Dr.M.G.R.
Educational and Research Institute
(DEEMED TO BE UNIVERSITY)
(An ISO Certified Institution)
University with Graded Autonomy Status
Maduravoyal , Chennai - 600 095

In Collaboration With

Centre of Education in Digital Forensics, Chennai

CURRICULUM & SYLLABUS (2020-REGULATION)

MASTER OF SCIENCE
CYBER FORENSICS AND INFORMATION SECURITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

DECLARATION

I, **Dr. S. GEETHA**, Head of Computer Science and Engineering Department, hereby declare that this copy of the syllabus (M.Sc. – **CYBER FORENSICS AND INFORMATION SECURITY-** 2020 Regulation) is the final version which is being taught in the class and uploaded in our University website. I assure that the Syllabi available in our University website is verified and found correct. The Curriculum and Syllabi have been ratified by our Academic Council / Vice Chancellor.

Date: **Signature**

I SEMESTER							
S.NO.	**SUBJECT CODE**	**SUBJECT NAME**	**Ty/ Lb/ ETL**	**L**	**T/ SLr**	**P/R**	**C**
1	HMMA20003	Mathematics For Information Security	Ty	3	1	0	4
2	HMCS20G01	Cyber Criminology and Criminal Justice Administration	Ty	3	0	0	3
3	HMCS20G02	Information Security Risk Management	Ty	3	0	0	3
4	HMCS20G03	Network Security	Ty	3	0	0	3
5	HMCS20G04	E-Mail Security And Forensics	Ty	3	0	0	3
PRACTICALS*							
1	HMCS20GL1	Network Security Lab	Lb	0	0	3	1
2	HMCS20GL2	Information Security Risk Management Lab	Lb	0	0	3	1
Credits Sub Total							**18**

II SEMESTER							
S.NO.	**SUBJECT CODE**	**SUBJECT NAME**	**Ty/ Lb/ ETL**	**L**	**T/ SLr**	**P/R**	**C**
1	HMCS20G05	Cyber Forensics Fundamentals	Ty	3	0	0	3
2	HMCS20G06	Business Continuity Planning and Disaster Recovery Management	Ty	3	0	0	3
3	HMCS20G07	Vulnerability Assessment and Penetration Testing ~~(VA/PT)~~	Ty	3	0	0	3
4	HMCS20G08	Malware Analysis and Security	Ty	3	1	0	4
5	HMCS20G09	Cyber Law	Ty	3	0	0	3
PRACTICALS*							
1	HMCS20GL3	Cyber Forensics Fundamentals Lab	Lb	0	0	3	1
2	HMCS20GL4	Vulnerability Assessment and Penetration Testing Lab ~~VA/PT Lab~~	Lb	0	0	3	1
Credits Sub Total							**18**

III SEMESTER							
S.NO.	**SUBJECT CODE**	**SUBJECT NAME**	**Ty/ Lb/ ETL**	**L**	**T/ SLr**	**P/R**	**C**
1	HMCS20G10	Advanced Information Security	Ty	3	1	0	4
2	HMCS20G11	Advanced Digital Forensics	Ty	3	0	0	3
3	HMCS20G12	Cloud Security	Ty	3	0	0	3
4	HMSCS20GEX	Elective – I	Ty	3	0	0	3
PRACTICALS*							
1	HMCS20GL5	Advanced Information Security Lab	Lb	0	0	3	1
2	HMCS20GL6	Advanced Digital Forensics Lab	Lb	0	0	3	1
3	HMCS20P01	Project Phase -I	Lb	0	0	12	5

	Credits Sub Total	**20**

IV SEMESTER							
S.NO.	**SUBJECT CODE**	**SUBJECT NAME**	**Ty/ Lb/ ETL**	**L**	**T/ SLr**	**P/R**	**C**
1	HMCS20G13	Social Media Crimes and Security	Ty	3	0	0	3
2	HMCS20GEX	Elective-II	Ty	3	0	0	3
3	HMCS20GEX	Elective – III	Ty	3	0	0	3
PRACTICALS*							
1	HMCS20P02	Project Phase -II	Lb	0	0	20	10
			Credits Sub Total				**19**

ELECTIVE-I							
S.NO.	**SUBJECT CODE**	**SUBJECT NAME**	**Ty/ Lb/ ETL**	**L**	**T/ SLr**	**P/R**	**C**
1	HMCS20GE1	Forensic Science and Crime Investigation	Ty	3	0	0	3
2	HMCS20GE2	Frauds in BFSI , Telecom Sectors and Security	Ty	3	0	0	3
3	HMCS20GE3	Web Application Security	Ty	3	0	0	3

ELECTIVE-II							
S.NO.	**SUBJECT CODE**	**SUBJECT NAME**	**Ty/ Lb/ ETL**	**L**	**T/ SLr**	**P/R**	**C**
1	HMCS20GE4	Vigilance and Security Management	Ty	3	0	0	3
2	HMCS20GE5	Digital Frauds	Ty	3	0	0	3
3	HMCS20GE6	Mobile Security and Forensics	Ty	3	0	0	3

ELECTIVE-III							
S.NO.	**SUBJECT CODE**	**SUBJECT NAME**	**Ty/ Lb/ ETL**	**L**	**T/ SLr**	**P/R**	**C**
1	HMCS20GE7	IOT Security	Ty	3	0	0	3
2	HMCS20GE8	Intellectual Property Rights	Ty	3	0	0	3
3	HMCS20GE9	Data Privacy	Ty	3	0	0	3

C: Credits L: Lecture T: Tutorial S.Lr: Supervised Learning P: Problem / Practical R: Research
Ty/Lb/ETL: Theory /Lab/Embedded Theory and Lab * Internal Evaluation

Credit Summary

1st Semester: 18
2nd Semester: 18
3rd Semester: 20
4th Semester: 19

Total Credits: 75

SEMESTER – I

Subject Code: HMMA20003	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Mathematics For Information Security	Ty	3	1	0	4

OBJECTIVES:

This paper will help a student to understand:

- The basic mathematic concepts used in information security field.
- The different cryptographic algorithm and generation of keys
- The working of cryptographic hashing functions and their applications.
- The message authentication codes and its various applications.

UNIT I - INTRODUCTION TO MATHEMATIC CONCEPTS 12Hrs

Number Theory – Divisibility, Factors, Prime numbers – Properties of Divisibility - Representation of Integers in Different Bases –Conversion of Decimal to Binary, Octal and Hexadecimal values - Greatest Common Divisor and Least Common Multiple - The Integers — Primitive Roots and the Discrete Logarithm – Polynomials and Finite Fields – The Ring of Polynomials —Congruence Calculus or Modular Arithmetic – Modular Square Roots.

UNIT II - INTRODUCTION TO CRYPTOGRAPHY 12Hrs

Introduction to Cryptography – The Objectives of Cryptography – Symmetric-Key Encryption – Steam Ciphers – Block Ciphers – DES – AES – Modes of Operation – Public-Key Cryptography – Concepts of Public-Key Cryptography – RSA – Key Generation and Encryption – Digital Signatures – Attacks against RSA –

UNIT III–CRYPTOGRAPHIC HASH FUNCTIONS 12Hrs

Cryptographic Hash Functions – Security requirements for Hash functions – Construction of Hash functions – Data Integrity and Message Authentication – Signatures with Hash functions – Message Digest – MD5 - Secure Hashing Algorithm – SHA1 and SHA2.

UNIT IV–DISCRETEAL GORITHM AND PROTOCOLS 12Hrs

Elgamal's Encryption – ElGamal's Signature Scheme – Digital Signature Algorithm – Rabin's Encryption – Rabin's Signature Scheme – Key Exchange and Entity Authentication – Kerberos – Diffie-Hellman Key Agreement – Key Exchange and Mutual Authentication – Station-to-Station Protocol – Public-Key Management Techniques.

UNIT V–MESSAGE AUTHENTICATION CODES 12Hrs

Secure communication and Message integrity – Encryption vs Message Authentication – Message Authentication Codes – Constructing Secure Message Authentication Codes – CBC-MAC – Collision Resistant Hash Functions – Weaker notions of Security for Hash functions – A Generic "Birthday" Attack – The Merkle -Damgard Transform – Collision-Resistant Hash Functions in Practice.

Total Hrs:60

TEXT BOOKS:

1. Hans Delfs, Helmut Knebl, "*Introduction to Cryptography*" Principles and Applications, 2nd Edition (Information Security and Cryptography), ISBN-13 978-3-540-49243-6, Springer 2007.
2. Jonathan Katz and Yehuda Lindell (2008) *Introduction to Modern Cryptography*, Chapman & Hall/CRC, ISBN-13: 978-1-58488-551-1.

Subject Code: HMCS20G01	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Cyber Criminology and Criminal Justice Administration	Ty	3	0	0	3

Course Objectives:

1. Explain the concept of crimes, various forms of crimes and cyber crimes
2. To state Cyber Crime from Sociological, Psychological and Criminological Perspectives
3. To discuss the Role of Criminal Justice Administration and Cyber Crimes

Course Outcomes:

Students will be able to:

1. Explain the concepts of crime and cyber crimes
2. Outline the principles of crime, cause and extent of cyber crimes
3. Discuss various forms of cyber crimes
4. Debate the cyber frauds happening in the major sectors such as Banking sector, Telecom sector, Health sector, Travel sector
5. Give theoretical perspectives of cyber crimes
6. Describe the Role of Criminal Justice Administration and Cyber Crimes

UNIT I:Basic Concepts of Crime, Law and Criminal Justice: 9Hrs

Crime, Tort, Misdemeanor, Juvenile Delinquency, Status Offences, Conventional Crimes Vs Cyber Crimes, Economic Offences, White Collar Crime, Media and Crime, Terrorism, Cyber Law, Indian Penal Code, Indian Evidence Act, Criminal Procedure Code.

UNIT II: Principles and Concepts of Cyber Criminology: **9Hrs**

Cyber Space, Cyber Crime, Cyber Criminology, Information Security, Penetration Testing, Incident Response, GRC, Significance of Cyber Crime, Causes and Extent of Cyber Crimes, Types of Cyber Criminals – Modus Operandi of Cyber Criminals – Profiling of Cyber Criminals - Tools and Techniques adopted by Cyber Criminals

UNIT III: Forms of Cyber Crimes and theories relating to cyber crimes: 15 **Hrs**

Types of Cyber Crimes – Cyber Crimes Against property, Person, Nation and Organizations – Cyber Theft, Phishing, Denial of Service, Distributed Denial of Service, Malwares, Cyber Bullying, Cyber Stalking, Cyber Pornography, Cyber Espionage, Cyber Defamation, Web Defacement, Hacking, Cracking, Chat Room Crimes, Cyber Terrorism, Cyber Warfare, Data Theft, Data Diddling, Cyber Violence, Cyber Vandalism, Insider Threats, National and International Cyber Crimes, Cyber based Political Crimes, IPR related frauds, social engineering, Criminological Theories and Cyber Crime – Routine Activity Theory, Social Learning Theory, Differential Association Theory, Differential Opportunity Theory.

UNIT IV: Forms of Cyber Frauds: 6 Hrs

Internet Frauds, Cyber Scams, Job Frauds, Electronic Mailing Frauds, Card frauds, charity frauds, online marketing frauds, banking frauds, telecom frauds, frauds in health sector, frauds in travel sectors, E-Commerce and E-Business related frauds.

UNIT V: The Role of Criminal Justice Administration and Cyber Crimes: 6 Hrs

Police: Organizational structure of Police in India – Different wings in the Central ,States and Districts and their functions - Police & Law Enforcement – F.I.R. – cognizable and non-cognizable offences, bailable and non-bailable offences – on line complaints search&, seizure, search of cyber crimes and digital evidence, Online Surveillance –Cyber crime cells – structure & investigation of cyber crime cases –Courts – Cyber Appellate Court / Tribunals / Powers – Proceedings in the court: trial, sentencing. **Total Hrs:45**

TEXT BOOKS:

1. Roger HopkinsBurke, “An Introduction to Criminological Theory”, Routledge; 3rd edition (2009), ISBN-13: 978-1-84392-407
2. Dejey, Murugan, “Cyber Forensics”, Oxford University Press; First edition (1 June 2018), ISBN-13: 978-0199489442

REFERENCE BOOKS:

1. Larry J Siegel, “Criminology: Theories, Patterns and Typologies”, Cengage Learning; 13 edition (January 1, 2017), ISBN-13: 978-1337091848
2. Chuck Easttom, “CCFPSM Certified Cyber Forensics Professional Certification ALL-IN-ONE(Exam Guide)”, McGraw-Hill Education, 2015, ISBN: Book p/n 978-0-07-183611-1
3. Britz, “Computer Forensics and Cyber Crime: An Introduction”, Pearson Education India; 2 edition (2011), ISBN-13: 978-8131764015
4. Katherine S Williams, “Textbook on Criminology“, Oxford University Press; 7 edition (June 18, 2012), ISBN-13: 978-0199592708
5. Thilagaraj, R and Latha, S, “Readings in Criminology”, Gyan Book House, Delhi, (2012), ISBN - 9788121211444
6. Prof. N.V.Paranjape, “Criminology, Penology and Victimology”,Central Law Publications (CLP); 2017 edition (2017), ISBN-13: 978-9384961961

Subject Code: HMCS20G02	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Information Security Risk Management	Ty	3	0	0	3

Course Outcomes:

1. Explain the fundamental concepts of all security perception
2. List the techniques required to implement the various security features
3. Examine the security procedures set to secure a system against failure, theft, invasion and sabotage.
4. State the importance of access controls and the need for an access control
5. Understand risks and threats to information security and the need for good information security practices.
6. Apply the techniques, procedures, methods for combating these threats and attacks

UNIT I Introduction **9Hrs**

Information security - Security methodology - How to build a security program - Strategy and Tactics - Business Processes vs. Technical controls - The CIA triad and other models - defence models - zones of trust – IT Security policy framework - Data classification standards – Security policies, standards, baselines, guidelines

UNIT II Asset Security **9Hrs**

Securing Unstructured Data - structured Vs unstructured data - Approaches to securing unstructured data - newer approaches to securing unstructured data - Information Rights Management: Overview - Evolution from Encryption to IRM - IRM Technology - Storage security - Storage Security Evolution - Modern storage security - Risk Remediation - Database Security - Concepts - Database security layers - Database-level security.

UNIT III Operations Management **9Hrs**

Security Operations Management - Communication and reporting - change management - acceptable use enforcement - administrative security - management practices - accountability controls

UNIT IV Technical (Logical) & Physical Access Controls **9Hrs**

Passwords – Smartcards – Encryption –Steganography - Network Access - System Access - Physical Access Controls - Network Segregation - Perimeter Security - Security Guards - Badge Systems - Biometric Access Controls - Access Control Strategies - Discretionary Access Control (DAC) - Mandatory Access Control (MAC) - Role-Based Access Control (RBAC) - Attribute Based Access Control

UNIT V Risk Management **9Hrs**

Risk Management concepts – Risk Terminology – Identify threats and vulnerabilities – Risk Assessment – Risk Assignment – Countermeasures selection and assessment – Implementation – Types of Control – Monitoring and Measurement – Asset valuation – Continuous Improvement – Risk framework –Enterprise Security Risk assessment- Standards, Limits, Ethical Hacking, Penetration testing - System Availability

Total Hrs:45

TEXT BOOKS

1. David Kim, Michael G. Solomon, "Fundamentals of Information Systems Security", THIRD EDITION, 2018 by Jones & Bartlett Learning, ISBN 9781284116458
2. James M. Stewart, Mike Chapple, Darril Gibson, "(ISC)2 Certified Information Systems Security Professional Official Study Guide) – CISSP", Seventh Edition, 2015, Sybex (2015), ISBN: 978-1-119-04271-6
3. Thomas R. Peltier, "Information Security Fundamentals", Auerbach Publications; 2 edition (29 June 2017), ISBN-13: 978-1138436893

REFERENCE BOOKS:

1. Umesha Nayak, Umesh Rao, "The InfoSec Handbook: An Introduction to Information Security", Apress; 1st ed. edition (10 September 2014), ISBN-13: 978-1430263821
2. Adam Gordon, "Official (ISC)2 Guide to the CISSP CBK ((ISC)", Auerbach Publications; 4 edition (March 11, 2015), ISBN-13: 978-1482262759
3. Jason Andress "The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice", Syngress; 2 edition (14 July 2014), ISBN-13: 978-0128007440
4. Michael E. Whitman, Herbert J. Mattord, "Principles of Information Security", 6th edition, Cengage Learning India Private Limited, 2018, ISBN-13: 978-9387994232
5. John Vacca, "Computer and Information Security", Handbook, 3rd edition, Morgan Kaufman, 2017, ISBN: 9780128038437.
6. Mark Rhodes-Ousley, "Information Security: The Complete Reference", McGraw Hill Education; Second edition (1 May 2013), ISBN-13: 978-1259098345

Subject Code: HMCS20G03	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Network Security	Ty	3	0	0	3

Unit I **9Hrs**

Introduction: Seven layers in action – Network security model classical Encryption techniques (Symmetric cipher model, substitution techniques, transposition Techniques, steganography).– Topology – Cabling - Networking Industry Standards IEEE - Ethernet topology.

Unit II **9Hrs**

TCP/IP Basics & Routing: Introduction to MAC address - Introduction to IP address - Classes of IP address - Need for subnetting - Basics of IPV6 - Static IP addressing, Dynamic IP addressing, Special IP addresses - How routers work - Routing tables - Network Address Translation - Dynamic routing – distance vector, link state – EIGRP – OSPF - Dynamic routing – Working with routers - Connecting to routers, basic router configuration, router problems

Unit III **9Hrs**

Packet Switched Connection: Types of connections – Circuit switched, Packet switched - Why packet switched is preferred - Types of protocols and need for protocols - Packet switched Protocols - TCP/ IP - RSA Algorithm - Knapsack Algorithm - Blowfish Algorithm

Unit IV **9Hrs**

TCP/IP applications: Origins of TCP/ IP and evolution of Internet - IP Layers Vs OSI - IP number concepts - Network address - Classes of Networks-Subnet masking - Static and dynamic IP numbers - UDP - Establishing a TCP session (Three way handshake) - Name to address translation - Domain Name System - Transport layer protocols –TCP, UDP, ICMP, IGMP – the power of port numbers - registered ports, connection status, rules for determining good vs. bad communications – Common TCP/IP applications - the world wide web, Telnet, Email, FTP, Internet applications

Unit V **9Hrs**

Network Naming: Introduction to Domains and Work Groups - Network naming – DNS – how DNS works, DNS servers Troubleshooting DNS – WINS – Configuring WINS clients, Troubleshooting WINS – Diagnosing TCP/IP Networks - Introduction to ADS (Active Directory Service) - File sharing within network - Understanding DHCP - Introduction to Mail Exchange server and ISA server - Network operating system - Client Server applications - Peer to Peer Applications - Measuring performance - Monitoring tools.

Total Hrs:45

TEXT BOOKS:

1. Mike Meyers, "CompTIA Network+ Certification All-in-One Exam Guide", McGraw Hill Education; 5th edition, ISBN-10: 125902553, 2017
2. Dr. William Stallings, "Cryptography and Network Security", 7th Edition, Pearson Education Publication, 2017
3. Tanenbaum, "Computer Networks", 5e (5th Edition), Pearson Education India; 5 edition (2013)

REFERENCE BOOKS:

1. Todd Lammle, "Comptia Network+ Study Guide";Wiley, Third edition, ISBN-10: 8126556412, 2015
2. Todd Lammle, "CCNA Routing and Switching Complete Study Guide", Wiley; Second edition (2016)
3. Wm. Arthur Conklin, Chuck Cothren, Roger Davis, Dwayne Williams, Greg White, "CompTIA Security+ All-in-One Exam Guide", McGraw-Hill Education; 4 edition (16 December 2014)
4. William Stallings, "Cryptography and Network Security", Pearson Education, 6 th Edition, SBN 10: 0133354695, 2013.
5. AtulKahate, "Cryptography and Network Security", McGraw Hill Education India (Pvt Ltd),2nd edition, ISBN 10: 0070151458, 2009.
6. Charlie Kaufman, Radia Perlman, Mike Speciner, " Network Security: Private Communication in a Public World", Prentice Hall, 2 nd edition, ISBN 10: 0130460192, 2002. 4. Charles Pfleeger, Shari Lawrence Pfleeger "Security in computing", Prentice Hall,4th Edition, ISBN 10: 0132390779, 2006.

Subject Code: HMCS20G04	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	E-Mail Security and Forensics	Ty	3	0	0	3

OBJECTIVES:

This paper will help a student to understand:

- The Email infrastructure and its components.
- The Email etiquette, Corporate practices and policies.
- The Email security, attacks and email related crimes.
- The Email Forensics and email header analysis.

UNIT I - Introduction to Email **9Hrs**

Evolution of Communication System – Postal Communication System – Analogy of Email System - How email system works? – The role of Mail User Agent, Mail Delivery Agent, Mail Transfer Agent, and DNS Servers - An overview of various protocols SMTP, POP, IMAP - involved in a typical email infrastructure – Characteristics of an Email - Advantages of Email communication system.

UNIT II - Email Etiquette and Corporate Practices **9Hrs**

Significance of Email etiquette – Standard fonts and formatting – Subject Line – Professional email address – Greetings message – Introduction – Culture – Reply All options – Use of sentence case – Email attachments – Proof read – Be positive – Revert as soon as possible – Professional tone – Recipient ID validation – Beware of Malicious and shorten URLs – Configuring email signatures, Out of Office – Auto replies – Email Policies and corporate practices – Personal Use – Misuse of email infrastructure – DLP – Data Leak Prevention / Data Loss Prevention Policy – Email Archive.

Unit III - E-mail Security **9Hrs**

A brief introduction to security issues relevant to emails as well as the typical email infrastructure - Entities in an Email infrastructure - Risks to an Email infrastructure – Threats, Vulnerabilities, Exploits and Impact with respect to Email Users, Mail clients, Mail Server, Email Protocols - SMTP, IMAP4 and POP3 - How to secure the email infrastructure – Management Controls, Operational Controls, Technical Controls with suitable examples for Confidentiality, Integrity and Availability – Implementation of controls to secure the email infrastructure – Information asset classification and handling – Physical protection – Securing email server applications. Transmission and supporting operating environment.

UNIT IV - Email Frauds and Crimes **9Hrs**

Email related crimes – Email Spoofing – Email Phishing and Countermeasures – Email Bombing – Spam Emails – Email Frauds – Email Hacking – Spreading malicious codes through Emails and Countermeasures – Nigerian Fraud – Defamatory emails – Threatening Emails – Case studies.

Unit V - Email Forensics **9Hrs**

IP address management - IANA – WHOIS.com – Regional Internet Registries - Understanding message headers – Email Header Analysis – Online Email tracer tool – MX Tool Box Email Header analysis – SPF – DKIM – DMARC – How to identify spoofed emails – Origin hostname, IP address trace and validation – Email traversal path analysis – Date and time stamp analysis – Email attachment analysis - Email Investigation – Case studies – The Offer of Money – The Alert – Phishing Email – The Inside Scoop – The Masked Email – The Big Lie – The Little Lie. **Total Hrs:45**

TEXT BOOK:

1. **Tony Bradley and Harlan Carvey**, "*Essential Computer Security: Everyone's Guide to E-Mail, Internet and Wireless Security*, ISBN:1-59749-114-4, Syngress 2006.
2. **Bill Nelson, Amelia Phillips and Chris Steuart**, "*Guide to Computer Forensics and Investigations*" – 5th Edition, 2016, Cengage Learning. ISBN:978-1-285-06003-3.

Subject Code: HMCS20GL1	**Subject Name**	**Ty/Lb/ ETL**	**L**	**T/ S.Lr**	**P/R**	**C**
	Network Security Lab	Lb	0	0	3	1

1) Implementation Of Client-Server Communication Using TCP.
2) Implementation Of File Transfer Protocol.
3) Implementation Of Domain Name space.
4) Java Program For Message Passing Using Message window .
5) Java Window Chat Program.

Subject Code: HMCS20GL2	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Information Security Risk Management Lab	Lb	0	0	3	1

1. Windows Password Management Policy and Windows Group Policy
2. Windows Firewall and it's Configuration of Rules
3. Network firewall ACL review
4. Windows Monitoring Tool Viewing the cache data of Microsoft Internet Explorer
5. Steganography
6. Scanning and Enumeration
7. Risk Assessment Scenarios
8. Create Security Policy for an Enterprise
9. Creation of process, procedure, guideline

SEMESTER – II

Subject Code: HMCS20G05	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Cyber Forensics Fundamentals	Ty	3	0	0	3

Course Objective:

1. Understand the basic principles of digital forensics
2. Choose appropriate digital forensics tools to identify, classify, locate and recover the evidence
3. Learn the emerging digital forensic trends and technologies

Course Outcome:

Students will be able to:

1. Describe cyber forensics and the knowledge required to do the forensic analysis
2. Extending Scientific approaches to forensics that helps to identify, classify, locate and recover the evidence
3. Choose and apply current cyber forensics tools.
4. Devise basic network forensic analysis
5. Explore and keep track of the emerging forensic technology
6. Possess the required knowledge and expertise to become a proficient forensic investigator

Unit 1: Introduction to Forensics: 9Hrs

Cyber forensics – Understanding the science of forensics – cyber forensics knowledge needed: Operating Systems, Hardware, Networks – fundamental principles of cyber forensics – maintaining the chain of custody – law and cyber forensics

Unit 2: Principles and methods: 9 Hrs

Scientific approaches to forensics – Identify and classify evidence – Locations where evidence may reside: storage media, Hardware interfaces, File systems, file format, file types, header analysis – Recovering data – media file forensic steps

Unit 3: Forensic Analysis: 6Hrs

Hard drive specifications – Recovering data from the damaged media – Operating system specifics – Extracting deleted files – Encrypted files - Cryptography – Steganography – Cryptanalysis - Log tampering – Other techniques: spoofing, wiping, Tunnelling

Unit 4: Network Forensics: 3Hrs

Network packet analysis – Wireless – Router forensics – Firewall forensics – Logs to examine

Unit 5: Emerging forensics technology: 9Hrs

Social Networks – New devices: Google Glass, Cars, Medical devices – control systems and infrastructure – Online gaming – Electronic discovery: types of investigation, liability and proof, big data, steps in electronic data discover, disaster recovery Forensic tools – Open source forensic suite – Proprietary forensic suite – Drive Imaging and validation tools – forensic tool for integrity verification and hashing – forensic tools for Password recovery – Applying Digital Forensics in Social media

Total Hrs: 45

TEXT BOOKS:

1. Chuck Easttom, "CCFPSM Certified Cyber Forensics Professional Certification ALL-IN-ONE(Exam Guide)", McGraw-Hill Education, 2015, ISBN: Book p/n 978-0-07-183611-1

REFERENCE BOOKS:

1. Dejey, Murugan, "Cyber Forensics", Oxford University Press; First edition (1 June 2018), ISBN-13: 978-0199489442
2. Bill Nelson Amelia Phillips Christopher Steuart, "Guide to Computer Forensics and Investigations: Processing Digital Evidence", Fifth Edition, Cengage Learning, ISBN: 978-1-285-06003-3
3. Cory Altheide, Harlan Carvey, "Digital Forensics with Open Source Tools", 2011, Elsevier, ISBN: 978-1-59749-586-8
4. John Sammons, "The Basics of Digital Forensics The Primer for Getting Started in Digital Forensics", 2012 Elsevier, ISBN 978-1-59749-661-2
5. John Vacca, "Computer Forensics: Computer Crime Scene Investigation", Laxmi Publications; First edition (2015)
6. Marjie T. Britz, "Computer Forensics and Cyber Crime: An Introduction", 3rd Edition, Prentice Hall, 2011

Subject Code:	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
HMCS20G06	**Business Continuity Planning and Disaster Recovery Management**	Ty	3	0	0	3

Unit 1: **9Hrs**

Introduction - Introduction to Business Continuity Management (BCM) and Disaster Recovery (DR) - Terms and definitions - BCM principles - BCM lifecycle - (BCM programme management, Understanding the organization - Determining business continuity strategy, Developing and implementing a BCM response, BCM exercising, Maintaining and reviewing BCM arrangements, Embedding BCM in the organization's culture) - BCM in business: Benefits and consequence - Contemporary landscape: Trends and directions

Unit 2: **9Hrs**

Risk Management - BCM and DR – The relationship with Risk Management - Risk Management concepts and framework - Concepts of threat, vulnerabilities and hazard - Risk Management process - Risk assessment, risk control options analysis, risk control implementation, risk control decision, and risk reporting - Business Impact Analysis (BIA) concept, benefits and responsibilities - BIA methodology - Assessment of financial and operational impacts, identification of critical IT systems and applications, identifications of recovery requirements and BIA reporting - Relationship between BIA and Risk Management

Unit 3: **9Hrs**

Business Continuity Strategy and Business Continuity Plan (BCP) Development - Business continuity strategy development framework - Cost-benefit assessment - Site assessment and selection - Selection of recovery options - Strategy considerations and selection - Linking strategy to plan - Coordinating with External Agencies - Business continuity plan contents - Information Systems aspects of BCP - Crisis Management - Emergency response plan and crisis communication plan - Awareness, training and communication - Plan activation - Business Continuity Planning Tools

Unit 4: **9Hrs**

Business Continuity Plan Testing and Maintenance - Test plan framework - Types of testing - Business Continuity Plan Testing - Plan maintenance requirements and parameters - Change management and control - Business Continuity Plan Audits

Unit 5: **9Hrs**

Disaster Recovery – Definitions - Backup and recovery - Threat and risk assessment - Site assessment and selection - Disaster Recovery Roadmap - Disaster Recovery Plan (DRP) preparation - Vendor selection and implementation - Difference between BCP and DRP - Systems and communication security during recovery and repair

Total Hrs: 45

Text Book

1. Thomas R. Peltier, "Information Security Fundamentals", Auerbach Publications; 2 edition (29 June 2017), ISBN-13: 978-1138436893
2. Umesha Nayak, Umesh Rao, "The InfoSec Handbook: An Introduction to Information Security", Apress; 1st ed. edition (10 September 2014), ISBN-13: 978-1430263821

Reference Book

1. Adam Gordon, "Official (ISC)2 Guide to the CISSP CBK ((ISC)", Auerbach Publications; 4 edition (March 11, 2015), ISBN-13: 978-1482262759
2. Jason Andress "The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice", Syngress; 2 edition (14 July 2014), ISBN-13: 978-0128007440
3. Michael E. Whitman, Herbert J. Mattord, "Principles of Information Security", 6th edition, Cengage Learning India Private Limited, 2018, ISBN-13: 978-9387994232
4. John Vacca, "Computer and Information Security", Handbook, 3rd edition, Morgan Kaufman, 2017, ISBN: 9780128038437.
5. Mark Rhodes-Ousley, "Information Security: The Complete Reference", McGraw Hill Education; Second edition (1 May 2013), ISBN-13: 978-125909834

Subject Code:	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
HMCS20G07	**Vulnerability Assessment and Penetration Testing ~~(VA/PT)~~**	Ty	3	0	0	3

Objectives:

Students would learn:

1. the degree of exposure to external and internal attacks
2. the methodologies of assessing the appropriate defence systems ; and
3. the importance of patch management

Unit I **9Hrs**

Overview – What is VA & PT? – Need & Benefits of VA & PT – Types of VA & PT – Application – How is VA & PT performed – Challenges & Limitations of VA & PT – Skillset Required – Ethics

Unit II **9Hrs**

Introduction Hacking Methodology- Hacking Methodology, Process of Malicious Hacking, Footprinting and Scanning: Footprinting, Scanning. Enumeration: Enumeration. System Hacking and Trojans: System Hacking, Trojans and Black Box Vs White Box Techniqueslogy

Unit III **9Hrs**

Web and Network Hacking Vulnerability Assessment – SQL Injection, Hacking Wireless Networking, Viruses, Worms Denial of Service, Sniffers, Session Hijacking and Hacking Web Servers: Session Hijacking, Hacking Web Servers. Web Application Vulnerabilities and Web Techniques Based Password Cracking: Web Application Vulnerabilities, Web Based Password Cracking Techniques

Unit IV **9Hrs**

Penetration Testing – Pen Testing Strategies **-** Usefulness of Test Results – Assets Connection Testing – Security Risk Assessment – Manual VS. Automated Testing – Various Tools for PT

Unit V **9Hrs**

Report writing & Mitigation – Introduction to Report Writing & Mitigation, requirements for low level reporting & high level reporting of Penetration testing results, Demonstration of vulnerabilities and Mitigation of issues identified including tracking

Total Hrs: 45

Text Book:

1. Mark Dowd, John McDonald, Justin Schuh (2006) *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities*, Addison Wesley

REFERENCE BOOKS:

1. Georgia Weidman (2014) *Penetration Testing: A Hands-On Introduction to Hacking*, No Starch Press
2. Felicia M. Nicastro (2011) *Security Patch Management*, CRC Press
3. Hacking Exposed 7th Edition, by Stuart McClure, Joel Scambray, George Kurtz – McGraw Hill-2010
4. Basic of Hacking and Penetration – Patrick Engerbrestson 2010

Subject Code: HMCS20G08	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Malware Analysis and Security	Ty	3	1	0	4

Course Objective:

1. To introduce the fundamentals of malware, types and its effects
2. To identify and analyze various malware types
3. To deal with detection, analysis, understanding, controlling, and eradication of malware

Course Outcome:

Students will be able to:

1. Understand the concept of malware analysis, types of malware analysis and differentiate malware and a virus
2. Classifying and comparing the malware samples and Extract strings, functions, and metadata associated with the file
3. Learn Dynamic analysis tools and their features, steps involved in dynamic analysis
4. Describe the possibilities that can make experience with sandboxes and multi-AV scanners even better
5. Identify and correlate information regarding domains, hostnames, and IP addresses
6. Discuss the challenges encountered in the field of malware analysis

Unit 1: Malware Analysis Introduction: 10 Hrs

Malware – Malware Analysis – Why malware analysis - Malware categories – Malware analysis techniques: Static malware analysis – Dynamic Malware Analysis – Analysis tools – Sandbox tools and techniques

Unit 2: Static Analysis: 10 Hrs

Identifying file type using manual method, using tools – Hashing – Multiple antivirus scanning – String extraction – File obfuscation – Inspecting PE header information – Comparing and classifying the malware

Unit 3: Dynamic Analysis: 10 Hrs

Monitoring system and networks – dynamic analysis tools: Monitoring with process monitor, viewing processes with process explorer, Comparing registry snapshots with Regshot, Packet sniffing with Wireshark - Dynamic Analysis steps

Unit 4: Scanning and Analyzing Malware: 10 Hrs

Scanning files with virus total, Jotti, NovirusThanks – Multi-Antivirus Scanner Comparison - Analyzing malware with threat expert, CW sandbox, Anubis - Identifying malware passwords - Bypassing authentication - Advanced malware analysis Virus, Trojan.

Unit 5: Domain and IP addresses research: 10 Hrs

Researching domains - WHOIS with Sysinternals on Windows – Resolving DNS hostnames on Windows – Researching IP addresses - Researching with Passive DNS and Other Tools – Performing a reverse IP search with domain tools – Brute force attack – Reverse Brute Force attack

Unit 6: Malware Challenges: 10 Hrs

Antimalware – Anti malware strategy – Anti malware engine – Common challenges – Scanning approaches - Virtual environment - Live internet connection - Real, fake, and virtual services -Anti-debug

Total Hrs: 60

TEXT BOOKS:

1. Monnappa K A, "Learning Malware Analysis", 2018 Packt Publishing, ISBN 978-1-78839-250-1

REFERENCE BOOKS:

1. Michael Hale Ligh, Steven Adair,BlakeHartstein, Matthew Richard, "Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code", 2011 by Wiley Publishing, ISBN: 978-0-470-61303-0
2. Cameron H. Malin, Eoghan Casey, James M. Aquilina, Curtis W . Rose, "Malware Forensics Field Guide for Windows Systems", 2012 Elsevier, ISBN: 978-1-59749-472-4
3. M. Sikorski and A. Honig, "Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software", San Francisco: No Starch Press San Francisco, CA, 2012. (ISBN No.: 978-1-59-327290-6)
4. Gerard Johansen, "Digital Forensics and Incident Response", 2017 Packt Publishing, ISBN 978-1-78728-868-3
5. Victor Marak, "Windows Malware Analysis Essentials", 2015 Packt Publishing, ISBN 978-1-78528-151-8
6. Mihai Christodorescu Somesh Jha, Douglas Maughan, Dawn Song, Cliff Wang, "Malware Detection", 2007 Springer, ISBN-13: 978-0-387-32720-4

Subject Code: HMCS20G09	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Cyber Law	Ty	3	0	0	3

Objectives:

1. To understand the fundamentals of cyber law.
2. Study IT ACT 2000 (INDIA).
3. Understanding Intellectual Property Rights .

Unit 1: Fundamentals of Cyber Law **9 Hrs**

Introduction on cyber space - Jurisprudence of Cyber Law - Scope of Cyber Law

9 Hrs

Unit II – Indian Penal Code - relevant sections to cyber crimes – Criminal Procedure Code – Indian Evidence Act and Cyber Crimes

9 Hrs

Unit III

IT Act 2000: Enhance and adhere to the cyber law violations: Acceptance terms- resposibiliites and registration violations – privacy policy – registration and password – third party services – indemnification – site editors service – conduct – submission of content in the website – disclaimer of warranties – limitation of liability – reservation of rights – notification of copyright and infringement – applicable law – miscellaneous information

Unit IV **9 Hrs**

Practices in Cyber Jurisprudence – Regional and Global - Important Case Laws in India and other countries – Need for International cooperation for cybercrime investigation and enforcement-Need for separate cyber court - cyber laws in other countries

Unit V **9 Hrs**

E- Governance and E – Commerce: Electronic Governance**:** Procedures in India - Essentials & System of Digital Signatures - The Role and Function of Certifying Authorities - Digital contracts – Validity of Electronic Contract-Types of Electronic Contract - UNCITRAL Model law on Electronic Commerce - Cryptography – Encryption and decryption –Legal Issues In E banking transactions.

Total Hrs: 45

Text BookS:

1. Saurabh Sharma, “Information Security and Cyber Law”,Vikas publication, 2010

Referenc Books:

1. Peggy E Chaudhary, “Protecting Your Intellectual Property Rights: Understanding the Role of Management, Governments, Consumers and Pirates”, Springer, 2013
2. Brain Craig, “Cyber Law: The Law of Internet and IT”, Prentice Hall, 2012

Subject Code: HMCS20GL3	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Cyber Forensics Fundamentals Lab	Lb	0	0	3	1

Course Objective:

1. To understand bits, bytes and numbering systems
2. To understand the Seizure issues
3. To gain insight into evidence creation and interpretation

Course Outcome:

At the end of the course students will be able to

- Understand Forensic Software tools
- Understand bits, bytes and numbering systems
- Use the Windows System, Linux System, Mobile Phone OS
- Handle Seizure issues
- Understand continuity and hashing
- Identify evidence location
- Understand evidence creation and interpretation

The faculty conducting the laboratory will prepare a list of 12 experiments and get the approval of HoD/Director and notify it at the beginning of each semester.

Subject Code:	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
HMCS20GL4	Vulnerability Assessment and Penetration Testing Lab ~~**VA/PT Lab**~~	Lb	0	0	3	1

Objectives:

This lab session focus on training the students in

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

Sessions:

1. Monitoring Network Traffic
2. Host & Services Discovery using Nmap
3. Vulnerability Scanning using OpenVAS
4. Internal Penetration Testing
   - Mapping
   - Scanning
   - Gaining access through CVE's
   - Sniffing POP3/FTP/Telnet Passwords
   - ARP Poisoning
   - DNS Poisoning
5. External Penetration Testing
   - Evaluating external Infrastructure
   - Creating topological map & identifying IP address of target
   - Lookup domain registry for IP information
   - Examining use of IPV6 at remote location

SEMESTER – III

Subject Code: HMCS20G10	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Advanced Information Security	Ty	3	1	0	4

Unit 1: **12 Hrs**

Digital Rights Management - Meaning of Digital Rights Management (DRM) - Need for DRM and preventing illegal file sharing on the Internet - DRM schemes - Microsoft DRM 2.0, and the Content Scrambling System - Reasons why DRM schemes have been unsuccessful so far - Requirements for a good DRM scheme - secure hardware, secure software, and an efficient legal system

Unit 2: **15 Hrs**

Operating System and Security - Overview of operating systems, functionalities and characteristics of OS - concept of a process, operations on processes, process states, concurrent processes, process control block, process context - Interrupt processing, operating system organization - Job and processor scheduling, scheduling algorithms, process hierarchies - Problems of concurrent processes, critical sections, mutual exclusion, synchronization, deadlock – Inter process Communication (IPC), Message Passing, Direct and Indirect - Deadlock: prevention, detection, avoidance - Memory organisation and management - Virtual memory concepts, paging and segmentation - File organization and directory structure - OS and Security - Security breaches - Types of attacks - Attack prevention methods - Access control lists – support for internet and general network security.

Unit 3: **9 Hrs**

Common Authentication Protocols - Authentication concepts - Various authentication protocols - Password Authentication Protocol (PAP) - Challenge Handshake Authentication Protocol and MS Chap - Extensible Authentication Protocols - Remote Access with RADIUS and TACACS - Single Sign on – Kerberos, SEASAME – Authentication in Wireless networks

Unit 4: **9 Hrs**

Real World Protocols – IPSec, SSL, IKH, AH and ESP - Introduction to IPSec - IPSec building blocks - Security Associations (SAs) - Security Parameter Index (SPI) - IPSec Architecture - IPSec Protocols - Authentication Header (AH) - Encapsulation Security Payload (ESP) - Tunneling and Transport Mode - Internet Key Exchange (IKE) – ISAKMP

Unit 5: **15 Hrs**

Application System Security - SDLC concepts - Different SDLC and cost estimation models - Testing: types, methods and issues - Program coding and security to be built into it - Software maintenance and change control processes - Configuration management - Software Capability Maturity model (CMM) - DBMS concepts & terms: types, with focus on Relational model - Data dictionary – Interfaces to databases (ODBC, ADOJDBC, XML) - Database security features - User access rights – Database auditing features and logs.

Total Hrs: 60

Text Books:

1. James M. Stewart, Mike Chapple, Darril Gibson, "(ISC)2 Certified Information Systems Security Professional Official Study Guide) – CISSP", Seventh Edition, 2015, Sybex (2015), ISBN: 978-1-119-04271-6
2. Thomas R. Peltier, "Information Security Fundamentals", Auerbach Publications; 2 edition (29 June 2017), ISBN-13: 978-1138436893

Reference Books:

1. Umesha Nayak, Umesh Rao, "The InfoSec Handbook: An Introduction to Information Security", Apress; 1st ed. edition (10 September 2014), ISBN-13: 978-1430263821
2. Adam Gordon, "Official (ISC)2 Guide to the CISSP CBK ((ISC)", Auerbach Publications; 4 edition (March 11, 2015), ISBN-13: 978-1482262759
3. Jason Andress "The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice", Syngress; 2 edition (14 July 2014), ISBN-13: 978-0128007440
4. Michael E. Whitman, Herbert J. Mattord, "Principles of Information Security", 6th edition, Cengage Learning India Private Limited, 2018, ISBN-13: 978-9387994232
5. John Vacca, "Computer and Information Security", Handbook, 3rd edition, Morgan Kaufman, 2017, ISBN: 9780128038437.
6. Mark Rhodes-Ousley, "Information Security: The Complete Reference", McGraw Hill Education; Second edition (1 May 2013), ISBN-13: 978-1259098345

Subject Code: HMCS20G11	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Advanced Digital Forensics	Ty	3	0	0	3

Course Objective:

1. To understand forensic software and hardware
2. To understand the windows and linux file systems
3. To gain insight data recovery tools

Course Outcome:

Students will be able to:

1. Define the information security, information risk
2. Learn partitioning and disk layouts
3. Handle windows and linux file systems
4. Learn advanced tools
5. Learn tools that are used for data recovery

Unit I **9 Hrs**

Digital Forensics: Forensic Software and Hardware - Analysis and Advanced Tools - Forensic Technology and Practices - Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis.

Unit II **9 Hrs**

Disk and file system analysis: Media analysis concepts – the sleuth kit – partitioning and disk layouts – special containers – hashing – carving – forensic imaging

Unit III **9 Hrs**

Windows systems artifacts: Windows file systems – Registry – event logs – prefetch files – shortcut files – windows executables

UnitIV **9 Hrs**

Linux systems artifacts: linux file systems – linux boot process and services – linux system organization and artifacts – user accounts – home directories – logs – scheduling tasks

UnitV **9 Hrs**

Overview of various Tools and Data Recovery – Overview of tools that are used for recovery of deleted files and deleted partitions – tools used in the industry and Best Practices

Total Hrs: 45

TEXT BOOKS:

1. Cory Altheide, Harlan Carvey Digital Forensics with Open Source Tools: Using Open Source Platform Tools for Performing Computer Forensics on Target Systems: Windows, Mac, Linux, Unix, etc, Syngress; 1 edition (29 March 2011)
2. The basics of Digital Forensics by John Sammons, 2nd Edition, Elsevier Publication, 2012
3. Windows Forensics Analysis Tool kit by Harlan Carvey, 3rd Edition, Syngress Publication, 2007

REFERENCE BOOKS:

1. Kevin Mandia, Chris Prosise, Matt Pepe, “Incident Response and Computer Forensics“, Tata McGraw -Hill, New Delhi, 2006.
2. ”Understanding Forensics in IT “, NIIT Ltd, 2005.

Subject Code: HMCS20G12	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Cloud Security	Ty	3	0	0	3

Course Objective:

1. To introduce the broad perceptive of cloud architecture and model
2. To understand the concept of Virtualization
3. To be familiar with the lead players in cloud.

Course Outcome:

Students will be able to:

1. Compare the strengths and limitations of cloud computing
2. Identify the architecture, infrastructure and delivery models of cloud computing
3. Apply suitable virtualization concept.
4. Choose the appropriate cloud player
5. Design Cloud Services
6. Set a private cloud

Unit I **9 Hrs**

Fundamentals of Cloud Computing, Cloud Platforms / Categories, Cloud Components, cloud deployment models, Virtualization, benefits of cloud computing, cloud computing roles.

Unit 2 **9 Hrs**

Cloud data lifecycle, data security strategies for securing cloud data, Data discovery and classification technologies

Unit 3 **9 Hrs**

Cloud Platform and Infrastructure Security – Security Requirements of Cloud Infrastructure: Network – Virtualization - Types of Virtualization - Implementation Levels of Virtualization - Virtualization Structures - Tools and Mechanisms - Virtualization of CPU, Memory, I/O Devices - Virtual Clusters and Resource management – Virtualization for Data-center Automation. – Storage - Physical and Environmental.

Unit 4 **9 Hrs**

Cloud Application Security with respect to Access Control – Identity and Access Management, Federation, Multifactor Authentication. OWASP and SANS recommendation of Cloud Security requirementsDescribe the software development lifecycle process for a cloud environment
Identify the necessary functional and security testing for software assurance.

Unit 5 **9 Hrs**

Best practices and the future of cloud computing – Establishing a baseline and metrics – Phased in vs flash cut approaches – Researcher predictions – Responding to change - Security Overview – Cloud Security Challenges and Risks – Software-as-a-Service Security – Security Governance – Risk Management – Security Monitoring – Security Architecture Design – Data Security – Application Security – Virtual Machine Security - Identity Management and Access Control – Autonomic Security.

Total Hrs:45

TEXT BOOKS:

1. Kai Hwang, Geoffrey C Fox, Jack G Dongarra, “Distributed and Cloud Computing, From
2. Parallel Processing to the Internet of Things”, Morgan Kaufmann Publishers, 2012.
3. John W.Rittinghouse and James F.Ransome, “Cloud Computing: Implementation,
4. Management, and Security”, CRC Press, 2010.
5. Toby Velte, Anthony Velte, Robert Elsenpeter, “Cloud Computing, A Practical Approach”,TMH, 2009.

REFERENCE BOOKS:

1. George Reese, “Cloud Application Architectures: Building Applications and Infrastructure in the Cloud” O'Reilly
2. James E. Smith, Ravi Nair, “Virtual Machines: Versatile Platforms for Systems and Processes”, Elsevier/Morgan Kaufmann, 2005.
3. Katarina Stanoevska-Slabeva, Thomas Wozniak, Santi Ristol, “Grid and Cloud Computing – A Business Perspective on Technology and Applications”, Springer.
4. Ronald L. Krutz, Russell Dean Vines, “Cloud Security – A comprehensive Guide to Secure Cloud Computing”, Wiley – India, 2010.
5. Rajkumar Buyya, Christian Vecchiola, S.Thamarai Selvi, ‘Mastering Cloud Computing”, TMGH,2013.
6. Gautam Shroff,

Subject Code: HMCS20GL5	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Advanced Information Security Lab	Lb	0	0	3	1

1) Use of security tools like
   a) Freeware Vulnerability Scanners
   b) Freeware Packet Analysers
   c) Disk Editors
   d) Backup Tools
   e) Firewalls
2) Installing typical operating systems and hardening them
3) Identifying missing security patches for typical OS
4) Installing and Configuring anti-virus suites
5) Interpreting email headers
6) Collecting data about internet websites from public sources
7) Exercises in using check digits
8) Simple exercises in encryption and hashing tools and understanding effect of tampering data
9) Obtaining Digital Certificates of a few sites and interpreting their features
10) Generating digital certificates and validating them in a private LAN

Subject Code: HMCS20GL6	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Advanced Digital Forensics Lab	Lb	0	0	3	1

Course Objective:

- To Handle electronic evidence
- To dismantle and re-build PCs
- To examine of File systems of Windows, Linux and Mac
-

Course Outcome:

At the end of the course students will be able to

- Handle electronic evidence using forensic standards
- Dismantling and re-building PCs in order to access the storage media safely
- Boot sequence and Power On Self-Test mode analysis
- Examine of File systems of Windows, Linux and Mac
- Analyze Word processing and Graphic file format
- Handle Network data sniffing

The faculty conducting the laboratory will prepare a list of 12 experiments and get the approval of HoD/Director and notify it at the beginning of each semester.

Subject Code:	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
HMCS20P01	Project Phase-I	Lb	0	0	12	5

OBJECTIVE:

The objective of the Main Project is to culminate the academic study and provide an opportunity to explore a problem or issue , address through focused and applied research under the direction of a faculty mentor. The project demonstrates the student's ability to synthesize and apply the knowledge and skills acquired to real-world issues and problems. This project affirms the students to think critically and creatively, find an optimal solution, make ethical decisions and to present effectively.

In Phase I ,Students are expected to

(i) Identify a Problem.
(ii) Have the feasibility explored.
(iii) Freeze the Requirement specification (both user and system).
(iv) Construct the architectural model (as many as required).
(v) Design the solution.
(vi) If possible publish the Feasibilty study as a survey paper

SEMESTER – IV

Subject Code: HMCS20G13	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Social Media Crimes and Security	Ty	3	0	0	3

Course Objective:

1. To understand Social Media, Social Networks and Crime
2. To be familiar with the types of Media, Social Media and the services offered by various social networking sites.
3. To know various types of social media crimes and the response of the criminal Justice System.

Course Outcome:

Students will be able to:

1. Learn about media, social media and social networks
2. Understand Social Networks and crime
3. understand the types of social working crimes, causes, consequences and countermeasures
4. Present a Case Studies
5. Understand the response of the Criminal Justice System towards the social networking sites.
6. Know about data privacy and legal measures to prevent social media crimes.

Unit I : 13 Hrs

Introduction to Social Media : Definitions – Social Media, Social Network, Social Networking Sites, Digital Identify , Instant Messaging, Types of Media, History of Social Media – Genesis of Internet, WWW, Emergence of Social Networking Sites, Web 2.0 – Current Social Media and Social Networking Usage in various countries – Trends in Social Media.

Unit II : 9 Hrs

Types of Social media – Various types of social media, types of social networking sites, - Profile based SNS – Content Based SNS – White label SNS – Multi user virtual environment – Mobile based SNS – Community based SNS – Instant Messaging Applications – Mobile based applications, their types and their vulnerabilities - Micro Blogging – People Search – Other forms of SNS – List of Social Networking Sites , Applications and their history

Unit III : 9 Hrs

Social Media Services – Types of services of social media – Usage of social media – Friendng, Trending, Chatting, Wall Posts, Tweets, Selfies, Forwards, Community networking, Gaming, Memes, Talent displays, Use of social networking sites for small businesses – Use of social networking sites for large scale businesses – Use of Social Media in Politics – Social media as other advertisement platforms – Different types of Promotions and Social Media

Unit IV : 9 Hrs

Social Media and Crimes against women and Children: - Types of Social Media Crimes against women and Children, causes, consequences and countermeasures – Pornography – Child Pornography – Non Consensual Pornography – Revenge Porn - Indecent Representation of Women – Insult to Modesty of Women - Online Violence – Cyber/virtual Rape - Online Harassment – Cyber Bullying – Cyber Stalking – Chat room based crimes – Emotional Targets – Toxic contents – Causing Disrespect - Online Predators – Abuse of Children online – Patterns of women and child sexual victimization – Trends and Analysis

Unit V: 5 Hrs

Other forms of social media crimes – Online Frauds – Frauds targeting children, women, youngsters, senior citizens – Business related frauds – Hacking – Cyber Defamation – Cyber Terrorism – Financial Frauds – Fake News – Fake Memes – Online challenges, selfie, facebook, whats app victimization – Digital Cloning Frauds – Morphing – Identity Theft – Data Theft – Human Flesh Search Engine – Intellectual Property Related Crimes in Social Media.

Total Hrs: 45

TEXT BOOKS:

- Brutny, Joshwa and Katherine " Social Media Investigation For Law Enforcement" Catherine D. Marcum, George E. Higgins, "Social Networking as a Criminal Enterprise (Kindle Edition) ", CRC Press; 1 edition (28 April 2014),
- Thaddeus A. Hoffmeister, "Social Media in the Courtroom: A New Era for Criminal Justice", Hardcover import, Praeger (August 11, 2014)

REFERENCE BOOKS:

- Venessa Garcia, Samantha G. Arkerson "Crime, Media, and Reality: Examining Mixed Messages About Crime and Justice in Popular Media Kindle Edition", Rowman & Littlefield Publishers (8 December 2017)
- Michael Salter, "Crime, Justice and Social Media (New Directions in Critical Criminology) ",Kindle Edition, Routledge (4 October 2016)

Subject Code:	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
HMCS20P02	Project Phase-II	Lb	0	0	20	10

OBJCETIVE:

The objective of the Main Project is to culminate the academic study and provide an opportunity to explore a problem or issue , address through focused and applied research under the direction of a faculty mentor. The project demonstrates the student's ability to synthesize and apply the knowledge and skills acquired to real-world issues and problems. This project affirms the students to think critically and creatively, find an optimal solution, make ethical decisions and to present effectively.

Students are expected to carry out the following :

(i) Implement the Design using suitable technologies.

(ii) Generate the test cases.

(iii) Demonstrate the solution with suitable user interface.

(iv) Prepare a project report consolidating the phase-I and II activities.

ELECTIVES

Subject Code: HMCS20GE1	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Forensic Science and Crime Investigation	Ty	3	0	0	3

Course Objective:

1. To understand the history and development of forensic science.
2. To understand the roles of different types of professionals involved in evaluating a crime scene, analysis of crime exhibits and expert witness.
3. To understand the methodology to collect, preserve and present evidence in a professional (courtroom) setting.

Course Outcome:

Students will be able to:
Understand the history of the forensic sciences
Define the roles of different types of professionals involved in evaluating a crime scene and collecting the evidence
Understand the aspects of the justice system followed.
Learn the methodology of collecting & interpreting data, avoiding contamination, and preservation of chain of custody
Define the importance pertaining to forensic examination
Present evidence in a professional (courtroom) setting

Module 1: Introduction to Forensic Science: **9Hrs**

History and Development of Forensic Science - Functions of the Forensic Scientist –Divisions of Forensic Science – Forensic Setup in India - Evolving Forensic Science Services- Role of forensic expert in the court of law - Aspects of the Criminal Justice System - Aspects of Trials.

Module 2: Crime Scene Investigation: **9Hrs**

Concepts – Nature and type of crime scene – Crime scene search methods: Recovery and packaging of evidences – Crime scene documentation - Preservation of evidences – National and International scenario on crime scene investigation – Physical evidences

Module 3: Crime Scene Reconstruction (CSR): **9Hrs**

Nature and importance of CSR– Basic principles and stages involved – Types and classification of reconstruction – Pattern evidence and shooting scene reconstruction – Manual and computer -assisted reconstruction of BPA – Role of logic in CSR – Writing a reconstruction report – Correlation of crime scene analysis with behavioural analysis – Cases of special importance pertaining to forensic examination

Module 4: Forensic Analysis: **9Hrs**

Basics of Forensic Biology – Forensic Serology – DNA Typing – Forensic Chemistry – Forensic Toxicology – Forensic Medicine.

Module 5: Cyber Crime & Computer Forensics: **9Hrs**

How Does the Computer Work - How Data Is Stored -Processing the Electronic Crime Scene - Evidentiary Data– Cyber Crimes – Computer Crime Scene Investigation – Computer Forensic Analysis – - Voice identification – Forensic Psychology –Polygraph - Narco - analysis – Brain fingerprinting – Criminal profiling and their legal status in India

Total hours: 45

TEXT BOOKS:

1. Stuart H. James and Jon J. Nordby, Suzanne Bell "Forensic Science: An Introduction to Scientific and Investigative Techniques", Fourth Edition, CRC Press; 4 edition (4 September 2015), ISBN-13: 978-1439853832

REFERENCE BOOKS:

1. Safarstein R, "Criminalistics – An Introduction to Forensic Science", Pearson; 11 edition (26 June 2014), ISBN-13: 978-1292062020
2. Jaising P. Modi, Justice K Kannan, "A text book of medical jurisprudence and toxicology", Lexi Nexis; Twenty Sixth edition (10 April 2018), ISBN-13: 978-9386515438
3. Albert J. Marcellaa and Robert S. Greenfiled (Ed), "Cyber Forensics, A Field Manual for collecting, examining and preserving evidence of computer crimes", Auerbach publications, 2 edition (19 December 2010)
4. Peter Stephenson, Keith Gilbert, "Investigating Computer-Related Crime", Routledge; 2 edition (5 June 2013), ISBN-13: 978-0849319730
5. Stuart James, "Studyguide for Forensic Science: An Introduction to Scientific and Investigative Techniques", Cram101 (2013), ISBN-13: 978-1490278629

Subject Code: HMCS20GE2	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Frauds in BFSI, Telecom Sector and Security	Ty	3	0	0	3

UNIT I - INTRODUCTION: **9Hrs**

Banking Concepts - Broad features of Deposit and Loan Products - Types of banks: Retail, Corporate, Investment, Development, Private, etc. - Ancillary services like Trade Finance, Remittances - Anti Money Laundering and KYC concepts – ATM Frauds

UNIT II - COMPUTERIZED OPERATIONS OF BANKS: **9Hrs**

Banking Concepts - Core Banking Solution - Security mechanisms to secure network and devices – Internet Banking - Mobile banking - Cyber Security Attacks On Banks – Fraud Detection – Fraud opportunities

UNIT III - VULNERABLE AREAS IN CBS AND THEIR EXPLOITATION: **9Hrs**

Application related - Parameters and freedom available to users - Empowerment of users - Access to - organization -wide data - Direct access to database and records - Multiple interfaces with other applications ATM Network

9Hrs

UNIT IV - TELECOM FRAUD:

'Telecommunication Fraud' - Telecommunication Technologies - About Fraudsters - Benefits to Fraudsters - Using a service without - Call selling to others - Root Causes of Fraud - Mitigation and Demographics - Penetration of new technology - Staff Dissatisfaction – Illustrative cases

UNIT V - SECURITY CONTROLS **9Hrs**

Log of User activities in the application - Change management procedures - Internal data consistency checks - Account related frauds - Internet Banking related - Social Engineering, Phishing tactics - Corruption in BFSI Sector - Counter Measures.

Total Hrs:45

TEXT BOOKS:

1. Retail Banking by Raghu Palat

REFERENCE BOOKS:

1. *Information System for Banks – Indian Institute of Banking & Finance*
2. *Core Banking Solution – Evaluation of Security & Controls by M Revathy Sriram, P K Ramanan and R Chandrasekhar*

Subject Code: HMCS20GE3	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Web Application Security	Ty	3	0	0	3

Course Objective:

1. To explain the fundamental techniques adopted in developing secure web based applications.
2. To identify the vulnerabilities of web based applications and to protect those applications from attacks
3. To understand security-related issues in Web-based systems and applications.

Course Outcome:

Students will be able to:

Understand the fundamentals of web application, web security vulnerabilities and principles
Describe high level security principles and also learn some popular methods of classifying threats and prioritizing them
Discuss the authentication to be performed and the best practices in performing it.
Discuss the terminology, methodology and dangers involved in web application authorization
Explain two common vulnerabilities cross site scripting and cross site request forgery
Learn some secure development and deployment methodologies

Module 1: Introduction to Web application: **9Hrs**

Introduction - Web Application Security - Defence Mechanisms - Handling User Access - hacker methodologies -Review of hackers - Managing the Application - The OWASP Top Ten List

Module 2: Web application Security fundamentals: **6Hrs**

HTML – HTTP – Client side scripting – Server side scripting – Input validation – Blacklist validation – White list validation – Defence in depth – Attack surface reduction – Classifying and prioritizing threats

Module 3: Web Authentication: **9Hrs**

Authentication Fundamentals- Two Factor and Three Factor Authentication – Web application authentication - Secured Password Based Authentication: Attacks against Password, Importance of Password Complexity - Design Flaws in Authentication Mechanisms –Implementation Flaws in Authentication Mechanisms - Securing Authentication

Module 4: Web Authorization: **3Hrs**

Understanding authorization - Need for Session Management – Attack against session - Session IDs and Cookies - Hijacking URLs - Protecting Authorization

Module 5: Web, Database and file Security Principles: **9Hrs**

Cross Site Scripting - Cross Site Request Forgery – Introduction to SQL - SQL Injection - Database Platform Attacks and Security - Database Encryption - Source code security – Forceful browsing - Directory Traversals

Module 6: Web application security development and deployment **9Hrs**

Understanding Vulnerabilities in web application – Penetrate and patch methodology - Application Security approach: Training, Threat modeling, Secure coding, Code review, security testing, Incident response planning – Secure Development methodologies and maturity models

Total hours: 45

TEXT BOOKS:

1. B. Sullivan, V. Liu, and M. Howard, "Web Application Security", McGraw-Hill Education, 2012. (ISBN No.: 978-0-07-177612-7).

REFERENCE BOOKS:

1. Mike Shema, Web Application Security for Dummies, John Wiley & Sons, Ltd, ISBN: 978-1-119-99487-9
2. Wade Alcorn, Christian Frichot, The Browser Hacker′s Handbook, John Wiley & Sons, Inc, ISBN-13: 978-1118662090,
3. Gene Spafford and Simson Garfinkel, Web Security, Privacy & Commerce, O'Reilly Media, Inc., ISBN-13: 978-0596000455, 2001
4. Andrew Hoffman, Web Application Security, O'Reilly Media, Inc., **ISBN:** 9781492053101, 2020
5. DafyddStuttard, Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2ed, ISBN-13: 978-81265334042011
6. Hanqing Wu, Liz Zhao, Web Security: A WhiteHat Perspective, Auerbach Publications 1st Edition, ISBN 9781466592612, 2015.
7. Steven Splaine,Testing Web Security: Assessing the Security of Web Sites and Applications 1st Edition, John Wiley & Sons, Inc, ISBN-13: 978-0471232810, 2002
8. Saumil Shah, Shreeraj Shah, Web Hacking: Attacks and Defense, Addison Wesley, ISBN-13: 978-0201761764, 2002

Subject Code: HMCS20GE4	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Vigilance and Security Management	Ty	3	0	0	3

Course Objective:

1. To develop the knowledge and skills required to effectively lead and facilitate investigations.
2. To train and develop the security professionals to handle the issues related to vigilance and investigation.
3. To provide basic conceptual understanding of disaster management theory, policy and practice.

Course Outcome:

Students will be able to:

1. Understand the fundamentals of investigation and its types and effectively plan an investigation strategy.
2. Acquire solid grounding in all key aspects of vigilance
3. Understand the common physical security measures, threats, risk reduction and good practices.
4. State security and safety practices
5. Explain the techniques for secure system deployment and operation
6. Use various methods and techniques for appropriate and timely preparation and mitigation of disasters

Unit I **9Hrs**

Investigation: Definitions - Key concepts - Private investigation - Historical background of private security – Security threats –Types of investigation – Espionage –Surveillance – Survey – Verification –First aid - Security survey/audit – Private Security Agencies (Regulation) Act, 2005

Unit II **9Hrs**

Vigilance Information and Intelligence: Collection, collation and timely reporting - Confidential enquiries – Classifying assets – Official Secrets Act, 1923

Unit III **9Hrs**

Physical Security Devices: Access control system - Computer security systems – Security alarm systems – Fire Exposure – Water Damage – Air conditioning – Electric – Emergency preparedness plan – Security guards – Segregation of Duties and responsibilities –

Unit IV **9Hrs**

Security and safety practices: Financial institutions - Industrial organizations and commercial establishments – Dealing with trespass/intrusion – Terrorists movement and hideouts – Emergency procedures –Security Ethics

Unit V **9Hrs**

Disaster Management: Definitions - Types of disasters: Man-Made Disasters: Fires - Bombings/Explosions - Acts of Terrorism - Power Outages - Other Utility and Infrastructure Failures - Hardware/Software Failures – Strikes - Theft/Vandalism- Natural disasters: Earthquakes – Floods – Storms – Fires - Other Regional Events

TEXT BOOKS: **Total hours: 45**

- Shon Harris and Fernando Maymi "CISSP All-in-One Exam Guide", 7th Edition, McGraw-Hill Education.
- Copeland, W. D. (2001), "Private investigation: How to be successful",Phoenix, AZ:Absolutely Zero Loss Inc.

REFERENCE BOOKS:

- Sinha, R. K,"Crimes affecting state security- problems and recent trends",New Delhi: Deep & Deep Publications.
- Woodhull, A,"Private investigation: Strategies and techniques", Texas: Thomas Investigations Publications.

Subject Code: HMCS20GE5	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Digital Frauds	Ty	3	0	0	3

Course Objective:

1. To conceptualize the Nature of Fraud
2. To identify financial statement fraud exposures
3. To detect and prevent fraud in e-commerce

Course Outcome:

Students will be able to:

CO1: Classify frauds into various types.

CO2: Establish a management system for detecting and responding to fraud

CO3: Understand the nature of bank frauds committed and the procedure of commission of bank frauds

CO4: Design and evaluate controls to prevent, detect and respond appropriately to corporate fraud and misconduct

CO5: Identify controls that prevent and/or detect fraudulent behavior.

CO6: Detect e-business fraud and take appropriate measures to prevent fraud in e-commerce

Unit I **9Hrs**

Introduction: Fraud introduction and overview - "Standard" fraud types - recent fraud types - The next generation of fraud – Fraud Detection – Fraud opportunities - Countermeasures

Unit II **9Hrs**

Banking Fraud: Banking Concepts - Core Banking Solution - Security mechanisms to secure network and devices – Internet Banking - Mobile banking - Cyber Security Attacks On Banks – Fraud Detection – Fraud opportunities

Unit III **9Hrs**

Corporate Fraud: Nature of Fraud - Elements of crimes of theft and fraud – Role of ethics in fighting fraud – Controlling fraud – fraud risk management – Investigating fraud – Computer fraud and countermeasures

Unit IV **9Hrs**

Financial Fraud: The Origin of Financial Fraud - Treadway to Sarbanes-Oxley - The Sarbanes-Oxley Act - The Audit Committee - Detection and Its Aftermath - Investigating Financial Fraud - Finding the False Numbers - Getting a New Audit Report on the Financial Statements - The Securities and Exchange Commission - The Future of Financial Reporting

Unit V **9Hrs**

Trends in e-commerce & digital fraud: Introduction-Methods of payment fraud - Decoding the methods of online or e-commerce fraud - The financial impact of online or e-commerce fraud - e-commerce fraud prevention capabilities - Use of technology

Total hours: 45

TEXT BOOKS:

- Richard E. Cascarino, Corporate Fraud and Internal Control Workbook: A Framework for Prevention, Wiley, Dec 2012
- Michael R. Young, Financial Fraud Prevention and Detection: Governance and Effective Practices, Wiley, Oct 2013

REFERENCE BOOKS:

- Zabihollah Rezaee, Richard Riley, Financial Statement Fraud: Prevention and Detection, Wiley, 2nd edition, 2009
- Managing the risk of fraud and misconduct by Richard H Girgenti, and Timothy P Hedley, first edition, Mc Graw Hill Education Publication, 09 Mar 2011
- Detecting Accounting Fraud: Analysis and Ethics by Cecil W Jackson, 1st Edition, Pearson Education Publication, 26 Jan 2014
- Anatomy of a fraud investigation by Stephen Pedeault, 1st Edition, John Wiley & Sons Publication, 2010
- Telecom and Network Security: Toll Fraud and Telabuse update by Jan Wilson, 2nd Edition, Telecommunications reports International Publication, 22 April 2010

Subject Code: HMCS20GE6	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Mobile Security and Forensics	Ty	3	0	0	3

Course Objective:

- To know about the basics of mobile security.
- To be familiar with mobile application security techniques.
- To acquire knowledge on current trends

Course Outcome:

Students will be able to:

- Understand the fundamentals of mobile devices
- Learn the evolution of mobile device
- Learn the multiple access techniques like frequency division multiple access, time division multiple access, code division multiple access, space division multiple access
- Understand the Global System for Mobile Communications
- Familiar with mobile application security models
- Discuss the security issues in real time mobile communication

Unit I **9Hrs**

Handheld Devices/Communications: Introduction of handheld devices - History of mobile devices - Evolution of mobile device – Carriers – Spectrum -Communication Topology - **Mobile fundamentals and channels**: Multiple access techniques like Frequency division multiple access (FDMA) - Time division multiple access (TDMA) - Code division multiple access (CDMA) - Space division multiple access (SDMA).

Unit II **9Hrs**

Global System for Mobile Communications: GSM Architecture - Network Aspects in GSM - GSM Frequency Allocation - Authentication and Security- Mobile Computing over Short Message (SMS) - GPRS

Unit III **9Hrs**

Mobile application security: Mobile Malware and App Security - Android Security Model - IOS Security Model - Security Model of the Windows Phone

Unit IV **9Hrs**

Mobile Forensics: Collection of data from various kinds of mobiles – basic models – smart phones – Mobile Forensics Tools

Unit V **9Hrs**

Recent Trends: Introduction to Wi-Fi –WiMAX - ZigBee Networks - Software Defined Radio - UWB Radio - Wireless Adhoc - Network and Mobile Portability - Security issues and challenges in a Wireless network.

Total Hrs:45

TEXT BOOKS:

- Mazliza Othman, “Principles of Mobile Computing & Communications”, SPD publications.
- Rajkamal, “Mobile Computing, 2/e”, Oxford University Press.
- Raksha Shende, “Mobile Computing for beginners”, SPD publications.
- V.Jeyasri Arokiamary,“Mobile Computing”, Technical Publications.
- Kumkum Garg, “Mobile Computing:Theory and Practice”, Pearson Education India.

REFERENCE BOOKS:

- Asoke K Talukder, Hasan Ahmed, Roopa R Yavagal, “Mobile Computing: Technology,Applications and Service Creation”, 2nd edition, Tata McGraw Hill.
- Noureddine Boudriga, “Security of Mobile Communications”, CRC Press.
- Himanshu Dwivedi, Chris Clark and David Thiel, “Mobile ApplicationSecurity”, McGraw-Hill, 1st Edition.

Subject Code: HMCS20GE7	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	IOT Security	Ty	3	0	0	3

Course Objective:

1. To discuss in detail the IoT technology and its applications.
2. To transfer the expertise knowledge needed to design security policies for IoT.
3. To provide leaners with the required knowledge to design IoT systems.

Course Outcome:

Students will be able to:

1. Understand IoT system.
2. Design IoT devices.
3. Develop identity and access management system.
4. Implement IoT privacy.
5. Devise Cloud base IoT devices.
6. Understanding Fog computing.

Module 1: Introduction: **9Hrs**

IoT – IoT ecosystem – Common IoT attacks and countermeasures – Threat modelling an IoT system – Secure Development Life Cycle – Nonfunctional requirements - Challenges of secure IoT development

Module 2: Secure Design of IoT Devices: **9Hrs**

Challenges of secure IoT development – Secure design goals – Defining security policies – Configuring gateway and network security – Managing Keys and Certificates – Managing accounts – Monitoring – Managing compliance and incidents

Module 3: Cryptography and IAM: **9Hrs**

Cryptography role in securing the IoT – Cryptographic key management – Cryptography controls for IoT protocols – Identity life cycle – Authentication credentials – IoT 1AM infrastructure – Authorization and access control

Module 4: IoT privacy and Compliance: **9Hrs**

Privacy challenges in IoT – guide to performing an IoT PIA – Privacy engineering recommendations – IoT compliance – Complex compliance environment

Module 5: Cloud Security for IoT: **9Hrs**

Role of cloud in IoT – Cloud based security for IoT – IoT incidence response – Detection and analysis – IoT forensics

Total hours: 45

Text Book

1. Pethuru Raj Anupama C. Raman, "The Internet of Things Enabling Technologies, Platforms, and Use Cases", Taylor & Francis Group, ISBN: -13: 978-1-4987-6128-4, 2017
2. Sunil Cheruvu Anil Kumar Ned Smith David M. Wheeler, "Demystifying Internet of Things Security", Apress Media LLC, ISBN-13 (pbk): 978-1-4842-2895-1, 2020.
3. Miguel de Sousa ,"Internet of Things with Intel Galileo", Packt Publishing, ISBN 978-1-78217-458-5, 2015.

Reference Books:

1. Aditya Gupta ,"The IoT Hacker's Handbook", Apress Media LLC, ISBN-13: 978-1-4842-4299-5, 2019
2. Neil Wilkins, "Internet of Things: What You Need to Know About IoT, Big Data, Predictive Analytics, Artificial Intelligence, Machine Learning, Cybersecurity, Business Intelligence, Augmented Reality and Our Future", Amazon.com Services LLC, ASIN: B07PG317XS, 2019
3. Amitha Kapoor, "Hands-On Artificial Intelligence for IoT: Expert machine learning and deep learning techniques for developing smarter IoT systems", Packt Publishing, 1st edition ASIN: B07C5YMBZT, 2019.
4. Andrew Minteer, "Analytics for the Internet of Things (IoT)", Packt Publishing, ISBN-13: 978-1787120730, 2017
5. Qusay F. Hassan, Atta ur Rehman Khan, Sajjad A. Madani, "Internet of Things Challenges, Advances, and Applications", Chapman and Hall/CRC, ISBN 9780367111878, 2018
6. Navveen Balani, Rajeev Hathi, "Enterprise IoT: A Definitive Handbook" 4th edition, CreateSpace Independent Publishing Platform, ISBN-13: 978-1535505642, 2016

Subject Code: HMCS20GE8	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Intellectual Property Rights	Ty	3	0	0	3

Course Objective:

- To understand basic Intellectual Property and the need for protection
- To understand Patents and Trade Mark
- To understand Copyright and Industrial Design

Course Outcome:

Students will be able to:

- Learn the concept of intellectual property and the need for protection
- Compare intellectual property vs physical property
- Understand salient features of patents and trade Mark
- Learn cyber squatting and trademark
- Learn copyright and recent amendments
- Learn industrial designs

Unit I **9Hrs**

Intellectual Property and World Trade Organization (WTO): Intellectual Property: Intellectual Property vs physical property – importance of Intellectual Property – introduction of WTO – basic principles of trade system under WTO – Dispute Settlement – Trade policy reviews – Agreeement on TRIPS.

Unit II **9Hrs**

Patents: Patent – History of patent in India – Conditions for grant of patent – Inventions that are not patentable – process and product patent – procedure for grant of patent – e-filing of patent application – temporal and spatial aspect of patent – opposition to grant patent – rights of patentee - patent office and power of Controller – PCT patent - exclusive marketing rights – milestones in India patent law – transfer and infringement of patent rights

Unit III **9Hrs**

Trade Marks: Trademark – Developing a trademark – Conditions for trademark registration – Register of trademarks – Trends in trademark applications – Procedure for trademark application in India – Term of trademark – Assignment and Transmission – Madrid system – Certification trademark – infringement of trademark – remedies against infringement of trademark - Appellate board – cyber squatting and trademark

Unit IV **9Hrs**

Copyright: Copyright - meaning of copyright - ownership of copyright - rights of the owner - term of copyright - Registration of copyright - International copyright – infringement of copyright - remedies against infringement of copyright - copyright amendment act – internet and copyright issues

Unit V **9Hrs**

Industrial Designs -Industrial Designs - registration of designs - copyright in registered designs – conditions for registration of Industrial Designs – procedure for Industrial Designs - terms of Industrial Designs - register of designs - piracy of registered designs - powers and duties of Controller - infringement of Industrial Designs - remedies against infringement of Industrial Designs – Hague agreement - integrated circuit layout – trade secrets

Total Hrs:45

TEXT BOOKS:

- Neeraj Pandey, Khushdeep Dharni, "Intellectual Property Rights", PHI Learning; 1st edition.
- Dr. B.L. Wadehra, "Law relating to patents, trademarks, copyright, design and geographical indications", 5th edition, Universal law Publication.
- Dr. S.R. Myneni, "Law of Intellectual Property", 6th Edition, Asia Law House Publication.

REFERENCE BOOKS:

- David I. Bainbridge, "International Property", 9th Edition, Pearson Education Publication.
- W.R. Cornish, D Llewelyn, "Intellectual Property, Patents, Copyright, trademarks and allied rights", sweet and Maxwell Publication.

Subject Code: HMCS20GE9	Subject Name	Ty/Lb/ ETL	L	T/ S.Lr	P/R	C
	Data Privacy	Ty	3	0	0	3

Subject Description: The course will detail the concepts in privacy.

Goals: The students will be expected to understand the concepts and how personal data should be handled.

Objective: On successful completion of the course the student would have understood the benefits of privacy, handling of PII, Information security requirements in privacy.

Contents

Unit 1 **9Hrs**

Common Principles and Approaches to Information Privacy and Data Protection.
Defining privacy, classes of privacy, historical and social origins of privacy, Personal and Non personal information, Fair Information practices, OECD

Unit 2 **9Hrs**

Privacy and Data protection regulations around the world- Sources of privacy protection, world models of data protection, role of data protection and privacy authorities

Unit 3 **9Hrs**

Sectors of privacy and data protection law- Healthcare sector, financial sector, online privacy, public sector

Unit 4 **9Hrs**

Information security- Safeguarding personal information- Introduction to Information security, Information identification and assessment, Security Infrastructure, security controls, access control, Human resource Security and impact on privacy

Unit 5 **9Hrs**

Online Privacy- Overview of web technologies, privacy considerations for online information

Total Hrs:45

REFERENCES:

Foundations of Information privacy and data protection