics measures
3	Demonstrate handling of missing data
4	Demonstrate Scatter Plot
5	Demonstrate Histogram Plot
6	Demonstrate Linear Regression for a given dataset
7	Demonstrate Multiple Linear Regression for a given dataset
8	Demonstrate Logistic Regression for a given dataset
9	Demonstrate Clustering for a given dataset
10	Demonstrate random Forest method for a given dataset
Open Ended Experiments / New Experiments	
1	Demonstrate Classification for a given dataset
2	Demonstration of data analysis on virtual Lab
Details of on line Laboratory Resource Material Instruction / Operating Manuals	
1.	https://www.iiitmk.ac.in/DAVirtalLab/#work

Course Title:E-II_IOT using Robotics_NEP										
Semester	VI	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	EVEN	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	Core	2	-	2	2	10	15	50	25	--
Course Code										
Teaching Mode	Offline	2			Total	75			-	
Duration of ESE	3 Hrs.					75				

Course Objectives	To introduce the fundamental concepts of IoT and robotics
	To develop understanding of sensors, actuators, microcontrollers, and embedded systems
	To provide hands-on experience in programming, interfacing, and deploying IoT-enabled robots.
Course Outcomes	Upon successful completion of this course, student will be able to:
	CO1: Explain the fundamental concepts, architecture, and components of IoT and robotics.
	CO2: Identify and interface sensors, actuators, microcontrollers, and communication modules used in IoT-enabled robotic systems.
	CO3: Design IoT-based robotic applications for data acquisition, monitoring, and control.
	CO4: Develop and program embedded systems (Arduino, Raspberry Pi, etc.) for IoT-robotics integration.
	CO5: Analyze real-time data, networking protocols, and security issues in IoT-robotic environments.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO2	PSO3
CO1	1	2	3	--	--	--	--	--	--	--	--	--	-	-	1
CO2	--	2	3	--	--	--	--	--	--	--	--	--	2	2	1
CO3	--	3	3	--	--	--	--	--	--	--	--	--	2	--	-
CO4	--	3	2	--	--	--	--	--	--	--	--	--	3	3	1
CO5	--	3	2	--	--	--	--	--	--	--	--	--	--	3	-

Course Contents:

Unit	Contents	Hours
I	**Introduction to IoT and Robotics** Overview of Internet of Things (IoT): Definition, characteristics, applications Basics of Robotics: Types of robots, components of a robotic system, IoT Architecture: Perception, Network, Middleware, Application layers, Embedded Systems for IoT and Robotics,Communication technologies: Wi-Fi, Bluetooth, ZigBee, RFID, LoRa ,Role of IoT in modern robotics and automation	8
II	**Sensors, Actuators, and Interfacing** Sensors used in robotics: Proximity, IR, Ultrasonic, Temperature, Motion, IMU Actuators: DC motors, Servo motors, Stepper motors, Relay modules, Sensor Integration with microcontrollers, Motor driver circuits: L293D, L298N ,Data acquisition and signal processing basics, Practical Interfacing with Arduino/Raspberry Pi	8
III	**Microcontrollers and IoT Platforms** Arduino: Architecture, digital & analog I/O, timers, interrupts, Raspberry Pi: Architecture, GPIO programming, Python-based control, ESP8266/ESP32: Wi-Fi-enabled microcontrollers, IoT communication protocols: MQTT, HTTP, CoAP Cloud Platforms: ThingsSpeak, Blynk, AWS IoT, Google Firebase,Building IoT-based robotic control systems	8
IV	**Robotics Control & Automation** Robot control algorithms: Line following, obstacle avoidance, path planning ,Autonomous robot design concepts ,Interfacing sensors/actuators for robotic decision-making ,Real-time data monitoring and control, Wireless robotic control using IoT apps, Integration of robotics with cloud dashboards ,Case studies: Smart car, home automation robot, surveillance robot	8
V	**Security, OT Systems, Real-Time, Edge Computing & Tools** Operational Technology (OT) & Cyber-Physical Security Introduction to OT systems: PLC, SCADA, DCS, ICS,Difference between IT vs OT networks,OT hardware in robotics & automation,Communication protocols used in OT: Modbus, OPC-UA, Profibus, BACnet,Definition of real-time systems in IoT-robotics ,Hard vs Soft real-time systems ,Example applications: autonomous robots, AGVs, industrial robots, drones ,What is edge computing & why it is needed ,Reduce latency for real-time robot control,Edge devices: Raspberry Pi, Jetson Nano, ESP32,IoT security basics: Vulnerabilities, authentication, encryption ,Secure communication for IoT-enabled robots , Real-time data analytics and remote diagnostics .Security Tools for IoT, OT & Robotics: Wireshark,Nmap,Kali Linux Tools,Metasploit.	8

Text Books	1	Internet of Things: Architecture and Design Principles **Author:** *Raj Kamal*
	2	Robotics: Control, Sensing, Vision, and Intelligence **Author:** *K. S. Fu, R. C. Gonzalez, C. S. G. Lee*
	3	Getting Started with Arduino **Authors:** *Massimo Banzi & Michael Shiloh*
	4	Learning Robotics Using Python **Author:** *Lentin Joseph*
	5	Designing the Internet of Things **Authors:** *Adrian McEwen & Hakim Cassimally*
Reference Books	1	Internet of Things: Robotic and Drone Technology **Author:** *C. S. R. Prabhu*
	2	Embedded Robotics: Mobile Robot Design and Applications with Embedded Systems ***Author:*** Thomas Bräunl
	3	Introduction to Embedded Systems and Robotics: A Practical Guide **Author:** *N. Yadav, M. Sharma, D. Shukla*
online TL Material	1	NPTEL – Introduction to Internet of Things
	2	Coursera – IoT Specialization (University of California, Irvine)

EXP NO.	**LIST OF EXPERIMENT**	**Mapping with CO**
	Mini Project: IoT Surveillance Robot **Objective:** Integrate sensors, camera, wireless control, telemetry, and cloud dashboard into a working prototype.	
1	Study IoT Architecture,Wi-Fi connectivity using ESP32/NodeMCU,Robotics, Real-time image streaming	CO-1
2	To design and integrate an **IoT-controlled mobile robot** for surveillance purposes.	CO-1
3	Requirements (Hardware & Software)like Arduino/NodeMCU/ESP32, Motor driver (L293D/L298N), DC motors or robotic chassis, ESP32-CAM or USB camera, PIR sensor / Ultrasonic sensor, IoT platform: Blynk / Firebase / MQTT Dashboard, Mobile app or Web dashboard	CO-2
4	To interface sensors (camera, PIR, obstacle sensors) with a microcontroller.	CO-2
5	To Assemble the robotic chassis and connect motors to the motor driver. Interface ESP32/NodeMCU with sensors and camera module.	CO-3
6	To implement **real-time remote monitoring** using IoT platforms (Blynk/Thingspeak/Firebase).	CO-4
7	Configure IoT app dashboard for robot control and live monitoring.	CO-4
8	To evaluate system performance and demonstrate applications in security automation.	CO-5

Course Title: Web Application Security										
Semester	VI	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	EVEN	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	Elective -II	3	-	2	4	10	15	50	25	-
Course Code	23BTCYLXXX/ 23BTCYLXXX									
Teaching Mode	Offline	5Hrs			Total	75			25	
Duration of ESE	3 Hr					100				

Course Objectives	1. To reveal the underlying in web application.
	2. To identify and aid in fixing any security vulnerabilities during the web development process
	3. To understand the security principles in developing a reliable web application.
Course Outcomes	CO1.Identify the vulnerabilities in the web applications.
	CO2. Identify the various types of threats and mitigation measures of web applications.
	CO3. Apply the security principles in developing a reliable web application.
	CO4 Use industry standard tools for web application security.
	CO5. Apply penetration testing to improve the security of web applications

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	2	3	1	2	3	1	0	2	1	1	0	2	3	2	1
CO2	2	3	2	2	3	2	1	2	1	1	0	2	3	3	1
CO3	2	2	3	1	3	1	1	2	1	2	1	2	2	3	1
CO4	1	2	2	2	3	1	0	1	1	1	1	2	2	3	1
CO5	2	3	2	3	3	2	1	2	1	2	1	3	3	3	2

Course Contents:

Unit	Contents	Hours
I	**Overview of Web Applications Security Fundamentals** Introduction history of web applications interface ad structure benefits and drawbacks of web applications Web application Vs Cloud application Security Fundamentals: Input Validation - Attack Surface Reduction Rules of Thumb- Classi- fying and Prioritizing Threads. Origin Policy - Exceptions to the Same-Origin Policy - Cross-Site Scripting and Cross-Site Request Forgery - Reflected XSS - HTML Injection	8
II	**Web Application Vulnerabilities** Understanding vulnerabilities in traditional client server application and web applications, client state manipulation, cookie based attacks, SQL injection, cross domain attack (XSS/XSRF/XSSI) http header injection. SSL vulnerabilities and testing - Proper encryption use in web application- Session vulnerabilities and testing - Cross-site request forgery.	8
III	**Web Application Mitigations** Http request , http response, rendering and events , html image tags, image tag security, issue, java script on error , JavaScript timing , port scanning , remote scripting , running remote code, frame and iframe , browser sandbox, policy goals, same origin policy, library import, domain relaxation	8
IV	**Secure Website Design** Secure website design : Architecture and Design Issues for Web Applications, Deployment Considerations Input Validation, Authentication, Authorization, Configuration Management , Sensitive Data, Session Management, Cryptography, Parameter Manipulation, Exception Management, Auditing and Logging, Design Guidelines, Forms and validity, Technical implementation	8
V	**Cutting Edge Web Application Security** Clickjacking - DNS rebinding - Flash security - Java applet security - Single-sign-on solution and security - IPv6 impact on web security	8

Text Books	1.	Sullivan, Bryan, and Vincent Liu. Web Application Security, A Beginner's Guide. McGraw Hill Profe ssional, 2011. 2. Stuttard, Dafydd, and Marcus Pinto. The Web Application Hacker's Handbook: Finding and **Exploiting Security Flaws. John Wiley Sons, 2011**
E--Books	1.	
Reference Books	1.	Web Application Security: Exploitation and Countermeasures for Modern Web Applications Paperback – Import, 13 March 2020 by Andrew Hoffman (Author)

Sr No	Name of Experiment	CO
1	Study and Analysis of Web Application Architecture and Security Fundamentals	CO1
2	Demonstration of Input Validation and Detection of HTML Injection / Reflected XSS	CO1
3	Study of Client-Side State Management and Cookie-Based Attacks	CO2
4	Identification and Testing of SQL Injection & HTTP Header Injection Vulnerabilities	CO2
5	Analysis of the Security Vulnerabilities of E-commerce services	CO3
6	Analysis of the security vulnerabilities of E-Mail Application	CO3
7	Make a Detailed Report on Network Security Threats covering Structured, Unstructured, Internal and External Threats	CO4
8	Configuring IPSec VPN Tunnel Mode using Packet Tracer	CO5
9	Open Ended	--
10	Open Ended	--

Course Title: Digital Forensics (E-III)										
Semester	VI	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term		Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	E-III	4	-	-	4	10	15	50	-	-
Course Code	**23BTCYL321**									
Teaching Mode	Offline	4 Hrs			Total	75			-	
Duration of ESE	3 Hrs					75				

Course Objectives	To understand underlying principles and many of the techniques associated with the digital forensic practices and cyber-crime.
	To develop an excellent understanding of current cyber security issues (Computer Security Incident) and analyze the ways that exploits in securities.
	To investigate attacks, IDS. Technical exploits and router attacks and "Trap and Trace" computer networks.
	To learn the importance of evidence handling and storage for various devices.
	To apply digital forensic knowledge to use computer forensic tools and investigation report writing.
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1: Analyze threats in order to protect or defend it in cyberspace from cyber-attacks.
	CO2: Develop appropriate security solutions against cyber attacks..
	CO3: Select different types of tools for various phases of forensics investigation
	CO4: Create reports as per standards of digital forensics.
	CO5: Understand he method to generate legal evidence and supporting investigation reports and will also be able to use various digital forensic tools.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1		**1**		**3**				**2**		**2**		**3**	**3**	
CO2			**2**	**1**	**3**							**3**		**2**
CO3		**1**		**2**	**3**							**3**	**1**	
CO4		**3**									**1**	**2**		
CO5				**1**	**3**							**2**		

Unit	Contents	Hours
I	**Fundamentals of Digital Forensics** Foundations of Digital Forensic: Digital evidence, Awareness, Principles of Digital Forensic,Challenging aspects of digital evidence, Cyber trail. Language of Computer Crime Investigation:Role of Computers in crime, Cybercrime law, offenses, jurisdiction. Traffic analysis, Fraud, IT Act	6
II	**Computer Forensic** Digital Evidence : Digital evidence in courtroom: Duty of experts, Admissibility, Locard's exchange principle, Types of Evidence, The Rules of Evidence, Volatile Evidence, Evidence collection andArchiving , Methods of Collection , Collection Steps, Controlling Contamination: The Chain of Custody. Processing Computer Crime : Introduction to Crime Scenes, Seizing and storing digital evidence at scene, Documenting the Scene and the Evidence , Dealing with Live Systems and Dead Systems, Using Hashing to Verify the Integrity of Evidence.	7
III	**Data Acquisition and Data Recovery** Data acquisition- Understanding storage formats and digital evidence, determining the best acquisition method, acquisition tools, validating data acquisitions, performing RAID data acquisitions, remote network acquisition tools, other forensics acquisitions tools Data Recovery: Data Backup and Recovery, The Role of Backup in Data Recovery, The Data-Recovery Solution Hiding and Recovering Hidden Data, Data Handling tools, ISO 27001.	6
IV	**Mobile device Forensic and Email Forensics** Mobile Device Forensics, Types of evidence on mobile device, Handling mobile device as a sources of evidence, Forensic prevention of mobile devices, Forensic examination , analysis of mobile devices, Forensic acquisition , examination of SIM cards (Architecture, Data Storage, Files, Mobile Operating System), Investigative reconstruction using mobile devices, Mobile Forensics and its challenges, Email Forensics: EMail Header Analysis, Function & Forensics, Chat and Social Networking Evidence. Case study	7
V	**Forensic Investigation Report and Forensic Tools:** Goals of Report, Layout of an Investigative Report, Guidelines for Writing a Report, sample for writing a Forensic report. Computer Forensic Tools: need and types of computer forensic tools, task performed by computer forensic tools. Study of open source Tools like SFIT, Autopsy etc. to acquire, search, analyze and store digital evidence. Case study	7

Text Books	1. Digital Evidence ; Computer Crime – Forensic science, Computers ; The Internet', Eoghan Casey, 3rd edition 2. 'Computer Forensics Computer Crime scene investigation', 2nd edition, Johm R. Vacca 3. Cyber Law Simplified, Vivek Sood 4. Basics of Digital Forensics, Second edition – John Sammons
Reference Books	4.Computer Forensics Investigating Network Intrusions & Cybercrime', EC–Council press, Cengage Learning 5. Guide to Computer Forensics & Investigations, 4th edition, Bill Nelson, Amelia Phillips & Christopher Steuart, Cengage Learning 6. 'Guide to Integrating Forensic Techniques into Incident Response', NIST, Karen Kent, Suzanne Chevalier Tim Grance, Hung Dang

Course Title: Privacy and Security in IOT/OT										
Semester	7^{th}	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term		Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	E-III	4	-	-	4	10	15	50	-	-
Course Code	23BTCYL323									
Teaching Mode	Offline	4			Total	75			-	
Duration of ESE	3 Hr					75				

Course Objectives	1. Understand the foundational concepts of IoT security and privacy
	2. Investigate the privacy challenges posed by IoT data collection
	3. Apply security protocols and cryptographic techniques to IoT systems
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1: Understand the IoT Vulnerabilities and authentication issues
	CO2: Analyze IoT-specific privacy issues and identify potential security threats
	CO3: Apply cryptographic and authentication techniques to secure IoT devices.
	CO4: Develop IoT security frameworks and solutions, including privacy-preserving protocols.
	CO5: Evaluate real-world IoT security scenarios and design secure IoT systems

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	**2**	**2**	**0**	**1**	**2**	**1**	**0**	**2**	**0**	**1**	**0**	**2**	**3**	**2**	**1**
CO2	**2**	**3**	**2**	**2**	**3**	**1**	**0**	**2**	**0**	**1**	**1**	**2**	**2**	**3**	**1**
CO3	**2**	**2**	**2**	**1**	**2**	**1**	**0**	**1**	**0**	**1**	**0**	**2**	**3**	**2**	**1**
CO4	**3**	**2**	**2**	**3**	**3**	**1**	**0**	**2**	**0**	**1**	**1**	**2**	**2**	**3**	**3**
CO5	**2**	**3**	**2**	**3**	**2**	**1**	**0**	**2**	**1**	**2**	**3**	**3**	**2**	**2**	**3**

Course Contents:

Unit	Contents	Hours
I	**Introduction to IoT and its Security Challenges :** Overview of IoT: Definition, architecture, and applications. Components of IoT Systems: Sensors, actuators, gateways, and cloud platforms, Security Challenges in IoT: Device security, data privacy, network security, authentication, and authorization issues. IoT Vulnerabilities: Security and privacy threats in IoT devices and communication protocols. IoT Security Standards: Overview of current IoT security standards and best practices (e.g., IEEE 802.15.4, ZigBee, 6LoWPAN, etc.).	8Hrs.
II	**Privacy in IoT Systems :** Privacy Issues in IoT: The role of IoT in data collection, personal data, and privacy risks, Data Sensitivity in IoT: Types of data (location, health, personal activities) and their sensitivity, Privacy Regulations: GDPR, CCPA, and other privacy laws impacting IoT data, Indian Law,Digital DPDP,Privacy Preservation Techniques: Data anonymization, differential privacy, and privacy-preserving protocols, Case Studies: Real-world IoT privacy violations and the lessons learned.	7Hrs.
III	**IoT Security Mechanisms :** IoT Security Requirements: Confidentiality, integrity, availability, authentication, non-repudiation, Cryptographic Techniques: Symmetric and asymmetric encryption, hashing, and digital signatures, Authentication and Authorization: Multi-factor authentication (MFA), public key infrastructure (PKI), OAuth, and access control models, Secure Communication Protocols: TLS/SSL, MQTT, CoAP, and secure channels in IoT, Intrusion Detection and Prevention Systems (IDPS) for IoT.	3
IV	**IoT Security Frameworks and Protocols :** Security Frameworks for IoT: Design principles, architecture of secure IoT systems,NIST-100-2A, IoT-Specific Security Protocols: ZigBee, Bluetooth LE, 6LoWPAN, and their security features, Block-chain for IoT Security: Introduction to Blockchain and its application for secure, decentralized IoT systems, Edge and Fog Computing Security: Security mechanisms in distributed IoT architectures, Threat Modeling and Risk Assessment: Evaluating IoT system vulnerabilities.	3
V	**Real-World IoT Security Case Studies and Applications:** IoT Security in Healthcare: Security and privacy in medical devices, wearable sensors, and health data, IoT Security in Smart Cities: Infrastructure, traffic management, and surveillance systems, Security Challenges in IoT-Enabled Industry 4.0: IoT in manufacturing, robotics, and automation, Designing Secure IoT Solutions: Hands-on project to secure a sample IoT system or application. Case Studies: Real-world security breaches in IoT (e.g., Mirai Botnet, Stuxnet),	3

Text Books	1.	Internet Of Things by Raj Kamal (Author) Publisher-McGraw Hill Education Edition-First Edition, Publication Date-10 March 2017, ISBN-13-978-9352605224
	2.	Security and Privacy in Internet of Things (IoTs): Models, Algorithms, andImplementations by Fei Hu (Author) Publisher-Taylor & Francis Books India Pvt., Edition-1,Publication Date- 29 June 2020, ISBN-13- 978-1032707150
	3.	Privacy and Security in IoT by Harish Chowdhary (Author), Brijesh KumarVerma (Author), Dr. Shaik Mohammad Rafi (Author), Dr. Umesh Sehgal (Author)Publisher- ACADEMIC GURU PUBLISHING HOUSE, Publication Date- 1 January2022, ISBN-13-978-93954689092nd Edition, Pearson, 2004.
E--Books	1.	Security and Privacy in Internet of Things (IoTs) by Fei HU, Publisher -CRC Press Taylor & Francis Group 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742, International Standard Book Number-13: 978-1-4987-2319-0 (eBook - PDF)
	2.	IoT SECURITY GUIDE" By Ministry of Electronics & Information technology Government of India, DSCI, National Center of Excellence, Cyber Security Centre of Excellence Aug-2022
TL Materials	1.	Udemy: Security in IoT (IoT Security) by Parag Achaliya. https://www.udemy.com/course/security-in-iot-
	2.	NPTEL-Internet of Things (IoT)- Prof. Sudip Misra, IIT Kharagpur Duration: 12 weeks https://onlinecourses.nptel.ac.in/noc22_cs96/preview

MD4

Course Title: Network Security										
Semester	VI	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	EVEN	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	MD 4	2	-	-	2	10	15	50		-
Course Code										
Teaching Mode	Offline	2 Hrs			Total	75				
Duration of ESE	3 Hrs					75				

Course Objectives	To develop a fundamental understanding of computer and network security proper practices, policies, technologies and standards
	To impart familiarity with the security techniques that provide information and network security
	To evaluate the security of communication systems networks and protocols based on a multitude of security factors
Course Outcomes	Up on successful completion of this course, student will be able to:
	CO1 – Describe the fundamental concepts and principles of computer and network security.
	CO2 - Identify and evaluate various network defense mechanisms and security tools.
	CO3 - Implement raw sockets for packet handling and sniffing, and compare key routing algorithms and protocols.
	CO4 - Develop TCP/UDP client–server applications and design iterative, concurrent, and multithreaded server architectures.
	CO5 - Apply symmetric encryption techniques and utilize number theory concepts for pseudorandom generation and stream cipher implementation.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	**PO 1**	**PO 2**	**PO 3**	**PO 4**	**PO 5**	**PO 6**	**PO 7**	**PO 8**	**PO 9**	**PO 10**	**PO 11**	**PO 12**	**PSO 1**	**PS O 2**
CO1				2									1	
CO2					3									2
CO3				1									2	
CO4					2									3
CO5					3								3	

Course Contents:

Unit	Contents	Hours
I	**Introduction to ISO's OSI Network Architecture:** Internet Model, IP Design and Implementation, Internetworking and routing protocols, Transport layer services and variants, Peer to Peer Networks, Application Layer protocols,	5
II	**Introduction to Network Security and Associated Techniques:** Firewall fundamentals ,Firewall features & advanced capabilities,Firewall Design principles, VPNs, Worms, Viruses, Vaccine Programs, Security of Network Layer, Security of Application layer protocols, BSD sockets, Elementary and Advanced system calls.	5
III	**Raw sockets:** Raw Socket Creation, Raw socket output, raw socket input, packet sniffing and routing algorithms: Router IOS- Static and Default Routing- Interior Gateway Routing Protocols: RIP V1&V2, OSPF, EIGRP- Exterior Gateway Routing Protocol: BGP	5
IV	**Introduction to socket programming-** Concurrent Processing in Client-Server, Software-Byte ordering and address conversion functions – Socket Interface - System calls used with sockets - Iterative server and concurrent server- Multi protocol and Multi service server- TCP/UDP Client server programs – Thread Creation and Termination – TCP Echo Server using threads- Remote Procedure Call.	5
V	**Symmetric ciphers:**Classical Encryption Techniques: SubstitutionTechniques, Transposition Techniques, Steganography. Block Ciphers and the Data Encryption Standard, Block Cipher Principles, The Data Encryption Standard. Basic Concepts in Number Theory and Finite Fields: Divisibility and the Division Algorithm, The Euclidean Algorithm. Advanced Encryption Standard, Pseudorandom Number Generation and Stream Ciphers.	5

Text Books	1.	Data Communications and Networking" by Behrouz A. Forouzan
	2.	Cryptography and Network Security: Principles and Practice" by William Stallings
Reference Books	1.	Richards Stevens, Unix network programming, , Vol I & Vol II, 4th edition, Prentice Hall, 2007 .
	2.	William Stallings, Cryptography and Network Security, Pearson Education,2007
Online Material	1.	Computer Networking: Principles, Protocols and Practice" by Olivier Bonaventure (Free online resource)

VSEC

Course Title: Information Coding Technique										
Semester	6^{TH}	Teaching Scheme				Evaluation Scheme				
						Theory			Practical	
Term	EVEN	Th	Tu	Pr	Credits	TAE	CAE	ESE	INT	EXT
Course Category	VSEC	1	-	2	2	10	15	-	25	-
Course Code										
Teaching Mode	Offline				Total	25			25	
Duration of ESE	3 Hr					50				

Course Objectives	**To introduce the fundamental principles of information theory** by explaining the concepts of information, entropy, mutual information, and channel capacity, and to help students understand how information is measured and transmitted efficiently.
	To develop knowledge of coding theory by studying different types of codes, including Huffman codes and convolutional codes, and enabling students to apply these codes through numerical problem-solving
	To provide a strong understanding of cyclic codes by explaining their generation, algebraic structure, and matrix representation, and to train students in solving problems related to cyclic encoding and decoding
	To familiarize students with error detection and correction techniques and enable them to analyze, design, and evaluate basic error control mechanisms through appropriate numerical examples
	To impart knowledge of linear block codes by teaching systematic block code encoding, syndrome computation, and decoding methods, along with developing proficiency in solving related numerical problems.
Course Outcomes	**CO1:** Interpret and apply the fundamental concepts of information theory, including information measure, entropy, mutual information, and channel capacity.
	CO2: Analyze and construct different coding techniques, such as Huffman coding and convolutional coding, and solve numerical problems related to source and channel coding
	CO3: Explain the structure and properties of cyclic codes and perform encoding and decoding using generator polynomials and matrix representations
	CO4: Apply error detection and correction methods to identify, detect, and correct errors in digital communication systems through appropriate numerical techniques
	CO5: Design and evaluate linear block codes using systematic encoding, syndrome decoding, and solve related analytical and numerical problems.

Mapping of Course Outcomes with Program Outcomes and Program Specific Outcomes:

Course Outcomes	Program Outcomes and Program Specific Outcomes														
	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2	PSO 3
CO1	**3**	**2**	**0**	**1**	**2**	**1**	**0**	**2**	**0**	**1**	**0**	**2**	**3**	**2**	**1**
CO2	**2**	**3**	**2**	**2**	**3**	**1**	**0**	**2**	**0**	**1**	**1**	**2**	**1**	**3**	**1**
CO3	**2**	**2**	**1**	**1**	**2**	**1**	**0**	**1**	**0**	**1**	**0**	**2**	**3**	**2**	**1**
CO4	**3**	**2**	**2**	**2**	**3**	**1**	**0**	**2**	**0**	**1**	**1**	**2**	**2**	**3**	**2**
CO5	**2**	**3**	**2**	**3**	**2**	**1**	**0**	**2**	**1**	**2**	**2**	**3**	**2**	**2**	**3**

Course Contents:

Unit	Contents	Hours
I	**Unit-I:Information Theory** Definition of Information,Measure of Information,Rate of Information,Shannon-Hartley Theorem,Entropy,Relationship between Entropy and Mutual Information.	3
II	**Unit-II:Coding Theory** Classification of Codes,Huffman Coding,Convolutional Coding and Numerical.	3
III	**Unit-III:Cyclic Code** Cyclic Codes Generation,Matrix Description of Cyclic Codes and Numerical.	3
IV	**Unit-IV:Error Detection & Correction Code** Introduction to Error Detection and Error Correction Code and Numerical.	3
V	**Unit-V:Linear Block Codes** Systematic Linear Block Codes encoding,Syndrome decoding and Numerical.	3

Text Books	1.	Thomas M.Cover,Joy A Thomas,Elements of Information Theory,2 nd Edition,Wiley,2015
	2.	Bose,Ranjan.Information theory,Coding and Cryptography,2 nd Edition,Tata McGraw-Hill Education,2008.
	3.	Shu Lin, Daniel J. Costello Jr., *Error Control Coding: Fundamentals and Applications*, 2nd Edition, Pearson, 2004.
E--Books	1.	David J.C. MacKay, Information Theory, Inference, and Learning Algorithms, Cambridge University Press, 2003 (Free Online Edition).

	2.	Raymond W. Yeung, A First Course in Information Theory, Springer, 2002 (Open Access via Chinese University of Hong Kong).
	3.	Rüdiger Urbanke, Tom Richardson, Modern Coding Theory, Cambridge University Press, 2008 (Free Online Draft).
	4.	Igal Sason, Lecture Notes on Information Theory and Coding, Technion – Israel Institute of Technology, 2018 (Free Academic e-Book).
TL Materials	1.	NPTEL, *Information Theory and Coding*, Video & Web Course, IIT Kharagpur, 2019.
	2.	MIT OpenCourseWare, Information Theory, Lecture Notes & Assignments, Massachusetts Institute of Technology, 2016.
	3.	NPTEL, *Digital Communications*, Video Lectures & PDFs, IIT Madras, 2018.
	4.	Coursera, *Error Control Coding and Information Theory*, Online Course Materials, University of Colorado, 2020.

Practical No.	Topic to be covered	COs
1	Implement Coding and Decoding of BCH and RS Codes.	CO1
2	Write a program for determination of various entropies and mutual information of a given channel.Test various types of channel such as CO1 a)Noise free channel b)Error free channel c)Binary Symmetric channel d)Noisy Channel Compare channel capacity of above channels.	CO1
3	Introduction to MATLAB CO2 a)To define and use variables and functions in MATLAB. b)To define and use Vectors and Matrices in MATLAB. c)To study various MATLAB arithmetic operators and mathematical functions. d)To create and use m-files.	CO2
4	Basic plotting of signals CO2 a)To study various MATLAB commands for creating two and three dimensional plots. b)Write a MATLAB program to plot the following continuous time and discrete time signals. i.Step Function ii.Impulse Function iii.Exponential Functions iv.Ramp Function v.Sine Function	CO2
5	Write a MATLAB program to perform amplitude-scaling,time-scaling and time shifting on a given signal.	CO2
6	Write a MATLAB program to obtain linear convolution of the given sequences.	CO2
7	Write a MATLAB program to plot magnitude and phase response of a given system.	CO2
8	Checking linearity/non-linearity of a system using SIMULINK.Build a system that amplifies a sine wave by a factor of two.	CO2
9	Study of Sampling theorem,effect of undersampling.	CO3
10	Sampling of band limited signal:Nyquist theorem.	CO3
11	Sampling of non bandlimited signal:Anti aliasing filter.	CO3
12	Implement a program for generation and evaluation of variable length source coding using Huffman Coding and decoding(C/MATLAB).	CO4
13	Implement coding and decoding of Cyclic codes.	CO4
14	Implement coding and decoding of Convolutional codes.	CO4
15	Implement coding and decoding of Linear block codes.	CO5
16	Write a simulation program to implement source coding and channel coding for transmitting a text file.	CO5
17	Implement a program to study performance of a coded and uncoded communication system(calculate the error probability)	CO5