AC – **07/07/2023**
Item No. – **6.38 (N)**

As Per NEP 2020

University of Mumbai

Title of the program

A- P.G. Diploma in Cyber Security Law and Forensics(PGDCSLF)

Syllabus for

Semester – Sem I & II

Ref: GR dated 16th May, 2023 for Credit Structure of PG

(With effect from the academic year 2023-24)

Preamble

1) Introduction

The PG Diploma in Cyber Security Law and Forensics is a specialized program designed to equip students with the necessary knowledge and skills to tackle the complex legal and technical challenges of cybersecurity and digital forensics. It focuses on the legal aspects of cybersecurity, information security, and digital forensics, preparing students to handle cyber threats, investigations, and related legal matters effectively.

2) Aims and Objectives

PG Diploma in Cyber Security Law and Forensics providing students with specialized knowledge and skills in the intersection of cybersecurity, law, and digital forensics.

1. Understanding Cybersecurity Laws and Regulations:
The program aims to familiarize students with the legal frameworks, national and international cyber laws, and regulations related to cybersecurity and cybercrime. Students will gain an understanding of the legal implications of cyber activities and the measures taken by governments and organizations to address cyber threats.

2. Developing Digital Forensics Expertise:
The objective is to equip students with the necessary skills and techniques to conduct digital investigations and forensic analysis of digital evidence.

3. Building Information Security Management Knowledge:
The program seeks to provide students with a comprehensive understanding of information security management principles.

4. Enhancing Incident Response and Mitigation Skills:
Students will learn how to respond to and manage cyber incidents effectively. This includes learning incident handling procedures, mitigation techniques, and best practices to minimize the impact of security breaches and attacks.

5. Fostering Ethical Hacking and Penetration Testing Abilities:
The program aims to introduce students to ethical hacking concepts, techniques, and tools used to identify and address vulnerabilities in computer systems and networks.

6. Promoting Data Privacy and Protection Awareness:
The objective is to educate students about data privacy laws, regulations, and best practices.

7. Understanding Cybersecurity Risk Management:

The program will teach students how to assess and manage cybersecurity risks in organizations.

8. Equipping for Cybercrime and Digital Investigations:
Students will gain knowledge about different types of cybercrimes and the methodologies used to investigate and prosecute cybercriminals.

9. Providing E-Discovery and Legal Proceedings Insights:
The program aims to familiarize students with e-discovery procedures and their role in legal proceedings involving digital evidence.

10. Emphasizing Cybersecurity Compliance and Governance:
Students will learn about industry standards, best practices, and compliance frameworks in cybersecurity.

3) Learning Outcomes

The learning outcomes from a PG Diploma in Cybersecurity Law and Forensics are designed to ensure that students acquire the necessary knowledge, skills, and competencies to excel in the field of cybersecurity, digital forensics, and legal aspects of cyber activities. Upon completing the program, students should be able to demonstrate the following learning outcomes:

1. Comprehensive Understanding of Cybersecurity Laws and Regulations:
Students will have a deep understanding of the legal frameworks, national and international cyber laws, and regulations related to cybersecurity and cybercrime. They will be able to interpret and apply these laws to real-world scenarios.

2. Proficiency in Digital Forensics Techniques:
Graduates will be proficient in digital forensics techniques, including data acquisition, preservation, analysis, and presentation. They will be able to conduct effective digital investigations and uncover digital evidence from various devices and networks.

3. Expertise in Information Security Management:
Students will have the skills to develop and implement information security strategies, policies, and measures to protect digital assets from cyber threats and data breaches.

4. Competence in Incident Response and Mitigation:
Graduates will be capable of responding to cyber incidents promptly and effectively. They will have the knowledge to mitigate the impact of security breaches and prevent future incidents.

5. Ability to Perform Ethical Hacking and Penetration Testing:

Students will be proficient in ethical hacking techniques, enabling them to identify vulnerabilities in computer systems and networks and recommend appropriate security measures.

4) Any other point (if any)

The Post Graduate Diploma in Cybersecurity Law and Forensics seeks to produce competent professionals who can address the complex challenges of cybersecurity, digital forensics, and legal aspects of cyber activities. Graduates of the program will be well-equipped to contribute to the protection of digital assets, the investigation of cybercrimes, and the development of cybersecurity policies and practices in various industries and governmental organizations.

5) Credit Structure of the Program (Sem I, II)

R:_____

Credit Distribution Structure for One Year
Post Graduate Diploma in Cyber Security Law and Forensics (PGDCSLF)

Year	Level	Sem	Major				RM	OJT/ FP	RP	Cum. Cr.	Degree
			Mandatory			Electives					
1	6.0	Sem I	2*4+2*2 + 2			4	4	4	-	22	PG Diploma (after 3 Years Degree)
			Cybercrime investigation – I (Crime Scene Management and Incident response) 501	TH	4	Introduction to Artificial Neural Networks (506a) **(OR)** Cloud Computing (506b) **(OR)** Cryptography and Network Security (506c)	Research Methodology (510)				
			Introduction to Digital devices and networks 502	PR	2						
			Cybercrime investigation – II 503	TH	4						
			Introduction to Cyber law, Electronic Evidence, Data privacy law and types of cybercrime 504	PR	2						
			Forensic technologies and Digital forensics 505	TH	2						
		Sem II	2*4+2*2 + 2			4	-	517	-	22	
			Dark web and Cyber warfare 511	TH	4	Fuzzy Systems & Genetic Algorithms (516a) **(OR)** Virtualization (516b) **(OR)** Security Fundamentals for Cloud (516c)					
			Cyber Psychology and Ethics 512	PR	2						
			Crime Scene Management 513	TH	4						
			Cyber Security Technology and Regulations 514	PR	2						
			IT Act 2000, IT Act Amendments and IPR in cyberspace 515	TH	2						
Cum. Cr. For PG Diploma			28			8	4	4		44	
Exit Option: PG Diploma (44 credits) after Three Year UG Degree											

Sign of HOD
Dr. Mrs. R. Srivaramangai
Dept of Information Technology

Sign of Dean
Prof. Shivram Garje
Science & Technology

Syllabus for
Post Graduate Diploma in Cyber Security Law and Forensics
(PGDCSLF)

SEMESTER I

Programme Name: PG Diploma in Cyber Security Law and Forensics (PGDCSLF)

Course Code: 501[Mandatory] **Total Credits:** 04 (60 Lecture Hrs) **University assessment:** 50 marks	**Course Name:** Cybercrime investigation – I (Theory) **Total Marks:** 100 marks **College/Department assessment:** 50 marks

Course Objectives (COs):
To enable the students to:

CO 1: Present an overview of types of cybercrime.

CO 2: Analyze the different crimes that pertain to use of Emails, various Social Media platforms, dark Web.

CO 3: Identify strategies to track, document and use Emails, Social Media platforms, and the dark web, data as evidence.

MODULE I:	**(2 CREDITS)**
Unit I a) **Cybercrimes and cybercrime investigation:** Cyber-crime- Scope, characteristics and landscape over the years and present scenarios in cyber space. Development of cyber-crime,Classification of cyber-crime cyber criminals – Individual criminals / Organized criminals / sponsored criminals / hired criminals ,Various types of cybercrimes and their modus operandi and predictive policing,Challenges to investigators / Challenges in investigations,Safeguarding from cyber crimes,Investigation of the most common cybercrimes reported to LEA, Emerging trends in cybercrime Dos and don'ts while investigating cybercrime complaints,Difference between investigation of traditional crime and cyber crime,Common mistakes done by IO (Crime Scene, Search and Seizure, transportation, labeling, documentation – incorrect entries in seizure memo, irregularities in seizure memo, irrelevant or vague questions in forwarding note to FSL) Importance of documentation b) **Email Investigation:** Working of Email.,Types of email, configurations – IMAP / POP., Various parts of an email. Components of an email header. Email header analysis. Differences between emails headers of various service providers. Identifying spoofed email, phishing email. Step action guide on Email tracking and tracing. Requesting details from intermediaries. Collection of email as an evidence – single email, multiple emails, entire mailbox etc. Presentation of email as an evidence in court. Restoring deleted emails from web and app. Challenges such as proxy and VPN. Regaining access to hacked email IDs. Email tracking through lawful interception under 91 C.R.P.C. Email tracking through extra lawful interception. c) **Social Media related investigations: Facebook related investigations:** Identity theft related cases, Difference type of cybercrime associated (Cyber stalking / Bullying / Harassment) , Content investigation (obscenity / nudity / defamatory related cases), Content removal, FB live stream blocking methods, Accused character estimation through FB ,Missing people/human trafficking surveillance in FB, FB posts share-tag-comment-like related offences, Facebook analytics, Downloading complete profile from Facebook, Facebook for law enforcements, Collection, preservation of digital evidences, presentation in the court of law. **Twitter Related investigations:** Identity theft related cases, Difference type of cybercrime associated (Cyber stalking / Bullying / Harassment), Content investigation (obscenity / nudity / defamatory related cases) , Content removal, Investigation on Tweet, Retweet, Tags, Handlers, Twitter Analytics, Web patrolling using Twitter, Downloading complete tweets from a profile, keyword etc. , Sentiment analysis, Collection, preservation of digital evidences, presentation in the court of law	15 Hrs

Unit II **a) Social Media related investigations Instagram Related Investigations:** Identity theft related cases, Difference types of cybercrime associated (Cyber stalking / Bullying / Harassment), Content investigation (obscenity / nudity / defamatory related cases) , Content removal, Downloading complete content, Instagram for law enforcement, Collection, preservation of digital evidences, presentation in the court of law **Linkedin Related Investigations:** Identity theft related cases, Cyber stalking / harassment, Content investigation, Content removal, Job frauds, Downloading complete user data. Collection, preservation of digital evidences, presentation in the court of law **b) Snapchat Related Investigations:** Identity theft related cases, Cyber stalking / Cyber Bullying / harassment, Content investigation (obscenity / nudity / defamatory related cases), Content investigation, Content removal, Downloading complete user data, Collection, preservation of digital evidences, presentation in the court of law. **Youtube Related Investigations:** Content investigation (obscenity / nudity / defamatory related cases), Copyright infringement related cases, Youtube Video content removal, Youtube Tracing video uploaded user details, Youtube Video comment analysis, Youtube video tracking through geolocation/geotagging, Collection, preservation of digital evidences, presentation in the court of law **c) Matrimonial / Dating / Adultery Related Investigations:** Content investigation (obscenity / nudity / defamatory related cases), Tinder / Happn / Locanto / Tagged / Escort Services Related Apps / Websites, Collection, preservation of digital evidences, presentation in the court of law. **Other Social Media Apps / Websites Related Investigations:** Tiktok / Sharechat / Musically, Games Related Investigations – Blue Whale, PubG, Fortnite, MoMo Games, Advisory content for Cyber Safety Awareness	15 Hrs
MODULE II:	**(2 CREDITS)**
Unit III **a) Investigation of Fin-Tech related cases**: Various kinds of Fin-Tech options available in India,Common misconceptions,Investigating e-wallets Investigating ATM related frauds,Investigating OTP related frauds, Investigating Payment gateways, Investigating identity theft related cases Database forensics, Job frauds, Gambling, Betting, Financial transactions for illegal activities **b) WhatsApp / Telegram investigations:** Live WhatsApp investigation-digital foot prints, Deleted WhatsApp chat retrieving methods, WhatsApp-cloud chatting extraction methods, WhatsApp image or video offences related investigation, Cyber harassment through WhatsApp, Investigation on WhatsApp groups, Spy on WhatsApp groups through masking, methods-left-extreme-fundamental-radical groups, How to request details from WhatsApp via legal approach, Originator of post (Content, Image, Video), WhatsApp Call Investigations (Audio, Video).	15 Hrs
Unit IV **a) Introduction to location / cloud based investigations:** Introduction to Location Based Services., Types of Location Based Services. Triangulation and GPS Techniques to pinpoint the actual location of the criminals., By using CDR and Cell ID. By using Triangulation techniques. By using GPS tagging on photographs. By using Google Photos. Etc. By using WhatsApp, Facebook, Viber etc. Types of cloud service providers (Android / Apple / Blackberry etc.) Tracking of missing / stolen mobile phones or tablets, Gathering data created using various Google services, Requesting details from Google via legal approach Introduction to Location Based Services. Retrieval of data from Google / iCloud /Microsoft cloud services. Tracing missing/stolen mobile By Using IMEI No. Tracing missing/stolen mobile By Using MAC No. **b) Introduction to Dark Web Investigations:** Introduction of Deep & Dark Net. Surface Internet vs Deep Internet. Indexed Website vs Non Indexed Websites. Red Rooms, Galaxy, Hidden WIKI, Wiki leaks, Silk Road, Pandora other Onion links. Modus operandi of cyber-crimes committed using Dark Web. Working principle of Block Chain. Concepts of Crypto currencies and mechanism behind	15 Hrs

	it. Wallet Tracking, Public Key vs Private Key (Wrt Crypto Currencies) Introduction to track cryptocurrencies. Challenges in investigations.	

Books and References:

Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives		2018
2.	Digital Forensics and Incident Response	Gerard Johansen	Gerard Johansen	2nd	2020
3.	Security and Incident Response	Keith J. Jones, Richard Bejtloich and Curtis W. Rose		1st	
4.	First Responder's Guide to Computer Forensics	Richard Nolan	Carnegi Mellon	1st	2005
5.	Computer Forensics and Cyber Crime	Marjie T. Britz	Pearson	3rd	2009

Course Outcomes (OCs)

Upon completing this course, the student will be able to:

OC 1: Articulate an overview of types of cybercrime.
OC 2: Analyse the different crimes that pertain to use of Emails, various Social Media platforms, and the dark web.
OC 3: Identify strategies to track, document and use Emails and Social Media platforms as evidence.

Course Code: 502[Mandatory] **Total Credits:** 02 (60 Lecture Hrs) **University assessment:** 25 marks	**Course Name:** Introduction to Digital devices and networks Practical **Total Marks:** 50 marks **College/Department assessment:** 25 marks

Course Objectives (COs):

To enable the students to:

CO 1: To Focus on information sharing and networks.
CO 2: To Introduce flow of data, categories of network, different topologies.
CO 3: To Focus on different digital devices and their applications

Course Outcomes (OCs)

Upon completing this course, the student will be able to:

MODULE I:	(2 CREDITS)
Unit 1: **a) Computer** – Classification of computers, features and specifications of various computer generations, functionalities of a computer, data processing and storage.,Hardware components and their uses, Introduction to types of computing devices – desktops, laptops, MacBook, iMac,All in One computers, tablets, wearable devices. Different Operating Systems and their relevance to Law Enforcement Officers. Demo of disassembling a Computer and showing various components and peripherals. Types of Data Storage – primary, secondary etc. Types of storage device technology – magnetic tapes, flash (Semiconductor memories), difference between mobile phone storage and computer storage etc. **b) Hard Disk Drive overview** – physical and logical structure, Types of Hard Disk Drive interfaces – SATA, IDE, SCSI, SSD etc., Parts of Hard Disk Drive – spindle, disk, Structure of Hard Disk Drive – sector, track, cluster size etc., Hard Disk Drive data addressing, metadata, disk capacity, calculation and measuring performance of Hard Disk Drive. Partitioning and formatting of Hard Disk Drive – low level and high level formatting. Boot	30 Hrs

process – master boot record, types of Operating System, file systems, understanding File System, shared disk file systems, special purpose file systems, etc. CDROM/DVD file system – CDFS, ISO, Joliet, and UDF. **c) Introduction to Computer Networks:** Need of computer,networks,Different types of computer networks,Bluetooth technology / Wi-Fi technology / WiMAX technology,HAN / PAN, LAN, MAN, WAN,Network Architecture and topology,Networking devices – Firewalls, Hub, Bridge, Switch, Routers, IDS/IPS etc.,Concept of physical addressing system,Identification of MAC Addresses,Concept of logical addressing system,Types of IP Addresses – static, dynamic, public, private,Concept of IP address assignment – DHCP, static, Types of IP address versions - Ipv4, Ipv6, difference between IPv4 and IPv6. Intranet vs Internet vs Extranet, Concept of website, DNS and URLs, Identification of IP address of a user device or website	
Unit 2: **a) Introduction to Mobile Devices:** Basics of Mobile phone & communications: Components of Cellular Network,, Different Mobile Devices, Hardware Characteristics of Mobile Devices, Software Characteristics of Mobile Devices, Mobile Operating Systems : Classification of Mobile Operating Systems (WebOS, Symbian OS, Android OS,RIM BlackBerry OS, Windows Phone 7, Apple iOS), difference between desktop operating system and mobile operating system. **b) CCTV and BOTS:** Video Enhancement, Demultiplexing, Footage Restoration, Visual Authentication, Enhancement & Speed Correction, Format Conversion, Audio Enhancement, Tampering Investigations, Alexa Devices (BOT).	30 Hrs

Books and References:

Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	**E-Discovery: Introduction to Digital Evidence**	Amelia Phillips, Ronald Godfrey, Christopher Steuart, Christine Brown.	Security Pub ISBN-13: 978-1285427423	1st	2000
2.	Practical Guide to Digital Forensics Investigations	Darren Hayes	Pearson	2nd	2020
3.	Data communication & Networking	Bahrouz Forouzan	PHI	2nd	2005
4.	Computer Networks	Andrew S. Tanenbaum	Pearson	1st	2001

Course Outcomes (OCs)

Upon completing this course, the student will be able to:

OC 1: Acquire the basic knowledge of data sharing, transmission media and their protocols.

OC 2: Apply the basic knowledge of computer networks and digital devices.

Course Code: 503[Mandatory]	**Course Name:** Cybercrime investigation –II (Theory)
Total Credits: 04 (60 Lecture Hrs)	**Total Marks:** 100 marks
University assessment: 50 marks	**College/Department assessment:** 50 marks

Course Objectives (COs):

To enable the students to:

CO 1: Present an overview of Dark Web Investigations.

CO 2: Present an overview of Cyber Terrorism and Network Forensics.

MODULE I:	**(4 CREDITS)**
Unit I **a) Dark Web Investigations:** Introduction of Deep & Dark Net., Surface Internet vs Deep Internet., Indexed Website vs Non Indexed Websites. Red Rooms, Galaxy, Hidden WIKI, Wiki leaks, Silk Road, Pandora other Onion links. Modus	15 Hrs

operandi of cyber-crimes committed using Dark Web. Working principle of Block Chain. Concepts of Crypto currencies and mechanism behind it. Wallet Tracking, Public Key vs Private Key (Wrt Crypto Currencies), Introduction to track cryptocurrencies. Challenges in investigations. **b) Cyber Terrorism:** Misuse of Internet by terrorists, Recruitment, spread of propaganda on Internet, Phony websites & Cyber Herding, Web crawlers and use of data mining, Proactive measures to combat misuse of Internet by the terrorists.	
Unit II a) **Network Forensics:** Network Evidence Types and Sources, Network Packet Capture, Encapsulation and decapsulation methods, Session reconstruction for protocols – TCP and HTTP, Log collection, aggregation, and analysis, Wireless Packet Analysis, Challenges- Encoding, Encryption, VPN, MITM - Man-in-the-Middle Methods, Tools. Investigation of critical information infrastructure (CII) related crimes: SCADA Networks, Railway Networks, Power Grid Networks, Water Grid Networks, Nuclear Power Plants, defense networks b) **Arriving at the Scene: Initial Response/ Prioritization of Effort**s : Initial Response/ Receipt of Information, Safety Procedures , Emergency Care, Secure and Control Persons at the Scene , Boundaries: Identify, Establish, Protect and Secure, Turn Over Control of the Scene and Brief Investigator(s) in Charge, Document Actions and Observations, Establish a Command Post (Incident Command System) and Make Notifications, Manage Witnesses, Preliminary Documentation and Evaluation of the Scene, Conduct Scene Assessment, Conduct Scene "Walk-Through" and Initial Documentation , Note-Taking and Logs	15 Hrs
MODULE II:	**(2 CREDITS)**
Unit III **a) Processing the Scene:** Determine Team Composition, Ensure Contamination Control, Documentation, Sketching, Photography, Videography, Prioritize Collection of Evidence, Crime Scene Search Methods, Collect, Preserve, Inventory, Package, Transport, and Submit Evidence, Detailed Crime Scene Evidence Collection	15 Hrs
Unit IV a) **Completing and Recording the Crime Scene Investigation**: Establish Crime Scene Debriefing Team, Perform Final Survey of the Crime Scene, Documentation of the Crime Scene, Acknowledge Specialized Crime Scene Circumstances, Crime Scene Investigation in Correctional and Custodial Facilities, Time-Limited Crime Scene Investigation **a) Crime Scene Equipment:** Initial Responding Officer(s), Crime Scene Investigator/Evidence Technician, Evidence Collection Kits (Examples)	15 Hrs

Books and References:

Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Crime Scene Investigation A Guide for Law Enforcement	Kevin Lothridge, Frank Fitzpatrick	National Forensic Science Technology Center	1st	2013
2.	Practical Crime Scene Processing and Investigation,	Ross M. Gardner, Donna Krouskup	CRC Press	Third Edition	2019
3.	Computer Forensics: Principals and Practices	Linda Volonino, Reynaldo Anzaldua and Jana Godwin	Pearson Prentice – Hall	1st	2007
4.	Computer Forensics: Computer Crime Scene Investigation	John R. Vacca, Charles	River Media	2nd	2005

5.	Cyber Forensics - Concepts and Approaches	Ravi Kumar & B Jain	ICFAI press	1st	2009
6.	Computer Forensics: Investigating Network Intrusions and Cyber Crime	Ec-Council Press Series: Computer Forensics	EC-Council	2nd	2010

Course Outcomes (OCs)

Upon completing this course, the student will be able to:

OC 1: Discuss data and identify data sources
OC 2: Describe and discuss digital evidence
OC 3: Compare and contrast the differences between digital evidence and traditional evidence
OC 4: Discuss the ways in which digital evidence is authenticated
OC 5: Describe and critique digital forensics process models
OC 6: Critically evaluate standards and good practices for digital evidence and digital forensics

Course Code: 504[Mandatory] **Total Credits:** 02 (60 Lecture Hrs) **University assessment:** 25 marks	**Course Name:** Introduction to Cyber law, Electronic Evidence, Data privacy law and types of cybercrime Practical **Total Marks:** 50 marks **College/Department assessment:** 25 marks

Course Objectives (COs):

To enable the students to:

CO 1: Acquire the knowledge of Cyber Law with reference to the IT Act and its amendments.
CO 2: Explain the types of digital evidence
CO 3: Demonstrate the processes for data carving.
CO 4: Demonstrate the process for data collection and analysis.
CO 5: Analyse the varying levels of freedom in data privacy.

MODULE I:	**(2 CREDITS)**
Unit 1: **a) Introduction to IT Act and IT Act Amendments:** Cybercrimes and their respective sections., Section 79, Government Examiner of Digital Evidence. Requirement of certification under different sections. Understanding the report given by cyber forensics. Relevant sections of Indian Evidence Act, Admissibility of electronic evidence, Frame proper notice with clauses, Indian Penal Code and cybercrimes, Code of Criminal Procedure 1973 – search and seizure provisions, examination of witnesses through audio and video by police Section 46 the role of adj. officer - IT Act , Difference between 79 3b IT, 91 Cr PC and 149 Cr PC, Relevant International laws and acts Mutual Legal Assistance Treaty, Letter Rogatory , Procedural aspects of law, Federal laws, GDPR, TRIPS and other global law practices related to IT Act., CERT.IN, MEITY, TERM, TRAI, ICANN / IANA etc b) **Digital Evidence:** Digital evidence – definition, characteristics, types, source of digital evidence etc. Classification of Digital evidence – user created, user protected and system created. Difference between volatile and non-volatile memory, Rules of Evidence – best evidence rule, hearsay evidence etc., Traditional forensic evidence vs digital evidence. Cyber forensics – definition, classification, Cyber forensics v/s traditional forensics – Locard's Exchange Principle, Daubert's Rule, Repeatability and Reproducibility, peer review techniques, Introduction to forensic tools, techniques and technology. Discussion on its application to Computer Systems, Network, communication devices, volatile memory, storage systems, Internet Data, Cloud, SCADA Systems and Databases, Computer Forensic Imaging and Hashing, Anti-forensics - Data hiding techniques **c) Data carving:** Hashing – importance, process, algorithm and tools. Best practices – ACPO, Interpol, STCIA, DOJ guidelines and best practices in Indian environment. Responsive toolkit – preparation, portable software tools, validation of tools, things to carry. Cyber forensics process – Identify, preview, acquire, authenticate, analyze and document. Areas to search – Active files, deleted files, slack space, unallocated space,	30 Hrs

hibernation file, page file, metadata and registry etc. Steps in crime scene investigation – securing crime scene, interviews, shutdown process, collecting evidence, packaging and transportation Process model – triage process, dual process model and utility Collection of important data – tools and techniques for collecting volatile data from RAM from a live system.	
Unit 2: a) **Mobile forensics** - Mobile Forensics Definition, Information available in Mobile Phones, Memory Considerations in Mobiles, Subscriber Identity Module (SIM), SIM File System, Integrated Circuit Card Identification (ICCID), International Mobile Equipment Identifier (IMEI), International Mobile Subscriber Identity (IMSI), Electronic Serial Number (ESN), difference between mobile forensics and computer forensics, identification, isolation of mobile devices, search and seizure of mobile devices, acquisition methods (physical, logical, file system, JTAG, Chip off), Analysis of mobile images, understanding a mobile forensic report. Imaging the drive at scene of crime using various tools and techniques – Use of write blocker devices, imaging, cloning, hashing, authentication of evidence, CRC, tools for hashing Volatile data capture and analysis – Capturing system info, network info. Packaging and transportation and preservation Documentation – seizure memo, Chain of Custody, forwarding note to FSL, 65 B, etc. b) **Fundamental Concept of Data Privacy:** , Definitions, Statistics, Data Privacy Attacks, Data linking and profiling, access control models, role based access control, privacy policies, their specifications, languages and implementation, privacy policy languages, privacy in different domains- medical, financial, etc **c) Technology, Policy, Privacy and Freedom:** Medical privacy legislation, policies and best practices, Examination of privacy matters specific to the World Wide Web, Protections provided by the Freedom of Information Act or the requirement for search warrants.	30 Hrs

Books and References:

Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Cyber Law and Cyber Crime	Adv.(Dr) Prashant Mali	SnowWhite / Cyber Infomedia	2nd	2020
2.	Digital Evidence and Computer Crime	Eoghan Casey	Academic Press	2nd	2004
3.	The Complete Book of Data Anonymization: From Planning to Implementation	B. Raghunathan	Auerbach Pub	1st	2013
4.	Guide to Cyber Laws	Rodney D. Ryder	Wadhwa and Compan		2009
5.	Security and Incident Response	Keith J. Jones, Richard Bejtloich and Curtis W. Rose		1st	

Course Outcomes (OCs)

Upon completing this course, the student will be able to:

OC 1: Articulate the various IT Acts pertinent to Data Privacy and Security.
OC 2: Explain what constitutes digital evidence.
OC 3: Identify the best practices for data carving.
OC 4: Use appropriate process model for data collection and analysis.
OC 5: Analyse the levels of freedom in data privacy with respect to the roles of the actors and the context.

Course Code: 505[Mandatory] **Total Credits:** 02 (30 Lecture Hrs) **University assessment:** 25 marks	**Course Name**: Forensic Technologies and Digital Forensics **Total Marks:** 50 marks **College/Department assessment:** 25marks

Course Objectives (COs):

To enable the students to:

CO 1: Describe digital forensics and relate it to an investigative process.

CO 2: Explain the legal issues of preparing for and performing digital forensic analysis based on the investigator's position and duty.

CO 3: Perform basic digital forensics.

CO 4: Demonstrate use of digital forensics tools.

CO 5: Guide a digital forensics exercise.

CO 6: Recognize the state of the practice and the gaps in technology, policy, and legal issues.

MODULE I:	**(2 CREDITS)**
Unit 1: a) Computer forensics fundamentals, Benefits of forensics, computer crimes, computer forensics evidence and courts, legal concerns and private issues. Introduction to legal issues, context, and digital forensics, Media Analysis: disk structure, file systems (NTFS, EXT 2/3, HFS), and physical layer issues. b) Understanding Computing Investigations – Procedure for corporate High-Tech investigations, understanding data recovery work station and software, conducting and investigations. c) 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.	15 Hrs
Unit 2: a) Processing crimes and incident scenes, securing a computer incident or crime, seizing digital evidence at scene, storing digital evidence, obtaining digital hash, reviewing case. b) Current computer forensics tools- software, hardware tools, validating and testing forensic software, addressing data-hiding techniques, performing remote acquisitions, E-Mail investigations- investigating email crime and violations, understanding E-Mail servers, specialized E-Mail forensics tool.	15 Hrs

Books and References:

Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	**Computer Forensics: Incident Response Essentials**	**Warren G. Kruse II and Jay G. Heise**	Addison Wesley	1st	2002
2.	Guide to Computer Forensics and Investigations	Nelson, B, Phillips, A, Enfinger, F, Stuart, C.	Thomson Course Technology	2nd	2006
3.	Computer Forensics, Computer Crime Scene Investigation	Vacca, J	Charles River Media	2nd	2005
4.	The Best Damn Cybercrime and Digital Forensics	Book Perio,Jack Wiles, Anthony Reyes , Jesse Varsalone	Syngress Publishing	1st	2007
5.	Computer Evidence and Computer Crime: Forensic Science, Computers, and the Internet	Casey, Eoghan	Cambridge University Press	1st	2000

Course Outcomes (OCs)

Upon completing this course, the student will be able to:

OC 1: Know how to apply forensic analysis tools to recover important evidence for identifying computer crime.

OC 2: To be well-trained as next-generation computer crime investigators.

OC 3: Know how to apply the skills of forensic investigation

OC 4: know how to apply the forensic tools for forensic investigation

Course Code: 506a [Elective] **Total Credits:** 04 (60 Lecture Hrs) **University assessment:** 50 marks	**Course Name**: Introduction to Artificial Neural Networks **Total Marks:** 100 marks **College/Department assessment:** 50 marks

Pre-requisite:

a. Basics of Artificial Intelligence
b. Knowledge of AI algorithms

Course Objectives (COs):

To enable the students to:

CO 1. Understand the fundamentals of Artificial Neural Network
CO 2. Understand the difference between pattern and data
CO 3. Understand the basic neural network structure
CO 4. Understand the neural network structure for complex tasks

MODULE I:	**(2 CREDITS)**
Unit 1: a) **Introduction**: Trends in Computing, Pattern and Data, Pattern recognition Tasks and its Methods b) **Basics of Artificial Neural Networks**: Characteristics and History of Neural Network, Terminologies of ANN, Models of Neuron, Topology, Basic Learning Laws, Demonstration and implementation: simple neural network, calculate the output of the neural network c) **Activation and Synaptic Dynamics** – Activation Dynamics Models, Synaptic Dynamics Models, Learning Methods, Stability and Convergence, Recall	15 Hrs [OC1, OC2, OC3]
Unit 2: a) **Functional units of ANN for pattern Recognition Tasks**: Problems of Pattern Recognition, Basic Functional Units, Pattern Recognition Tasks by the Functional Units, Demonstration and Implementation: AND, XOR, AND/NOT function using McCulloch Pitts Neural Network, Hebb's Rule and Delta Rule b) **Feedforward Neural Networks**: Analysis of Pattern Association Networks, Analysis of Pattern Classification Networks, Analysis of Pattern Mapping Networks, Demonstration and Implementation: Linear Separable Problem, Back Propagation, Supervised Learning Algorithms	15 Hrs [OC3, OC4, OC5]
MODULE II :	**(2 CREDITS)**
Unit 3: a) **Feedback Neural Networks**: Analysis of Linear Autoassociative FF Network, Analysis of Pattern Storage Networks, Stochastic Networks and Simulated Annealing, Boltzmann Machine, Demonstration and Implementation: Autoassociative Memor, Boltzmann Machine **b) Competitive Learning Neural Network**: Components of Competitive Learning Network, Analysis of Feedback Layer for Different Output Functions, Analysis of Pattern Clustering Network, Analysis of Feature Mapping Network, Demonstration and Implementation: Unsupervised Learning, Kohenon Self-organizing map.	15 Hrs [OC6, OC7]
Unit 4: a) **Architectures for Complex Pattern Recognition Tasks**: Associative Memory, Pattern Mapping, Stability-Plasticity Dilemma- ART, Temporal Patterns, Pattern Variability: Neocognitron, Demonstration and Implementation: ART b) **Applications of ANN**: Direct Application of ANN, Application Areas, Demonstration and Implementation: Radial Basis Function	15 Hrs [OC1 & OC8]

References:

1. Artificial Neural Network, B. Yegnanarayana, PHI
2. Principles of Soft computing, S.N.Sivanandam S.N.Deepa, 3rd, Wiley
3. Neural Networks, Fuzzy Logic and Genetic Algorithms: Synthesis & Applications, S.Rajasekaran,G. A.Vijayalakshami, Prentice Hall of India

Course Outcome (OCs)

Upon completing this course, the student will be able to:

OC 1. Recognizes the areas where ANN is applied and used
OC 2. Understands the basic difference between data and patterns, recognition and understanding
OC 3. Understands the basic terminologies used in ANN
OC 4. Understands the basic architectural structure of neural networks
OC 5. Able to identify the areas where feedforward network can be used
OC 6. Able to identify the areas where feedback network can be used
OC 7. Understands the concepts of pattern clustering and feature mapping
OC 8. Able to identify which structure to be applied for the complex pattern recognition tasks

Course Code: 506b [Elective]	**Course Name**: Cloud Computing
Total Credits: 04 (60 Lecture Hrs)	**Total Marks:** 100 marks
University assessment: 50 marks	**College/Department assessment:** 50 marks

Pre-requisite: Knowledge of operating systems, Networking, Databases & Basics of Security and Privacy

Course Objectives (COs)

To enable the students to:

CO 1. Understand the fundamental concepts of cloud computing
CO 2. Acquire knowledge of various cloud technologies.
CO 3. Learn different types of Virtualization Techniques.
CO 4. Evaluate the cloud services offered by major cloud players
CO 5. Understand the different types of cloud storage and cloud security

MODULE I:	**(2 CREDITS)**
Unit I **a) Overview of Cloud Computing**: Introduction to cloud computing, Characteristics of cloud computing, Advantages of cloud computing, Disadvantages of cloud computing, Cloud service models, Cloud computing deployment models, Cloud computing deployment models **b) Cloud Architecture and Applications:** Cloud architecture, Components of cloud computing architecture, Working of cloud computing, Applications of cloud computing **c) Case Study**: public cloud, Private cloud and hybrid cloud, Infrastructure as a Service, Software as a Service and Platform as a service	15 Hrs OC1
Unit II **a) Scalability and Redundancy:** Meaning of scalability, Key features of cloud scalability, Types of scalability, Ways to scale cloud, Concept of redundancy, Benefits of redundancy **b) Cloud Services:** Cloud services, Benefits of cloud services, Types of cloud service models-Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Network as a Service (NaaS), Identity as a Service (IdaaS) **c) Case Study:** Study and implementation of Storage as a Service (IaaS), Working with Goggle Docs, Sheets and Notes (SaaS)	15 Hrs OC2
MODULE II:	**(2 CREDITS)**
Unit III **a) Cloud Deployment Models:** Public Cloud-Public cloud architecture, Private cloud deployment model, Comparison between private and public cloud, Community cloud deployment model, Hybrid cloud deployment model, Comparative study for all clouds, Multi cloud **b) Virtualization:** Features of virtualization How does virtualization work? Benefits of virtualization Difference between cloud computing and virtualization, Types of virtualization-Hardware virtualization, Software virtualization, Server virtualization, Storage virtualization, Operating system virtualization **c) Cloud Management:** Cloud provisioning, Cloud management benefits, Cloud management tools, Components of cloud computing management Cloud management security Challenges faced during cloud management Demonstrate and Implement Software Virtualization using Hypervisors (VMWARE). eg VMware ESX and ESXi , Microsoft Hyper-V, Citrix XenServer	15 Hrs OC3

a) Data Storage and Security: Cloud storage basics, Types of cloud storage, Advantages and risks of cloud storage, Infrastructure Data protection process Cloud security Measures and controls in cloud security, Encryption **b) Cloud Operations and Challenges:** Defining cloud operations, Cloud operations objective, Cloud operations management, Benefits of cloud operations, Challenges related to cloud computing **c) Technologies and Service Models Structure:** Cloud computing technologies, Types of cloud computing technologies. Service providers, MeghRaj, Case study on data storage security in private cloud, A Case Study on Cyber-Attacks in Cloud Computing, Case Study on data breaches in cloud computing	15 Hrs OC4

References:

a) Cloud Computing Simplified Explore Application of Cloud, Cloud Deployment Models, Service Models and Mobile Cloud Computing by Surbhi Rastogi ,1st edition BPB Publications, India
b) Cloud Computing - Master the Concepts, Architecture and Applications with Real-world examples and Case studies by Kamal Kant Hiran Ruchi Doshi Dr. Temitayo Fagbola Mehul Mahrishi,1st edition, BPB Publications, India
c) Cloud Computing, Sandeep Bhowmik by 1st edition Cambridge University Press
d) Cloud Computing For Dummies®, by Daniel Kirsch & Judith Hurwitz, 2nd Edition John Wiley & Sons, Inc

Course Outcomes (OCs)

Upon completing this course, the student will be able to:

OC 1. Explain concepts, features of cloud delivery model, Service Model, and advantages and disadvantages of cloud computing as well as determine the cloud computing architecture and infrastructure
OC 2. Differentiate the different types of Cloud Services, their advantage and disadvantages, needs of cloud scalability and redundancy.
OC 3. Differentiate the different types of cloud's deployment model, different types of virtualization techniques, Cloud managements tools,
OC 4. Analyze cloud storage systems, cloud security, as well as the associated risks, cloud operations and their challenges in the cloud computing, different types of cloud computing technologies

Course Code: 506c [Elective]	**Course Name**: Cryptography and Network Security
Total Credits: 04 (60 Lecture Hrs)	**Total Marks:** 100 marks
University assessment: 50 marks	**College/Department assessment:** 50 marks

Pre requisite: Basic Algebra, Set theory, Logical Reasoning, Fundamentals of Computer Networks and Internet.

Course Objectives (COs)

To enable the students to:

CO 1. Understand the basic principles of security, types security.
CO 2. Understand the Standard algorithms used for security.
CO 3. Analyze and use methods for cryptography
CO 4. Develop a workable knowledge of the mathematics used in Cryptography
CO 5. Differentiate various hardware and software security systems
CO 6. Know the applications of these techniques in real world
CO 7. Have the basic knowledge on Image Forgery and protection

MODULE I:	**(2 CREDITS)**
Unit 1: a) **Attacks on Computer and Computer Security**: Introduction, Need for Security, Security Approaches, principles of Security, Types of Attacks. **b) Cryptography Concepts and Techniques**: Introduction to Plain text and Cipher text, Substitution Techniques, Transpositions Techniques, **c) Encryption and Decryption**: Symmetric and Asymmetric key Cryptography, Steganography, Key range and size, Possible types of Attacks.	15 Hrs [OC1, OC2]
Unit 2: **a) Symmetric Key Cryptography:** Introduction, Algorithmic types and	15 Hrs

modes, An Overview of symmetric key cryptography, DES, IDEA, RC4, RC5, Blowfish, AES . **b) Asymmetric Key Cryptography and Digital Signatures:** Introduction, Overview of AKC, RSA algorithm. **c) Digital Signatures and Other Methods**: Digital Signatures, Knapsack Algorithm, Hybrid algorithms with symmetric and Asymmetric techniques.	[OC3, OC4]
MODULE II:	**(2 CREDITS)**
Unit 3: **a) Digital Certificates and PKI:** Introduction, Digital Certificates, Private key management, PXIX Model, PKCS, PKI and Security. **b) Internet Security Protocols:** Introduction, Basic Concepts, SSL, TLS, SHTTP, TSP, SET, 3D secured Protocol. **c) Security in technologies**: Electronic Money, Email Security, WAP Security, Security in GSM, Security in 3G,4G,5G.	15 Hrs [OC5]
Unit 4: **a) User Authentication and Kerberos:** Introduction, Authentication basics, passwords and tokens, Certificate based authentications, biometric authentication, Kerberos, KDC, SSO Approaches **b) Network Security, Firewalls and VPN:** Introduction, TCP/IP, Firewalls, VPN, Intrusion. c) **Case Studies:** SSO, DDOS, IP Spoofing Attacks, Cookies and Privacies, VPN creation, Latest attacks.	15 Hrs [OC6, OC7]

References:

1. Atul Kahate, "Cryptography and Network Security", 2nd Edition and above, TMH
2. William Stallings, "Cryptography and Network Security, Principles and Practice", 7th Edition, Pearson.
3. Behrouz, Forouzon, Debdeep Mukhopadyay, "Cryptography and Network Security", McGrawHill

Course Outcomes (OCs)

Upon completing this course, the student will be able to:

OC 1. Acquire knowledge on standard algorithms used to meet the principles of security such as confidentiality, integrity and Authenticity

OC 2. Understand the mathematical concepts and techniques for encryption and decryption

OC 3. Understand the applications of symmetric key, asymmetric key cryptographic algorithms

OC 4. Understand the technique and use of digital signatures.

OC 5. Understand and implement the technologies of internet such as digital certificates, Internet security protocols and tools

OC 6. Understand authentication mechanisms and network security mechanisms like firewall, VPN etc.

OC 7. Understand clearly the various real-time case studies on how to implement the acquired knowledge on the syllabus

Course Code: 510	**Course Name**: Research Methodology
Total Credits: 04 (60 Lecture Hrs)	**Total Marks:** 100 marks
University assessment: 50 marks	**College/Department assessment:** 50 marks

Pre requisite:

Basic programming skills, orientation towards research and conceptual understanding of IT subjects

Course Objectives (COs)

To enable the students to:

CO1. Know basics of how research problems are defined, research methods are adopted and/or developed, research is undertaken

CO2. Make understand how research results are communicated to the peers.

CO3. Learn research methods, some of which are general in nature and the remaining specific to the field of Information Technology and the specialization.

MODULE I:	**(2 CREDITS)**
Unit 1: **Research Methodology and Problem Identification and Formulation:** Meaning and objectives, motivation of research, types of research, research methods v/s methodology, research and scientific methods, research process and stages of research, defining and formulating the research problem, technique involved in defining a problem, importance of literature review in defining a problem, role of literature review, ways to perform literature review, methods to find open problem and research problems, critical literature review, identifying gap areas from literature study, hypothesis building	15 Hrs [OC1]
Unit 2: **Research Design and Data Collection and Analysis:** Need of research design, concepts related to research design, different research designs, research plan, basic principles of experimental design and setup, collection of primary data, observation methods, interview methods, collection of data through questionnaire and schedules, collection of secondary data, selection of appropriate method for data collection, case study method, guidelines for developing questionnaire, successful interview, survey v/s experiment, processing and data analysis, use of statistical packages, measure of asymmetries and other measures. Fieldwork-The Nature of Field Work, Selection and Training of Investigators, Sampling Frame and Sample Selection, Field Operation, Field Administration.	15 Hrs [OC2, OC3]
MODULE II:	**(2 CREDITS)**
Unit 3: **Probability Distribution and Hypothesis Testing:** Sampling and probability distribution, definitions and basic concepts of hypothesis testing, procedures of hypothesis testing, flow diagram for hypothesis testing, test of hypothesis, important parametric test, hypothesis testing of mean, proportion, tests for equality of mean and variances of two population, confidence interval, z-test, and X2 test for goodness to fit, limitation of test of hypothesis. **Analysis of Variance and Covariance:** Basic principle of Analysis of Variance, ANOVA Technique, Setting up Analysis of Variance Table, short-cut method for one- way ANOVA, Coding method, Two-way ANOVA, ANOVA in Latin-square design, analysis of co-variance (ANCOVA), assumptions in ANCOVA.	20 Hrs [OC4]
Unit 4: **Academic Ethics:** Plagiarism, exposure on anti-plagiarism tools. **Technical Writing and IPR:** Academic writing, sources of information, assessment of quality of journals and articles, writing scientific report, structure	10 Hrs

and component of research report, types of report – technical reports and thesis, SCOPUS Index, citations, search engines beyond google, impact factor, H-Index. **IPR:** What is IPR?, importance of patents, types of IPR, process of patent.	[OC5, OC6, OC7]

References:

1. Dawson, Catherine, 2002, Practical Research Methods, New Delhi, UBS Publishers' Distributors.
2. Kothari, C.R.,1985, Research Methodology-Methods and Techniques, New Delhi, Wiley Eastern Limited.
3. Kumar, Ranjit, 2005, Research Methodology-A Step-by-Step Guide for Beginners, (2nd.ed), Singapore, Pearson Education.
4. Neeraj Pandey, Intellectual Property Rights ,1st Edition, PHI
5. Shrivastava, Shenoy& Sharma, Quantitative Techniques for Managerial Decisions, Wiley
6. Goode W J &Hatt P K, Methods in social research, McGraw Hill
7. Basic Computer Science and Communication Engineering – R. Rajaram (SCITECH)

Course Outcomes (OCs)

Upon completing this course, the student will be able to:

OC1: Basic understanding of research and how to formulate a research problem
OC2: Understand and develop methodological design for the research problem
OC3: Identify the required data and use data collection methods for acquiring data
OC4: Set hypothesis for the given research problem and apply testing methods
OC5: Follow the research ethics
OC6: Write research proposals, documentations related with research
OC7: Understand and apply IPR and patent filing

SEMESTER II

Course Code: 511[Mandatory]	**Course Name:** Dark web and Cyber warfare (Theory)
Total Credits: 04 (60 Lecture Hrs)	**Total Marks:** 100 marks
University assessment: 50 marks	**College/Department assessment:** 50 marks

Course Objectives (COs):

To enable the students to:

CO 1: To have deep understanding of the web

CO 2: To gain knowledge on the working of Dark Web

CO 3: To identify the security aspects of dark net.

CO 4: To understand the operational procedures of cyber war and to have clarity on defense mechanism

MODULE I:	**(2 CREDITS)**
Unit I a) Introduction. Surface Web, Deep Web and Dark Web. Usage of Dark Web. Working of dark web.The TOR browser and its history. Introduction to cyber weapons and its types, types of cyber attacks, types of state and non-state actors. Known cyber gang and non-state actor group.	15 Hrs
Unit II a) Cryptocurrency and other currencies used in dark web, known market places on dark net, Silk Road case study	15 Hrs
MODULE II:	**(2 CREDITS)**
Unit III **a)** Anatomy of a Ransomware attack, Ransomware as a service. Wannacry, Locky. Sodinokibi - ransomware. Case study of ransomware attacks across the world, Selling access to servers. Renting Infrastructure. Selling Financial Details. Selling Personal Details.	15 Hrs
Unit IV a) Identifying Darknet Cybersecurity risks.Dark web intelligence. The gray areas. Policing the shadows. Need for new regulations. Open source Intelligence (OSINT) tools. Intra-country data exchange of cyber criminals and regulations around it. **b)** Cyber warfare, Security Measures, Dealing with Cyber terrorists, Stages of Defense: Prevention, Incident Management, Mitigating an Attack, Damage Limitation and Consequence Management. International cyber crime treaties. Law against darkweb and cyber warfare: World and Indian Scenario	15 Hrs

Books and References:

Sr. No.	Title	Author/s	Publisher	Edition	Year
1. .	Dark Web Investigation (Security Informatics and Law Enforcement)	Babak Akhgar (Editor), Marco Gercke (Editor), Stefanos Vrochidis (Editor)	Springer	1st	2021
2.	Inside the Dark Web	Erdal Ozkaya and Rafiqul Islam	CRC Press	1st	2020
3.	Tor and the Dark Net	James Smith	CRC Presss	1st	2016
4.	Online Privacy An Introduction to TOR Network and Online Security: How to stay anonymous in the Internet	Wiliam Rowley	--	1st	2016
5	Tor And The Deep Web	Leonard Eddison	The Complete Guide To Stay Anonymous In The Dark Net	1st	2018

Course Outcomes (OCs)

Upon completing this course, the student will be able to:

OC 1: Able to work in Law enforcement for cybercrime investigation w.r.t to dark web and warfare
OC 2: able to understand the deep / dark web attacks
OC 3: able to identify the dark web attacks and handle the scenario
OC 4: able to use the deep web operating system and apply the security measures

Course Code: 512[Mandatory] **Total Credits:** 02 (60 Lecture Hrs) **University assessment:** 25 marks	**Course Name:** Cyber Psychology and Ethics Practical **Total Marks:** 50 marks **College/Department assessment:** 25 marks

Course Objectives (COs):

To enable the students to:

1. Acquaint learners with basic psychological terminology used in forensic psychology and cyber psychology
2. Understand and apply psychological assessment system
3. Interpret psychological profiles of offenders
4. Understand apply techniques to psychologically help the victims.
5. Apply psychological principles for public awareness and society.

MODULE I:	**(2 CREDITS)**
Unit 1: a) **Understanding Psychology and Cybersecurity:** Basic Principals of Psychology, Introduction to Forensic psychology, Ethical aspects of Psychological assessment and counselling, Professional aspects of psychological assessment and counselling, Documentation of the assessment and its utility as evidence **b) Psychology of Offenders:** Motivations for Cybercrime, Individual Differences (Personality), Social and Contextual Aspects, Observer described characteristics. Eye-witness testimony. Crime types and Psychology: instrumental crimes (ultimate aim is not harming victim) and expressive crimes (intent of harming the victim). Online dating, relationships, sex and related crimes. Financial Crimes. **c) Forensic and Psychological Assessment:** Psychological Profiling of Offenders. Detection of Malingering and Deception, Personality Profile: FFM, Dark Tried, Clinical profiles. Interpreting profiles. Profiling and Linking Crimes: Sex crimes, revenge porn, and child pornography; Cyberbullying and Cyberstalking; Identity Theft; Financial crimes. Use of Brain mapping signatures: BEOS Psychological techniques for dealing with Offenders.	15 Hrs
Unit 2: a) **Psychological Reaction of Victim and Victim Counselling:** Psychological Reactions for Cyberbullying and Cyberstalking, Revenge Porn, Identity Theft, Financial Loss. Cyber terrorism. Basic communication Skills. Crisis Intervention, Dealing with Loss and Grief. Psycho-education. Supportive Psychotherapy. Cognitive-Behaviour Interventions. Suicide/ Homicide risk assessments. Supporting further steps, Corrective action. b) **Public Awareness and Society:** Psychological Aspects of Decision-Making: Financial, Interpersonal (romantic and sexual relations). Using Psychological Principles for Prevention of Cybercrime. Educating Parents, Schools and Colleges: Financial Crimes and Sex-crimes in cyber space. Principles of large scale awareness and advocacy.	15 Hrs

Books and References:

Sr. No.	Title	Author/s	Publisher	Edition	Year

1.	Cybercrime: Psychology of Online Offenders	Kirwan, G., & Power, A.	Cambridge University Press.	1st	2012
2.	Cyberpsychology: The Study of Individuals, Society and Digital Technologies	Whitty, M. and Young, G.	BPS Blackwell	1st edition	2016
3.	The psychology of Cybercrime.	Kirwan, G., & Power, A.	Information Science Reference	1st	2012
4	Forensic psychology	Scott, Adrian	Palgrave MacMillan.	1st	2010
5	Forensic Psychology (4 Vol set)	Bull, R. (ed)	Sage publications	1st	2011
6	Investigative Psychology: Offender Profiling and the Analysis of Criminal Action	Canter, D. and Youngs, D.	Wiley	1st	2009
7	The Cyber Effect	Aiken, M.	John Murray	1st	2016
8	Handbook of crime prevention and community safety	N. Tilley & A. Sidebottom (Eds.),	Routledge.	1st edition	2005

Course Outcomes (OCs)

Upon completing this course, the student will be able to:

OC 1: Apply understanding of Psychological Intervention for dealing with Victims
OC 2: Apply understanding of Psychological Intervention for dealing with Offenders
OC 3: Apply understanding of Psychological Intervention for educating society at large
OC 4: Use psychological profiling typologies of following types of online crime:

a. Cybertrespass - hackers, crackers, breakers and online scammers, Cyberterrorism, Cyberdeception and theft – including identity theft and fraud, Cyberpornography and obscenity - from child to adult pornography and trafficking online, Cyberviolence – stalking, bullying, harassment, domestic abuse and hate speech
b. Classwork: Interpret Five profiles of different crimes as a class activity
c. Classwork: Learn to interpret reports of at least two kinds of psychological assessment
d. Interpret psychological profiles of offenders.
e. Understand and apply ethical and Professional aspects of the psychological intervention.

Course Code: 513[Mandatory] **Total Credits:** 04 (60 Lecture Hrs) **University assessment:** 50 marks	**Course Name:** Crime Scene Management (Theory) **Total Marks:** 100 marks **College/Department assessment:** 50 marks

Course Objectives (COs):

To enable the students to:

CO 1: Crime scene management skills are an extremely significant task component of investigation because evidence that originates at the crime scene will provide a picture of events for the court to consider in its deliberations.
CO 2: The significance of forensic science to human society.
CO 3: The fundamental principles and functions of forensic science
CO 4: The divisions in a forensic science laboratory.
CO 5: The working of the forensic establishments in India and abroad.

MODULE I:	(2 CREDITS)
Unit I a) Primary Survey, Barrication, Scene Documentation, Forensic Photography – scene photography and its method, Identification b) Recognition and Recovery of evidences, Basic types of evidence- visible, plastic, latent, micro & macro, trace and ultra-trace, pattern, fragile and digital evidence. Method for Search, Collection (preservation), Handling packaging, Important evidence such as Impression evidence	15 Hrs
Unit II a) Panchnaama (Spot Investigations and recording) - conducting, recording, authenticating with Pancha's, recovery of hard disk, mobile phone, CCTV (DVR), electronic devices.	15 Hrs
MODULE II:	**(2 CREDITS)**
Unit III a) Practical Scene videography (Clockwise and anti-Clockwise videography) special segment videography, CCTV(DVR machine) handling and export of logs and video files. Handling of voice recorder and specimen voice recording	15 Hrs
Unit IV **a)** Crime Scene - Onsite Forensic Investigation Tools, Live data acquisition from standalone computer , network server, mobile phone, triage data acquisition	15 Hrs

Books and References:

Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Forensic Science in India : A vision for the Twenty First Centrury	B.B. Nanda and R.K Tiwari	Select publisher	1st	2001
2.	An Introduction to Forensic Sciences	W.G. Eckert and R.K. Wright	CRC Press	2nd	1997
3.	Fisher's Techniques of Crime scene Investigation	R. Saferstein, M.L. Hastrup and C.Hald	CRC Press	2nd	2013
4.	Fisher's Techniques of Crime Scene Investigation	W.J. Tilstone, M.L. Hastrup and C.Hald	CRC Press	2nd	2013
5.	Crime Scene Investigation: A Guide for Law Enforcement	Janet Reno,Daniel Marcus Acting Associate, Laurie Robinson, General Noël Brennan, General Jeremy Travis	Department of Justice Response Center	1st	2000

Course Outcomes (OCs)

Upon completing this course, the student will be able to:

OC 1: handle the crime scenes with standard operating procedures
OC 2: implement the skills use to investigate different types of crime scenes such as CCTV and other digital evidence.
OC 3: apply the skills for data recovery at the crime scene
OC 4: apply skills used for data acquisition using forensic tools

Course Code: 514[Mandatory] **Total Credits:** 02 (60 Lecture Hrs) **University assessment:** 25 marks	**Course Name:** Cyber Security Technology and Regulations Practical **Total Marks:** 50 marks **College/Department assessment:** 25 marks

Course Objectives (COs):

To enable the students to:

CO 1: Learn hacking skills and practice the professional ethics
CO 2: Provide the knowledge of tools and techniques used by hackers and information security professionals alike to break into an organization.

CO 3: Learn to secure the system and protect from the cyber attacks
CO 4: Perform the network analysis using the forensic analysis tool

MODULE I:	**(2 CREDITS)**
Unit 1: a) Ethical hacking process, Hackers behaviour & mindset, Maintaining Anonymity, Hacking Methodology, Information Gathering, Active and Passive Sniffing, Physical security vulnerabilities and countermeasures. Internal and External testing. Preparation of Ethical Hacking and Penetration Test Reports and Documents. b) Social Engineering attacks and countermeasures. Password attacks, Privilege Escalation and Executing Applications, Network Infrastructure Vulnerabilities, IP spoofing, DNS spoofing, Wireless Hacking: Wireless footprint, Wireless scanning and enumeration, Gaining access (hacking 802.11), WEP, WPA, WPA2. c) DoS attacks. Web server and application vulnerabilities, SQL injection attacks, Vulnerability Analysis and Reverse Engineering, Buffer overflow attacks. Client-side browser exploits, Exploiting Windows Access Control Model for Local Elevation Privilege. Exploiting vulnerabilities in Mobile Application	15 Hrs
Unit 2: a) Malware Forensics Using TSK for Network and Host Discoveries, Using Microsoft Offline API to Registry Discoveries , Identifying Packers using PEiD, Registry Forensics with Reg Ripper Plu-gins:, Bypassing Poison Ivy's Locked Files, Bypassing Conficker's File System ACL Restrictions, Detecting Rogue PKI Certificates. b) Memory Forensics and Volatility Memory Dumping with MoonSols Windows Memory Toolkit, Accessing VM Memory Files Overview of Volatility, Investigating Processes in Memory Dumps, Code Injection and Extraction, Detecting and Capturing Suspicious Loaded DLLs, Finding Artifacts in Process Memory, Identifying Injected Code, Using WHOIS to Research Domains, DNS Hostname Resolution, Querying, Passive DNS, Checking DNS Records, Reverse IP Search New Course Form, Creating Static Maps, Creating Interactive Maps. Case study of Finding Artifacts in Process Memory, Identifying Injected Code with Malfind and YARA c) Introduction to Metreter, Introduction to Armitage, Installing and using Kali Linux Distribution, Introduction to penetration testing tools in Kali Linux. Case Studies of recent vulnerabilities and attacks, parrot.	15 Hrs

Books and References:

Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Ethical Hacking and Penetration Testing Guide	Baloch, R	CRC Press	1st	2015
2	Computer Forensics: Investigating Network Intrusions and Cybercrime,	E.C Council	Cengage Learning	2nd	2010
3	The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory	Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters	Wiley	1st	2014
4	A Electronic Discovery and Digital Evidence in a Nut Shell	Daniel J Capra,Shira A scheindlin	The Sedona Conerence-Academic Press.	1st	2009
5	Anti-Hacker Tool Kit	Mike Shema	Mike Shema	1st	2007

Course Outcomes (OCs)

Upon completing this course, the student will be able to:

OC 1: Understand how our defense measure works and then to scan their networks & attack their own
OC 2: To identify the different threats posed by hackers and other malicious attackers and how to protect our network & devices from those attacks.

OC 3: Analyze the attacks and counterfeit them
OC 4: Apply the forensic tools required for ethical hacking

Course Code: 515[Mandatory] **Total Credits:** 02 (30 Lecture Hrs) **University assessment:** 25 marks	**Course Name**: IT Act 2000, IT Act Amendments and IPR in Cyberspace **Total Marks:** 50 marks **College/Department assessment:** 25marks

Course Objectives (COs):
To enable the students to:

1. Understand the ethics and laws by which cyberspace is governed in our country and worldwide
2. Understand the Cr.PC and Indian Evidence Law
3. Disseminate knowledge on patents, patent regime in India and abroad and registration aspects
4. Create awareness about current trends in IPR and Govt. steps in fostering IPR

MODULE I:	**(2 CREDITS)**
Unit 1: a) Cyber Space- Fundamental definitions -Interface of Technology and Law – Jurisprudence and-Jurisdiction in Cyber Space - Indian Context of Jurisdiction - Enforcement agencies – Need for IT act - UNCITRAL – E-Commerce basics, Information Technology Act, 2000 - Aims and Objects — Overview of the Act – Jurisdiction, New types of cyber crimes. Introduction to Indian Evidence Act, introduction to IT rules 2021 **b)** Electronic Governance – Legal Recognition of Electronic Records and Electronic Evidence -Digital/ electronic/ e-sign (Aadhaar) Signature - Securing Electronic records and secure digital signatures - Duties of Subscribers - Role of Certifying Authorities - Regulators (SEBI/RBI/AMPHI/IRDA) regulations for cyber space, Internet Service Providers and their Liability– Powers of Police under the Act – Impact of the Act on other Laws .	30 Hrs
Unit 2: a) Cr.P.C and Indian Evidence Law - Cyber crimes under the Information Technology Act,2000 - Cyber crimes under International Law - Hacking Child Pornography, Cyber Stalking, Denial of service Attack, Virus Dissemination, Software Piracy, Internet Relay Chat (IRC) Crime, Credit Card Fraud, Net Extortion, Phishing etc - Cyber TerrorismViolation of Privacy on Internet - Data Protection and Privacy – Indian Court cases. Importance of Section 65 B-certificate under Indian Evidence Act (IEA) b) Intellectual Property Rights – Copyrights- Software – Copyrights vs Patents debate - Authorship and Assignment Issues - Copyright in Internet - Multimedia and Copyright issues - Plagiarism- Software Piracy - Trademarks - Trademarks in Internet – Copyright and Trademark cases, Domain names -registration - Domain Name Disputes-Cyber Squatting-IPR cases, WIPO arbitration **c)** Patents - Understanding Patents - IP Types - European Position on Computer related Patents, Legal position on Computer related Patents - Indian Position on Patents – Case Law.	30 Hrs

Books and References:

Sr. No.	Title	Author/s	Publisher	Edition	Year
1.	Cyber Law and Cyber Crime	Adv.(Dr) Prashant Mali	SnowWhite / Cyber Infomedia	2nd	2020
2.	Cyber Laws	Justice Yatindra Singh	Universal Law Publishing Co	1st	2005
3.	Information Technology Law(Cyber Laws)	S.R.Myneni	Asia Law House	1st	2006
4.	Internet Law-Text and Material	Chris Reed	Cambridge University Pres	1st	2004
5.	Cyber Law- the Indian perspective U	Pawan Duggal	Universal Law Publishing Co	1st	2002

6	Intellectual Property Rights. India	Neeraj, P., & Khusdeep, D.	PHI learning Private Limited.	2nd	2014
7	WIPO Intellectual property Handbook	Handbook	World Intellectual Property Organisation		2004

Course Outcomes (OCs)

Upon completing this course, the student will be able to:

OC 1: Learn the general principles in legal research and types of research
OC 2: Learn various legal research methods
OC 3: Understand the legal research processes and legal source
OC 4: Learn writing legal reports
OC 5: get an adequate knowledge on patent and copyright
OC 6: Understand the Patent and policies

Course Code: 516a [Elective]	**Course Name:** Fuzzy Systems and Genetic Algorithms
Total Credits: 04 (60 Lecture Hrs)	**Total Marks:** 100 marks
University assessment: 50 marks	**College/Department assessment**: 50 marks

Pre-requisite:

a. Basic knowledge of Artificial Intelligence
b. Understanding of Artificial Intelligence algorithms
c. Basic concepts of set theory, relations

Course Objectives (COs):

To enable the students to:

CO1: Understand the concepts of fuzzy systems
CO2: Acquire knowledge about rule based and decision making with fuzzy systems
CO3: Understand the concepts of genetic algorithms
CO4: Acquire knowledge of various types of genetic algorithm
CO5: Acquire knowledge on genetic programming

MODULE I: Fuzzy Systems	**(2 CREDITS)**
Unit 1: a) **Introduction to fuzzy system, Classical sets and fuzzy Sets, Classical Relations and fuzzy relations**: Introduction to fuzzy systems, operations on classical sets and fuzzy sets, properties of classical sets and fuzzy sets, crisp relations, fuzzy relations, tolerance & equivalence, value assignment, Demonstrating and implementing membership and identity operator **b) Properties of Membership Functions, Fuzzification, Defuzzification, Logic & Fuzzy Systems**: Features of the membership function, fuzzification, defuzzification, α-cut for fuzzy relation, classical logic, fuzzy logic, natural language, linguistic hedges, fuzzy (rule-based) systems, graphical techniques of inference, Demonstrating and implementing fuzzy logic and tipping problem **c) Development of Membership function, Automated Methods for Fuzzy systems**: Membership value assignments, Batch squares algorithm, recursive least square algorithm, gradient method, clustering method	15 Hrs
Unit 2: **a) Fuzzy System Simulation, Rule base Reduction system & Decision Making with fuzzy Information**: fuzzy relational equations, nonlinear simulation using fuzzy systems, fuzzy associative memory, fuzzy system theory and rule reduction, singular value decomposition, combs method, Fuzzy synthetic evaluation, fuzzy ordering, preference and consensus, multi-objective decision making, fuzzy Bayesian decision method **b) Fuzzy Classification & Pattern Recognition Fuzzy Arithmetic and the extension principle, Fuzzy Control system**:, classification by equivalence relation, clustering analysis and validity, fuzzy c-means, classification metrics, feature analysis, multi	15 Hrs

feature pattern recognition, image processing, syntactic recognition, extension principle, fuzzy arithmetic, approximate methods of extension -vertex method, DSW algorithm, control design problems, fuzzy engineering process control, fuzzy statistical process control c) **Miscellaneous Topics, Monotone measures, Demonstration and implementation of examples**: Fuzzy optimization, fuzzy cognitive mapping, system identification, fuzzy linear regression, monotone measures, belief and plausibility, evidence theory, probability measures, possibility and necessity measures, possibility distribution as fuzzy sets, possibility distributions derived from empirical intervals, introduction to Fuzzy Logic Toolbox & Simulink in MATLAB, Demonstration and implementation of Water level control in tank, Temperature control in shower, Fuzzy PID Control with Type-2 FIS using MATLAB	
MODULE II: Genetic Algorithms	**(2 CREDITS)**
Unit 3: **a) Evolutionary computation, Genetic algorithms**: Historical development of Evolutionary Computation (EC), features of EC, advantages of EC, Applications of EC, Biological background, Genetic algorithm, conventional optimization and search techniques, a simple genetic algorithm, comparison of genetic algorithm with other optimization techniques, advantages and limitations of genetic algorithm, applications **b) Terminologies and Operators of GA**: Basic terminologies of genetic algorithm, data structure, search strategies, encoding, breeding, search termination, why do genetic algorithms work, solution evaluation, search refinement, constraints, fitness scaling c) **Advanced Operators & Techniques in GA**: Diploidy, Dominance and Abeyance, Multiploid, Inversion and Reordering, Niche and Speciation, Few Micro-operators, Non-binary Representation, Multi-Objective Optimization, Combinatorial Optimizations, Knowledge Based Techniques, Demonstration and Implementation in python: Simple Genetic algorithm, Travelling Salesman Problem, Function optimization	15 Hrs
Unit 4: **a) Classification of GA, Genetic Programming**: Simple Genetic Algorithm (SGA), Parallel and Distributed Genetic Algorithm (PGA and DGA), Hybrid Genetic Algorithm (HGA), Adaptive Genetic Algorithm (AGA), Fast Messy Genetic Algorithm (FmGA), Independent Sampling Genetic Algorithm (ISGA), Comparison of GP with Other Approaches, Primitives of Genetic Programming, Attributes in Genetic Programming, Steps of Genetic Programming, Characteristics of Genetic Programming, Applications of Genetic Programming, Haploid Genetic Programming with Dominance **b) Genetic Algorithm Optimization Problems, Applications of Genetic Algorithms**: Fuzzy Optimization Problems, Multi objective Reliability Design Problem, Combinatorial Optimization Problem, Scheduling Problems, Transportation Problems, Network Design and Routing Problems, Mechanical Sector, Electrical Engineering, Machine Learning, Civil Engineering, Image Processing, Data Mining, Wireless Networks, Very Large Scale Integration (VLSI) **c) Introduction to Particle swarm Optimization and Ant colony optimization, Demonstration and Implementation of examples**: Particle Swarm Optimization (PSO) – background, operation, basic flow, comparison between PSO & GA, application of PSO, Ant Colony Optimization (ACO) – biological, similarities between real ants and artificial ants, characteristics of ant colony optimization, ant colony optimization algorithms, applications of ACO, Demonstration and Implementation in MATLAB**:** Introduction to Global Optimization Toolbox, Direct Search, Particle Swarm, Simulated Annealing	15 Hrs

References:

1. Fuzzy Logic with Engineering Applications, Timothy J.Ross, McGraw-Hill
2. Introduction to Genetic algorithm, S.N.Sivanandam, S.N.Deepa, Springer
3. Fuzzy Sets and Fuzzy Logic - Theory Applications, George J Klir/ Bo Yuan, Prentice Hall
4. A course in Fuzzy Systems & Control, Li-Xin Wang, Prentice Hall

5. Fuzzy Set Theory-and Its Applications, Fourth Edition, H.-J. Zimmermann, 4th, Springer Science Business Media
6. Introduction to Fuzzy Sets, Fuzzy Logic, and Fuzzy Control Systems, Guanrong Chen, Trung Tat Pham, CRC Press
7. An Introduction to Genetic Algorithms for Scientists and Engineers, David A Coley , World scientific
8. An Introduction to Genetic Algorithms, Mitchell Melanie, MIT Press
9. https://in.mathworks.com/help/fuzzy/fuzzylogiccontroller.html
10. https://in.mathworks.com/help/gads/index.html?s_tid=CRUX_topnav

Course Outcomes (OCs)

Upon completing this course, the student will be able to:

OC1: Understands the basics terminologies, operators and concepts of fuzzy systems
OC2: Understands the difference between classical and fuzzy systems
OC3: Apply the knowledge how to perform fuzzification & defuzzification
OC4: Understands the monotone measures of fuzzy system
OC5: Identify the areas where fuzzy systems can be applied
OC6: Understands the basic terminologies, operators and concepts of genetic algorithms
OC7: Understands difference between genetic programming and traditional programming
OC8: Identify the areas where genetic algorithms can be applied
OC9: Understand the basic of Particle Swarm Optimization and Ant Colony Optimization.

Course Code: 516b [Elective] **Total Credits:** 04 (60 Lecture Hrs) **University assessment:** 50 marks	**Course Name:** Virtualization **Total Marks:** 100 **College/Department assessment:** 50 marks

Pre-requisite:

- Knowledge of operating systems and hardware, different types of Operating systems
- Knowledge of the networking concepts and storage devices
- Knowledge of cloud computing

Course Objectives (COs):

To enable the students to:

CO1: Understand the fundamentals of cloud computing and virtualization technologies.
CO2: Configure & implement virtual machines, hypervisors, virtual networks, and virtual storage interact with each other.
CO3: Implement and create cloud infrastructure
CO4: Acquire in-depth knowledge of virtualization and cloud computing technologies.
CO5: Manage virtual machines, virtual storage, virtual networking, and troubleshooting.

MODULE I:	**(2 CREDITS)**
Unit 1: a) **Understanding Virtualization:** Describing Virtualization, Microsoft Windows Drives Server Growth, Explaining Moore's Law, Understanding the Importance of Virtualization, Examining Today's Trends, Virtualization and Cloud Computing, Hyperconverged Infrastructure, Understanding Virtualization Software Operation, Virtualizing Servers, Virtualizing Desktops, Virtualizing Applications. Understanding Hypervisors: Describing a Hypervisor, Exploring the History of Hypervisors, Understanding Type 1 Hypervisors, Understanding Type 2 Hypervisors, Understanding the Role of a Hypervisor, Holodecks and Traffic Cops, Resource Allocation, Comparing Today's Hypervisors, VMware ESX, Citrix Hypervisor (Xen), Microsoft Hyper-V, Other Solutions. b) **Understanding Virtual Machines**: Describing a Virtual Machine, Examining CPUs in a Virtual Machine, Examining Memory in a Virtual Machine, Examining Network Resources in a Virtual Machine, Examining Storage in a Virtual Machine, Understanding How a Virtual Machine Works, Working with Virtual Machines, Understanding Virtual Machine Clones, Understanding Templates, Understanding Snapshots, Understanding	15 Hrs OC1

OVF, Understanding Containers. c) **Creating a Virtual Machine:** Performing P2V Conversions, Investigating the Physical-to-Virtual Process, Hot and Cold Cloning, Loading Your Environment, Loading VMware Workstation Player, Exploring VMware Workstation Player, Loading VirtualBox, building a New Virtual Machine, Thinking About VM Configuration, Creating a First VM.	
Unit 2: a) **Installing Windows on a Virtual Machine:** Loading Windows into a Virtual Machine, Installing Windows 11, Installing VMware Tools, Understanding Configuration Options, Optimizing a New Virtual Machine b) **Installing Linux on a Virtual Machine:** Loading Linux into a Virtual Machine, Exploring Oracle VM VirtualBox, Installing Linux into a Virtual Machine, Installing VirtualBox Guest Additions, Understanding Configuration Options, Optimizing a New Linux Virtual Machine. c) **Managing CPUs for a Virtual Machine:** Understanding CPU Virtualization, Configuring VM CPU Options, Tuning Practices for VM CPUs, Choosing Multiple vCPUs vs a Single vCPU, Hyperthreading, Working with Intel and AMD Servers.	15 Hrs OC2
MODULE II :	**(2 CREDITS)**
Unit 3: a) **Managing Memory for a Virtual Machine:** Understanding Memory Virtualization, Configuring VM Memory Options, Tuning Practices for VM Memory, Calculating Memory Overhead, Memory Optimizations b) **Managing Storage for a Virtual Machine:** Understanding Storage Virtualization, Configuring VM Storage Options, Tuning VM Storage. c) **Managing Networking for a Virtual Machine:** Understanding Network Virtualization, Configuring VM Network Options, Tuning Practices for Virtual Networks.	15 Hrs OC3
Unit 4: a) **Copying a Virtual Machine:** Cloning a Virtual Machine, Working with Templates, saving a Virtual Machine State, creating a Snapshot, Merging Snapshots. b) **Managing Additional Devices in Virtual Machines:** Using Virtual Machine Tools, Understanding Virtual Devices, configuring a CD/DVD Drive, Configuring a Floppy Disk Drive, Configuring a Sound Card, Configuring USB Devices, Configuring Graphic Displays, Configuring Other Devices. c) **Understanding Availability:** Increasing Availability, Protecting a Virtual Machine, Protecting Multiple Virtual Machines, Protecting Data Centers. Understanding Applications in a Virtual Machine: Examining Virtual Infrastructure Performance Capabilities, Deploying Applications in a Virtual Environment, Understanding Virtual Appliances and vApps, Open Stack and Containers, Cloud and the Future of Virtualization	15 Hrs OC4

References:

a. Virtualization Essentials by Matthew Portnoy, 3rd ed, John Wiley & Sons, Inc.
b. Virtualization for DUMMIES by Bernard Golden, 3rd ed, HP special edition
c. Virtualization A Manager's Guide by Dan Kusnetzky O'Reilly Media, Inc.

Course Outcomes (OC's)

Upon completing this course, the student will be able to:

OC 1. Understand the concept of Virtualization, Types of Virtualizations, different types of Virtual machine manager, creation of virtual machine of different types of operating systems using different types of Hypervisors

OC 2. Install Windows and Linux operating systems on virtual computers using VMWare Workstation, Workstation Player, Microsoft Hypervisor and Oracle VirtualBox, Types of Physical CPU Architectures, Calculating and Configuring VM CPU.

OC 3. Examine of Memory in a Virtual Machine, Creation of Virtual Storage Environments, Calculating and Configuring Memory Settings, Creation and Management of Virtual Network.

OC 4. Create a clone of VM, Understand the different types of data storage technologies and media, Utilization of Peripheral Devices in VM Environments, Configuration of USB and Other Devices to Work with VMs, employ standard procedures to demonstrate how to deploy applications in a virtual environment, Understand the important of "availability" in the context of virtual machines

Course Code: 516c [Elective] **Total Credits:** 04 (60 Lecture Hrs) **University assessment:** 50 marks	Course Name: Security Fundamentals for Cloud Total Marks: 100 marks College/Department assessment: 50 marks

Pre-requisite:

a. Knowledge of the fundamental concepts of security, types of cloud services models and deployment models.
b. Basic knowledge of Software Development Lifecycle (SDLC).

Course Objectives (COs):

To enable the students to:

CO1: Understand the physical and virtual elements of cloud-based systems.
CO2: Understand the issues while designing the cloud data security policy.
CO3: Learn about the components required to design the data center and importance of business continuity and disaster recovery plans for the data center.
CO4: Aware of the concerns, threats of cloud application security.
CO5: Learn about the different operations performed in a cloud environment.
CO6: Understand the legal & audit process in cloud environment

MODULE I:	**(2 CREDITS)**
Unit I **a) Identifying Information Security Fundamentals**: Exploring the Pillars of Information Security, Threats, Vulnerabilities, and Risks, Deciphering Cryptography, Grasping Physical Security, Realizing the Importance of Business Continuity and Disaster Recovery, Implementing Incident Handling **b) Cloud Concepts, Architecture and Design**: Cloud Computing Concepts, Cloud Reference Architecture, Identifying Security Concepts Relevant to Cloud Computing, Comprehending Design Principles of Secure Cloud Computing, Evaluating Cloud Service Providers	15 Hrs OC1
Unit II **a) Cloud Data Security**: Describing Cloud Data Concepts, Designing and Implementing Cloud Data Storage Architectures, Designing and Implementing Data Security Technologies and Strategies, Implementing Data Discovery, Implementing Data Classification, Designing and Implementing Information Rights Management (IRM), Planning and Implementing Data Retention, Deletion, and Archiving Policies, Designing and Implementing Auditability, Traceability and Accountability of Data Events, Case studies on Cloud Data Storage, Auditability, Traceability.	15 Hrs OC2
MODULE II:	**(2 CREDITS)**
Unit III **a) Cloud Platform and Infrastructure Security**: Comprehending Cloud Infrastructure Components, Designing a Secure Data Center, Analyzing Risks Associated with Cloud Infrastructure, Designing and Planning Security Controls, Planning Business Continuity (BC) and Disaster Recovery (DR). Case studies on Business Continuity Plan and Disaster Recovery in cloud. **b) Cloud Application Security:** Advocating Training and Awareness for Application Security, Describing the Secure Software Development Lifecycle (SDLC) Process, Applying the SDLC Process, Applying Cloud Software Assurance and Validation,	15 Hrs OC3, OC4

Using Verified Secure Software, Comprehending the Specifics of Cloud Application Architecture, Designing Appropriate Identity and Access Management (IAM) Solutions. Case studies on Security Issues on Software-as-a-Service	
Unit IV **a) Cloud Security Operations**: Implementing and Building a Physical and Logical Infrastructure for Cloud Environment, Operating Physical and Logical Infrastructure for a Cloud Environment, Managing Physical and Logical Infrastructure for a Cloud Environment, Implementing Operational Controls and Standards, Supporting Digital Forensics, Managing Communication with Relevant Parties, Case Studies on Digital Forensics in cloud. **b) Legal, Risk and Compliance:** Articulating Legal Requirements and Unique Risks within the Cloud Environment, Understanding Privacy Issues, Understanding Audit Process, Methodologies, and Required Adaptations for a Cloud Environment, Understanding the Implications of Cloud to Enterprise Risk Management, Understanding Outsourcing and Cloud Contract Design	15 Hrs OC4, OC5

References:

a. CCSP® For Dummies® with Online Practice by Arthur J. Deane, John Wiley & Sons, Inc.

b. (ISC)2® CCSP® Certified Cloud Security Professional Official Study Guide by Mike Chapple, David Seidl, 3rd edition, John Wiley & Sons, Inc.

c. ALL IN ONE CCSP® Certified Cloud Security Professional EXAM GUIDE by Daniel Carter 3rd edition McGraw Hill

d. Certified Cloud Security Professional (CCSP) Technology Workbook by Nouman Ahmed Khan, Abubakar Saeed, Muhammad Yousuf, Farah Qadir and Farah Qadir, Version 1. IPSpecialist LTD.

Course Outcomes (OCs):

Upon completing this course, the student will be able to:

OC1: Understand the cloud environment's risks, vulnerabilities, threats, and attacks.

OC2: Learn the concept and strategy for the security measures in the cloud infrastructure.

OC3: Gain knowledge of data storage in different platforms, data security techniques and designing of Information Rights Management.

OC4: Gain knowledge of designing and planning of security controls in cloud infrastructure.

OC5: Learn about risk, threats of applying the SLDC process in the cloud and countermeasures for the same.

OC6: Understand the importance of risk assessment, the principles of data privacy & the standards and operational controls to be implemented in a cloud environment.

Evaluation Scheme

Theory courses of 4 credits: Total marks 100. Out of the total, 50 % each for internal and external evaluation.

A. Internal Evaluation (30m + 10m + 10m = 50 Marks)

The internal assessment marks shall be awarded as follows:

1. **30 marks (Any one of the following):**
   a. Written Test of 30 Marks
   b. SWAYAM (Advanced Course) of minimum 20 hours and certification exam completed or
   c. NPTEL (Advanced Course) of minimum 20 hours and certification exam completed or
   d. Valid International Certifications (Prometric, Pearson, Certiport, Coursera, Udemy and the like)
   e. Certification marks of one completed exam shall be awarded to one course only. For four courses, the students will have to complete four certifications.
   (Note: Only those certification/courses suggested by the department shall be deemed valid, Student cannot do any certification on their own)
2. **10 marks**
   10 marks from every course (Two 4 credits mandatory courses, one 2 credits mandatory course, one 4 credits elective course) coming to a total of 40 marks, shall be awarded on publishing of research paper in UGC approved / Other Journal with plagiarism less than 15%. The marks can be awarded as per the impact factor of the journal, quality of the paper, importance of the contents published, social value.
3. **10 marks**
   Open Book examination based on problem solving related to the respective subject.

i. Suggested format of Question paper of 30 marks for the written test.

Q1.	Attempt *any two* of the following:	16 marks
a.		
b.		
c.		
d.		
Q2.	Attempt *any two* of the following:	14 marks
a.		
b.		
c.		
d.		

B. External Examination: (50 marks) Duration : 2 hrs

	All questions are compulsory	
Q1	(Based on all units) Attempt *any two* of the following:	10 marks
a.	Unit 1	
b.	Unit 2	
c.	Unit 3	
d.	Unit 4	
Q2	(Based on Unit 1) Attempt *any two* of the following:	10 marks
Q3	(Based on Unit 2) Attempt *any two* of the following:	10 marks
Q4	(Based on Unit 3) Attempt *any two* of the following:	10 marks
Q5	(Based on Unit 4) Attempt *any two* of the following:	10 marks

Theory courses of 2 credits: Total marks 50. Out of the total, 50 % each for internal and external evaluation.

A. Internal Evaluation (25 Marks)

The internal assessment marks shall be awarded as follows:

1. 10 marks from every course (Two 4 credits mandatory courses, One 2 credits mandatory course, One 4 credits elective course) coming to a total of 40 marks, shall be awarded on publishing of research paper in UGC approved / Other Journal with plagiarism less than 15%. The marks can be awarded as per the impact factor of the journal, quality of the paper, importance of the contents published, social value.
2. 10 marks - Open Book examination based on problem solving related to the respective subject.
3. 5 marks - Assignment/Group discussion.

B. External Examination: (25 marks) Duration : 1 hr

	All questions are compulsory	
Q1	(Based on Unit 1) Attempt *any two* of the following:	13 marks
Q2	(Based on Unit 2) Attempt *any two* of the following:	12 marks

Practical courses of 2 credits: Total marks 50. Out of the total, 50 % each for internal and external evaluation.

A. Practical Evaluation Internal (25 marks)

1.	Performance during all practical sessions	10
2.	Problem solving with the acquired programming skills	10
3.	Viva Voce	5

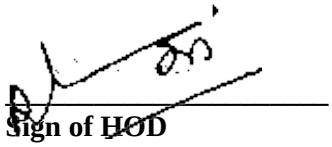
B. Practical Evaluation External (25 marks)

A Certified copy of hard-bound journal is essential to appear for the practical examination.

1.	Practical Question	15
2.	Journal	5
3.	Viva Voce	5

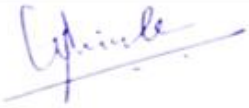
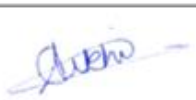
Letter Grades and Grade Points

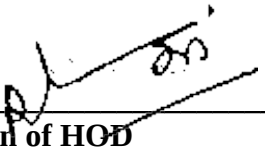
Semester GPA/Program CGPA Semester/Program	Percentage of Marks	Alpha-Sign/Letter Grade Result
9.00 – 10.00	90.00-100.00	O (Outstanding)
8.00 -<9.00	80.00-<90.00	A+ (Excellent)
7.00-<8.00	70.00-<80.00	A (Very Good)
6.00-<7.00	60.00-<70.00	B+ (Good)
5.50-<6.00	55.00-<60.00	B (Above Average)
5.00-<5.50	50.00-<55.00	C (Average)
4.00-<5.00	40.00-<50.00	P (Pass)
Below 4.00	Below 40.00	F (Fail)
Ab(Absent)	-	Absent



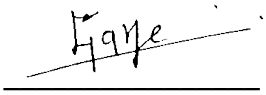
Sign of HOD
Dr. Mrs. R. Srivaramangai
Dept of Information Technology

Team for Creation of Syllabus

Name	Organization	Sign
Dr. Mrs. R. Srivaramangai	Dept of Information Technology	
Mrs. Shraddha Kadam Shah	Dept of Information Technology (Special Invitee)	
Mr. Jayesh Shinde	Dept of Information Technology (Special Invitee)	
Mr. Nikhil K Pawanikar	Dept of Information Technology (Special Invitee)	



Sign of HOD
Dr. Mrs. R. Srivaramangai
Dept of Information Technology



Sign of Dean
Prof. Shivram Garje
Science & Technology

Appendix B

Justification for (PG Diploma in Cyber Security Law and Forensics)

1.	Necessity for starting the course:	There is an increasing importance of cybersecurity and digital forensics in today's interconnected world. As technology continues to advance, so do cyber threats, making it essential to have skilled professionals who can address the complex challenges posed by cybercrime, data breaches, and legal aspects related to digital activities.
2.	Whether the UGC has recommended the course:	Yes
3.	Whether all the courses have commenced from the academic year 2023-24	The program has commenced from 2022-2023 academic year onwards
4.	The courses started by the University are self-financed, whether adequate number of eligible permanent faculties are available?:	Yes. Some experts are called as visiting faculties
5.	To give details regarding the duration of the Course and is it possible to compress the course?:	1 year. Not possible to compress the program
6.	The intake capacity of each course and no. of admissions given in the current academic year:	30 seats. 2023-2024 admission is yet to start
7.	Opportunities of Employability / Employment available after undertaking these courses:	The employability prospects for individuals with a PG Diploma in Cybersecurity Law and Forensics are highly promising due to the increasing demand for cybersecurity professionals with a strong understanding of legal aspects and digital forensics. Graduates of this program can explore various career paths in both the public and private sectors, as well as opportunities for entrepreneurship.

Sign of HOD
Dr. Mrs. R. Srivaramangai
Dept of Information Technology

Sign of Dean
Prof. Shivram Garje
Science & Technology