MANONMANIAM SUNDARANAR UNIVERSITY
TIRUNELVELI-627 012, TAMILNADU, INDIA

CENTRE FOR INFORMATION TECHNOLOGY AND ENGINEERING

Board of Studies Meeting held on 24.06.2019

Master of Science (M.Sc.) Degree course in CYBER SECURITY

(CBCS-University Department)

Regulations, Scheme and Syllabus

For those who joined from the academic year 2019-20 onwards

Submitted By

Chairman, BOS and Head ,
Centre for Information Technology and Engineering, MSU

To

The Registrar

Manonmaniam Sundaranar University
Tirunelveli – 626 012

MANONMANIAM SUNDARANAR UNIVERSITY
TIRUNELVELI-627 012, TAMILNADU, INDIA

CENTRE FOR INFORMATION TECHNOLOGY AND ENGINEERING

Master of Science (M.Sc.) Degree course in CYBER SECURITY

(CBCS-University Department)

Regulations, Scheme and Syllabus

(For those who joined from the academic year 2019-20 onwards)

A. Regulations

M.Sc. degree programme in Cyber Security exposes students, **Learn a practical skill-set in defeating all online threats**, including - advanced hackers, trackers, malware, zero days, exploit kits, cybercriminals and more.

A1: Duration of the Course:

The M.Sc. programme is a 2 years full time programme spread over two years under semester pattern, with Choice Based Credit System.

A2: Eligibility for Admission:

The minimum eligibility conditions for admission to the M.Sc. programme in Cyber Security are given below.

The candidates who seek admission into the first semester of the M.Sc. programme in Cyber Security course will be required to have passed the Bachelor's degree (B.Sc./ B.C.A./B.E. equivalent) from Manonmaniam Sundaranar University or any other Indian University or equivalent in any one of the following disciplines:

1. Information Technology

2. Information Technology and E-Commerce
3. Computer Science
4. Computer Technology
5. Software Engineering
6. Computer Applications
7. Physics
8. Forensics
9. Electronics
10. Any other discipline with Mathematics or Computer Applications as a subject.

A3. Structure of the Programme:

This Master's programme will consist of:

a. *Core courses* and *Elective courses* which are compulsory for all students;

b. ***I Semester*****:** 4 Core, 1 Elective **and 2 Practical– *II Semester*:** 3 Core, 1 Elective, 1 supportive course **and 2 Practicals – *III Semester*:** 3 Core, 1 Elective , 1 supportive course **and 2 Practicals – *IV Semester*:** 1 Core and 1 Major Project / Dissertation.

c. Supportive courses which students can choose from amongst the courses offered in other departments of this University

d. **Institutional Visits (Field work), Internship and Dissertation/ Project** are compulsory and included as core.

A4: Credit Requirement for the Degree:

The general Regulations of the Choice Based Credit System programme of Manonmaniam Sundaranar University are applicable to this programme. The University requirement for the M.Sc. programme is completion of 90 credits of course work, out of which 5 credits should be through the mini project, 10 credits should be through the 4th semester main project work, remaining 75 credits should be through Core, Elective and Supportive Course papers. A typical theory course (Core/ Elective/ Supportive Course) has 4 credits and lab course weighs 3 credits. No candidate will be eligible for the Degree of Master of Science in Cyber Security, unless the candidate has undergone the prescribed courses of study for a period not less than 4 semesters and has acquired 90 credits and other passing requirements in all subjects of study. The marks, M_i obtained by the student in each subject, *i* shall be multiplied by the credit of that subject, C_i; such marks of all '*n*' subjects are added up and divided by the total credit (90) to obtain the Consolidated Percentage of Marks.

$$\text{Consolidated Percentage of Marks} = \frac{\sum_{i=0}^{n} C_i \times M_i}{\sum_{i=0}^{n} C_i}$$

A5: Attendance Requirement:

A candidate will be permitted to appear for the semester examination only if the candidate keeps not less than 75 percent attendance. The University condonation rules are applicable for those who lack minimum of 75% attendance. The candidates with less than 60% attendance will have to repeat the concerned entire semester.

A6: Assessment

The assessment will comprise Continuous Internal Assessment (CIA) comprising of tests, seminars and assignments carrying a maximum of 25% marks and end-semester Examination carrying a maximum of 75% marks in each theory subject (Core/Elective/Supportive Course). For practical subjects, Mini Project and Major Project, the CIA is carried out for 40% marks and the External Assessment (Final Lab Exam, Lab Report, Viva-Voce for Practical Subjects and Final Project Presentation, Project Report, Viva-Voce for Mini Project and Major Project) is for 60% marks.

Semester examination will be conducted for all subjects of study, at the end of each Semester.

If a Student wants to carry out the final Major project work in 4^{th} semester in an IT company, the student can get permission from the concerned Project Supervisor and Head of the Department after submitting the Acceptance Letter from the IT Company.

A7: Passing Requirements

A candidate who secures not less than 50 percent marks in end-semester examination and not less than 50 percent of the total marks (Continuous Internal Assessment + end-semester examination) in any subject of study will be declared to have passed the subject.

A Candidate who successfully completes the course and satisfies the passing requirements in all the subjects of study and curricular requirements will be declared to have qualified for the award of the Degree.

A8: Classification of successful candidates

The candidates who passed written papers, practical papers and Projects shall be classified as follows. Total Marks secured in written papers, practical papers and Project work altogether put as overall percentage along with the credits.

The classification is as follows,

	Marks Overall %	**Classification**
1.	75% and above with a First attempt Pass in all subjects	I Class with Distinction
2.	i) 75% above from multiple attempts	I Class
	ii) 60% to below 75%	I Class
3.	50% to below 60%	II Class

A9. Power to Modify

The University may from time to time revise, amend or change the regulations, scheme of examinations and syllabus, if found necessary and such amendments, changes shall come into effect from the date prescribed.

The academic year normally begins in July every year and ends in April. These regulations will come into effect from the academic year 2019-20 onwards.

MANONMANIAM SUNDARANAR UNIVERSITY

TIRUNELVELI, TAMILNADU

DEPARTMENT OF CENTRE FOR INFORMATION TECHNOLOGY AND ENGINEERING

The Objective of CITE Department is to create IT manpower catering to the need and expectations of IT Industry capable of making decisions that demonstrate their standing of being an ethical computing professional; Impart Applied communication skills to students in order to promote ideas in IT engineering and technology fields.

Vision

The CITE Department Aims to become a Center of Excellence in Core fields of Information Technology and Engineering with its efficient teaching and innovative research environment that makes knowledgeable and competent professionals who are socially oriented human beings.

Mission

The mission of Information Technology and Engineering Department is to educate students in IT And Engineering fields by providing in state-of-art knowledge IT in order to enable them create and consume information for an Ever Dynamic Information Society in an ethical way.

PROGRAMME OBJECTIVES

PO1: Graduates of the programme will be able communicate to effectively both orally and in writing in a variety of audiences.

PO2: Graduates of the programme will be able to demonstrate critical thinking by analyzing situations and by constructing and selecting solutions to problems.

PO3: Graduates of the programme will be able to understand and appreciate the legal and ethical environment impacting individuals as well as business organizations and have an understanding of the ethical implications of IT legal decisions.

PO4: Graduates of the programme will be able to understand fundamentals and advanced issues of various threats faced by today's cyberinfrastructure.

Specialization of M.Sc Cyber Security Programme:

Core Papers

1. Fundamentals of Cyber Security Domain
    - Cyber Criminology and Cyber Forensics (e-pathshala)
    - Foundations of Information Security
    - Introduction to Hardware, Software, Networks and Databases
    - Introduction to Data Privacy
2. Introduction to Digital forensics and Crimes
    - Cyber frauds in the BFSI sector
    - Introduction to Digital Forensics
    - Cyber Laws and Regulations
    - Internet of Things (TANSCHE)
3. Advanced Cyber Security
    - Advanced Digital Forensics
    - Cryptography And Network Security (TANSCHE)
    - IT Governance, Risk and Compliance
4. Industrial paper
    - Capacity development for risk/disaster management (e-pathshala)

PROGRAM SPECIFIC OUTCOMES

PSO1: Evaluate the computer network and information security needs of an organization. Explain concepts and theories of networking and apply them to various situations, classifying networks, analyzing performance and implementing new technologies.

PSO2: Assess cyber-security risk management policies in order to adequately protect an organization's critical information and assets.

PSO3: Measure the performance of security systems within an enterprise-level information system. Troubleshoot, maintain and update an enterprise-level information security system.

PSO4: Implement continuous network monitoring and provide real-time security solutions.

PSO5: Formulate, update and communicate short- and long-term organizational cyber-security strategies and policies.

PSO6: Explain the concepts of confidentiality, availability and integrity in Information Assurance, including physical, software, devices, policies and people. Analyze these factors in an existing system and design implementations.

PSO7: Analyze and evaluate the cyber security needs of an organization.

PSO8: Manage multiple operating systems, systems software, network services and security. Evaluate and compare systems software and emerging technologies.

PSO9: Effectively communicate technical information verbally, in writing, and in presentations.

PSO10: Implement cyber security solutions. Be able to use cyber-security, information assurance, and cyber/computer forensics software/tools. Design operational and strategic cyber-security strategies and policies.

PEO vs. PO Mapping

	PCO1	PCO2	PCO3	PCO4	PCO5	PCO6	PCO7	PCO8	PCO9	PCO10
PO1 Career Accomplishments	S	S	S	S	S	S	S	S	M	S
PO2 Research	M	L	M	L	M	S	L	M	S	S
PO3 Sustained Learning	S	L	S	L	S	M	L	S	L	S
PO4 Activity Skills	S	M	S	M	L	S	M	M	L	S

S- Strong

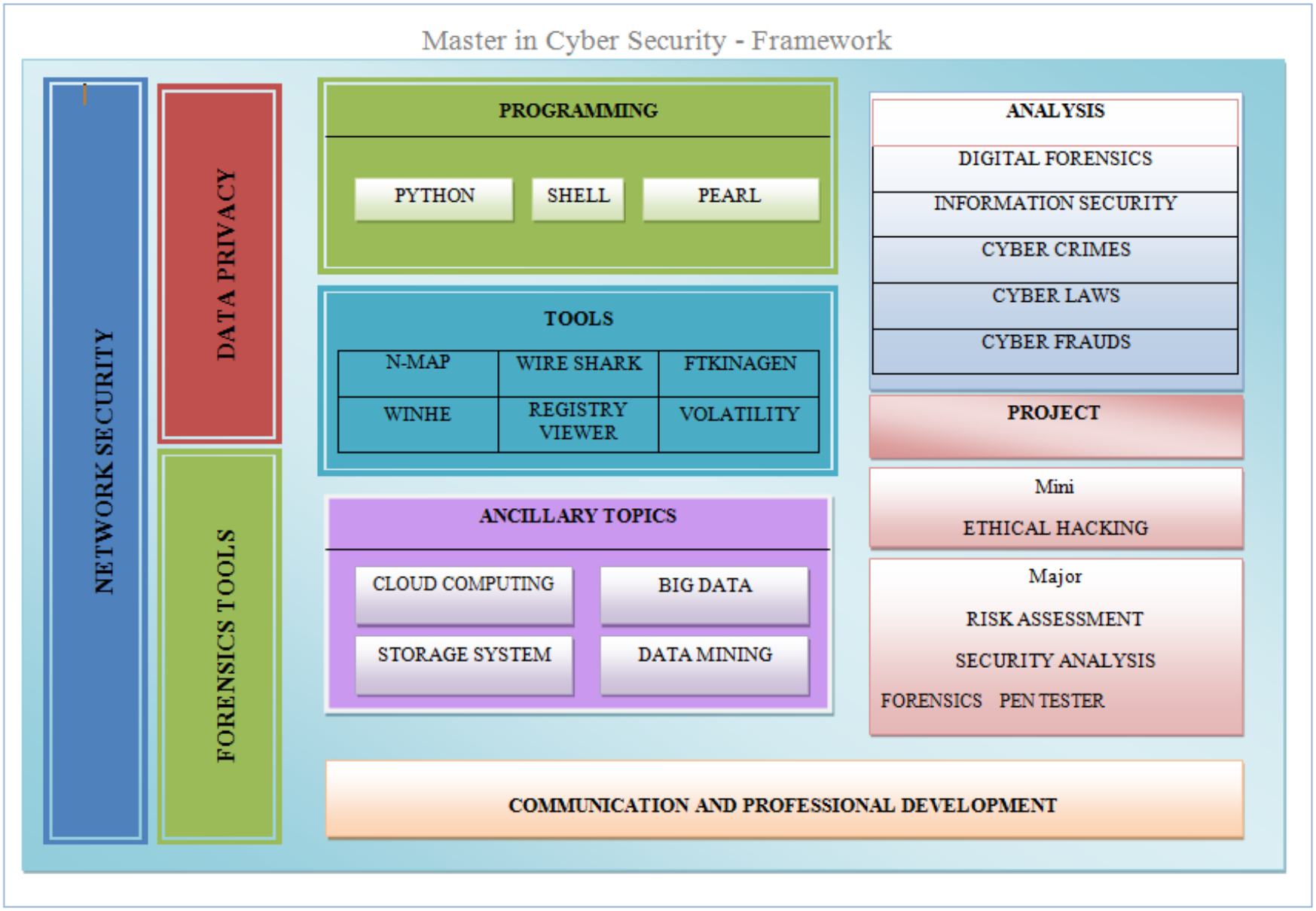
M – Middle

L – Low

GRADUATE ATTRIBUTES

1. Evaluate the computer network and information security needs of an organization. Explain concepts and theories of networking and apply them to various situations, classifying networks, analyzing performance and implementing new technologies.
2. Assess cyber-security risk management policies in order to adequately protect an organization's critical information and assets.
3. Measure the performance of security systems within an enterprise-level information system. Troubleshoot, maintain and update an enterprise-level information security system.
4. Implement continuous network monitoring and provide real-time security solutions.
5. Formulate, update and communicate short- and long-term organizational cyber-security strategies and policies.
6. Explain the concepts of confidentiality, availability and integrity in Information Assurance, including physical, software, devices, policies and people. Analyze these factors in an existing system and design implementations.
7. Analyze and evaluate the cyber security needs of an organization.
8. Manage multiple operating systems, systems software, network services and security. Evaluate and compare systems software and emerging technologies.
9. Effectively communicate technical information verbally, in writing, and in presentations.
10. Implement cyber security solutions. Be able to use cyber-security, information assurance, and cyber/computer forensics software/tools. Design operational and strategic cyber-security strategies and policies.

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
GA1										
GA2										
GA3										
GA4										
GA5										
GA6										
GA7										
GA8										
GA9										
GA10										


Master in Cyber Security - Framework
NETWORK SECURITY
DATA PRIVACY
FORENSICS TOOLS
PROGRAMMING
PYTHON
SHELL
PEARL
TOOLS
N-MAP
WIRE SHARK
FTKINAGEN
WINHE
REGISTRY VIEWER
VOLATILITY
ANCILLARY TOPICS
CLOUD COMPUTING
BIG DATA
STORAGE SYSTEM
DATA MINING
ANALYSIS
DIGITAL FORENSICS
INFORMATION SECURITY
CYBER CRIMES
CYBER LAWS
CYBER FRAUDS
PROJECT
Mini
ETHICAL HACKING
Major
RISK ASSESSMENT
SECURITY ANALYSIS
FORENSICS PEN TESTER
COMMUNICATION AND PROFESSIONAL DEVELOPMENT

Scheduling of Courses for M.Sc. CYBER SECURITY – For Students admitted in the Academic year 2019-20

Semester	Theory						Practical		Special Courses	Credit
1.	Cyber Criminology and Cyber Forensics (e-pathshala) (4)	Foundations of Information Security (4)	Introduction to Hardware, Software, Networks and Databases (4)	Introduction to Data Privacy (4)		Elective 1 (3)	Information Security Lab (2)	Networking and Databases Lab (2)		**23**
2.	Cyber frauds in the BFSI sector (4)	Introduction to Digital Forensics (4)	Cyber Laws and Regulations (4)	/ Internet of Things (TANSCHE) (4)	Elective 2 (3)	Supportive Course 1 (3)	Digital Forensics Lab (2)	Programming in Python Lab (2)		**26**
3.	Advanced Digital Forensics (4)	Cryptography And Network Security (4)	IT Governance, Risk and Compliance (4)	Elective 3 (3)		Supportive Course 2 (3)	Advanced Digital Forensics lab (2)	Advanced Information Security Lab (2)	Internship / Industrial Training (2)	**24**
4.	/ **Capacity development for risk/disaster management (e-pathshala)** (4)						Dissertation / Major Project work (16)			**20**

DISTRIBUTION OF COURSES WITH FOCUS ON SPECIALIZATION

Fundamentals of Cyber Security Domain	**Introduction to Digital forensics and Crimes**	**Advanced Cyber Security**
Program Core		
Cyber Criminology and Cyber Forensics (e-pathshala)	Cyber frauds in the BFSI sector	Advanced Digital Forensics
Foundations of Information Security	**Introduction to Digital Forensics**	Cryptography And Network Security
Introduction to Hardware, Software, Networks and Databases	**Cyber Laws and Regulation**	IT Governance, Risk and Compliance
Introduction to Data Privacy	**Internet of Things**	
Program Electives		
Foundations of Cloud Computing Security	Fundamentals of Blockchains and Crypto-currency	Fundamentals of Research Methods and Statistical Applications
Introduction to Networking	Storage Management and Security	Mobile and Digital Forensics
Data Mining and Warehousing	Big Data Technology	Email, Mobile Devices Security
Mobile and Wireless Security	Android Mobile Application Development	Big Data Security
	IT Governance, Risk and Compliance	Detecting and Investigating Cyber Frauds
	Business Continuity & Disaster Recovery Management Systems	Incident Response

B. Scheme of Examination
M.Sc. Cyber Security (CBCS) - FULL - TIME
(For those who joined from the academic year 2019-2020 onwards)
Duration: Two Years (Four Semesters – 93Credits)

Sem-ester	Title of the Subject	Status*	Hrs / week	Credits	Maximum Marks			Passing Minimum Percentage	
					Inte-rnal	Exte-rnal	Total	External	Total
FIRST SEMESTER									
I	Cyber Criminology and Cyber Forensics (e-pathshala)	C	4	4	25	75	100	50	50
I	Foundations of Information Security	C	4	4	25	75	100	50	50
I	Introduction to Hardware, Software, Networks and Databases	C	4	4	25	75	100	50	50
I	Introduction to Data Privacy	C	4	4	25	75	100	50	50
I	Elective A	E	3	3	25	75	100	50	50
I	Information Security Lab	L	4	2	25	75	100	50	50
I	Networking and Databases Lab	L	4	2	25	75	100	50	50
I Semester Total Credits				**23**					
SECOND SEMESTER									
II	Supportive Course	S	3	3	25	75	100	50	50
II	Cyber frauds in the BFSI sector	C	4	4	25	75	100	50	50
II	Introduction to Digital Forensics	C	4	4	25	75	100	50	50
II	Cyber Laws and Regulations	C	4	4	25	75	100	50	50
II	Internet of Things (TANSCHE)	C	4	4	25	75	100	50	50
II	Elective B	E	3	3	25	75	100	50	50
II	Digital Forensics Lab	L	4	2	25	75	100	50	50
II	Programming in Python Lab	L	4	2	25	75	100	50	50
II Semester Total Credits				**26**					
THIRD SEMESTER									

III	Supportive Course	S	3	3	25	75	100	50	50
III	Internship / Industrial Training * / Mini Project	I	4	2	25	75	100	50	50
III	Advanced Digital Forensics	C	4	4	25	75	100	50	50
III	Cryptography And Network Security (TANSCHE)	C	4	4	25	75	100	50	50
III	IT Governance, Risk and Compliance	C	4	4	25	75	100	50	50
III	Elective C	E	3	3	25	75	100	50	50
III	Advanced Information Security lab	L	4	2	25	75	100	50	50
III	Advanced Digital Forensics lab	L	4	2					
III Semester Total Credits				**24**					
FOURTH SEMESTER									
IV	Capacity development for risk/disaster management (e-pathshala)	C	4	4	25	75	100	50	50
IV	Dissertation / Major Project work	P	6	16	25	75	100	50	50
IV Semester Total Credits				**20**					
OVERALL TOTAL CREDITS				**93**					

Subjects for Electives A									
Sl. No.	Title of the Subject	Status	Hrs/week	Credits	Maximum Marks			Passing Minimum Percentage	
					Inte-rnal	Exte-rnal	Total	External	Total
A1	Foundations of Cloud Computing Security	E	3	3	25	75	100	50	50
A2	Introduction to Networking	E	3	3	25	75	100	50	50
A3	Email, Mobile Devices Security	E	3	3	25	75	100	50	50
A4	Mobile and Wireless Security	E	3	3	25	75	100	50	50
Subjects for Electives B									
B1	Fundamentals of Block chains and Crypto-currency	E	3	3	25	75	100	50	50
B2	Storage Management and Security	E	3	3	25	75	100	50	50
B3	Big Data Technology	E	3	3	25	75	100	50	50
B4	Android Mobile Application Development	E	3	3	25	75	100	50	50
Subjects for Electives C									
C1	Fundamentals of Research Methods and Statistical Applications	E	3	3	25	75	100	50	50
C2	Mobile and Digital Forensics	E	3	3	25	75	100	50	50
C3	Data Mining and Warehousing	E	3	3	25	75	100	50	50
C4	Big Data Security	E	3	3	25	75	100	50	50

MANONMANIAM SUNDARANAR UNIVERSITY

TIRUNELVELI, TAMILNADU

M.Sc CYBER SECURITY DEGREE PROGRAMME

LIST OF CORES

(For The Candidates Admitted From 2019-20 Onwards)

SI. No.	Course code	Course name
1.	NCYCPA	Cyber Criminology and Cyber Forensics (e-pathshala)
2.	NCYC11	Foundations of Information Security
3.	NCYC12	Introduction to Hardware, Software, Networks and Databases
4.	NCYC13	Introduction to Data Privacy
5.	NCYL11	Information Security Lab
6.	NCYL12	Networking and Databases Lab
7.	NCYC21	Cyber frauds in the BFSI sector
8.	NCYC22	Introduction to Digital Forensics
9.	NCYC23	Cyber Laws and Regulations
10.	NCYC24	Internet of Things (TANSCHE)
11.	NCYL21	Digital Forensics Lab
12.	NCYL22	Programming in Python Lab
13.	NCYC31	Advanced Digital Forensics
14.	NCYC32	Cryptography And Network Security (TANSCHE)
15.	NCYC33	IT Governance, Risk and Compliance
16.	NCYP31/NCYI31	Internship / Industrial Training * /Mini Project

17.	NCYL31	Advanced Information Security lab
18.	NCYL32	Advanced Digital Forensics lab
19.	NCYCPB	Capacity development for risk/disaster management (e-pathshala)
20.	NCYP41	Dissertation / Major Project work

PC: Program Core

Core 1	**NCYCPA**-Cyber Criminology and Cyber Forensics (e-pathshala)	Category PC	L 4	P 0	Credit 4

Preamble

Cybercrime, or computer oriented crime, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

Prerequisite

- Nil

Course Outcomes

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

Course Outcomes		Level
CO1	Concepts of Criminology	Understanding
CO2	Apply theoretical concepts to different cybercrimes	Apply
CO3	Cyber Crime – Sociological and Criminological Perspectives	Apply
CO4	Describe various legal responses to cybercrime	Understanding
CO5	Contemporary crime prevention approaches	Apply

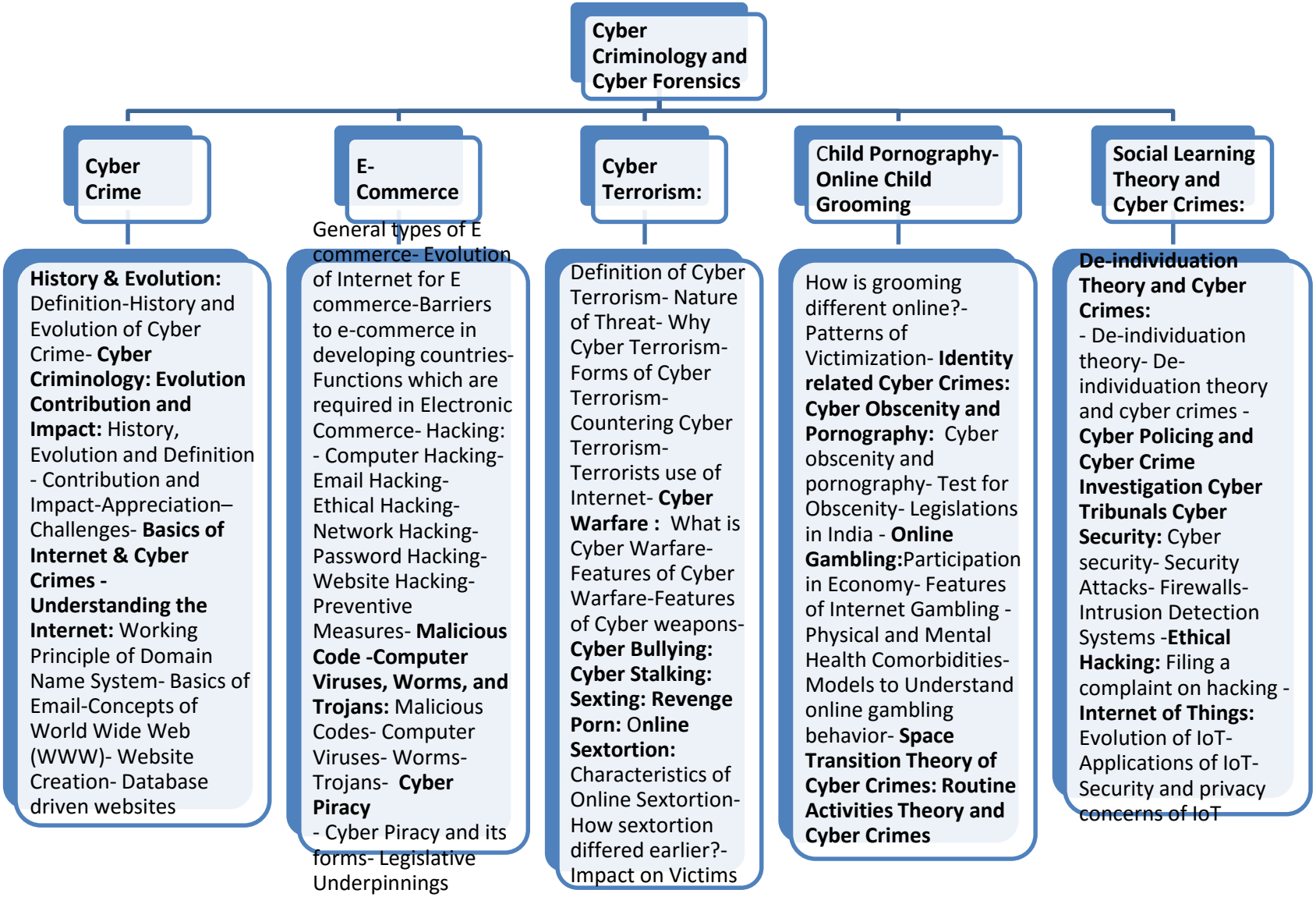
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1		M								M
CO2		S					M			S
CO3			M							
CO4					M					
CO5						L				

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


Cyber Criminology and Cyber Forensics
Cyber Crime
History & Evolution: Definition-History and Evolution of Cyber Crime- Cyber Criminology: Evolution Contribution and Impact: History, Evolution and Definition - Contribution and Impact-Appreciation–Challenges- Basics of Internet & Cyber Crimes - Understanding the Internet: Working Principle of Domain Name System- Basics of Email-Concepts of World Wide Web (WWW)- Website Creation- Database driven websites
E-Commerce
General types of E commerce- Evolution of Internet for E commerce-Barriers to e-commerce in developing countries-Functions which are required in Electronic Commerce- Hacking: - Computer Hacking-Email Hacking-Ethical Hacking-Network Hacking-Password Hacking-Website Hacking-Preventive Measures- Malicious Code -Computer Viruses, Worms, and Trojans: Malicious Codes- Computer Viruses- Worms-Trojans- Cyber Piracy - Cyber Piracy and its forms- Legislative Underpinnings
Cyber Terrorism:
Definition of Cyber Terrorism- Nature of Threat- Why Cyber Terrorism-Forms of Cyber Terrorism-Countering Cyber Terrorism-Terrorists use of Internet- Cyber Warfare : What is Cyber Warfare-Features of Cyber Warfare-Features of Cyber weapons-Cyber Bullying: Cyber Stalking: Sexting: Revenge Porn: Online Sextortion: Characteristics of Online Sextortion-How sextortion differed earlier?-Impact on Victims
Child Pornography-Online Child Grooming
How is grooming different online?-Patterns of Victimization- Identity related Cyber Crimes: Cyber Obscenity and Pornography: Cyber obscenity and pornography- Test for Obscenity- Legislations in India - Online Gambling:Participation in Economy- Features of Internet Gambling - Physical and Mental Health Comorbidities-Models to Understand online gambling behavior- Space Transition Theory of Cyber Crimes: Routine Activities Theory and Cyber Crimes
Social Learning Theory and Cyber Crimes:
De-individuation Theory and Cyber Crimes: - De-individuation theory- De-individuation theory and cyber crimes - Cyber Policing and Cyber Crime Investigation Cyber Tribunals Cyber Security: Cyber security- Security Attacks- Firewalls-Intrusion Detection Systems -Ethical Hacking: Filing a complaint on hacking - Internet of Things: Evolution of IoT-Applications of IoT-Security and privacy concerns of IoT

Syllabus

Unit 1: Cyber Crime: History & Evolution: Definition-History and Evolution of Cyber Crime- **Cyber Criminology: Evolution Contribution and Impact:** History, Evolution and Definition - Contribution and Impact-Appreciation– Challenges- **Basics of Internet & Cyber Crimes - Understanding the Internet:** Working Principle of Domain Name System- Basics of Email-Concepts of World Wide Web (WWW)- Website Creation- Database driven websites **(12hrs)**

Unit 2: E-Commerce: General types of E commerce- Evolution of Internet for E commerce- Barriers to e-commerce in developing countries- Functions which are required in Electronic Commerce- Hacking: - Computer Hacking- Email Hacking- Ethical Hacking- Network Hacking- Password Hacking- Website Hacking- Preventive Measures- **Malicious Code -Computer Viruses, Worms, and Trojans:** Malicious Codes- Computer Viruses- Worms- Trojans- **Cyber Piracy** - Cyber Piracy and its forms- Legislative Underpinnings **(14hrs)**

Unit 3: Cyber Terrorism: Definition of Cyber Terrorism- Nature of Threat- Why Cyber Terrorism- Forms of Cyber Terrorism- Countering Cyber Terrorism- Terrorists use of Internet- **Cyber Warfare :** What is Cyber Warfare- Features of Cyber Warfare-Features of Cyber weapons- **Cyber Bullying: Cyber Stalking: Sexting: Revenge Porn:** O**nline Sextortion:** Characteristics of Online Sextortion- How sextortion differed earlier?- Impact on Victims **(10hrs)**

Unit 4: **Child Pornography- Online Child Grooming** - How is grooming different online?- Patterns of Victimization- **Identity related Cyber Crimes: Cyber Obscenity and Pornography:** Cyber obscenity and pornography- Test for Obscenity- Legislations in India - **Online Gambling:**Participation in Economy- Features of Internet Gambling - Physical and Mental Health Comorbidities- Models to Understand online gambling behavior- **Space Transition Theory of Cyber Crimes: Routine Activities Theory and Cyber Crimes(12hrs)**

Unit 5: **Social Learning Theory and Cyber Crimes: De-individuation Theory and Cyber Crimes:** De-individuation theory- De-individuation theory and cyber crimes - **Cyber Policing and Cyber Crime Investigation Cyber Tribunals Cyber Security:** Cyber security- Security Attacks- Firewalls-Intrusion Detection Systems -**Ethical Hacking:** Filing a complaint on hacking - **Internet of Things:** Evolution of IoT- Applications of IoT- Security and privacy concerns of IoT **(12hrs)**

TOTAL (60hrs)

Textbook

https://epgp.inflibnet.ac.in/ahl.php?csrno=1608

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1.	**Cyber Crime:**	
1.1	**: History & Evolution:** Definition-History and Evolution of Cyber Crime- **Cyber Criminology:**	2
1.2	**Evolution Contribution and Impact:** History, Evolution and Definition	1
1.3	- Contribution and Impact-Appreciation– Challenges-	1
1.4	**Basics of Internet & Cyber Crimes - Understanding the Internet:** Working Principle of Domain Name System-	3
1.5	Basics of Email-Concepts of World Wide Web (WWW)- Website Creation-Database driven websites	3
2.	**E-Commerce:**	
2.1	General types of E commerce- Evolution of Internet for E commerce-Barriers to e-commerce in developing countries-	2
2.2	Functions which are required in Electronic Commerce- Hacking: - Computer	1
2.3	Hacking- Email Hacking- Ethical Hacking- Network Hacking- Password Hacking-	1
2.4	Website Hacking- Preventive Measures- **Malicious Code -Computer**	1
2.5	**Viruses, Worms, and Trojans:** Malicious Codes- Computer Viruses- Worms-Trojans- s	1
2.6	**Cyber Piracy** - Cyber Piracy and its forms- Legislative Underpinning	1
3.	**Cyber Terrorism:** Definition of Cyber Terrorism- Nature of Threat- Why Cyber Terrorism-	
3.1	Forms of Cyber Terrorism- Countering Cyber Terrorism- Terrorists use of Internet-	1
3.2	**Cyber Warfare :** What is Cyber Warfare- Features of Cyber Warfare-Features of Cyber weapons-	1
3.3	**Cyber Bullying:Cyber Stalking:Sexting:Revenge Porn:** O**nline Sextortion:**	1
3.4	Characteristics of Online Sextortion- How sextortion differed earlier?- Impact on Victims	1
4.	C**hild Pornography- Online Child Grooming**	
4.1	How is grooming different online?- Patterns of Victimization- **Identity related Cyber Crimes:**	1
4.2	**Cyber Obscenity and Pornography:** Cyber obscenity and pornography-	1
4.3	Test for Obscenity- Legislations in India - **Online Gambling:**P	2
4.4	articipation in Economy- Features of Internet Gambling - Physical and Mental Health Comorbidities **Activities Theory and Cyber Crimes**	1
4.5	- Models to Understand online gambling behavior- **Space Transition Theory of Cyber Crimes: Routine**	2
5.	**Social Learning Theory and Cyber Crimes:**	
5.1	**De-individuation Theory and Cyber Crime:** De-individuation theory- De-individuation theory and cyber crimes	2
5.2	**Cyber Policing and Cyber Crime Investigation Cyber Tribunals**	1
5.3	**Cyber Security:** Cyber security- Security Attacks- Firewalls-Intrusion Detection Systems	2
5.4	**Ethical Hacking:** Filing a complaint on hacking - **Internet of Things:** Evolution of IoT- Applications of IoT- Security and privacy concerns of IoT	1

Core 2	**NCYC12-Foundations of Information Security**	Category	L	P	Credit
		PC	4	0	4

Preamble

The module provides an overview over several foundational areas in information security. The core of the module is given over to a rigorous discussion of security models and their relation to access control models with selected issues in identification and authentication and their required trust and reputation models also covered.

Prerequisite

- Basic Computer Technology Security

Course Outcomes

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

Course Outcomes		Level
CO1	Understand the conceptual foundation of information security awareness.	Understanding
CO2	Analysis the risk events, treatment plans, assessment	Understanding
CO3	Detail evaluation of information classification, roles and responsibilities	Apply
CO4	Examining the access controls, monitoring, management and review process	Apply
CO5	Study the physical and logical perimeters of information assets and its security.	Apply

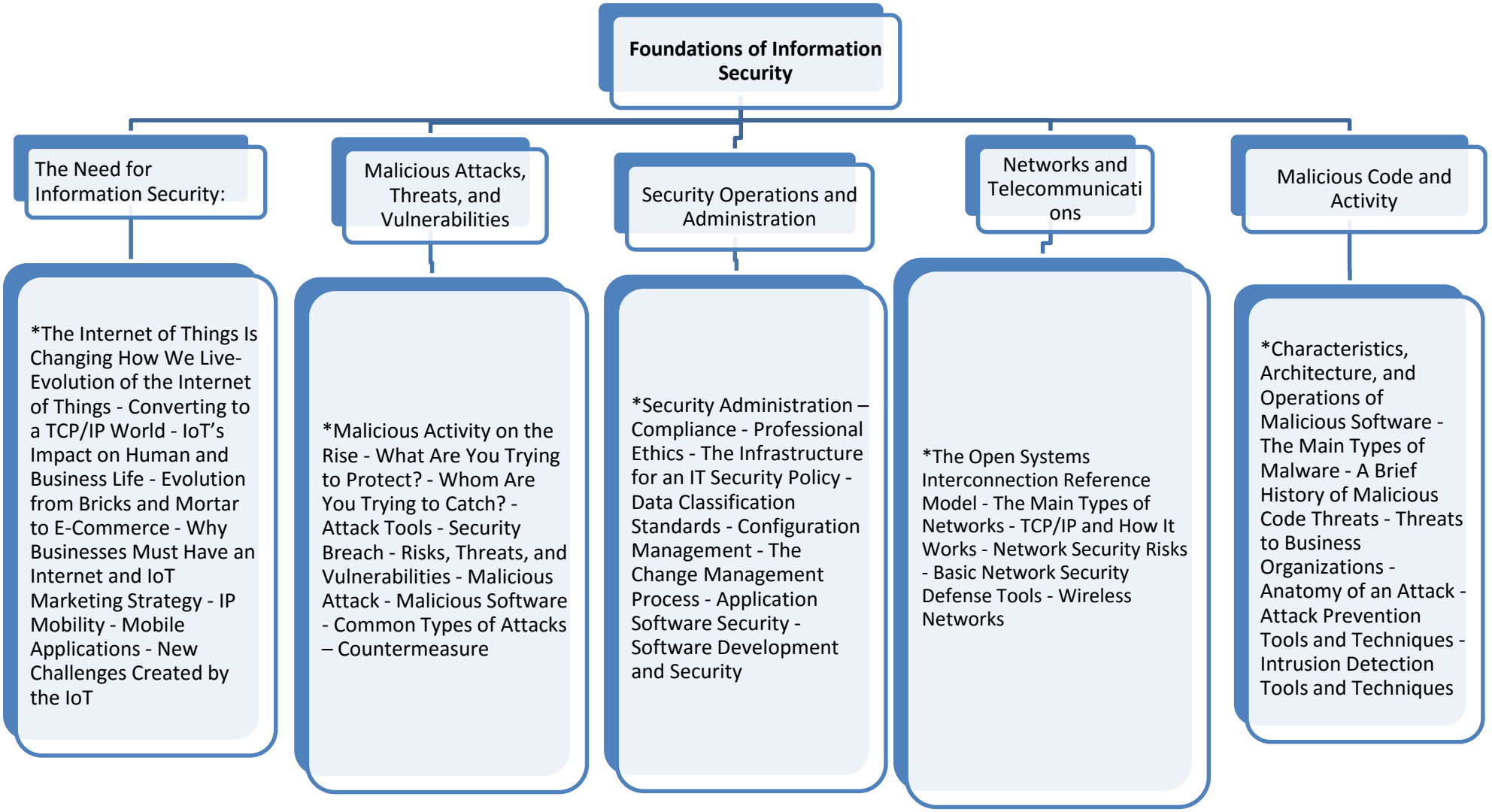
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	M									
CO2		M								
CO3	M						M			
CO4			M		S			M		
CO5										M

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


Foundations of Information Security
The Need for Information Security:
Malicious Attacks, Threats, and Vulnerabilities
Security Operations and Administration
Networks and Telecommunications
Malicious Code and Activity
*The Internet of Things Is Changing How We Live- Evolution of the Internet of Things - Converting to a TCP/IP World - IoT's Impact on Human and Business Life - Evolution from Bricks and Mortar to E-Commerce - Why Businesses Must Have an Internet and IoT Marketing Strategy - IP Mobility - Mobile Applications - New Challenges Created by the IoT
*Malicious Activity on the Rise - What Are You Trying to Protect? - Whom Are You Trying to Catch? - Attack Tools - Security Breach - Risks, Threats, and Vulnerabilities - Malicious Attack - Malicious Software - Common Types of Attacks – Countermeasure
*Security Administration – Compliance - Professional Ethics - The Infrastructure for an IT Security Policy - Data Classification Standards - Configuration Management - The Change Management Process - Application Software Security - Software Development and Security
*The Open Systems Interconnection Reference Model - The Main Types of Networks - TCP/IP and How It Works - Network Security Risks - Basic Network Security Defense Tools - Wireless Networks
*Characteristics, Architecture, and Operations of Malicious Software - The Main Types of Malware - A Brief History of Malicious Code Threats - Threats to Business Organizations - Anatomy of an Attack - Attack Prevention Tools and Techniques - Intrusion Detection Tools and Techniques

Syllabus

Unit 1: The Need for Information Security: The Internet of Things Is Changing How We Live-Evolution of the Internet of Things - Converting to a TCP/IP World - IoT's Impact on Human and Business Life - Evolution from Bricks and Mortar to E-Commerce - Why Businesses Must Have an Internet and IoT Marketing Strategy - IP Mobility - Mobile Applications - New Challenges Created by the IoT **(13hrs)**

Unit 2: Malicious Attacks, Threats, and Vulnerabilities-Malicious Activity on the Rise - What Are You Trying to Protect? - Whom Are You Trying to Catch? - Attack Tools - Security Breach - Risks, Threats, and Vulnerabilities - Malicious Attack - Malicious Software - Common Types of Attacks – Countermeasure **(11hrs)**

Unit 3: Security Operations and Administration-Security Administration – Compliance - Professional Ethics - The Infrastructure for an IT Security Policy - Data Classification Standards - Configuration Management - The Change Management Process - Application Software Security - Software Development and Security **(12hrs)**

Unit 4: Networks and Telecommunications-The Open Systems Interconnection Reference Model - The Main Types of Networks - TCP/IP and How It Works - Network Security Risks - Basic Network Security Defense Tools - Wireless Networks **(11hrs)**

Unit 5: Malicious Code and Activity-Characteristics, Architecture, and Operations of Malicious Software - The Main Types of Malware - A Brief History of Malicious Code Threats - Threats to Business Organizations - Anatomy of an Attack - Attack Prevention Tools and Techniques - Intrusion Detection Tools and Techniques **(13hrs)**

TOTAL (60Hrs)

Textbook:

1. Fundamentals of information systems security- Dividkim | Michael G.solomon - 3rd edition

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**The Need for Information Security:**	
1.1	The Internet of Things Is Changing How We Live- Evolution of the Internet of Things -	1
1.2	Converting to a TCP/IP World - IoT's Impact on Human and Business Life - Evolution from Bricks and Mortar to E-Commerce -	1
1.3	Policies and procedures to protect information assets – the AAA paradigm Why Businesses Must Have an Internet and IoT Marketing Strategy	3
1.4	- IP Mobility - Mobile Applications - New Challenges Created by the IoT	3
2	**Malicious Attacks, Threats, and Vulnerabilities**	
2.1	Malicious Activity on the Rise - What Are You Trying to Protect? - Whom Are You Trying to Catch?	3
2.2	Attack Tools - Security Breach - Risks, Threats, and Vulnerabilities - Malicious Attack	2
2.3	Malicious Software - Common Types of Attacks – Countermeasure	2
3	**Security Operations and Administration**	
3.1	Compliance - Professional Ethics - The Infrastructure for an IT Security Policy	2
3.2	Data Classification Standards - Configuration Management - The Change Management Process	2
3.3	Application Software Security -	2
3.4	Software Development and Security	3
4	Networks and Telecommunications-	
4.1	The Open Systems Interconnection Reference Model - The Main Types of Networks -	2
4.2	TCP/IP and How It Works - Network Security Risks	2
4.3	Basic Network Security Defense Tools - Wireless Networks	2
5	**Malicious Code and Activity**	
5.1	Architecture, and Operations of Malicious Software - The Main Types of Malware	2
5.2	A Brief History of Malicious Code Threats - Threats to Business Organizations	2
5.3	Anatomy of an Attack - Attack Prevention Tools and Techniques - Intrusion Detection Tools and Techniques	2

Core 3	**NCYC13 -** Introduction to Hardware, Software, Networks and Databases	Category PC	L 4	P 0	Credit 4

Preamble

An information system is the combining of users, technology and processes to complete a specific goal. The network model is a database model conceived as a flexible way of representing objects and their relationships.

Prerequisite

- Database Management

Course Outcomes

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

Course Outcomes		Level
CO1	Learn basic components of information technology	Understanding
CO2	Understand the interface of the components, roles and their difference	Understanding
CO3	Study the back end of the system in database security issues	Apply
CO4	Grasp the knowledge in networking components with its architecture and protocols	Apply
CO5	Know the standards for security in the cloud environment	Learn

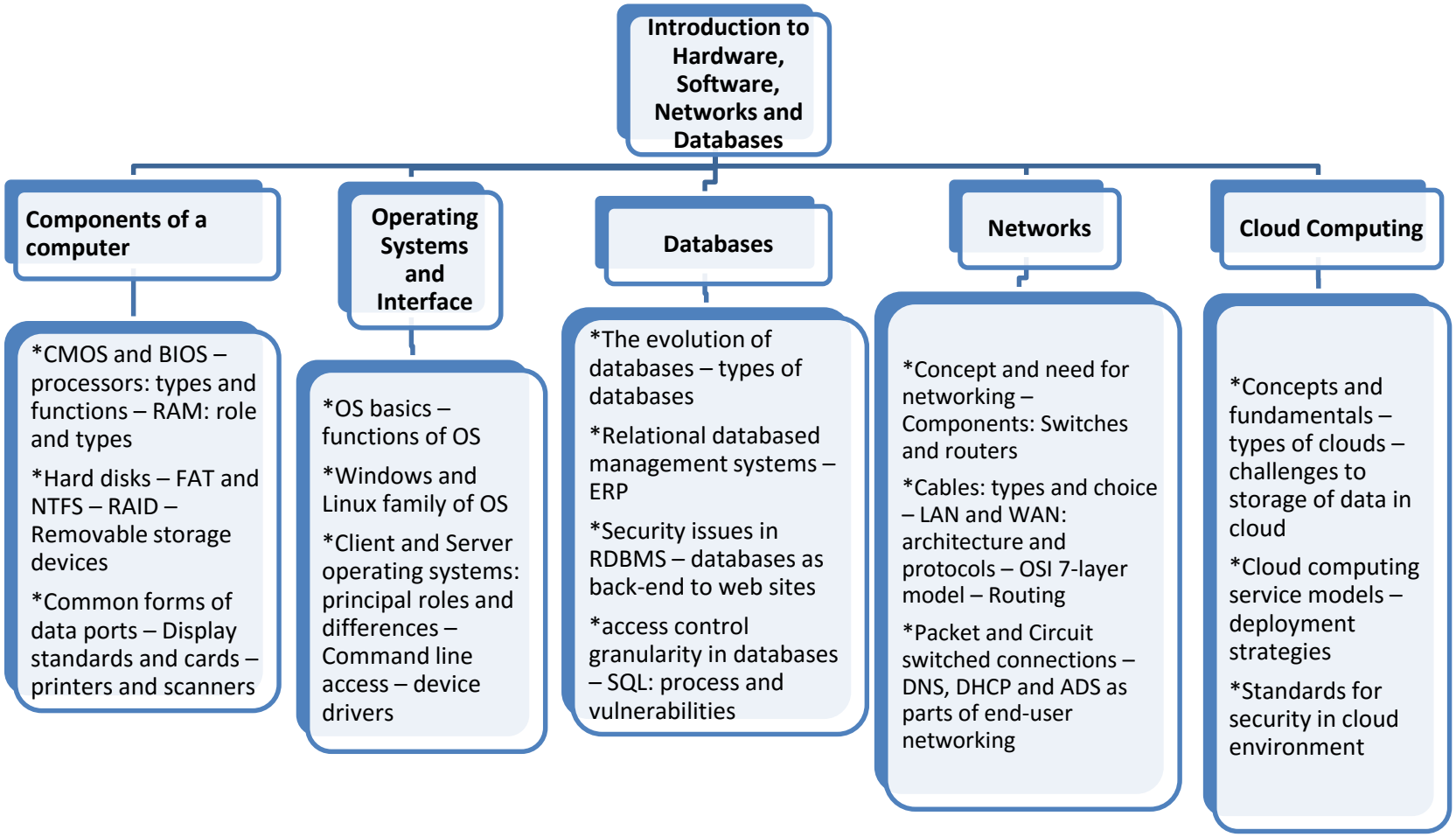
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	L									
CO2							L	S		
CO3			S	L		L				
CO4	S						L			
CO5										L

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


Introduction to Hardware, Software, Networks and Databases
Components of a computer
*CMOS and BIOS – processors: types and functions – RAM: role and types
*Hard disks – FAT and NTFS – RAID – Removable storage devices
*Common forms of data ports – Display standards and cards – printers and scanners
Operating Systems and Interface
*OS basics – functions of OS
*Windows and Linux family of OS
*Client and Server operating systems: principal roles and differences – Command line access – device drivers
Databases
*The evolution of databases – types of databases
*Relational databased management systems – ERP
*Security issues in RDBMS – databases as back-end to web sites
*access control granularity in databases – SQL: process and vulnerabilities
Networks
*Concept and need for networking – Components: Switches and routers
*Cables: types and choice – LAN and WAN: architecture and protocols – OSI 7-layer model – Routing
*Packet and Circuit switched connections – DNS, DHCP and ADS as parts of end-user networking
Cloud Computing
*Concepts and fundamentals – types of clouds – challenges to storage of data in cloud
*Cloud computing service models – deployment strategies
*Standards for security in cloud environment

Syllabus

Unit-1: Components of a computer – CMOS and BIOS – processors: types and functions – RAM: role and types – Hard disks – FAT and NTFS – RAID – Removable storage devices – Common forms of data ports – Display standards and cards – printers and scanners **(12hrs)**

Unit-2: Operating Systems and Interface OS basics – functions of OS – Windows and Linux family of OS – Client and Server operating systems: principal roles and differences – Command line access – device drivers **(12hrs)**

Unit-3: Databases The evolution of databases – types of databases – relational databased management systems – ERP – security issues in RDBMS – databases as back-end to web sites – access control granularity in databases – SQL: process and vulnerabilities **(13hrs)**

Unit-4: Networks Concept and need for networking – Components: Switches and routers – Cables: types and choice – LAN and WAN: architecture and protocols – OSI 7-layer model – Routing – Packet and Circuit switched connections – DNS, DHCP and ADS as parts of end-user networking **(11hrs)**

Unit-5: Cloud Computing Concepts and fundamentals – types of clouds – challenges to storage of data in cloud - cloud computing service models – deployment strategies – standards for security in cloud environment **(12hrs)**

TOTAL (60Hrs)

Books:

1. Basic of Networking – Prentice Hall (ISBN 8120324897)
2. Introduction to Networking – Prentice Hall (ISBN 8120313860)
3. Computer Networking First Step – Odom Wendell – (ISBN 8129706075)
4. Carl Hamacher V. Zvonko G.V. Safwat G. Z. (2002) Computer organization (5th ed.),Tata McGraw Hill
5. Morris Mano (2007) Computer System Architecture (3rd ed.), Pearson Education
6. Ramez, E. Shamkant, B. Navathe (2008) Fundamentals of database systems (5th ed.), Pearson Education
7. Date, C. J, (2012) An Introduction to Database Systems (8th ed.), Pearson Education

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**Components of a computer**	
1.1	CMOS and BIOS – processors: types and functions – RAM: role and types	2
1.2	Hard disks – FAT and NTFS – RAID – Removable storage devices	2
1.3	Common forms of data ports – Display standards and cards – printers and scanners	3
2	**Operating Systems and Interface**	
2.1	OS basics – functions of OS	3
2.2	Windows and Linux family of OS	2
2.3	Client and Server operating systems: principal roles and differences – Command line access – device drivers	3
3	**Databases**	
3.1	The evolution of databases – types of databases	2
3.2	Relational databased management systems – ERP	2
	Security issues in RDBMS – databases as back-end to web sites	2
	access control granularity in databases – SQL: process and vulnerabilities	3
4	**Networks**	
4.1	Concept and need for networking – Components: Switches and routers	2
4.2	Cables: types and choice – LAN and WAN: architecture and protocols – OSI 7-layer model – Routing	2
4.3	Packet and Circuit switched connections – DNS, DHCP and ADS as parts of end-user networking	2
5	**Cloud Computing**	
5.1	Concepts and fundamentals – types of clouds – challenges to storage of data in cloud	2
5.2	Cloud computing service models – deployment strategies	2
5.3	Standards for security in cloud environment	2

Core 4	**NCYC14 - Introduction to Data Privacy**	Category	L	P	Credit
		PC	4	0	4

Preamble

Data privacy, also called information privacy, is the aspect of information technology (IT) that deals with the ability an organization or individual has to determine what data in a computer system can be shared with third parties.

Prerequisite

- Nil

Course Outcomes

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

Course Outcomes		Level
CO1	Learn online privacy techniques in modern day and also sensitive online information	Understand
CO2	Understand the privacy lifecycle principles and risk management	Understand
CO3	Study the privacy principles of various standard organization	Apply
CO4	Provide the standard web protocols for online privacy	Understand
CO5	Know the sensitive online information and its privacy policies.	Apply

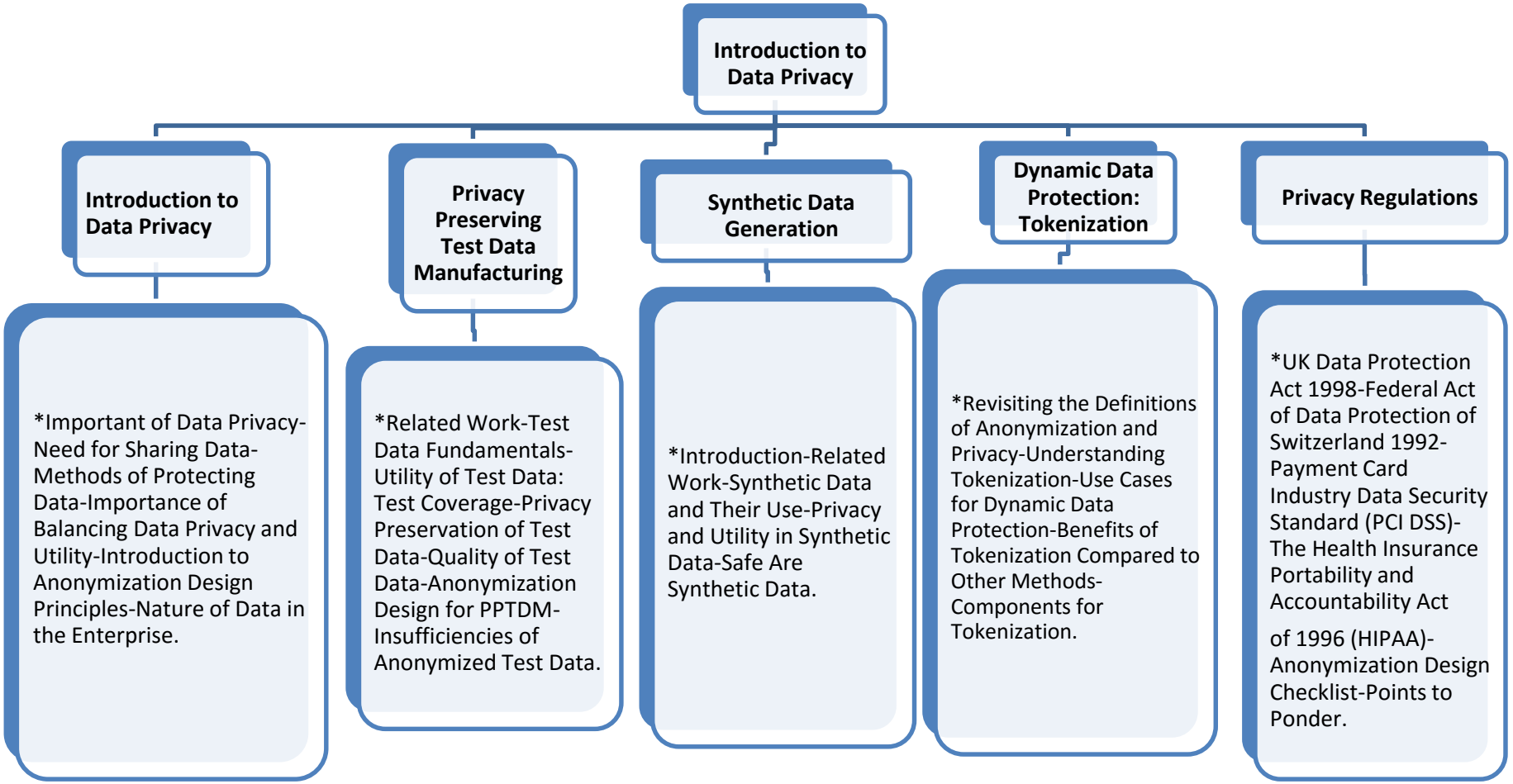
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	M									
CO2		S								
CO3					M					
CO4			L				L			
CO5		M	M							M

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


Introduction to Data Privacy
Introduction to Data Privacy
*Important of Data Privacy-Need for Sharing Data-Methods of Protecting Data-Importance of Balancing Data Privacy and Utility-Introduction to Anonymization Design Principles-Nature of Data in the Enterprise.
Privacy Preserving Test Data Manufacturing
*Related Work-Test Data Fundamentals-Utility of Test Data: Test Coverage-Privacy Preservation of Test Data-Quality of Test Data-Anonymization Design for PPTDM-Insufficiencies of Anonymized Test Data.
Synthetic Data Generation
*Introduction-Related Work-Synthetic Data and Their Use-Privacy and Utility in Synthetic Data-Safe Are Synthetic Data.
Dynamic Data Protection: Tokenization
*Revisiting the Definitions of Anonymization and Privacy-Understanding Tokenization-Use Cases for Dynamic Data Protection-Benefits of Tokenization Compared to Other Methods-Components for Tokenization.
Privacy Regulations
*UK Data Protection Act 1998-Federal Act of Data Protection of Switzerland 1992-Payment Card Industry Data Security Standard (PCI DSS)-The Health Insurance Portability and Accountability Act of 1996 (HIPAA)-Anonymization Design Checklist-Points to Ponder.

Syllabus

Unit 1: Introduction to Data Privacy: Important of Data Privacy-Need for Sharing Data-Methods of Protecting Data-Importance of Balancing Data Privacy and Utility-Introduction to Anonymization Design Principles-Nature of Data in the Enterprise. **(12hrs)**

Unit 2: Privacy Preserving Test Data Manufacturing: Related Work-Test Data Fundamentals-Utility of Test Data: Test Coverage-Privacy Preservation of Test Data-Quality of Test Data-Anonymization Design for PPTDM-Insufficiencies of Anonymized Test Data. **(13hrs)**

Unit 3: Synthetic Data Generation: Introduction-Related Work-Synthetic Data and Their Use-Privacy and Utility in Synthetic Data-Safe Are Synthetic Data. **(11hrs)**

Unit 4: Dynamic Data Protection: Tokenization: Revisiting the Definitions of Anonymization and Privacy-Understanding Tokenization-Use Cases for Dynamic Data Protection-Benefits of Tokenization Compared to Other Methods-Components for Tokenization. **(12hrs)**

Unit 5: Privacy Regulations: UK Data Protection Act 1998-Federal Act of Data Protection of Switzerland 1992-Payment Card Industry Data Security Standard (PCI DSS)- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)- Anonymization Design Checklist-Points to Ponder. **(12hrs)**

TOTAL (60hrs)

Textbook:

Data privacy principles and practice - NatarajVenkataramanan, Ashwin Shriram

References:

1. Cannon, J.C. Privacy: What Developers and IT Professional Should Know. (Addison Wesley, 2004)
2. Cranor, Lorrie Faith. I Didn't Buy it for Myself, in Clare-Marie Karat, Jan O. Blom, and John Karat (ed.), Designing Personalized User Experiences in eCommerce. Kluwer Academic Publishers. 2004.
3. Microsoft Corporation. Privacy Guidelines for Developing Software Products and Services (Microsoft, 2007)

Total=45hrs

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**Introduction to Data Privacy**	
1.1	Important of Data Privacy-Need for Sharing Data-Methods of Protecting Data	2
1.2	Importance of Balancing Data Privacy and Utility	2
1.3	-Introduction to Anonymization Design Principles-Nature of Data in the Enterprise.	3
2	**Privacy Preserving Test Data Manufacturing**	
2.1	Related Work-Test Data Fundamentals-Utility of Test Data:	3
2.2	Test Coverage-Privacy Preservation of Test Data-	2
2.3	Quality of Test Data-Anonymization Design for PPTDM-Insufficiencies of Anonymized Test Data.	3
3	**Synthetic Data Generation:**	
3.1	Introduction-Related Work-Synthetic Data and Their Use	2
3.2	Privacy and Utility in Synthetic Data	2
3.3	Safe Are Synthetic Data.	2
4	**Dynamic Data Protection:**	
4.1	Revisiting the Definitions of Anonymization and Privacy-Understanding Tokenization-	2
4.2	Use Cases for Dynamic Data Protection-Benefits of Tokenization Compared to Other Methods-Components for Tokenization.	2
5	**Privacy Regulations:**	
5.1	UK Data Protection Act 1998-Federal Act of Data Protection of Switzerland 1992-Payment Card Industry Data Security Standard (PCI DSS)-	2
5.2	The Health Insurance Portability and Accountability Act of 1996 (HIPAA)- Anonymization Design Checklist-Points to Ponder.	2

NCYL11	Information Security Lab	L	T	P	C
				4	2

1. User Identity and Access Management
2. Account Authorization
3. Access and Privilege Management
4. System and Network Access Control
5. Operating Systems Access Controls
6. Monitoring Systems Access Controls
7. Intrusion Detection System
8. Event Logging

NCYL12	Networking and Databases Lab	L	T	P	C
				4	2

1. Understanding network commands.
2. Understanding Client – Server Architecture.
3. Understanding the basics of cabling.
4. Understanding Domain controller.
5. Understanding User Controller and assigning the user rights.
6. Sql DDL commands
7. Sql DML commands
8. Sql aggression commands
9. Sql view commands
10. Sql Database commands

Core 5	**NCYC21 -** Cyber frauds in the BFSI sector	Category	L	P	Credit
		PC	4	0	4

Preamble

To know the various cyber attacks and crimes. Cyber crimes are criminal offenses committed via the Internet or otherwise aided by various forms of computer technology, such as the use of online social networks to bully others or sending sexually explicit digital photos with a smart phone.

Prerequisite

- Nil

Course Outcomes

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

Course Outcomes		Level
CO1	Learn the Banking and Financial Services Operations	Understand
CO2	Understand the Computerized CBS	Apply
CO3	Know the Security and Controls	Apply
CO4	Study the Money Laundering Controls	Apply
CO5	Know the Regulatory Frameworks	Apply

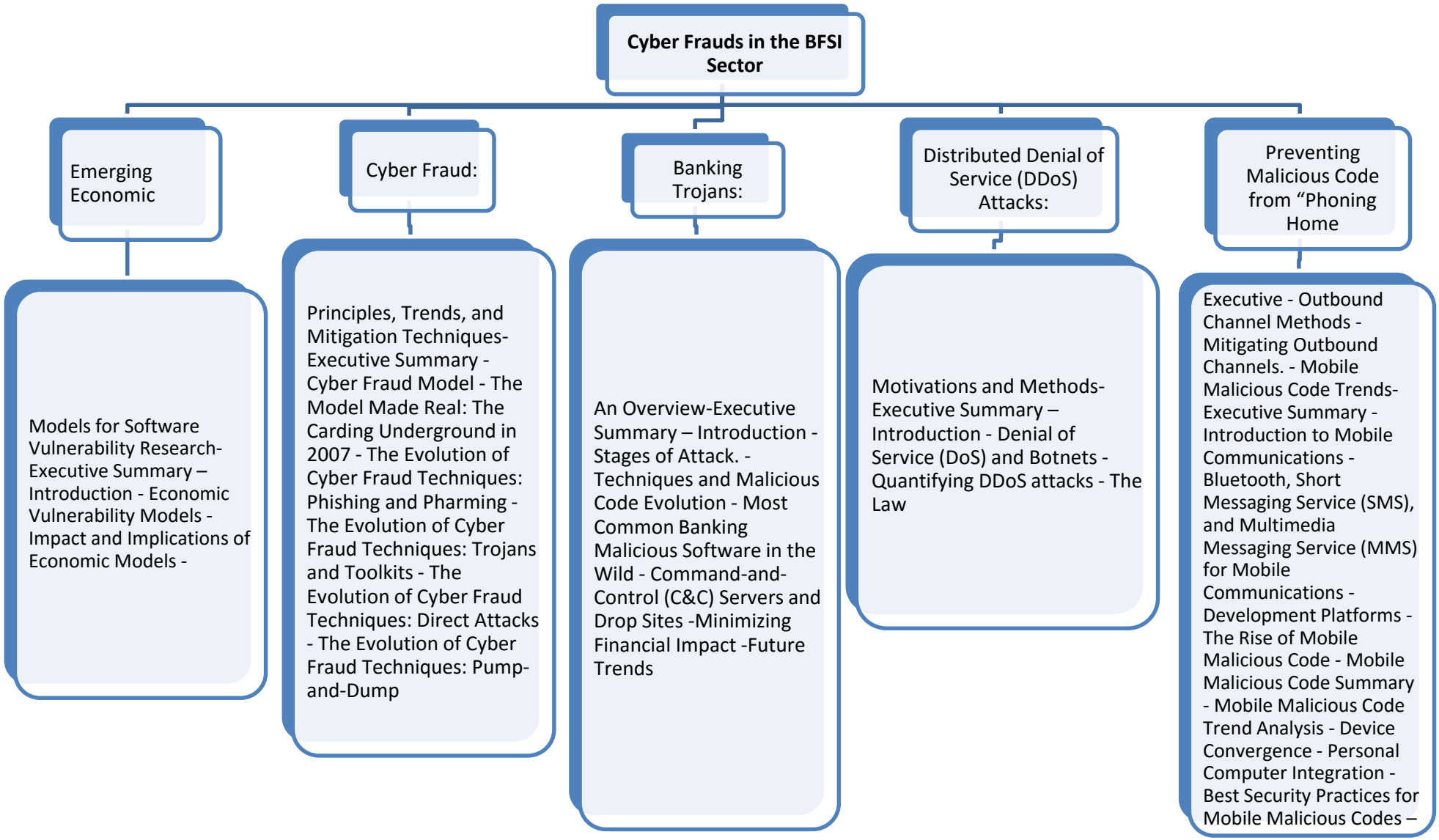
Mapping with Programme Outcomes

COs	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	M									
CO2		S	L							M
CO3				M				S		
CO4	L					L				
CO5										M

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

- Concept Map


Cyber Frauds in the BFSI Sector
Emerging Economic
Models for Software Vulnerability Research- Executive Summary – Introduction - Economic Vulnerability Models - Impact and Implications of Economic Models -
Cyber Fraud:
Principles, Trends, and Mitigation Techniques- Executive Summary - Cyber Fraud Model - The Model Made Real: The Carding Underground in 2007 - The Evolution of Cyber Fraud Techniques: Phishing and Pharming - The Evolution of Cyber Fraud Techniques: Trojans and Toolkits - The Evolution of Cyber Fraud Techniques: Direct Attacks - The Evolution of Cyber Fraud Techniques: Pump-and-Dump
Banking Trojans:
An Overview-Executive Summary – Introduction - Stages of Attack. - Techniques and Malicious Code Evolution - Most Common Banking Malicious Software in the Wild - Command-and-Control (C&C) Servers and Drop Sites -Minimizing Financial Impact -Future Trends
Distributed Denial of Service (DDoS) Attacks:
Motivations and Methods- Executive Summary – Introduction - Denial of Service (DoS) and Botnets - Quantifying DDoS attacks - The Law
Preventing Malicious Code from “Phoning Home
Executive - Outbound Channel Methods - Mitigating Outbound Channels. - Mobile Malicious Code Trends- Executive Summary - Introduction to Mobile Communications - Bluetooth, Short Messaging Service (SMS), and Multimedia Messaging Service (MMS) for Mobile Communications - Development Platforms - The Rise of Mobile Malicious Code - Mobile Malicious Code Summary - Mobile Malicious Code Trend Analysis - Device Convergence - Personal Computer Integration - Best Security Practices for Mobile Malicious Codes –

Syllabus

Unit 1: Emerging Economic Models for Software Vulnerability Research-Executive Summary – Introduction - Economic Vulnerability Models - Impact and Implications of Economic Models. **(10hrs)**

Unit 2: Cyber Fraud: Principles, Trends, and Mitigation Techniques-Executive Summary - Cyber Fraud Model - The Model Made Real: The Carding Underground in 2007 - The Evolution of Cyber Fraud Techniques: Phishing and Pharming - The Evolution of Cyber Fraud Techniques: Trojans and Toolkits - The Evolution of Cyber Fraud Techniques: Direct Attacks - The Evolution of Cyber Fraud Techniques: Pump-and-Dump **(14hrs)**

Unit 3: Banking Trojans: An Overview-Executive Summary – Introduction - Stages of Attack. - Techniques and Malicious Code Evolution - Most Common Banking Malicious Software in the Wild - Command-and-Control (C&C) Servers and Drop Sites -Minimizing Financial Impact - Future Trends **(13hrs)**

Unit 4: Distributed Denial of Service (DDoS) Attacks: Motivations and Methods-Executive Summary – Introduction - Denial of Service (DoS) and Botnets - Quantifying DDoS attacks - The Law - The Torpig Trojan Exposed-The Torpig Group, Part 1: Exploit Server and Master Boot Record Rootkit - The Torpig Group, Part 1: Exploit Server and Master Boot Record Rootkit. **(10hrs)**

Unit 5: Preventing Malicious Code from "Phoning Home"-Executive - Outbound Channel Methods - Mitigating Outbound Channels. - Mobile Malicious Code Trends-Executive Summary - Introduction to Mobile Communications - Bluetooth, Short Messaging Service (SMS), and Multimedia Messaging Service (MMS) for Mobile Communications - Development Platforms - The Rise of Mobile Malicious Code - Mobile Malicious Code Summary - Mobile Malicious Code Trend Analysis - Device Convergence - Personal Computer Integration - Best Security Practices for Mobile Malicious Codes **(14hrs)**

TOTAL (60hrs)

Textbook:

Cyber fraud - Tactics, Techniques, and Procedures:
Kellie, Bryan Kristen ,Dunnesen, Jayson Jean ,Eli Jellenc ,Josh Lincoln, Michael Ligh, Mike La Pilla, Ryan Olson ,Andrew ,Scholnick, Greg Sinclair, Tom Wills, Kimberly Zenz

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**Emerging Economic**	
1.1	Models for Software Vulnerability Research-Executive Summary – Introduction -	3
1.2	- Economic Vulnerability Models -	2
1.3	Impact and Implications of Economic Models	2
2	**Cyber Fraud: Principles, Trends, and Mitigation Techniques-**	
2.1	Executive Summary - Cyber Fraud Model - The Model Made Real: The Carding Underground in 2007 -	2
2.2	The Evolution of Cyber Fraud Techniques: Phishing and Pharming - The Evolution of Cyber Fraud Techniques: Trojans and Toolkits - mp	3
2.3	The Evolution of Cyber Fraud Techniques: Direct Attacks - The Evolution of Cyber Fraud Techniques: Pump-and-Du	2
3	**Banking Trojans:**	
3.1	An Overview-Executive Summary – Introduction - Stages of Attack. - Techniques and Malicious Code Evolution -	2
3.2	Most Common Banking Malicious Software in the Wild - nds	2
3.3	Command-and-Control (C&C) Servers and Drop Sites	2
3.4	-Minimizing Financial Impact -Future Tre	2
4	**Distributed Denial of Service (DDoS)**	
4.1	Attacks: Motivations and Methods-Executive Summary – Introduction -	2
4.2	Denial of Service (DoS) and Botnets - Quantifying DDoS attacks - The Law -	2
4.3	The Torpig Trojan Exposed-The Torpig Group, Part 1: Exploit Server and Master Boot Record Rootkit - The Torpig Group, Part 1: Exploit Server and Master Boot Record Rootkit.	2
5	**Preventing Malicious Code from "Phoning Home**	
5.1	Executive - Outbound Channel Methods - Mitigating Outbound Channels. -	2
5.2	Mobile Malicious Code Trends-Executive Summary - Introduction to Mobile Communications - Bluetooth, Short Messaging Service (SMS),	2
5.3	Multimedia Messaging Service (MMS) for Mobile Communications - Development Platforms - The Rise of Mobile Malicious Code - Mobile Malicious Code Summary - Mobile Malicious Code Trend Analysis - Device Convergence - Personal Computer Integration - Best Security Practices for Mobile Malicious Codes	2

Core 6	**NCYC22 -** Introduction to Digital Forensics	Category	L	P	Credit
		PC	4	0	4

Preamble

Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.

Prerequisite

- Introduction to Data privacy

Course Outcomes

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

Course Outcomes		Level
CO1	Study the different forms in digital forensic investigations and its life cycle	Understand
CO2	Understand the digital data that are used in digital data that are used in digital forensic investigation	Apply
CO3	Learn the various forensic principles propounded by different person that are applied to digital space	Apply
CO4	Study the principles in collecting the digital evidence	Understand
CO5	Learn the best practice guidelines and standards for digital evidence examination	Apply

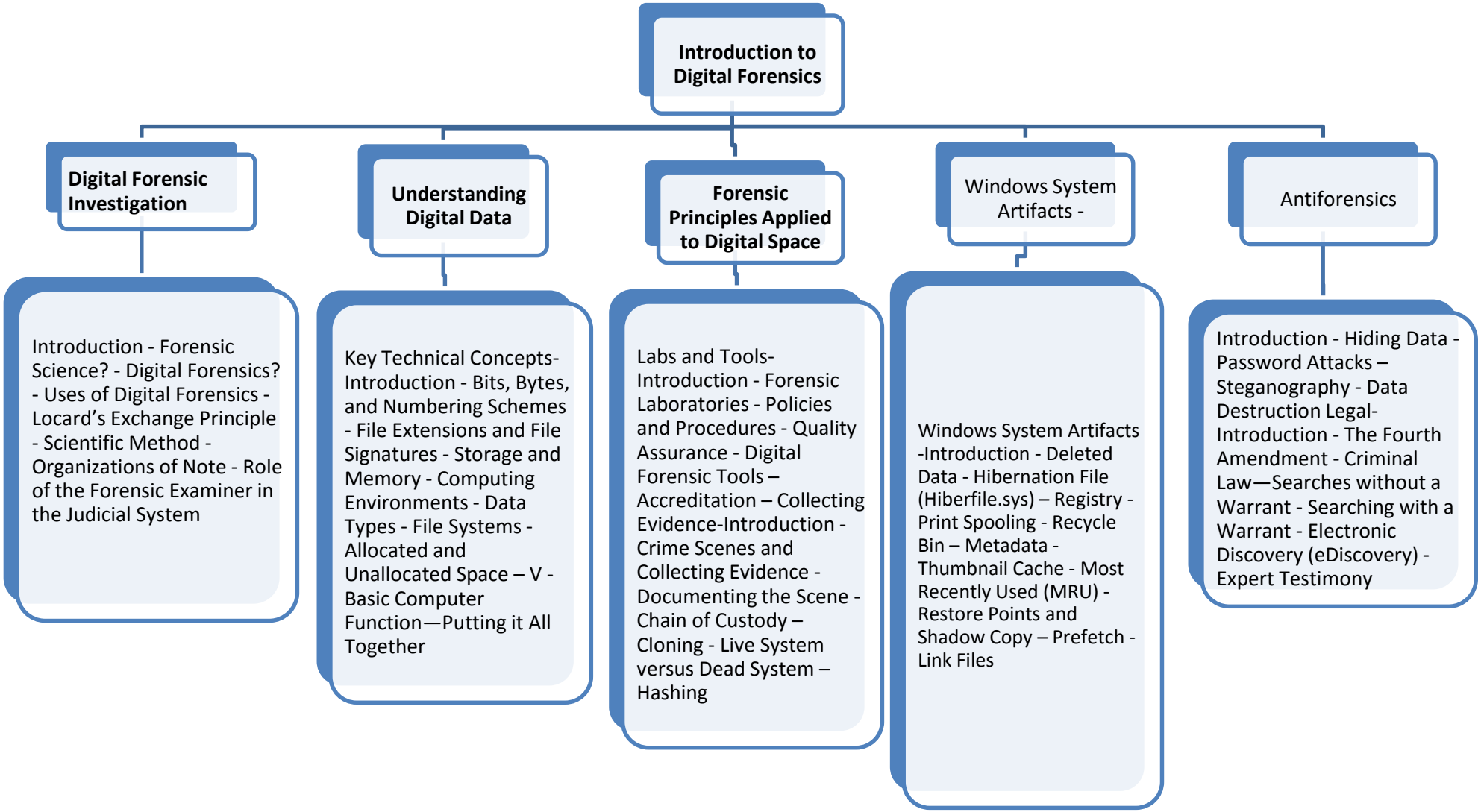
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	M									S
CO2		L								
CO3						M			M	
CO4			M					L		
CO5				M						S

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


Introduction to Digital Forensics
Digital Forensic Investigation
Introduction - Forensic Science? - Digital Forensics? - Uses of Digital Forensics - Locard's Exchange Principle - Scientific Method - Organizations of Note - Role of the Forensic Examiner in the Judicial System
Understanding Digital Data
Key Technical Concepts- Introduction - Bits, Bytes, and Numbering Schemes - File Extensions and File Signatures - Storage and Memory - Computing Environments - Data Types - File Systems - Allocated and Unallocated Space – V - Basic Computer Function—Putting it All Together
Forensic Principles Applied to Digital Space
Labs and Tools- Introduction - Forensic Laboratories - Policies and Procedures - Quality Assurance - Digital Forensic Tools – Accreditation – Collecting Evidence-Introduction - Crime Scenes and Collecting Evidence - Documenting the Scene - Chain of Custody – Cloning - Live System versus Dead System – Hashing
Windows System Artifacts -
Windows System Artifacts -Introduction - Deleted Data - Hibernation File (Hiberfile.sys) – Registry - Print Spooling - Recycle Bin – Metadata - Thumbnail Cache - Most Recently Used (MRU) - Restore Points and Shadow Copy – Prefetch - Link Files
Antiforensics
Introduction - Hiding Data - Password Attacks – Steganography - Data Destruction Legal- Introduction - The Fourth Amendment - Criminal Law—Searches without a Warrant - Searching with a Warrant - Electronic Discovery (eDiscovery) - Expert Testimony

Syllabus

Unit 1: Introduction - Forensic Science? - Digital Forensics? - Uses of Digital Forensics - Locard's Exchange Principle - Scientific Method - Organizations of Note - Role of the Forensic Examiner in the Judicial System **(12hrs)**

Unit 2: Key Technical Concepts-Introduction - Bits, Bytes, and Numbering Schemes - File Extensions and File Signatures - Storage and Memory - Computing Environments - Data Types - File Systems - Allocated and Unallocated Space – V - Basic Computer Function—Putting it All Together **(13hrs)**

Unit 3: Labs and Tools-Introduction - Forensic Laboratories - Policies and Procedures - Quality Assurance - Digital Forensic Tools – Accreditation – Collecting Evidence-Introduction - Crime Scenes and Collecting Evidence - Documenting the Scene - Chain of Custody – Cloning - Live System versus Dead System – Hashing **(13hrs)**

Unit 4: Windows System Artifacts -Introduction - Deleted Data - Hibernation File (Hiberfile.sys) – Registry - Print Spooling - Recycle Bin – Metadata - Thumbnail Cache - Most Recently Used (MRU) - Restore Points and Shadow Copy – Prefetch - Link Files **(10hrs)**

Unit 5: Antiforensics -Introduction - Hiding Data - Password Attacks – Steganography - Data Destruction Legal-Introduction - The Fourth Amendment - Criminal Law—Searches without a Warrant - Searching with a Warrant - Electronic Discovery (eDiscovery) - Expert Testimony **(12hrs)**

Total (60Hrs)

Textbook:

The Basics of Digital Forensics: The primer for getting started in Digital Forensics by John Sammons

References:

1) Computer Forensics, Computer Crime Investigation by John.R.Vacca, 2002, Firewall Media
2) Computer Intrusion Forensics by George Mohay et al, 2003, Artech House
3) Handbook of Digital Forensics by Eoghan Casey, 2010, Elsevier
4) NIST guidelines on digital forensic processes

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**Introduction**	
1.1	- Forensic Science? - Digital Forensics? -	2
1.2	Uses of Digital Forensics - Locard's Exchange Principle - Scientific Method -	3
1.3	Organizations of Note - Role of the Forensic Examiner in the Judicial System	3
2	**Key Technical Concepts**	
2.1	Introduction - Bits, Bytes, and Numbering Schemes	3
2.2	- File Extensions and File Signatures - Storage and Memory - Computing Environments -	2
2.3	Data Types - File Systems - Allocated and Unallocated Space – V - Basic Computer Function—Putting it All Together	3
3	**Labs and Tools-Introduction**	
3.1	Forensic Laboratories - Policies and Procedures - Quality Assurance - custody – Cloning - Live System versus Dead System – Hashing	2
3.2	Digital Forensic Tools – Accreditation – Collecting Evidence- Introduction - f C	2
3.3	Crime Scenes and Collecting Evidence - Documenting the Scene - Chain	2
4	**Windows System**	
4.1	Artifacts -Introduction - Deleted Data	2
4.2	- Hibernation File (Hiberfile.sys) –	2
4.3	Registry - Print Spooling - Recycle Bin – Metadata - Thumbnail Cache - Most Recently Used (MRU) - Restore Points and Shadow Copy – Prefetch - Link Files	2
5	**Antiforensics-**	
5.1	Introduction - Hiding Data - Password Attacks –	2
5.2	Steganography - Data Destruction Legal-Introduction - The Fourth Amendment - Criminal Law—	2
5.3	Searches without a Warrant - Searching with a Warrant - Electronic Discovery (eDiscovery) - Expert Testimony	3

Core 7	**NCYC23 / Cyber Laws and Regulations**	Category	L	P	Credit
		PC	4	0	4

Preamble

A cyber security regulation comprises directives that safeguard information technology and computer systems with the purpose of forcing companies and organizations to protect their systems and information from cyber attacks like viruses, worms, Trojan horses, phishing, denial of service attacks, unauthorized access and control system attacks. There are numerous measures available to prevent cyber attacks.

Prerequisite

- Nil

Course Outcomes

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

Course Outcomes		Level
CO1	Study the cyber laws in different countries	Understand
CO2	Learn the Indian laws related to cyber security	Understand
CO3	Understand the legal and related issues in cyber cases	Understand
CO4	Study the procedure / legal issues	Apply
CO5	Know the basic technology used in cyber law framework.	Apply

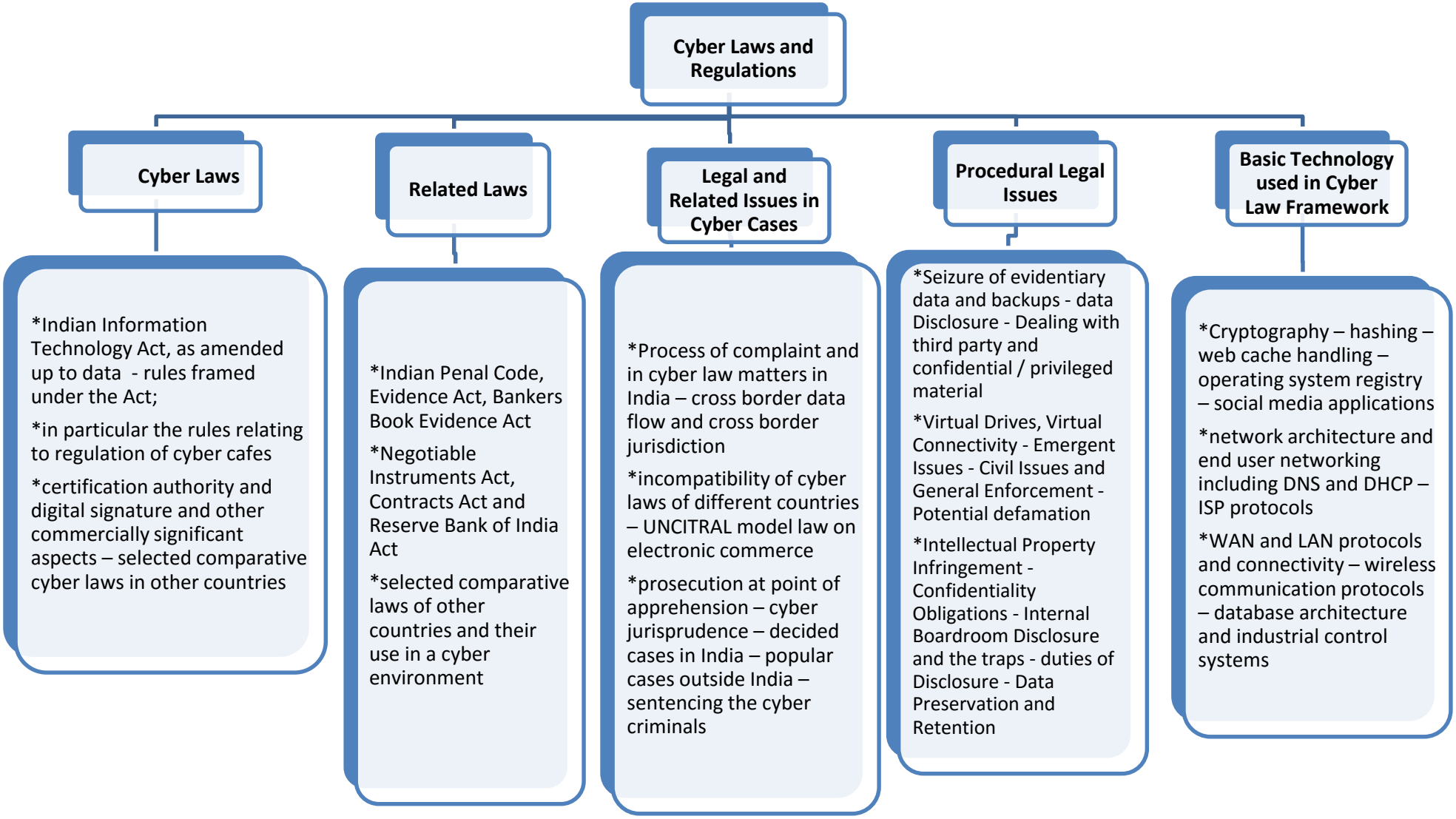
Mapping with Programme Outcomes

COs	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1		M								
CO2			M							
CO3					S					
CO4				S				M		
CO5						M	L			S

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


Cyber Laws and Regulations
Cyber Laws
*Indian Information Technology Act, as amended up to data - rules framed under the Act;
*in particular the rules relating to regulation of cyber cafes
*certification authority and digital signature and other commercially significant aspects – selected comparative cyber laws in other countries
Related Laws
*Indian Penal Code, Evidence Act, Bankers Book Evidence Act
*Negotiable Instruments Act, Contracts Act and Reserve Bank of India Act
*selected comparative laws of other countries and their use in a cyber environment
Legal and Related Issues in Cyber Cases
*Process of complaint and in cyber law matters in India – cross border data flow and cross border jurisdiction
*incompatibility of cyber laws of different countries – UNCITRAL model law on electronic commerce
*prosecution at point of apprehension – cyber jurisprudence – decided cases in India – popular cases outside India – sentencing the cyber criminals
Procedural Legal Issues
*Seizure of evidentiary data and backups - data Disclosure - Dealing with third party and confidential / privileged material
*Virtual Drives, Virtual Connectivity - Emergent Issues - Civil Issues and General Enforcement - Potential defamation
*Intellectual Property Infringement - Confidentiality Obligations - Internal Boardroom Disclosure and the traps - duties of Disclosure - Data Preservation and Retention
Basic Technology used in Cyber Law Framework
*Cryptography – hashing – web cache handling – operating system registry – social media applications
*network architecture and end user networking including DNS and DHCP – ISP protocols
*WAN and LAN protocols and connectivity – wireless communication protocols – database architecture and industrial control systems

Syllabus

Unit-1: Cyber Laws Indian Information Technology Act, as amended up to data - rules framed under the Act; in particular the rules relating to regulation of cyber cafes, certification authority and digital signature and other commercially significant aspects – selected comparative cyber laws in other countries **(12hrs)**

Unit-2: Related Laws Indian Penal Code, Evidence Act, Bankers Book Evidence Act, Negotiable Instruments Act, Contracts Act and Reserve Bank of India Act – selected comparative laws of other countries and their use in a cyber environment **(10hrs)**

Unit-3: Legal and Related Issues in Cyber Cases Process of complaint and in cyber law matters in India – cross border data flow and cross border jurisdiction – incompatibility of cyber laws of different countries – UNCITRAL model law on electronic commerce – prosecution at point of apprehension – cyber jurisprudence – decided cases in India – popular cases outside India – sentencing the cyber criminals **(13hrs)**

Unit-4: Procedural Legal Issues Seizure of evidentiary data and backups - data Disclosure - Dealing with third party and confidential / privileged material - Virtual Drives, Virtual Connectivity - Emergent Issues - Civil Issues and General Enforcement - Potential defamation - Intellectual Property Infringement - Confidentiality Obligations - Internal Boardroom Disclosure and the traps - duties of Disclosure - Data Preservation and Retention **(13hrs)**

Unit-5: Basic Technology used in Cyber Law Framework
Cryptography – hashing – web cache handling – operating system registry – social media applications – network architecture and end user networking including DNS and DHCP – ISP protocols – WAN and LAN protocols and connectivity – wireless communication protocols – database architecture and industrial control systems **(12hrs)**

Total (60hrs)

Books:

1. Cyber law by Nandan kamath, Fifth Edition, Universal law Publication, 01 Jan 2012
2. Intellectual property by Robert P Merges, 3rd Edition, Aspen Publication, 2003
3. Computers , Technology and the new internet laws by Karnika Seth, Updated Edition, Lexis nexis Publication, 01 Jan 2013
4. Legal dimensions of cyber space by S.K.Verma, Volume 1, Ashgate Publication, 01 Jan 2001

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**Cyber Laws**	
1.1	Indian Information Technology Act, as amended up to data - rules framed under the Act;	2
1.2	in particular the rules relating to regulation of cyber cafes	3
1.3	certification authority and digital signature and other commercially significant aspects – selected comparative cyber laws in other countries	3
2	**Related Laws**	
2.1	Indian Penal Code, Evidence Act, Bankers Book Evidence Act	3
2.2	Negotiable Instruments Act, Contracts Act and Reserve Bank of India Act	2
2.3	selected comparative laws of other countries and their use in a cyber environment	3
3	**Legal and Related Issues in Cyber Cases**	
3.1	Process of complaint and in cyber law matters in India – cross border data flow and cross border jurisdiction	2
3.2	incompatibility of cyber laws of different countries – UNCITRAL model law on electronic commerce	2
	prosecution at point of apprehension – cyber jurisprudence – decided cases in India – popular cases outside India – sentencing the cyber criminals	2
4	**Procedural Legal Issues**	
4.1	Seizure of evidentiary data and backups - data Disclosure - Dealing with third party and confidential / privileged material	2
4.2	Virtual Drives, Virtual Connectivity - Emergent Issues - Civil Issues and General Enforcement - Potential defamation	2
4.3	Intellectual Property Infringement - Confidentiality Obligations - Internal Boardroom Disclosure and the traps - duties of Disclosure - Data Preservation and Retention	2
5	**Basic Technology used in Cyber Law Framework**	
5.1	Cryptography – hashing – web cache handling – operating system registry – social media applications	2
5.2	network architecture and end user networking including DNS and DHCP – ISP protocols	2
5.3	WAN and LAN protocols and connectivity – wireless communication protocols – database architecture and industrial control systems	3

Core 8	**NCYC24 - Internet of Things (TANSCHE)**	Category	L	P	Credit
		PC	4	0	4

Preamble

In order to gain knowledge on bases of Internet of Things (IoT), IoT Architecture, and the Protocols related to IoT; and understand the concept of the Web of Thing and the relationship between the IoT and WoT.

Prerequisite

- Network security

Course Outcomes

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

Course Outcomes		Level
CO1	Learn the basics of IoT	Apply
CO2	Study the IoT architecture	Understand
CO3	Understand the IoT protocols	Understand
CO4	Learn the IoT in Web	Apply
CO5	Know the applications	Apply

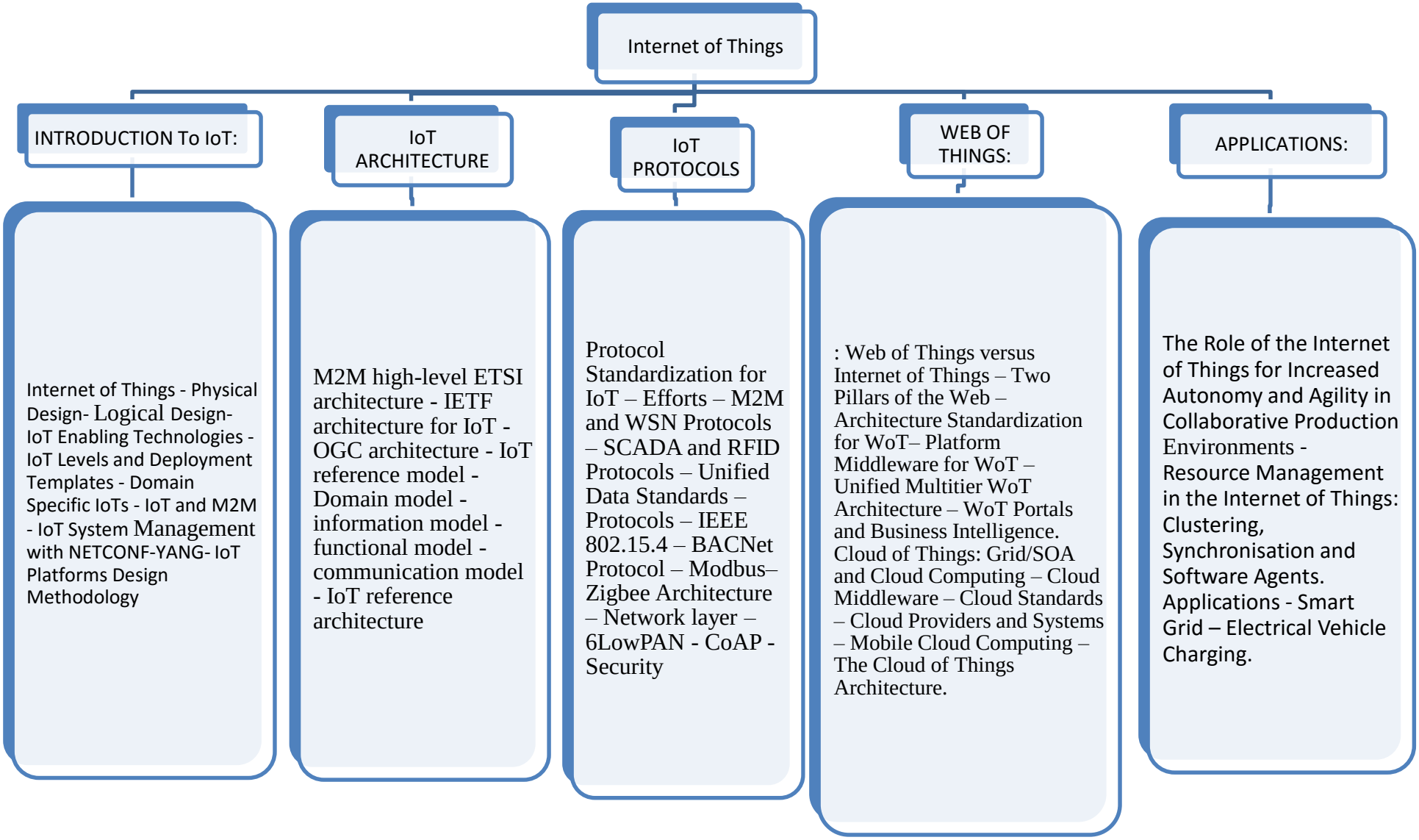
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	S									
CO2	M			M						
CO3							M			
CO4		M						S		
CO5					M	L				L

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


Internet of Things
INTRODUCTION To IoT:
IoT ARCHITECTURE
IoT PROTOCOLS
WEB OF THINGS:
APPLICATIONS:
Internet of Things - Physical Design- Logical Design- IoT Enabling Technologies - IoT Levels and Deployment Templates - Domain Specific IoTs - IoT and M2M - IoT System Management with NETCONF-YANG- IoT Platforms Design Methodology
M2M high-level ETSI architecture - IETF architecture for IoT - OGC architecture - IoT reference model - Domain model - information model - functional model - communication model - IoT reference architecture
Protocol Standardization for IoT – Efforts – M2M and WSN Protocols – SCADA and RFID Protocols – Unified Data Standards – Protocols – IEEE 802.15.4 – BACNet Protocol – Modbus– Zigbee Architecture – Network layer – 6LowPAN - CoAP - Security
: Web of Things versus Internet of Things – Two Pillars of the Web – Architecture Standardization for WoT– Platform Middleware for WoT – Unified Multitier WoT Architecture – WoT Portals and Business Intelligence. Cloud of Things: Grid/SOA and Cloud Computing – Cloud Middleware – Cloud Standards – Cloud Providers and Systems – Mobile Cloud Computing – The Cloud of Things Architecture.
The Role of the Internet of Things for Increased Autonomy and Agility in Collaborative Production Environments - Resource Management in the Internet of Things: Clustering, Synchronisation and Software Agents. Applications - Smart Grid – Electrical Vehicle Charging.

Syllabus

UNIT I INTRODUCTION To IoT: Internet of Things - Physical Design- Logical Design- IoT Enabling Technologies - IoT Levels and Deployment Templates - Domain Specific IoTs - IoT and M2M - IoT System Management with NETCONF-YANG- IoT Platforms Design Methodology. **(12hrs)**

UNIT II IoT ARCHITECTURE: M2M high-level ETSI architecture - IETF architecture for IoT - OGC architecture - IoT reference model - Domain model - information model - functional model - communication model - IoT reference architecture **(10hrs)**

UNIT III IoT PROTOCOLS: Protocol Standardization for IoT – Efforts – M2M and WSN Protocols – SCADA and RFID Protocols – Unified Data Standards – Protocols – IEEE 802.15.4 – BACNet Protocol – Modbus– Zigbee Architecture – Network layer –LowPAN - CoAP - Security **(13hrs)**

UNIT IV WEB OF THINGS: Web of Things versus Internet of Things – Two Pillars of the Web – Architecture Standardization for WoT– Platform Middleware for WoT – Unified Multitier WoT Architecture – WoT Portals and Business Intelligence. Cloud of Things: Grid/SOA and Cloud Computing – Cloud Middleware – Cloud Standards – Cloud Providers and Systems – Mobile Cloud Computing – The Cloud of Things Architecture. **(13hrs)**

UNIT V APPLICATIONS: The Role of the Internet of Things for Increased Autonomy and Agility in Collaborative Production Environments - Resource Management in the Internet of Things: Clustering, Synchronisation and Software Agents. Applications - Smart Grid – Electrical Vehicle Charging. **(12hrs)**

Total (60Hrs)

Text Books

1. Arshdeep Bahga, Vijay Madisetti, “Internet of Things – A hands-on approach”, Universities Press, 2015.
2. Dieter Uckelmann, Mark Harrison, Michahelles, Florian (Eds), “Architecting the Internet of Things”, Springer, 2011.
3. Jan Ho¨ ller, Vlasios Tsiatsis , Catherine Mulligan, Stamatis , Karnouskos, Stefan Avesand. David Boyle, "From Machine-to-Machine to the Internet of Things - Introduction to a New Age of Intelligence", Elsevier, 2014.
4. Networks, Crowds, and Markets: Reasoning About a Highly Connected World - David Easley and Jon Kleinberg, Cambridge University Press - 2010.
5. Olivier Hersent, David Boswarthick, Omar Elloumi , “The Internet of Things – Key applications and Protocols”, Wiley, 2012.

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**INTRODUCTION To IoT:**	
1.1	Internet of Things - Physical Design- Logical Design- IoT Enabling Technologies -.	2
1.2	IoT Levels and Deployment Templates -	2
1.3	Domain Specific IoTs - IoT and M2M logy	2
1.4	- IoT System Management with NETCONF-YANG- IoT Platforms Design Methodo	2
2	**IoT ARCHITECTURE:**	
2.1	M2M high-level ETSI architecture - IETF architecture for IoT - OGC architecture -	2
2.2	IoT reference model - Domain model - information model - functional model	2
2.3	- communication model - IoT reference architecture	2
3	**IoT PROTOCOLS:**	
3.1	Protocol Standardization for IoT – Efforts – M2M and WSN Protocols –	2
3.2	SCADA and RFID Protocols – Unified Data Standards – Protocols – IEEE 802.15.4 –	2
3.3	BACNet Protocol – Modbus– Zigbee Architecture –	2
3.4	Network layer – LowPAN - CoAP - Security	1
4	**WEB OF THINGS:**	
4.1	Web of Things versus Internet of Things – Two Pillars of the Web –	2
4.2	Architecture Standardization for WoT– Platform Middleware for WoT –	2
4.3	Unified Multitier WoT Architecture – WoT Portals and Business Intelligence.	2
	Cloud of Things: Grid/SOA and Cloud Computing – Cloud Middleware –	1
	Cloud Standards – Cloud Providers and Systems – Mobile Cloud Computing – The Cloud of Things Architecture	3
5	**APPLICATIONS:**	
5.1	The Role of the Internet of Things for Increased Autonomy and Agility in Collaborative Production Environments	2
5.2	- Resource Management in the Internet of Things: Clustering, Synchronisation and Software Agents.	2
5.3	Applications - Smart Grid – Electrical Vehicle Charging	2

NCYL21	Digital Forensics Lab	L	T	P	C
				4	2

1. **The Practice of Digital Forensics -** Boot Process – Partitions - File Systems - Procedures
2. **Forensic Hardware and Software tools –** Encase - Cyber Check Suite - Email Tracer – FTK - Open Source Tools
3. **Forensic Imaging Process –Acquiring the Digital Evidence -** Cyber Check Suite – Encase – FTK - Open Source Tools.
4. **Operating System Forensics**
   1. **Windows Forensics** - Windows dates and times - Adjusting for time zone offsets - Recycle Bin and INFO records - Windows Recycle Bin - Link files - Windows folders -Recent folder - Desktop folder - My Documents folder - Send To folder - Temp folders - Favorites folder - Windows Low folders - Cookies folder - History folder - Temporary Internet files - Swap file -Hibernation file - Printing artifacts - Windows volume shadow copy - Windows event logs.
   2. Linux Forensics
   3. MAC forensics
5. Data Loss Prevention software tools and techniques
6. Report Generation and Preparation

NCYL22	Programming in Python Lab	L	T	P	C
				4	2

1. Program using basics of python.
2. Program using conditional statement of python
3. Programs using different data structures in python
4. Programs using functions in python
5. Programs using different packages in python
6. Program for WEBSERVER FINGER PRINTING
7. Program for PORT SCANNING
8. Program for TRANSMISSION OF TRAFFIC IN THE NETWORK
9. Program for WEB APP TESTING

NCYI31/NCYP 31	Internship / Industrial Training / Mini Project	2

1. Industrial Training
2. Online course

Core 9	**NCYC31**/ Advanced Digital Forensics	Category	L	P	Credit
		PC	4	0	4

Preamble

Advanced digital forensics is education intended as an upgrade on basics of digital forensics. Goal is to introduce attender to advanced and more complex usage of digital forensics in real situations.

Prerequisite

- Introduction to Digital Forensics

Course Outcomes

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

Course Outcomes		Level
CO1	Learn the windows & virtual machine forensics	Apply
CO2	Study the forensic analysis of storage media and web	Understand
CO3	Understand the concepts to managing Forensic Data	Understand
CO4	Learn the forensics in memory	Apply
CO5	Know the form of Forensics in cloud and social media	Apply

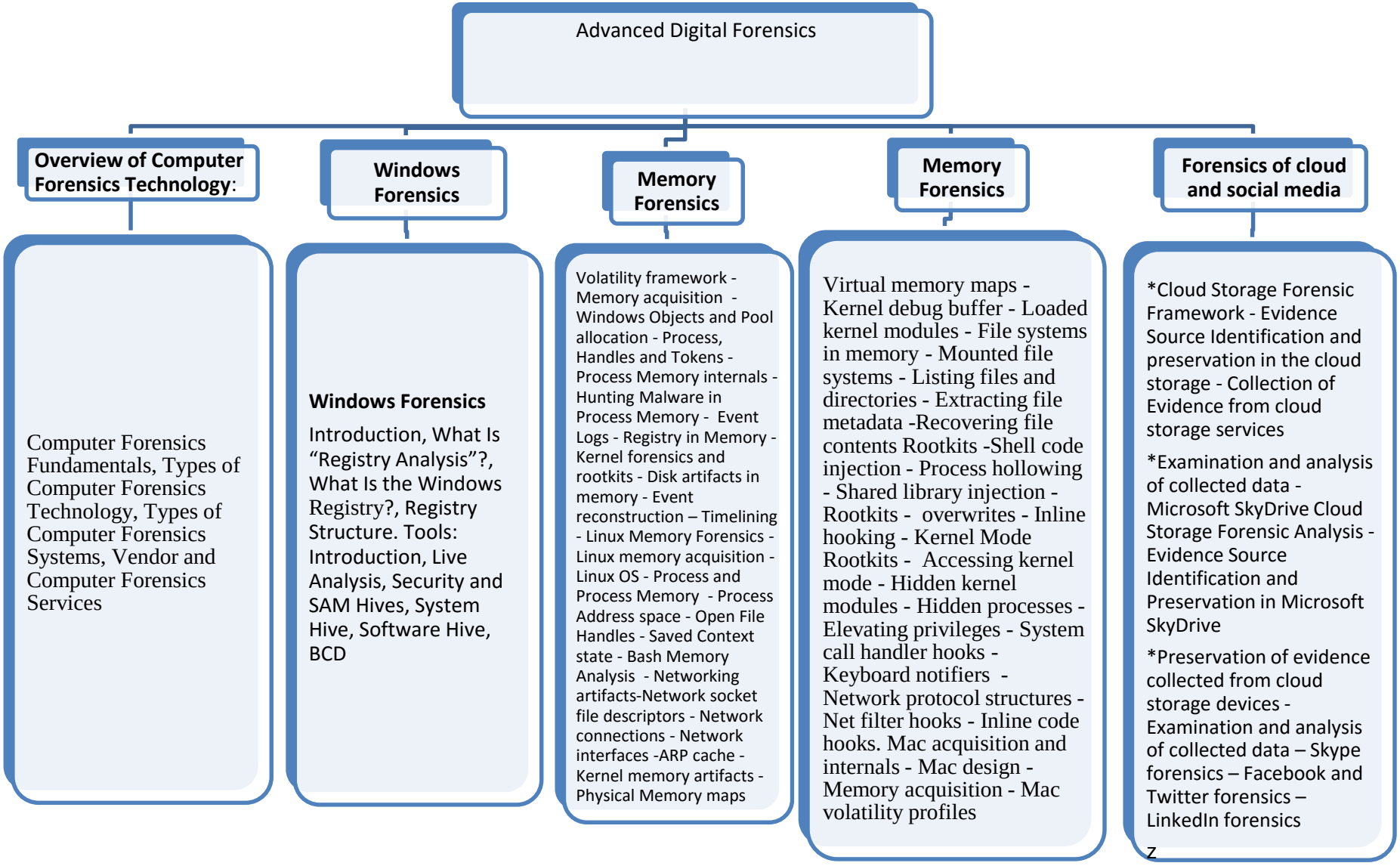
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	S									
CO2	M			M						
CO3							M			
CO4		M						S		
CO5					M	L				L

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map



z

Syllabus

Unit-1: Overview of Computer Forensics Technology: Computer Forensics Fundamentals, Types of Computer Forensics Technology, Types of Computer Forensics Systems, Vendor and Computer Forensics Services **(10hrs)**

Unit-2: Windows Forensics Introduction, What Is "Registry Analysis"?, What Is the Windows Registry?, Registry Structure. Tools: Introduction, Live Analysis, Security and SAM Hives, System Hive, Software Hive, BCD Hive **(10hrs)**

Unit-3: Memory Forensics Volatility framework - Memory acquisition -Windows Objects and Pool allocation - Process, Handles and Tokens - Process Memory internals - Hunting Malware in Process Memory - Event Logs - Registry in Memory - Kernel forensics and rootkits - Disk artifacts in memory - Event reconstruction – Timelining - Linux Memory Forensics - Linux memory acquisition - Linux OS - Process and Process Memory - Process Address space - Open File Handles - Saved Context state - Bash Memory Analysis - Networking artifacts-Network socket file descriptors - Network connections - Network interfaces -ARP cache - Kernel memory artifacts - Physical Memory maps **(14hrs)**

Unit 4: Memory Forensics Virtual memory maps - Kernel debug buffer - Loaded kernel modules - File systems in memory - Mounted file systems - Listing files and directories - Extracting file metadata -Recovering file contents Rootkits -Shell code injection - Process hollowing - Shared library injection - Rootkits - overwrites - Inline hooking - Kernel Mode Rootkits - Accessing kernel mode - Hidden kernel modules - Hidden processes - Elevating privileges - System call handler hooks - Keyboard notifiers - Network protocol structures - Net filter hooks - Inline code hooks. Mac acquisition and internals - Mac design - Memory acquisition - Mac volatility profiles **(14hrs)**

Unit-5: Forensics of cloud and social media Cloud Storage Forensic Framework - Evidence Source Identification and preservation in the cloud storage - Collection of Evidence from cloud storage services - Examination and analysis of collected data - Microsoft SkyDrive Cloud Storage Forensic Analysis - Evidence Source Identification and Preservation in Microsoft SkyDrive - Preservation of evidence collected from cloud storage devices -Examination and analysis of collected data – Skype forensics – Facebook and Twitter forensics – LinkedIn forensics**(12hrs)**

Total (60hrs)

Textbooks:

1. Computer Forensics by John R. Vacca , 2nd Edition
2. Windows Registry analysis by Harlan Carvey, 2010
3. The Art of Memory Forensics by Michael Hale Ligh, Andrew Case, Jamie Levy, Aron Walters
4. Cloud Storage Forensics by Darren Quick, 2014

References:

Malware Forensics Field Guide for Windows System , Camero H.Malin, Eoghan Casey, James M.Acuilina, Curtis W.Rose, Syngress, 2012 Books

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**Overview of Computer Forensics Technology**	
1.1	: Computer Forensics Fundamentals, Types of Computer Forensics Technology,	2
1.2	Types of Computer Forensics Systems, Vendor and Computer Forensics Services	2
2	**Windows Forensics**	
2.1	Introduction, What Is "Registry Analysis"?, What Is the Windows Registry?,	2
2.2	Registry Structure. Tools: Introduction, Live Analysis, Security and SAM Hives,	2
2.3	System Hive, Software Hive, BCD Hive	2
3	**Memory Forensics**	
3.1	Volatility framework - Memory acquisition -Windows Objects and Pool allocation - Process, Handles and Tokens - Process Memory internals - Hunting Malware in Process Memory - Event Logs	2
3.2	Registry in Memory - Kernel forensics and rootkits - Disk artifacts in memory - Event reconstruction – Timelining - Linux Memory Forensics - Linux memory acquisition	2
3.3	Linux OS - Process and Process Memory - Process Address space - Open File Handles - Saved Context state - Bash Memory Analysis - Networking artifacts- Network socket file descriptors - Network connections	2
4	**Memory Forensics**	
4.1	Network interfaces -ARP cache - Kernel memory artifacts - Physical Memory maps - Virtual memory maps - Kernel debug buffer - Loaded kernel modules - File systems in memory - Mounted file systems	2
4.2	- Listing files and directories - Extracting file metadata -Recovering file contents Rootkits -Shell code injection - Process hollowing - Shared library injection - Rootkits - overwrites - Inline hooking - Kernel Mode Rootkits	2
4.3	- Accessing kernel mode - Hidden kernel modules - Hidden processes - Elevating privileges - System call handler hooks - Keyboard notifiers - Network protocol structures - Net filter hooks	1
4.4	Inline code hooks. Mac acquisition and internals - Mac design - Memory acquisition - Mac volatility profiles – Mach – O executable format - Mac memory overview	3
5	**Forensics of cloud and social media**	
5.1	Cloud Storage Forensic Framework - Evidence Source Identification and preservation in the cloud storage - Collection of Evidence from cloud storage services	2
5.2	Examination and analysis of collected data - Microsoft SkyDrive Cloud Storage Forensic Analysis - Evidence Source Identification and Preservation in Microsoft SkyDrive	2
5.3	Preservation of evidence collected from cloud storage devices -Examination and analysis of collected data – Skype forensics – Facebook and Twitter forensics – LinkedIn forensics	2

Core 10	**NCYC32 / CRYPTOGRAPHY AND NETWORK SECURITY**	Category	L	P	Credit
		PC	4	0	4

Preamble

To attain the extensive knowledge on the information security, specifically, network security, software security, cryptography, authentication protocols, and protection of intellectual property, from the various viewpoints of the advanced information security.

Prerequisite

- Network Security

Course Outcomes

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

Course Outcomes		Level
CO1	Understand the concepts in cryptology	Apply
CO2	Know about **Symmetric Encryption and Message Confidentiality**	Understand
CO3	Study the Authentication Applications	Apply
CO4	Learn the IP security	Apply
CO5	Understand the concepts of Digital Rights Management	Understand

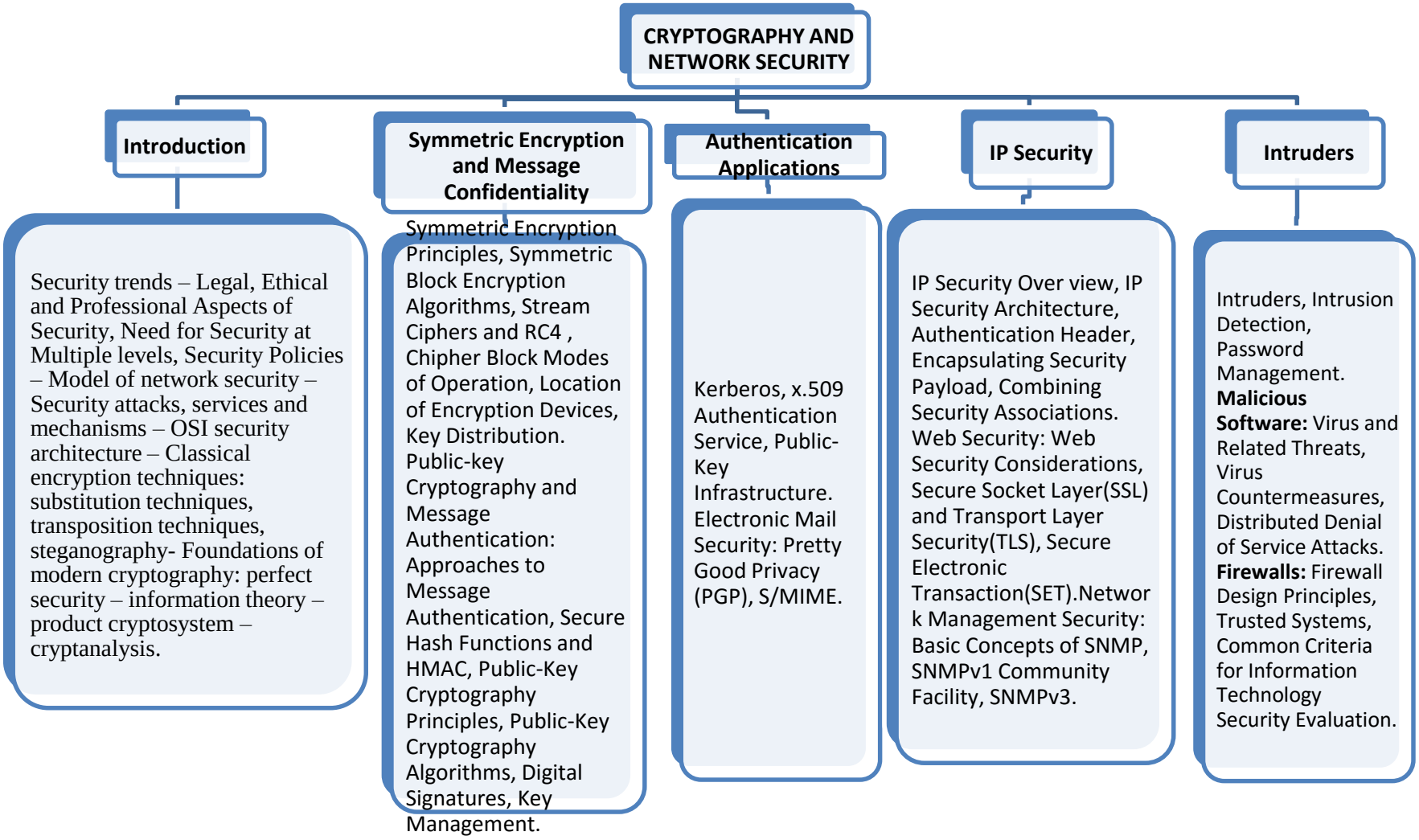
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1					M					
CO2	S		L				M			
CO3			L							M
CO4		M		M		L				
CO5	L						L		M	

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


CRYPTOGRAPHY AND NETWORK SECURITY
Introduction
Security trends – Legal, Ethical and Professional Aspects of Security, Need for Security at Multiple levels, Security Policies – Model of network security – Security attacks, services and mechanisms – OSI security architecture – Classical encryption techniques: substitution techniques, transposition techniques, steganography- Foundations of modern cryptography: perfect security – information theory – product cryptosystem – cryptanalysis.
Symmetric Encryption and Message Confidentiality
Symmetric Encryption Principles, Symmetric Block Encryption Algorithms, Stream Ciphers and RC4 , Chipher Block Modes of Operation, Location of Encryption Devices, Key Distribution. Public-key Cryptography and Message Authentication: Approaches to Message Authentication, Secure Hash Functions and HMAC, Public-Key Cryptography Principles, Public-Key Cryptography Algorithms, Digital Signatures, Key Management.
Authentication Applications
Kerberos, x.509 Authentication Service, Public-Key Infrastructure. Electronic Mail Security: Pretty Good Privacy (PGP), S/MIME.
IP Security
IP Security Over view, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations. Web Security: Web Security Considerations, Secure Socket Layer(SSL) and Transport Layer Security(TLS), Secure Electronic Transaction(SET).Network Management Security: Basic Concepts of SNMP, SNMPv1 Community Facility, SNMPv3.
Intruders
Intruders, Intrusion Detection, Password Management. Malicious Software: Virus and Related Threats, Virus Countermeasures, Distributed Denial of Service Attacks. Firewalls: Firewall Design Principles, Trusted Systems, Common Criteria for Information Technology Security Evaluation.

Syllabus

Unit I Introduction - Security trends – Legal, Ethical and Professional Aspects of Security, Need for Security at Multiple levels, Security Policies – Model of network security – Security attacks, services and mechanisms – OSI security architecture – Classical encryption techniques: substitution techniques, transposition techniques, steganography- Foundations of modern cryptography: perfect security – information theory – product cryptosystem – cryptanalysis. **(11hrs)**

Unit II Symmetric Encryption and Message Confidentiality - Symmetric Encryption Principles, Symmetric Block Encryption Algorithms, Stream Ciphers and RC4 , Chipher Block Modes of Operation, Location of Encryption Devices, Key Distribution. Public-key Cryptography and Message Authentication: Approaches to Message Authentication, Secure Hash Functions and HMAC, Public-Key Cryptography Principles, Public-Key Cryptography Algorithms, Digital Signatures, Key Management. **(12hrs)**

Unit III Authentication Applications - Kerberos, x.509 Authentication Service, Public-Key Infrastructure. Electronic Mail Security: Pretty Good Privacy (PGP), S/MIME. **(10hrs)**

Unit IV IP Security - IP Security Over view, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations. Web Security: Web Security Considerations, Secure Socket Layer(SSL) and Transport Layer Security(TLS), Secure Electronic Transaction(SET).Network Management Security: Basic Concepts of SNMP, SNMPv1 Community Facility, SNMPv3. **(13hrs)**

Unit V Intruders - Intruders, Intrusion Detection, Password Management. **Malicious Software:** Virus and Related Threats, Virus Countermeasures, Distributed Denial of Service Attacks. **Firewalls:** Firewall Design Principles, Trusted Systems, Common Criteria for Information Technology Security Evaluation. **(14hrs)**

TOTAL (60Hrs)

Text books

1. Behrouz A. Ferouzan, “Cryptography & Network Security”, Tata Mc Graw Hill, 2007, Reprint 2015.

2. Stallings William, “Cryptography and Network Security - Principles and Practice 2017.

3. **William Stallings, “Network Security Essentials Applications and Standards ”Third Edition, Pearson Education, 2008.**

References

1. Man Young Rhee, “Internet Security: Cryptographic Principles”, “Algorithms And Protocols”, Wiley Publications, 2003.

2. Charles Pfleeger, “Security In Computing”, 4th Edition, Prentice Hall Of India, 2006.

3. Ulysess Black, “Internet Security Protocols”, Pearson Education Asia, 2000.

4. Charlie Kaufman And Radia Perlman, Mike Speciner, “Network Security, Second Edition, Private Communication In Public World”, PHI 2002.

5. Bruce Schneier And Neils Ferguson, “Practical Cryptography”, First Edition, Wiley Dreamtech India Pvt Ltd, 2003.

6. Douglas R Simson “Cryptography – Theory And Practice”, First Edition, CRC Press, 1995.

7. Http://Nptel.Ac.In/.

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**Introduction -**.	
1.1	Security trends – Legal, Ethical and Professional Aspects of Security,	3
1.2	Need for Security at Multiple levels, Security Policies – Model of network security – Security attacks, services and mechanisms – OSI security architecture –	2
1.3	Classical encryption techniques: substitution techniques, transposition techniques, steganography-	2
1.4	Foundations of modern cryptography: perfect security – information theory – product cryptosystem – cryptanalysis	2
2	**Symmetric Encryption and Message Confidentiality**	
2.1	- Symmetric Encryption Principles, Symmetric Block Encryption Algorithms, Stream Ciphers and RC4 ,	2
2.2	Chipher Block Modes of Operation, Location of Encryption Devices, Key Distribution.	3
2.3	Public-key Cryptography and Message Authentication: Approaches to Message Authentication, Secure Hash Functions and HMAC,	2
2.4	Public-Key Cryptography Principles, Public-Key Cryptography Algorithms, Digital Signatures, Key Management.	
3	**Authentication Applications -**	
3.1	Kerberos, x.509 Authentication Service, Public-	2
3.2	Key Infrastructure. Electronic Mail Security: Pretty Good Privacy (PGP), S/MIME.	2
4	**IP Security**.	
4.1	- IP Security Over view, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations.	2
4.2	Web Security: Web Security Considerations, Secure Socket Layer(SSL) and Transport Layer Security(TLS), Secure Electronic Transaction(SET).	2
4.3	Network Management Security: Basic Concepts of SNMP, SNMPv1 Community Facility, SNMPv3	2
5	**Intruders -**	
5.1	Intruders, Intrusion Detection, Password Management. **Malicious Software:** Virus and Related Threats,	2
5.2	Virus Countermeasures, Distributed Denial of Service Attacks.	2
5.3	**Firewalls:** Firewall Design Principles, Trusted Systems, Common Criteria for Information Technology Security Evaluation.	2

Core 11	**NCYC33 - IT Governance, Risk and Compliance**	Category PC	L 4	P 0	Credit 4

Preamble

IT GRC ensures that Activities and functions of IT organisation(s) support objectives investments are maximised.IT delivers envisioned benefits against the strategy, costs are optimised, and relevant best practises incorporated.The optimal investments is made in IT and critical IT resources are responsibly, effectively and efficiently managed and used.

Prerequisite

- Nil

Course Outcomes

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

Course Outcomes		Level
CO1	Study of GRC basics	Understanding
CO2	Learn best practices for IT governance	Understanding
CO3	Understand the information security governance concepts	Understanding
CO4	Know the ISG practices	Apply
CO5	Detail study of the compliance	Apply

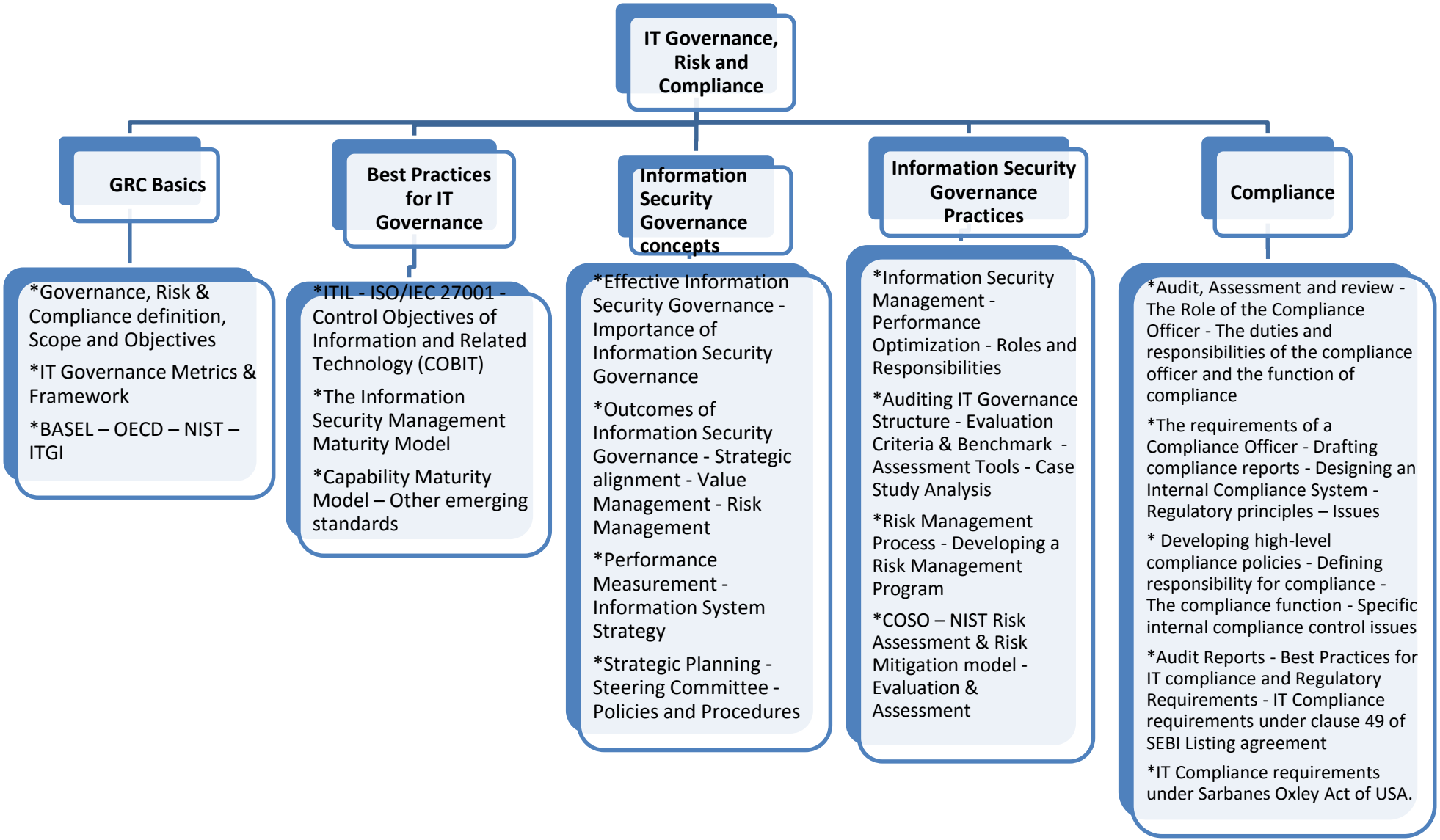
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	S									
CO2		M					S			L
CO3			M						L	
CO4				L						
CO5					M			M		

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


IT Governance, Risk and Compliance
GRC Basics
*Governance, Risk & Compliance definition, Scope and Objectives
*IT Governance Metrics & Framework
*BASEL – OECD – NIST – ITGI
Best Practices for IT Governance
*ITIL - ISO/IEC 27001 - Control Objectives of Information and Related Technology (COBIT)
*The Information Security Management Maturity Model
*Capability Maturity Model – Other emerging standards
Information Security Governance concepts
*Effective Information Security Governance - Importance of Information Security Governance
*Outcomes of Information Security Governance - Strategic alignment - Value Management - Risk Management
*Performance Measurement - Information System Strategy
*Strategic Planning - Steering Committee - Policies and Procedures
Information Security Governance Practices
*Information Security Management - Performance Optimization - Roles and Responsibilities
*Auditing IT Governance Structure - Evaluation Criteria & Benchmark - Assessment Tools - Case Study Analysis
*Risk Management Process - Developing a Risk Management Program
*COSO – NIST Risk Assessment & Risk Mitigation model - Evaluation & Assessment
Compliance
*Audit, Assessment and review - The Role of the Compliance Officer - The duties and responsibilities of the compliance officer and the function of compliance
*The requirements of a Compliance Officer - Drafting compliance reports - Designing an Internal Compliance System - Regulatory principles – Issues
* Developing high-level compliance policies - Defining responsibility for compliance - The compliance function - Specific internal compliance control issues
*Audit Reports - Best Practices for IT compliance and Regulatory Requirements - IT Compliance requirements under clause 49 of SEBI Listing agreement
*IT Compliance requirements under Sarbanes Oxley Act of USA.

Syllabus

Unit 1: GRC Basics Governance, Risk & Compliance definition, Scope and Objectives - IT Governance Metrics & Framework – BASEL – OECD – NIST - ITGI **(10hrs)**

Unit 2: Best Practices for IT Governance ITIL - ISO/IEC 27001 - Control Objectives of Information and Related Technology (COBIT) - The Information Security Management Maturity Model - Capability Maturity Model – Other emerging standards **(12hrs)**

Unit 3: Information Security Governance concepts Effective Information Security Governance - Importance of Information Security Governance - Outcomes of Information Security Governance - Strategic alignment - Value Management - Risk Management - Performance Measurement - Information System Strategy - Strategic Planning - Steering Committee - Policies and Procedures **(12hrs)**

Unit 4: Information Security Governance Practices Information Security Management - Performance Optimization - Roles and Responsibilities - Auditing IT Governance Structure - Evaluation Criteria & Benchmark - Assessment Tools - Case Study Analysis - Risk Management Process - Developing a Risk Management Program - COSO – NIST Risk Assessment & Risk Mitigation model - Evaluation & Assessment **(12hrs)**

Unit 5: Compliance Audit, Assessment and review - The Role of the Compliance Officer - The duties and responsibilities of the compliance officer and the function of compliance - The requirements of a Compliance Officer - Drafting compliance reports - Designing an Internal Compliance System - Regulatory principles – Issues - Developing high-level compliance policies - Defining responsibility for compliance - The compliance function - Specific internal compliance control issues - Audit Reports - Best Practices for IT compliance and Regulatory Requirements - IT Compliance requirements under clause 49 of SEBI Listing agreement - IT Compliance requirements under Sarbanes Oxley Act of USA. **(14hrs)**

TOTAL (60Hrs)

Books:

1. Information Security Governance: Guidance for Information Security Managers by W. KragBrotby, 1st Edition, Wiley Publication, 13 April 2009
2. Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition by W. KragBrotby, 2nd Edition, ISACA Publication, 01 Mar 2006
3. Security Governance Checklists: Business Operations, Security Governance, Risk Management, and Enterprise Security Architecture by Fred Cohen, Large Print Edition, Fred Cohen &Assosciates Publication, 2005
4. CISSP All-in-One Exam Guide by Shon Harris and Fernando Maymi, 7th Edition, McGraw-Hill Education, 1 June 2016
5. IT Compliance and Controls: Best Practices for Implementation by James J., IV DeLuccia, Illustrated Edition, Wiley Publication, 2008
6. The IT Regulatory and Standards Compliance Handbook: How to Survive Information Systems Audit and Assessments by Craig S. Wright, Brian Freedman, Dale Liu, 1st Edition, Syngress Publication, 2008

7. Auditor's Guide to Information Systems Auditing by Richard E. Cascarino, 2nd Edition, Wiley Publication, 03 Apr 2012

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**GRC Basics**	
1.1	Governance, Risk & Compliance definition, Scope and Objectives	1
1.2	IT Governance Metrics & Framework	1
1.3	BASEL – OECD – NIST – ITGI	3
2	**Best Practices for IT Governance**	
2.1	ITIL - ISO/IEC 27001 - Control Objectives of Information and Related Technology (COBIT)	2
2.2	The Information Security Management Maturity Model	2
2.3	Capability Maturity Model – Other emerging standards	2
3	**Information Security Governance concepts**	
3.1	Effective Information Security Governance - Importance of Information Security Governance	2
3.2	Outcomes of Information Security Governance - Strategic alignment - Value Management - Risk Management	2
	Performance Measurement - Information System Strategy	1
	Strategic Planning - Steering Committee - Policies and Procedures	1
4	**Information Security Governance Practices**	
4.1	Information Security Management - Performance Optimization - Roles and Responsibilities	2
4.2	Auditing IT Governance Structure - Evaluation Criteria & Benchmark - Assessment Tools - Case Study Analysis	2
4.3	Risk Management Process - Developing a Risk Management Program	2
4.4	COSO – NIST Risk Assessment & Risk Mitigation model - Evaluation & Assessment	2
5	**Compliance**	
5.1	Audit, Assessment and review - The Role of the Compliance Officer - The duties and responsibilities of the compliance officer and the function of compliance	2
5.2	The requirements of a Compliance Officer - Drafting compliance reports - Designing an Internal Compliance System - Regulatory principles – Issues	2
5.3	- Developing high-level compliance policies - Defining responsibility for compliance - The compliance function - Specific internal compliance control issues	2
5.4	Audit Reports - Best Practices for IT compliance and Regulatory Requirements - IT Compliance requirements under clause 49 of SEBI Listing agreement	2
5.5	IT Compliance requirements under Sarbanes Oxley Act of USA.	2

NCYL31	Advanced Information Security Lab	L	T	P	C
				3	2

1. Implement the following SUBSTITUTION & TRANSPOSITION TECHNIQUES concepts:

    a) Caesar Cipher

    b) Playfair Cipher

    c) Hill Cipher

    d) Vigenere Cipher

    e) Rail fence – row & Column Transformation

2. Implement the following algorithms

    a) DES

    b) RSA Algorithm

    c) Diffiee-Hellman

    d) MD5

    e) SHA-1

3. Implement the Signature Scheme - Digital Signature Standard

4. Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures (GnuPG)

5. Setup a honey pot and monitor the honeypot on network (KF Sensor)

6. Installation of rootkits and study about the variety of options

7. Perform wireless audit on an access point or a router and decrypt WEP and WPA. (Net Stumbler)

8. Demonstrate intrusion detection system (ids) using any tool (snort or any other s/w)

NCYL32	Advanced Digital Forensics lab	L	T	P	C
				3	2

1. Ethical hacking in mobile, system
2. Perform an experiment on Active and Passive finger printing using XProbe2 or nmap
3. Demonstrate Intrusion Detection System (IDS) using any tool such as Snort or any other Software
4. Perform an experiment for Port Scanning with nmap, superscan or any other equivalent software
5. Generate minimum 10 passwords of length 12 characters using OpenSSL command
6. Performa a experiment to demonstrate how to sniff for router traffic by using the tool Cain and Abel / Wireshark / tcpdump
7. Implement the Signature Scheme - Digital Signature Standard

Core 12	**NCYCPB - Capacity development for risk / disaster management (e-pathshala)**	Category PC	L 4	P 0	Credit 4

Preamble

To understand and comprehend the basic concepts, meanings and terminologies about training, teaching and capacity development and its related information. The paradigm shift from a reactive and relief centric approach to a more holistic and integrated approach being followed in disaster .Various institutions involved in capacity building and approaches and strategies being followed is incorporated.

Prerequisite

- Nil

Course Outcomes

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

Course Outcomes		Level
CO1	To understand Capacity Development	Understanding
CO2	Understand Institutions for Capacity Development:	Understanding
CO3	Understand Incident Response System (IRS)/ Incident Command System (ICS): I	Understanding
CO4	Learn Definitions and Scope of Capacity Development:	Apply
CO5	To learn National Fire Service College-Nagpur:	Apply

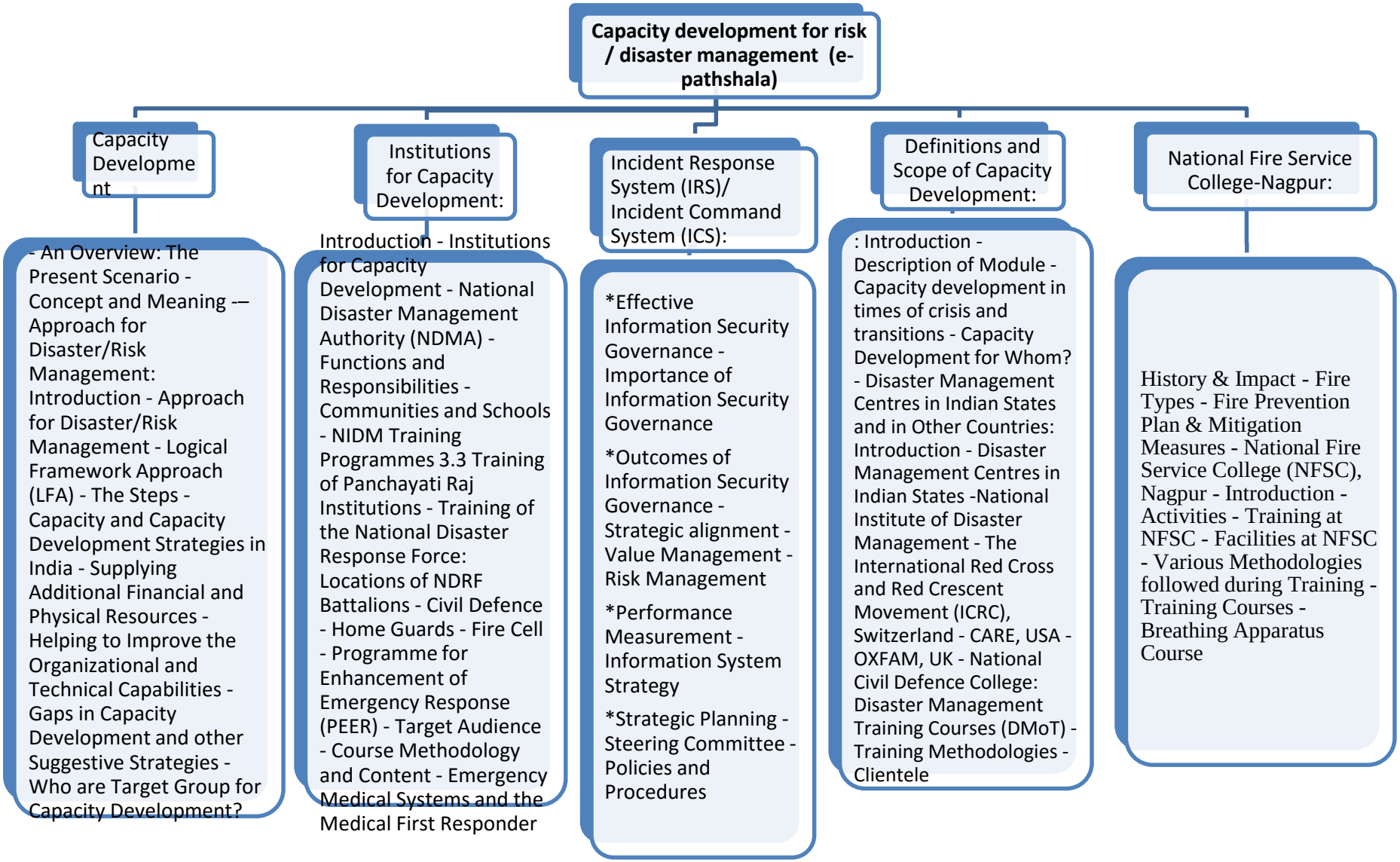
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	S									
CO2		M					S			L
CO3			M						L	
CO4				L						
CO5					M			M		

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


Capacity development for risk / disaster management (e-pathshala)
Capacity Development
- An Overview: The Present Scenario - Concept and Meaning -– Approach for Disaster/Risk Management: Introduction - Approach for Disaster/Risk Management - Logical Framework Approach (LFA) - The Steps - Capacity and Capacity Development Strategies in India - Supplying Additional Financial and Physical Resources - Helping to Improve the Organizational and Technical Capabilities - Gaps in Capacity Development and other Suggestive Strategies - Who are Target Group for Capacity Development?
Institutions for Capacity Development:
Introduction - Institutions for Capacity Development - National Disaster Management Authority (NDMA) - Functions and Responsibilities - Communities and Schools - NIDM Training Programmes 3.3 Training of Panchayati Raj Institutions - Training of the National Disaster Response Force: Locations of NDRF Battalions - Civil Defence - Home Guards - Fire Cell - Programme for Enhancement of Emergency Response (PEER) - Target Audience - Course Methodology and Content - Emergency Medical Systems and the Medical First Responder
Incident Response System (IRS)/ Incident Command System (ICS):
*Effective Information Security Governance - Importance of Information Security Governance
*Outcomes of Information Security Governance - Strategic alignment - Value Management - Risk Management
*Performance Measurement - Information System Strategy
*Strategic Planning - Steering Committee - Policies and Procedures
Definitions and Scope of Capacity Development:
: Introduction - Description of Module - Capacity development in times of crisis and transitions - Capacity Development for Whom? - Disaster Management Centres in Indian States and in Other Countries: Introduction - Disaster Management Centres in Indian States -National Institute of Disaster Management - The International Red Cross and Red Crescent Movement (ICRC), Switzerland - CARE, USA - OXFAM, UK - National Civil Defence College: Disaster Management Training Courses (DMoT) - Training Methodologies - Clientele
National Fire Service College-Nagpur:
History & Impact - Fire Types - Fire Prevention Plan & Mitigation Measures - National Fire Service College (NFSC), Nagpur - Introduction - Activities - Training at NFSC - Facilities at NFSC - Various Methodologies followed during Training - Training Courses - Breathing Apparatus Course

Syllabus

Unit 1: Capacity Development - An Overview: The Present Scenario - Concept and Meaning –– Approach for Disaster/Risk Management: Introduction - Approach for Disaster/Risk Management - Logical Framework Approach (LFA) - The Steps - Capacity and Capacity Development Strategies in India - Supplying Additional Financial and Physical Resources - Helping to Improve the Organizational and Technical Capabilities - Gaps in Capacity Development and other Suggestive Strategies - Who are Target Group for Capacity Development? **(12hrs)**

Unit 2: Institutions for Capacity Development: Introduction - Institutions for Capacity Development - National Disaster Management Authority (NDMA) - Functions and Responsibilities - Communities and Schools - NIDM Training Programmes 3.3 Training of Panchayati Raj Institutions - Training of the National Disaster Response Force: Locations of NDRF Battalions - Civil Defence - Home Guards - Fire Cell - Programme for Enhancement of Emergency Response (PEER) - Target Audience - Course Methodology and Content - Emergency Medical Systems and the Medical First Responder **(13hrs)**

Unit 3 : Incident Response System (IRS)/ Incident Command System (ICS): Introduction -What is an Incident Command System? - Background - Definition -Key concepts - Unity of command - Common terminology - - Command staff - General staff - Design - Personnel - Facilities - Human Resource Development: Training & Education - Disaster Management in School Curriculum in India - Open Learning and Distance Education: **(11hrs)**

Unit 4: Definitions and Scope of Capacity Development: Introduction - Description of Module - Capacity development in times of crisis and transitions - Capacity Development for Whom? - Disaster Management Centres in Indian States and in Other Countries: Introduction - Disaster Management Centres in Indian States -National Institute of Disaster Management - The International Red Cross and Red Crescent Movement (ICRC), Switzerland - CARE, USA - OXFAM, UK - National Civil Defence College: Disaster Management Training Courses (DMoT) - Training Methodologies - Clientele **(14hrs)**

Unit 5: National Fire Service College-Nagpur: History & Impact - Fire Types - Fire Prevention Plan & Mitigation Measures - National Fire Service College (NFSC), Nagpur - Introduction - Activities - Training at NFSC - Facilities at NFSC - Various Methodologies followed during Training -Training Courses - Breathing Apparatus Course **(10hrs)**

TOTAL (60 hrs)

Text book:

https://epgp.inflibnet.ac.in/ahl.php?csrno=774

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**Capacity Development -**	
1.1	An Overview: The Present Scenario - Concept and Meaning -– Approach for Disaster/Risk Management:	1
1.2	Introduction - Approach for Disaster/Risk Management - Logical Framework Approach (LFA) - The Steps - Capacity and Capacity Development Strategies in India -	1
1.3	Supplying Additional Financial and Physical Resources - Helping to Improve the Organizational and Technical Capabilities - Gaps in Capacity Development and other Suggestive Strategies - Who are Target Group for Capacity Development?	3
2	**Institutions for Capacity Development:**	
2.1	Introduction - Institutions for Capacity Development - National Disaster Management Authority (NDMA) - Functions and Responsibilities - Communities and Schools -	2
2.2	NIDM Training Programmes 3.3 Training of Panchayati Raj Institutions - Training of the National Disaster Response Force: Locations of NDRF Battalions - Civil Defence - Home Guards - Fire Cell	2
2.3	- Programme for Enhancement of Emergency Response (PEER) - Target Audience - Course Methodology and Content - Emergency Medical Systems and the Medical First Responder	2
3	**Incident Response System (IRS)/ Incident Command System (ICS): Introduction -What is an Incident Command System?**	
3.1	Background - Definition -Key concepts - Unity of command - Common terminology - - Command staff - General staff - Design - Personnel - Facilities	2
3.2	- Human Resource Development: Training & Education - Disaster Management in School Curriculum in India - Open Learning and Distance Education:	2
4	**Definitions and Scope of Capacity Development: entele**	
4.1	Introduction - Description of Module - Capacity development in times of crisis and transitions - Capacity Development for Whom? -	2
4.2	Disaster Management Centres in Indian States and in Other Countries: Introduction - Disaster Management Centres in Indian States	2
4.3	-National Institute of Disaster Management - The International Red Cross and Red Crescent Movement (ICRC),	2
4.4	Switzerland - CARE, USA - OXFAM, UK - National Civil Defence College: Disaster Management Training Courses (DMoT) - Training Methodologies - Cli	2
5	**National Fire Service College-Nagpur:**	
5.1	History & Impact - Fire Types - F	2
5.2	ire Prevention Plan & Mitigation Measures - National Fire Service College (NFSC), Nagpur - Introduction - Activities - Training at NFSC -	2
5.3	Facilities at NFSC - Various Methodologies followed during Training -Training Courses - Breathing Apparatus Course	2

MANONMANIAM SUNDARANAR UNIVERSITY

TIRUNELVELI, TAMILNADU

M.Sc CYBER SECURITY DEGREE PROGRAMME

LIST OF ELECTIVES

(For The Candidates Admitted From 2019-20 Onwards)

SI. No.	**Course code**	**Course name**
Electives – Group A		
1.	NCYEAA	Foundations of Cloud Computing Security
2.	NCYEAB	Introduction to Networking
3.	NCYEAC	Email, Mobile Devices Security
4.	NCYEAD	Mobile and Wireless Security
Electives – Group B		
5.	NCYEBA	Fundamentals of Blockchains and Crypto-currency
6.	NCYEBB	Storage Management and Security
7.	NCYEBC	Big Data Technology
8.	NCYEBD	Android Mobile Application Development
Electives – Group C		
9.	NCYECA	Fundamentals of Research Methods and Statistical Applications
10.	NCYECB	Mobile and Digital Forensics
11.	NCYECC	Data Mining and Warehousing
12.	NCYECD	Big Data Security

Foundations of Cloud Computing Security	Category	L	P	Credit
	PE	3	0	3

Preamble

Cloud computing security or, more simply, cloud security refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. It is a sub-domain of computer security, network security, and, more broadly, information security.

Prerequisite

- Network Security

Course Outcomes

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

Course Outcomes		Level
CO1	Basic concepts in Cloud computing	Understanding
CO2	Different Infrastructure Security in Cloud	Apply
CO3	Policy and Compliance in Cloud Environment	Understanding
CO4	Data lifecycle and encryption, architecture	Apply
CO5	Various Cloud Security Architecture	Apply

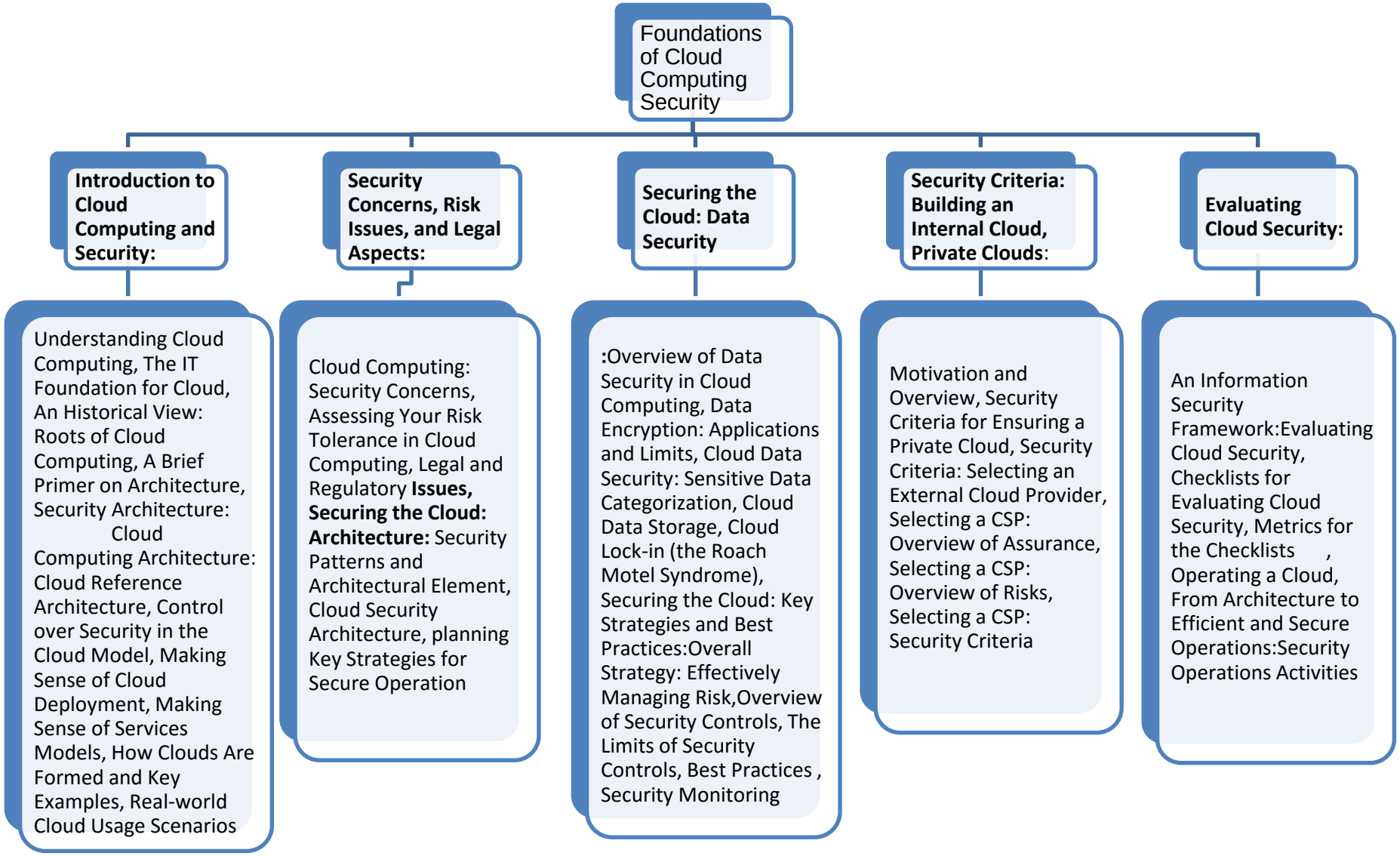
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	S									
CO2		L		M						
CO3						M				
CO4								M		
CO5			S							

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


Foundations of Cloud Computing Security
Introduction to Cloud Computing and Security:
Understanding Cloud Computing, The IT Foundation for Cloud, An Historical View: Roots of Cloud Computing, A Brief Primer on Architecture, Security Architecture: Cloud Computing Architecture: Cloud Reference Architecture, Control over Security in the Cloud Model, Making Sense of Cloud Deployment, Making Sense of Services Models, How Clouds Are Formed and Key Examples, Real-world Cloud Usage Scenarios
Security Concerns, Risk Issues, and Legal Aspects:
Cloud Computing: Security Concerns, Assessing Your Risk Tolerance in Cloud Computing, Legal and Regulatory **Issues, Securing the Cloud: Architecture:** Security Patterns and Architectural Element, Cloud Security Architecture, planning Key Strategies for Secure Operation
Securing the Cloud: Data Security
:Overview of Data Security in Cloud Computing, Data Encryption: Applications and Limits, Cloud Data Security: Sensitive Data Categorization, Cloud Data Storage, Cloud Lock-in (the Roach Motel Syndrome), Securing the Cloud: Key Strategies and Best Practices:Overall Strategy: Effectively Managing Risk,Overview of Security Controls, The Limits of Security Controls, Best Practices , Security Monitoring
Security Criteria: Building an Internal Cloud, Private Clouds:
Motivation and Overview, Security Criteria for Ensuring a Private Cloud, Security Criteria: Selecting an External Cloud Provider, Selecting a CSP: Overview of Assurance, Selecting a CSP: Overview of Risks, Selecting a CSP: Security Criteria
Evaluating Cloud Security:
An Information Security Framework:Evaluating Cloud Security, Checklists for Evaluating Cloud Security, Metrics for the Checklists , Operating a Cloud, From Architecture to Efficient and Secure Operations:Security Operations Activities

Syllabus

Unit-1: Introduction to Cloud Computing and Security: Understanding Cloud Computing, The IT Foundation for Cloud, An Historical View: Roots of Cloud Computing, A Brief Primer on Architecture, Security Architecture: Cloud Computing Architecture: Cloud Reference Architecture, Control over Security in the Cloud Model, Making Sense of Cloud Deployment, Making Sense of Services Models, How Clouds Are Formed and Key Examples, Real-world Cloud Usage Scenarios **(12hrs)**

Unit-2: Security Concerns, Risk Issues, and Legal Aspects: Cloud Computing: Security Concerns, Assessing Your Risk Tolerance in Cloud Computing, Legal and Regulatory **Issues, Securing the Cloud: Architecture:** Security Patterns and Architectural Element, Cloud Security Architecture, planning Key Strategies for Secure Operation **(11hrs)**

Unit-3: Securing the Cloud: Data Security : Overview of Data Security in Cloud Computing, Data Encryption: Applications and Limits, Cloud Data Security: Sensitive Data Categorization, Cloud Data Storage, Cloud Lock-in (the Roach Motel Syndrome), Securing the Cloud: Key Strategies and Best Practices:Overall Strategy: Effectively Managing Risk,Overview of Security Controls, The Limits of Security Controls, Best Practices , Security Monitoring **(13hrs)**

Unit-4: Security Criteria: Building an Internal Cloud, Private Clouds: Motivation and Overview, Security Criteria for Ensuring a Private Cloud, Security Criteria: Selecting an External Cloud Provider, Selecting a CSP: Overview of Assurance, Selecting a CSP: Overview of Risks, Selecting a CSP: Security Criteria **(12hrs)**

Unit-5: Evaluating Cloud Security: An Information Security Framework:Evaluating Cloud Security, Checklists for Evaluating Cloud Security, Metrics for the Checklists, Operating a Cloud, From Architecture to Efficient and Secure Operations:Security Operations Activities**(12hrs)**

Total (60Hrs)

Text Books:

1. Securing the Cloud: Cloud Computer Security Techniques and Tactics by Vic (J.R.) Winkler, Technical Editor Bill Meine
2. Mather, Kumaraswamy and Latif: Cloud Security and Privacy – An Enterprise Perspective on Risk and Compliance, O'Reilly
3. Kurtz and Vines: Cloud Security: A Comprehensive guide to secure cloud computing, Wiley
4. Buyya, Broberg and Goscinski: Cloud Computing – Principles and Paradigms, Wiley

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1.	**Introduction to Cloud Computing and Security**	
1.1	**:** Understanding Cloud Computing, The IT Foundation for Cloud, An Historical View:	1
1.2	Roots of Cloud Computing, A Brief Primer on Architecture, Security Architecture:	1
1.3	Cloud Computing Architecture: Cloud Reference Architecture, Control over Security in the Cloud Model, Making Sense of Cloud Deployment, Making Sense of Services Models,	1
1.4	How Clouds Are Formed and Key Examples, Real-world Cloud Usage Scenarios	2
2.	**Security Concerns, Risk Issues, and Legal Aspects:**	
2.1	Cloud Computing: Security Concerns, Assessing Your Risk Tolerance in Cloud Computing, Legal and Regulatory	1
2.2	**Issues, Securing the Cloud: Architecture:** Security Patterns and Architectural Element,	1
2.3	Cloud Security Architecture, planning Key Strategies for Secure Operation	1
3.	**Securing the Cloud: Data Security :**	
3.1	Overview of Data Security in Cloud Computing, Data Encryption: Applications and Limits,	1
3.2	Cloud Data Security: Sensitive Data Categorization, Cloud Data Storage, Cloud Lock-in (the Roach Motel Syndrome),	2
3.3	Securing the Cloud: Key Strategies and Best Practices:Overall Strategy: Effectively Managing Risk,	2
3.4	Overview of Security Controls, The Limits of Security Controls, Best Practices , Security Monitoring	1
4.	**Security Criteria: Building an Internal Cloud, Private Clouds**	
4.1	: Motivation and Overview, Security Criteria for Ensuring a Private Cloud,	1
4.2	Security Criteria: Selecting an External Cloud Provider, Selecting a CSP: Overview of Assurance,	1
4.3	Selecting a CSP: Overview of Risks, Selecting a CSP: Security Criteria	1
5.	**Evaluating Cloud Security**	
5.1	**:** An Information Security Framework:Evaluating Cloud Security, Checklists for Evaluating Cloud Security,	2
5.2	Metrics for the Checklists , Operating a Cloud, From Architecture to Efficient and Secure Operations:Security Operations Activities	2

Introduction to Networking	Category	L	P	Credit
	PE	3	0	3

Preamble

The security in computer networks is a rapidly growing area of concern. Most of thevaluable information resides on the network, making network an inevitable entity for survival.There is proliferation of the networks in daily lives, he it an academic or business environment.

Prerequisite

- Network Security

Course Outcomes

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

Course Outcomes		Level
CO1	Study the concepts in networking	Understanding
CO2	Learn the routing architecture and configuration	Understanding
CO3	Understand the different form of packet switched connection	Understanding
CO4	Detail study of OSI layers	Understanding
CO5	Analysis of networking to the end user	Apply

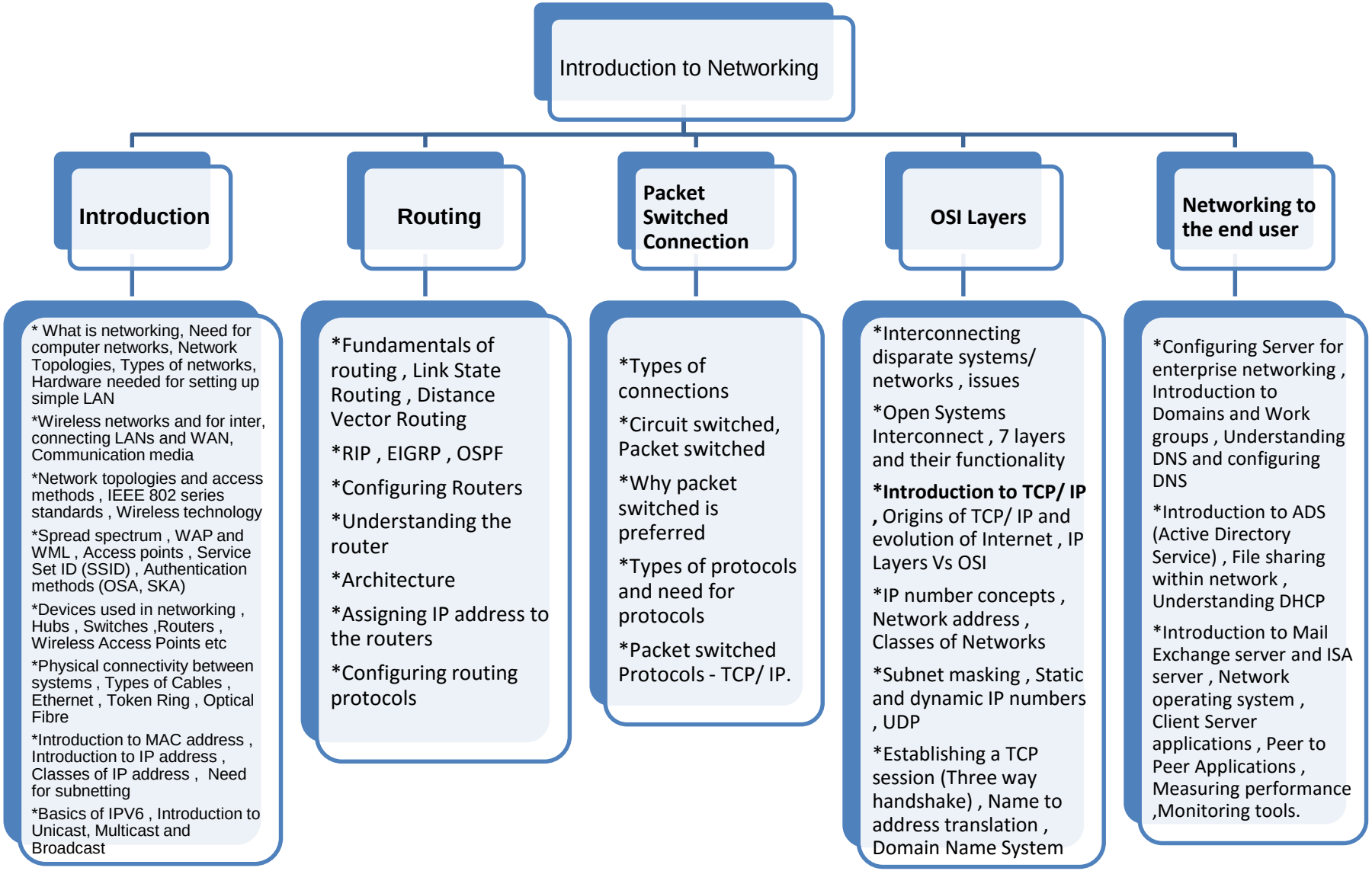
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1									L	
CO2	S				L					
CO3		M					L		M	
CO4				M						L
CO5								M		

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


Introduction to Networking
Introduction
* What is networking, Need for computer networks, Network Topologies, Types of networks, Hardware needed for setting up simple LAN
*Wireless networks and for inter, connecting LANs and WAN, Communication media
*Network topologies and access methods , IEEE 802 series standards , Wireless technology
*Spread spectrum , WAP and WML , Access points , Service Set ID (SSID) , Authentication methods (OSA, SKA)
*Devices used in networking , Hubs , Switches ,Routers , Wireless Access Points etc
*Physical connectivity between systems , Types of Cables , Ethernet , Token Ring , Optical Fibre
*Introduction to MAC address , Introduction to IP address , Classes of IP address , Need for subnetting
*Basics of IPV6 , Introduction to Unicast, Multicast and Broadcast
Routing
*Fundamentals of routing , Link State Routing , Distance Vector Routing
*RIP , EIGRP , OSPF
*Configuring Routers
*Understanding the router
*Architecture
*Assigning IP address to the routers
*Configuring routing protocols
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.
OSI Layers
*Interconnecting disparate systems/ networks , issues
*Open Systems Interconnect , 7 layers and their functionality
Introduction to TCP/ IP , 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
Networking to the end user
*Configuring Server for enterprise networking , Introduction to Domains and Work groups , Understanding DNS and configuring DNS
*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.

Syllabus

Unit 1: Introduction - What is networking - Need for computer networks - Network Topologies - Types of networks - Hardware needed for setting up simple LAN, Wireless networks and for inter-connecting LANs and WAN -Communication media - Network topologies and access methods - IEEE 802 series standards - Wireless technology - Spread spectrum - WAP and WML - Access points - Service Set ID (SSID) - Authentication methods (OSA, SKA) - Devices used in networking – Hubs – Switches – Routers - Wireless Access Points etc - Physical connectivity between systems - Types of Cables – Ethernet - Token Ring - Optical Fibre - Introduction to MAC address - Introduction to IP address - Classes of IP address - Need for subnetting - Basics of IPV6 - Introduction to Unicast, Multicast and Broadcast **(14hrs)**

Unit 2: Routing - Fundamentals of routing - Link State Routing - Distance Vector Routing – RIP – EIGRP – OSPF - Configuring Routers - Understanding the router architecture - Assigning IP address to the routers - Configuring routing protocols **(10hrs)**

Unit 3: 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 **(10hrs)**

Unit 4: OSI Layers - Interconnecting disparate systems/ networks – issues - Open Systems Interconnect - 7 layers and their functionality - **Introduction to TCP/ IP -** 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 **(13hrs)**

Unit 5: Networking to the end user - Configuring Server for enterprise networking - Introduction to Domains and Work groups - Understanding DNS and configuring DNS - 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. **(13hrs)**

Total (60hrs)

Reference Books:

1. Basic of Networking – Prentice Hall (ISBN 8120324897)
2. Introduction to Networking – Prentice Hall (ISBN 8120313860)
3. Computer Networking First Step – Odom Wendell – (ISBN 8129706075)

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1.	**Introduction**	
1.1	What is networking,Need for computer networks, Network Topologies, Types of networks,Hardware needed for setting up simple LAN	3
1.2	Wireless networks and for inter, connecting LANs and WAN, Communication media	1
1.3	Network topologies and access methods , IEEE 802 series standards , Wireless technology	1
1.4	Spread spectrum , WAP and WML , Access points , Service Set ID (SSID) , Authentication methods (OSA, SKA)	1
1.5	Devices used in networking , Hubs , Switches ,Routers , Wireless Access Points etc	1
1.6	Physical connectivity between systems - Types of Cables – Ethernet - Token Ring - Optical Fibre	1
1.7	Introduction to MAC address - Introduction to IP address - Classes of IP address - Need for subnetting	2
1.8	Basics of IPV6 - Introduction to Unicast, Multicast and Broadcast	1
2.	**Routing**	
2.1	Fundamentals of routing , Link State Routing , Distance Vector Routing	2
2.2	RIP , EIGRP , OSPF	1
2.3	Configuring Routers	1
2.4	Understanding the router	1
2.5	Architecture	1
2.6	Assigning IP address to the routers	1
2.7	Configuring routing protocols	1
3.	**Packet Switched Connection**	
3.1	Types of connections	1
3.2	Circuit switched, Packet switched	1
3.3	Why packet switched is preferred	1
3.4	Types of protocols and need for protocols	1
3.5	Packet switched Protocols - TCP/ IP.	1
4.	**OSI Layers**	
4.1	Interconnecting disparate systems/ networks , issues	1
4.2	Open Systems Interconnect , 7 layers and their functionality	1
4.3	**Introduction to TCP/ IP ,**Origins of TCP/ IP and evolution of Internet , IP Layers Vs OSI	1
4.4	IP number concepts , Network address , Classes of Networks	1
4.5	Subnet masking , Static and dynamic IP numbers , UDP	1
4.6	Establishing a TCP session (Three way handshake) , Name to address translation , Domain Name System	2

5.	**Networking to the end user**	
5.1	Configuring Server for enterprise networking , Introduction to Domains and Work groups , Understanding DNS and configuring DNS	2
5.2	Introduction to ADS (Active Directory Service) , File sharing within network , Understanding DHCP	1
5.3	Introduction to Mail Exchange server and ISA server ,Network operating system , Client Server applications , Peer to Peer Applications , Measuring performance ,Monitoring tools.	3

Email, Mobile Devices Security	Category	L	P	Credit
	PE	3	0	3

Preamble

Email security is a priority for all businesses, with the growing threat of hackers, viruses spam, phishing and identity theft, as well as the need to secure business information. Mobile security is the protection of smartphones, tablets, laptops and other portable computing devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing. Mobile security is also known as wireless security.

Prerequisite

- Network Security

Course Outcomes

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

Course Outcomes		Level
CO1	Understanding basics of email	Understanding
CO2	Study about simple mail transfer protocol	Apply
CO3	Learn focused attacks against email systems	Understanding
CO4	Understand the spam and phishing concepts	Apply
CO5	Study about mobile and wireless devices	Apply

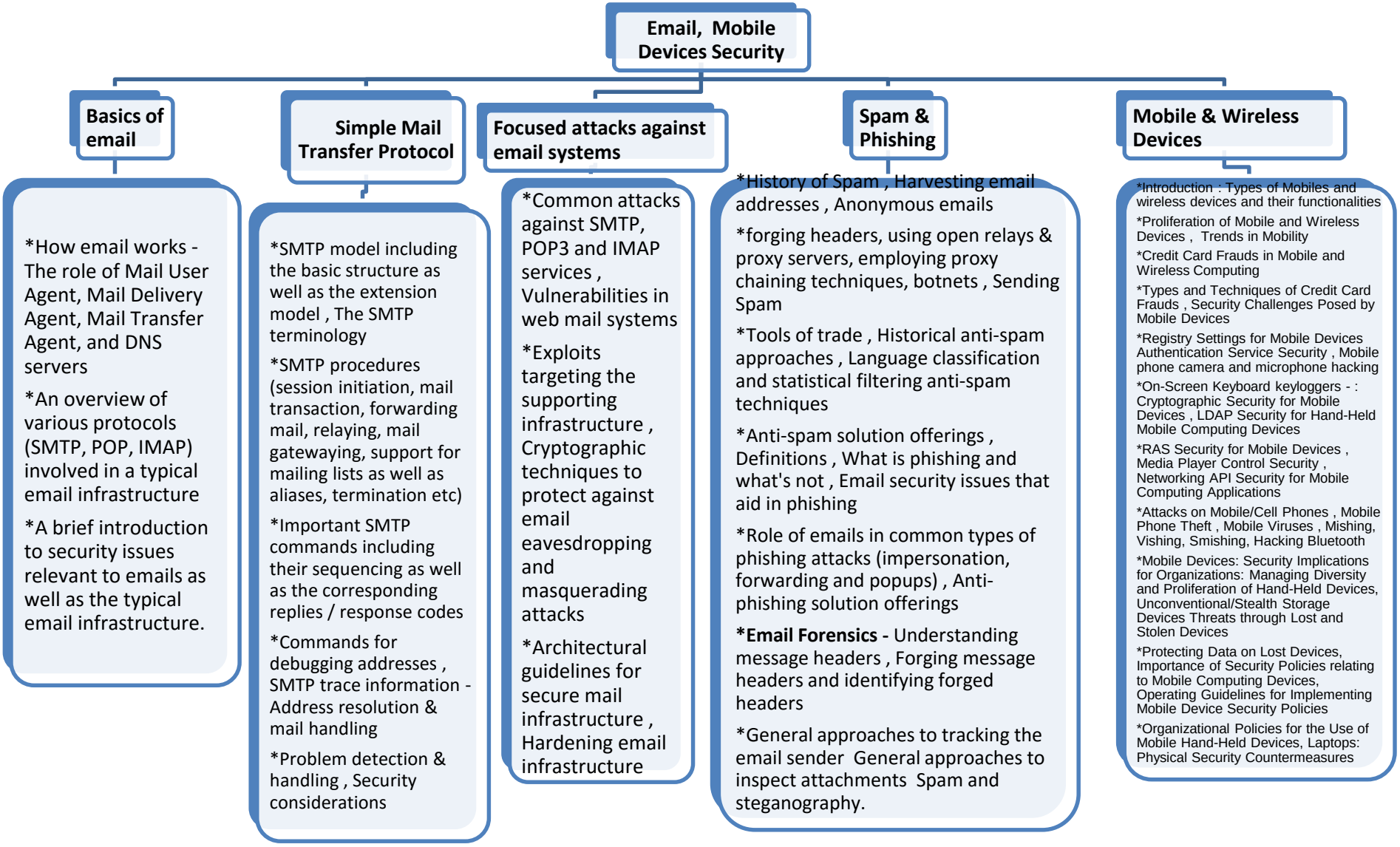
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	S									
CO2		L		M					L	
CO3					S	M				
CO4								L		
CO5			S							M

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

- Concept Map


Email, Mobile Devices Security
Basics of email
*How email 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
*A brief introduction to security issues relevant to emails as well as the typical email infrastructure.
Simple Mail Transfer Protocol
*SMTP model including the basic structure as well as the extension model , The SMTP terminology
*SMTP procedures (session initiation, mail transaction, forwarding mail, relaying, mail gatewaying, support for mailing lists as well as aliases, termination etc)
*Important SMTP commands including their sequencing as well as the corresponding replies / response codes
*Commands for debugging addresses , SMTP trace information - Address resolution & mail handling
*Problem detection & handling , Security considerations
Focused attacks against email systems
*Common attacks against SMTP, POP3 and IMAP services , Vulnerabilities in web mail systems
*Exploits targeting the supporting infrastructure , Cryptographic techniques to protect against email eavesdropping and masquerading attacks
*Architectural guidelines for secure mail infrastructure , Hardening email infrastructure
Spam & Phishing
*History of Spam , Harvesting email addresses , Anonymous emails
*forging headers, using open relays & proxy servers, employing proxy chaining techniques, botnets , Sending Spam
*Tools of trade , Historical anti-spam approaches , Language classification and statistical filtering anti-spam techniques
*Anti-spam solution offerings , Definitions , What is phishing and what's not , Email security issues that aid in phishing
*Role of emails in common types of phishing attacks (impersonation, forwarding and popups) , Anti-phishing solution offerings
Email Forensics - Understanding message headers , Forging message headers and identifying forged headers
*General approaches to tracking the email sender General approaches to inspect attachments Spam and steganography.
Mobile & Wireless Devices
*Introduction : Types of Mobiles and wireless devices and their functionalities
*Proliferation of Mobile and Wireless Devices , Trends in Mobility
*Credit Card Frauds in Mobile and Wireless Computing
*Types and Techniques of Credit Card Frauds , Security Challenges Posed by Mobile Devices
*Registry Settings for Mobile Devices Authentication Service Security , Mobile phone camera and microphone hacking
*On-Screen Keyboard keyloggers - : Cryptographic Security for Mobile Devices , LDAP Security for Hand-Held Mobile Computing Devices
*RAS Security for Mobile Devices , Media Player Control Security , Networking API Security for Mobile Computing Applications
*Attacks on Mobile/Cell Phones , Mobile Phone Theft , Mobile Viruses , Mishing, Vishing, Smishing, Hacking Bluetooth
*Mobile Devices: Security Implications for Organizations: Managing Diversity and Proliferation of Hand-Held Devices, Unconventional/Stealth Storage Devices Threats through Lost and Stolen Devices
*Protecting Data on Lost Devices, Importance of Security Policies relating to Mobile Computing Devices, Operating Guidelines for Implementing Mobile Device Security Policies
*Organizational Policies for the Use of Mobile Hand-Held Devices, Laptops: Physical Security Countermeasures

Syllabus

Unit 1: Basics of email - How email 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 - A brief introduction to security issues relevant to emails as well as the typical email infrastructure. **(9hrs)**

Unit 2: Simple Mail Transfer Protocol - SMTP model including the basic structure as well as the extension model - The SMTP terminology - SMTP procedures (session initiation, mail transaction, forwarding mail, relaying, mail gatewaying, support for mailing lists as well as aliases, termination etc) - Important SMTP commands including their sequencing as well as the corresponding replies / response codes - Commands for debugging addresses - SMTP trace information - Address resolution & mail handling - Problem detection & handling - Security considerations **(14hrs)**

Unit 3: Focused attacks against email systems - Common attacks against SMTP, POP3 and IMAP services - Vulnerabilities in web mail systems - Exploits targeting the supporting infrastructure - Cryptographic techniques to protect against email eavesdropping and masquerading attacks - Architectural guidelines for secure mail infrastructure - Hardening email infrastructure **(10hrs)**

Unit 4: Spam & Phishing - History of Spam - Harvesting email addresses - Anonymous emails - forging headers, using open relays & proxy servers, employing proxy chaining techniques, botnets - Sending Spam - Tools of trade - Historical anti-spam approaches - Language classification and statistical filtering anti-spam techniques - Anti-spam solution offerings - Definitions - What is phishing and what's not - Email security issues that aid in phishing - Role of emails in common types of phishing attacks (impersonation, forwarding and popups) - Anti-phishing solution offerings **Email Forensics -** Understanding message headers - Forging message headers and identifying forged headers - General approaches to tracking the email sender - General approaches to inspect attachments - Spam and steganography. **(14hrs)**

Unit -5 Mobile & Wireless Devices : Introduction – Types of Mobiles and wireless devices and their functionalities - Proliferation of Mobile and Wireless Devices - Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing - Types and Techniques of Credit Card Frauds - Security Challenges Posed by Mobile Devices - Registry Settings for Mobile Devices Authentication Service Security - Mobile phone camera and microphone hacking - On-Screen Keyboard keyloggers - : Cryptographic Security for Mobile Devices - LDAP Security for Hand-Held Mobile Computing Devices - RAS Security for Mobile Devices - Media Player Control Security - Networking API Security for Mobile Computing Applications - Attacks on Mobile/Cell Phones - Mobile Phone Theft - Mobile Viruses - Mishing, Vishing, Smishing, Hacking Bluetooth - Mobile Devices: Security Implications for Organizations: Managing Diversity and Proliferation of Hand-Held Devices, Unconventional/Stealth Storage Devices Threats through Lost and Stolen Devices, Protecting Data on Lost Devices, Importance of Security Policies relating to Mobile Computing Devices, Operating Guidelines for Implementing Mobile Device Security Policies, Organizational Policies for the Use of Mobile Hand-Held Devices, Laptops: Physical Security Countermeasures **(15hrs)**

TOTAL (60hrs)

Reference Books:

1.Mobile Security and Privacy1st EditionAdvances, Challenges and Future Research Directions by Man Ho Au Raymond Choo

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**Basics of email** -	
1.1	How email works - The role of Mail User Agent, Mail Delivery Agent, Mail Transfer Agent, and DNS servers	2
1.2	An overview of various protocols (SMTP, POP, IMAP) involved in a typical email infrastructure	1
1.3	A brief introduction to security issues relevant to emails as well as the typical email infrastructure.	1
2	**Simple Mail Transfer Protocol**	
2.1	SMTP model including the basic structure as well as the extension model , The SMTP terminology	1
2.2	SMTP procedures (session initiation, mail transaction, forwarding mail, relaying, mail gatewaying, support for mailing lists as well as aliases, termination etc)	2
2.3	Important SMTP commands including their sequencing as well as the corresponding replies / response codes	2
2.4	Commands for debugging addresses , SMTP trace information - Address resolution & mail handling	1
2.5	Problem detection & handling , Security considerations	1
3	**Focused attacks against email systems**	
3.1	Common attacks against SMTP, POP3 and IMAP services , Vulnerabilities in web mail systems	1
3.2	Exploits targeting the supporting infrastructure , Cryptographic techniques to protect against email eavesdropping and masquerading attacks	2
3.3	Architectural guidelines for secure mail infrastructure , Hardening email infrastructure	1
4	**Spam & Phishing**	
4.1	History of Spam , Harvesting email addresses , Anonymous emails	1
4.2	forging headers, using open relays & proxy servers, employing proxy chaining techniques, botnets , Sending Spam	1
4.3	Tools of trade , Historical anti-spam approaches , Language classification and statistical filtering anti-spam techniques	1
4.4	Anti-spam solution offerings ,Definitions , What is phishing and what's not , Email security issues that aid in phishing	1
4.5	Role of emails in common types of phishing attacks (impersonation, forwarding and popups) , Anti-phishing solution offerings	1
4.6	**Email Forensics -** Understanding message headers , Forging message headers and identifying forged headers	1
4.7	General approaches to tracking the email sender General approaches	1

	to inspect attachments Spam and steganography.	
5	**Mobile & Wireless Devices**	
5.1	Introduction : Types of Mobiles and wireless devices and their functionalities	1
5.2	Proliferation of Mobile and Wireless Devices , Trends in Mobility	1
5.3	Credit Card Frauds in Mobile and Wireless Computing	1
5.4	Types and Techniques of Credit Card Frauds , Security Challenges Posed by Mobile Devices	1
5.5	Registry Settings for Mobile Devices Authentication Service Security , Mobile phone camera and microphone hacking	1
5.6	On-Screen Keyboard keyloggers - : Cryptographic Security for Mobile Devices , LDAP Security for Hand-Held Mobile Computing Devices	1
5.7	RAS Security for Mobile Devices , Media Player Control Security , Networking API Security for Mobile Computing Applications	1
5.8	Attacks on Mobile/Cell Phones , Mobile Phone Theft , Mobile Viruses ,Mishing, Vishing, Smishing, Hacking Bluetooth	1
5.9	Mobile Devices: Security Implications for Organizations: Managing Diversity and Proliferation of Hand-Held Devices, Unconventional/Stealth Storage Devices Threats through Lost and Stolen Devices	2
5.10	Protecting Data on Lost Devices, Importance of Security Policies relating to Mobile Computing Devices, Operating Guidelines for Implementing Mobile Device Security Policies	2
5.11	Organizational Policies for the Use of Mobile Hand-Held Devices, Laptops: Physical Security Countermeasures	1

Mobile And Wireless Security	Category	L	P	Credit
	PE	3	0	3

Preamble

It is a sub-domain of computer security, network security, and, more broadly, information security.

Prerequisite

- Network Security

Course Outcomes

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

Course Outcomes		Level
CO1	Understanding security and privacy for mobile and wireless networks	Understand
CO2	Study the concepts in mobile security	Apply
CO3	Learn the securing wireless networks	Understanding
CO4	Study the adhoc network security concepts	Apply
CO5	Know about the RFID security	Understanding

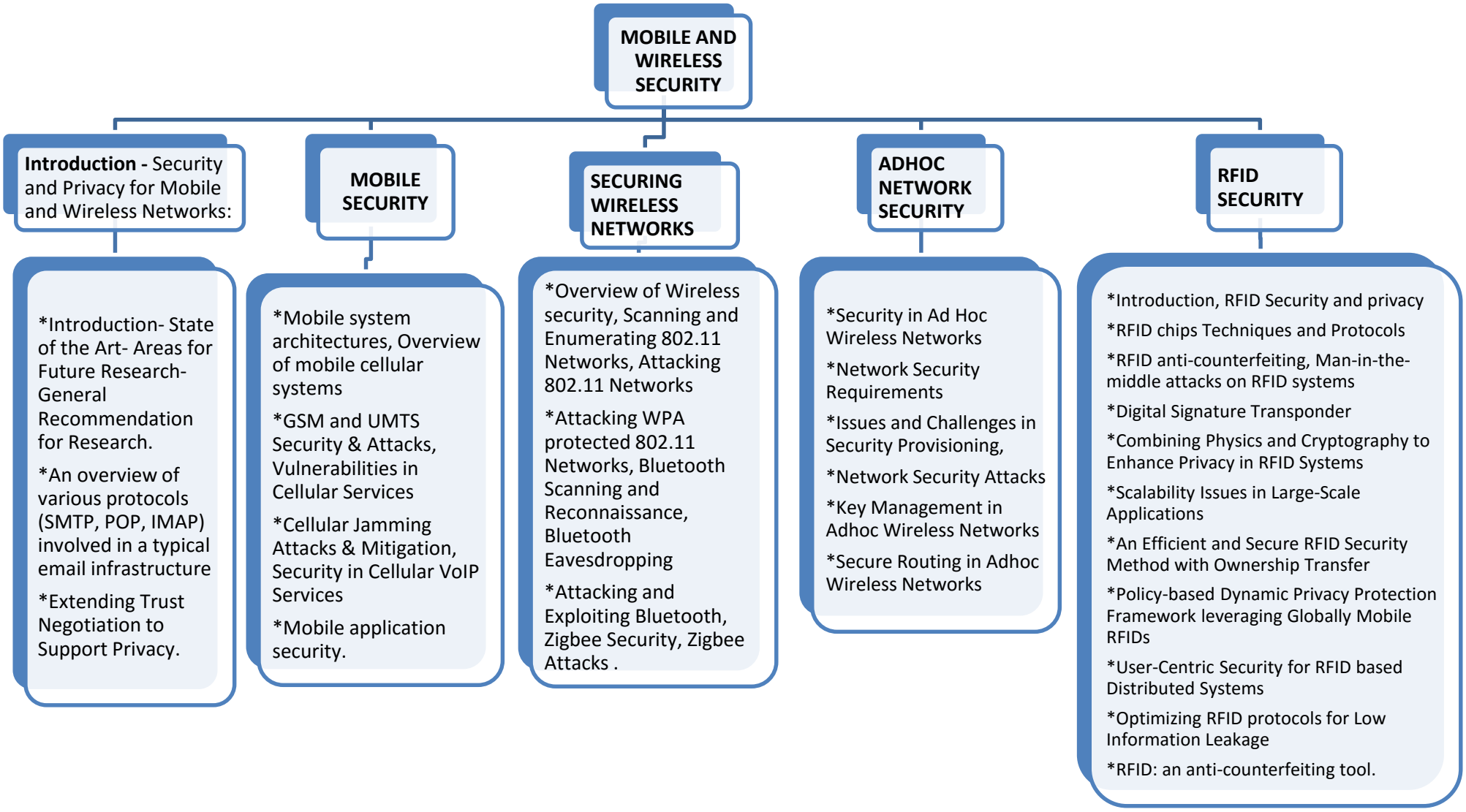
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1							M			
CO2	S	M		L						
CO3					M					
CO4			M					M		
CO5							L			M

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


MOBILE AND WIRELESS SECURITY
Introduction - Security and Privacy for Mobile and Wireless Networks:
*Introduction- State of the Art- Areas for Future Research- General Recommendation for Research.
*An overview of various protocols (SMTP, POP, IMAP) involved in a typical email infrastructure
*Extending Trust Negotiation to Support Privacy.
MOBILE SECURITY
*Mobile system architectures, Overview of mobile cellular systems
*GSM and UMTS Security & Attacks, Vulnerabilities in Cellular Services
*Cellular Jamming Attacks & Mitigation, Security in Cellular VoIP Services
*Mobile application security.
SECURING WIRELESS NETWORKS
*Overview of Wireless security, Scanning and Enumerating 802.11 Networks, Attacking 802.11 Networks
*Attacking WPA protected 802.11 Networks, Bluetooth Scanning and Reconnaissance, Bluetooth Eavesdropping
*Attacking and Exploiting Bluetooth, Zigbee Security, Zigbee Attacks .
ADHOC NETWORK SECURITY
*Security in Ad Hoc Wireless Networks
*Network Security Requirements
*Issues and Challenges in Security Provisioning,
*Network Security Attacks
*Key Management in Adhoc Wireless Networks
*Secure Routing in Adhoc Wireless Networks
RFID SECURITY
*Introduction, RFID Security and privacy
*RFID chips Techniques and Protocols
*RFID anti-counterfeiting, Man-in-the-middle attacks on RFID systems
*Digital Signature Transponder
*Combining Physics and Cryptography to Enhance Privacy in RFID Systems
*Scalability Issues in Large-Scale Applications
*An Efficient and Secure RFID Security Method with Ownership Transfer
*Policy-based Dynamic Privacy Protection Framework leveraging Globally Mobile RFIDs
*User-Centric Security for RFID based Distributed Systems
*Optimizing RFID protocols for Low Information Leakage
*RFID: an anti-counterfeiting tool.

Syllabus

UNIT I - INTRODUCTION: Security and Privacy for Mobile and Wireless Networks: Introduction- State of the Art- Areas for Future Research- General Recommendation for Research. Pervasive Systems: Enhancing Trust Negotiation with Privacy Support: Trust Negotiation- Weakness of Trust Negotiation- Extending Trust Negotiation to Support Privacy.
(12hrs)

UNIT II - MOBILE SECURITY: Mobile system architectures, Overview of mobile cellular systems, GSM and UMTS Security & Attacks, Vulnerabilities in Cellular Services, Cellular Jamming Attacks & Mitigation, Security in Cellular VoIP Services, Mobile application security.
(10hrs)

UNIT III - SECURING WIRELESS NETWORKS: Overview of Wireless security, Scanning and Enumerating 802.11 Networks, Attacking 802.11 Networks, Attacking WPA protected 802.11 Networks, Bluetooth Scanning and Reconnaissance, Bluetooth Eavesdropping, Attacking and Exploiting Bluetooth, Zigbee Security, ZigbeeAttacks . **(12hrs)**

UNIT IV - ADHOC NETWORK SECURITY : Security in Ad Hoc Wireless Networks, Network Security Requirements, Issues and Challenges in Security Provisioning, Network Security Attacks, Key Management in Adhoc Wireless Networks, Secure Routing in Adhoc Wireless Networks **(12hrs)**

UNIT V-RFID SECURITY : Introduction, RFID Security and privacy, RFID chips Techniques and Protocols, RFID anti-counterfeiting, Man-in-the-middle attacks on RFID systems, Digital Signature Transponder, Combining Physics and Cryptography to Enhance Privacy in RFID Systems, Scalability Issues in Large-Scale Applications, An Efficient and Secure RFID Security Method with Ownership Transfer, Policy-based Dynamic Privacy Protection Framework leveraging Globally Mobile RFIDs, User-Centric Security for RFID based Distributed Systems, Optimizing RFID protocols for Low Information Leakage, RFID: an anti-counterfeiting tool.
(14hrs)

Total(60hrs)

Reference Books:

1. Kia Makki, Peter Reiher, "Mobile and Wireless Network Security and Privacy", Springer, ISBN 978-0-387-71057-0, 2007.
2. C. Siva Ram Murthy, B.S. Manoj, "Adhoc Wireless Networks Architectures and Protocols", Prentice Hall, x ISBN 9788131706885, 2007.
3. NoureddineBoudriga, "Security of Mobile Communications", ISBN 9780849379413, 2010.
4. Kitsos, Paris; Zhang, Yan , "RFID Security Techniques, Protocols and System-On-Chip Design ", ISBN 978-0-387-76481-8, 2008.
5. Johny Cache, Joshua Wright and Vincent Liu," Hacking Wireless Exposed: Wireless Security Secrets & Solutions ", second edition, McGraw Hill, ISBN: 978-0-07-166662-6, 2010.

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**Introduction -** Security and Privacy for Mobile and Wireless Networks:	
1.1	Introduction- State of the Art- Areas for Future Research- General Recommendation for Research.	2
1.2	An overview of various protocols (SMTP, POP, IMAP) involved in a typical email infrastructure	2
1.3	Extending Trust Negotiation to Support Privacy.	1
2	**MOBILE SECURITY:**	
2.1	Mobile system architectures, Overview of mobile cellular systems	1
2.2	GSM and UMTS Security & Attacks, Vulnerabilities in Cellular Services	2
2.3	Cellular Jamming Attacks & Mitigation, Security in Cellular VoIP Services	2
2.4	Mobile application security.	1
3	**SECURING WIRELESS NETWORKS:**	
3.1	Overview of Wireless security, Scanning and Enumerating 802.11 Networks, Attacking 802.11 Networks	1
3.2	Attacking WPA protected 802.11 Networks, Bluetooth Scanning and Reconnaissance, Bluetooth Eavesdropping	2
3.3	Attacking and Exploiting Bluetooth, Zigbee Security, ZigbeeAttacks .	1
4	**ADHOC NETWORK SECURITY :**	
4.1	Security in Ad Hoc Wireless Networks	1
4.2	Network Security Requirements	1
4.3	Issues and Challenges in Security Provisioning,	1
4.4	Network Security Attacks	1
4.5	Key Management in Adhoc Wireless Networks	1
4.6	Secure Routing in Adhoc Wireless Networks	1
5	**RFID SECURITY :**	
5.1	Introduction, RFID Security and privacy	1
5.2	RFID chips Techniques and Protocols	1
5.3	RFID anti-counterfeiting, Man-in-the-middle attacks on RFID systems	2
5.4	Digital Signature Transponder	1
5.5	Combining Physics and Cryptography to Enhance Privacy in RFID Systems	1
5.6	Scalability Issues in Large-Scale Applications	1
5.7	An Efficient and Secure RFID Security Method with Ownership Transfer	1
5.8	Policy-based Dynamic Privacy Protection Framework leveraging Globally Mobile RFIDs	2
5.9	User-Centric Security for RFID based Distributed Systems	2
5.10	Optimizing RFID protocols for Low Information Leakage	2
5.11	RFID: an anti-counterfeiting tool.	1

Fundamentals of Blockchains and Crypto-currency	Category	L	P	Credit
	PE	3	0	3

Preamble

Blockchain and Cryptocurrencies are fast becoming a worldwide Tour De Force that is taking all markets and industries by storm.

Prerequisite

- Network Security

Course Outcomes

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

Course Outcomes		Level
CO1	Learn basic concepts of block-chains	Understanding
CO2	Understanding the crypto-currency technology	Understanding
CO3	Know the block chain architecture	Understanding
CO4	Study the block chain applications	Understanding
CO5	Learn the regulatory frameworks	Understanding

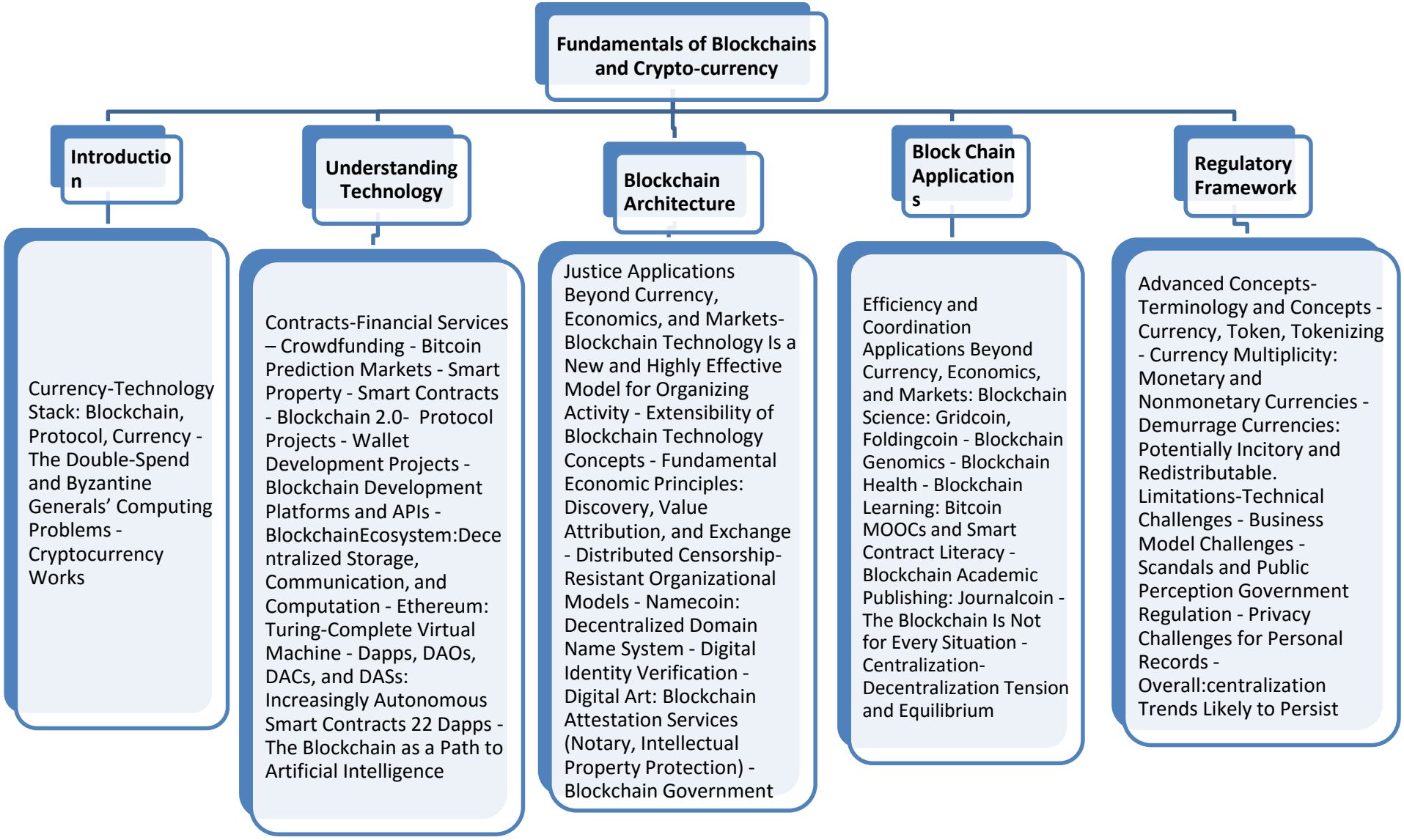
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1										
CO2	S							S		M
CO3				M					M	
CO4			L					L		
CO5	M	L				M				M

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


Fundamentals of Blockchains and Crypto-currency
Introduction
Currency-Technology Stack: Blockchain, Protocol, Currency - The Double-Spend and Byzantine Generals' Computing Problems - Cryptocurrency Works
Understanding Technology
Contracts-Financial Services – Crowdfunding - Bitcoin Prediction Markets - Smart Property - Smart Contracts - Blockchain 2.0- Protocol Projects - Wallet Development Projects - Blockchain Development Platforms and APIs - BlockchainEcosystem:Decentralized Storage, Communication, and Computation - Ethereum: Turing-Complete Virtual Machine - Dapps, DAOs, DACs, and DASs: Increasingly Autonomous Smart Contracts 22 Dapps - The Blockchain as a Path to Artificial Intelligence
Blockchain Architecture
Justice Applications Beyond Currency, Economics, and Markets- Blockchain Technology Is a New and Highly Effective Model for Organizing Activity - Extensibility of Blockchain Technology Concepts - Fundamental Economic Principles: Discovery, Value Attribution, and Exchange - Distributed Censorship-Resistant Organizational Models - Namecoin: Decentralized Domain Name System - Digital Identity Verification - Digital Art: Blockchain Attestation Services (Notary, Intellectual Property Protection) - Blockchain Government
Block Chain Applications
Efficiency and Coordination Applications Beyond Currency, Economics, and Markets: Blockchain Science: Gridcoin, Foldingcoin - Blockchain Genomics - Blockchain Health - Blockchain Learning: Bitcoin MOOCs and Smart Contract Literacy - Blockchain Academic Publishing: Journalcoin - The Blockchain Is Not for Every Situation - Centralization-Decentralization Tension and Equilibrium
Regulatory Framework
Advanced Concepts-Terminology and Concepts - Currency, Token, Tokenizing - Currency Multiplicity: Monetary and Nonmonetary Currencies - Demurrage Currencies: Potentially Incitory and Redistributable. Limitations-Technical Challenges - Business Model Challenges - Scandals and Public Perception Government Regulation - Privacy Challenges for Personal Records - Overall:centralization Trends Likely to Persist

Syllabus

Unit 1: Currency-Technology Stack: Blockchain, Protocol, Currency - The Double-Spend and Byzantine Generals' Computing Problems - Cryptocurrency Works **(12hrs)**

Unit 2: Contracts-Financial Services – Crowdfunding - Bitcoin Prediction Markets - Smart Property - Smart Contracts - Blockchain 2.0- Protocol Projects - Wallet Development Projects - Blockchain Development Platforms and APIs – Blockchain Ecosystem: Decentralized Storage, Communication, and Computation - Ethereum: Turing-Complete Virtual Machine - Dapps, DAOs, DACs, and DASs: Increasingly Autonomous Smart Contracts 22 Dapps - The Blockchain as a Path to Artificial Intelligence **(12hrs)**

Unit 3: Justice Applications Beyond Currency, Economics, and Markets-Blockchain Technology Is a New and Highly Effective Model for Organizing Activity - Extensibility of Blockchain Technology Concepts - Fundamental Economic Principles: Discovery, Value Attribution, and Exchange - Distributed Censorship-Resistant Organizational Models - Namecoin: Decentralized Domain Name System - Digital Identity Verification - Digital Art: Blockchain Attestation Services (Notary, Intellectual Property Protection) - Blockchain Government**(12hrs)**

Unit 4: Efficiency and Coordination Applications Beyond Currency, Economics, and Markets: Blockchain Science: Gridcoin, Foldingcoin - Blockchain Genomics - Blockchain Health - Blockchain Learning: Bitcoin MOOCs and Smart Contract Literacy - Blockchain Academic Publishing: Journalcoin - The Blockchain Is Not for Every Situation - Centralization-Decentralization Tension and Equilibrium **(12hrs)**

Unit 5: Advanced Concepts-Terminology and Concepts - Currency, Token, Tokenizing - Currency Multiplicity: Monetary and Nonmonetary Currencies - Demurrage Currencies: Potentially Incitory and Redistributable. Limitations-Technical Challenges - Business Model Challenges - Scandals and Public Perception Government Regulation - Privacy Challenges for Personal Records - Overall: centralization Trends Likely to Persist **(12hrs)**

TOTAL (60Hrs)

Textbook:

Blockchain - Blueprint for a New Economy : Melanie Swan, OREILLY

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**Introduction**	
1.1	Currency-Technology Stack: Blockchain, Protocol, Currency -	2
1.2	The Double-Spend and Byzantine Generals' Computing Problems -	2
1.3	Cryptocurrency Works	2
2	**Contracts-Financial Services**	
2.1	– Crowdfunding - Bitcoin Prediction Markets - Smart Property - Smart Contracts -	2
2.2	Blockchain 2.0- Protocol Projects - Wallet Development Projects - Blockchain Development Platforms and APIs -	3
2.3	BlockchainEcosystem:Decentralized Storage, Communication, and Computation - Ethereum: Turing-Complete Virtual Machine -	2
2.4	Dapps, DAOs, DACs, and DASs: Increasingly Autonomous Smart Contracts 22 Dapps - The Blockchain as a Path to Artificial Intelligence	1
3	**Justice Applications Beyond Currency, Economics, and Markets-**	
3.1	Blockchain Technology Is a New and Highly Effective Model for Organizing Activity -	2
3.2	Extensibility of Blockchain Technology Concepts - Fundamental Economic Principles: Discovery, Value Attribution, and Exchange - Distributed Censorship	2
3.3	-Resistant Organizational Models - Namecoin: Decentralized Domain Name System - Digital Identity Verification - Digital Art: Blockchain Attestation Services (Notary, Intellectual Property Protection) - Blockchain Government	2
4	**Efficiency and Coordination Applications Beyond Currency, Economics, and Markets:**	
4.1	Blockchain Science: Gridcoin, Foldingcoin - Blockchain Genomics - Blockchain Health -	1
4.2	Blockchain Learning: Bitcoin MOOCs and Smart Contract Literacy - Blockchain Academic Publishing:	2
4.3	Journalcoin - The Blockchain Is Not for Every Situation - Centralization-Decentralization Tension and Equilibrium	2
5	**Advanced Concepts-Terminology and Concepts -**	
5.1	Currency, Token, Tokenizing - Currency Multiplicity: Monetary and Nonmonetary Currencies - Demurrage	1
5.2	Currencies: Potentially Incitory and Redistributable. Limitations-Technical Challenges	1
5.3	- Business Model Challenges - Scandals and Public Perception Government Regulation -	2
5.4	Privacy Challenges for Personal Records - Overall:centralization Trends Likely to Persist	1

Storage management & security	Category	L	P	Credit
	PE	3	0	3

Preamble

Storage security is the collective processes, tools and technologies that ensure that only authorized and legitimate users store, access and use storage resources. It enables better security of any storage resource through the implementation of required technologies and policies on storage access and consumption and the denial of access to all unidentified and potentially malicious users.

Prerequisite

- Nil

Course Outcomes

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

Course Outcomes		Level
CO1	Study the concepts in storage systems	Understanding
CO2	Understand the idea of networking in network area	Understanding
CO3	Learn backup and recoversy mechanisms	Apply
CO4	Know the storage security	Understanding
CO5	Study the storage infrastructure management	Understanding

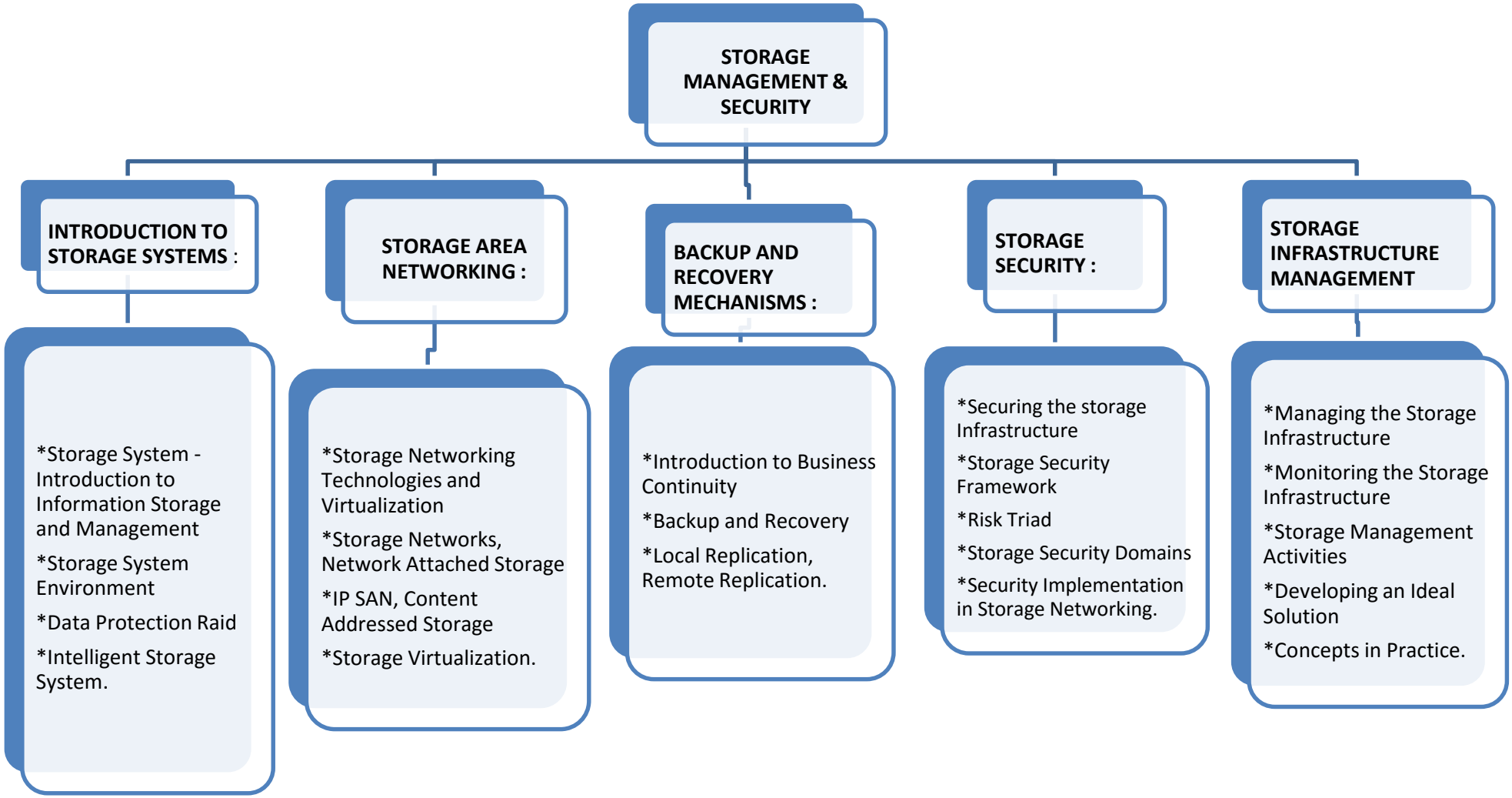
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	M									
CO2		M		S				S		
CO3					L					L
CO4							L			
CO5						M			M	

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


STORAGE MANAGEMENT & SECURITY
INTRODUCTION TO STORAGE SYSTEMS :
*Storage System - Introduction to Information Storage and Management
*Storage System Environment
*Data Protection Raid
*Intelligent Storage System.
STORAGE AREA NETWORKING :
*Storage Networking Technologies and Virtualization
*Storage Networks, Network Attached Storage
*IP SAN, Content Addressed Storage
*Storage Virtualization.
BACKUP AND RECOVERY MECHANISMS :
*Introduction to Business Continuity
*Backup and Recovery
*Local Replication, Remote Replication.
STORAGE SECURITY :
*Securing the storage Infrastructure
*Storage Security Framework
*Risk Triad
*Storage Security Domains
*Security Implementation in Storage Networking.
STORAGE INFRASTRUCTURE MANAGEMENT
*Managing the Storage Infrastructure
*Monitoring the Storage Infrastructure
*Storage Management Activities
*Developing an Ideal Solution
*Concepts in Practice.

Syllabus

Unit – I – Introduction to Storage Systems: Storage System - Introduction to Information Storage and Management, Storage System Environment, Data Protection Raid, Intelligent Storage System. **(12hrs)**

Unit – II – Storage Area Networking: Storage Networking Technologies and Virtualization, Storage Networks, Network Attached Storage, IP SAN, Content Addressed Storage, Storage Virtualization. **(12hrs)**

Unit – III - Backup and Recovery Mechanisms: Introduction to Business Continuity, Backup and Recovery, Local Replication, Remote Replication. **(12hrs)**

Unit – IV – Storage Security: Securing the storage Infrastructure, Storage Security Framework, Risk Triad, Storage Security Domains, Security Implementation in Storage Networking. **(12hrs)**

Unit – V – Storage Infrastructure Management: Managing the Storage Infrastructure, Monitoring the Storage Infrastructure, Storage Management Activities, Developing an Ideal Solution, Concepts in Practice. **(12hrs)**

Total (60Hrs)

Reference Books:

1. Information Storage and Management, "Storing, Managing, and Protecting Digital Information", Wiley; 1 edition, EMC Corporation, 2009.
2. John Chirillo, Scott Blaul, "Storage Security: Protecting SAN, NAS and DAS", Wiley Publishers, 2003.
3. David Alexander , Amanda French , David Sutton ,"Information Security Management Principles" The British Computer Society, 2008.

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**INTRODUCTION TO STORAGE SYSTEMS** :	
1.1	Storage System - Introduction to Information Storage and Management	2
1.2	Storage System Environment	2
1.3	Data Protection Raid	2
	Intelligent Storage System.	2
2	**STORAGE AREA NETWORKING :**	
2.1	Storage Networking Technologies and Virtualization	2
2.2	Storage Networks, Network Attached Storage	3
2.3	IP SAN, Content Addressed Storage	2
2.4	Storage Virtualization.	1
3	**BACKUP AND RECOVERY MECHANISMS :**	
3.1	Introduction to Business Continuity	2
3.2	Backup and Recovery	2
3.3	Local Replication, Remote Replication.	2
4	**STORAGE SECURITY :**	
4.1	Securing the storage Infrastructure	1
4.2	Storage Security Framework	2
4.3	Risk Triad	2
4.4	Storage Security Domains	1
4.5	Security Implementation in Storage Networking.	2
5	**STORAGE INFRASTRUCTURE MANAGEMENT :**	
5.1	Managing the Storage Infrastructure	1
5.2	Monitoring the Storage Infrastructure	1
5.3	Storage Management Activities	2
5.4	Developing an Ideal Solution	1
5.5	Concepts in Practice.	1

Big data technology	Category	L	P	Credit
	PE	3	0	3

Preamble

BIG DATA is a term used for a collection of data sets so large and complex that it is difficult to process using traditional applications/tools. It is the data exceeding Terabytes in size. Because of the variety of data that it encompasses, big data always brings a number of challenges relating to its volume and complexity.

Prerequisite

Nil

Course Outcomes

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

Course Outcomes		Level
CO1	Understand the concepts of distributed file system	Understanding
CO2	Learn abstraction of hadoop environment	Understanding
CO3	Study the hadoop architecture	Understanding
CO4	Know the hadoop ecosystem and yarn components	Understanding
CO5	Learn different architecture like HIVE and HIVEQL, HBASE	Apply

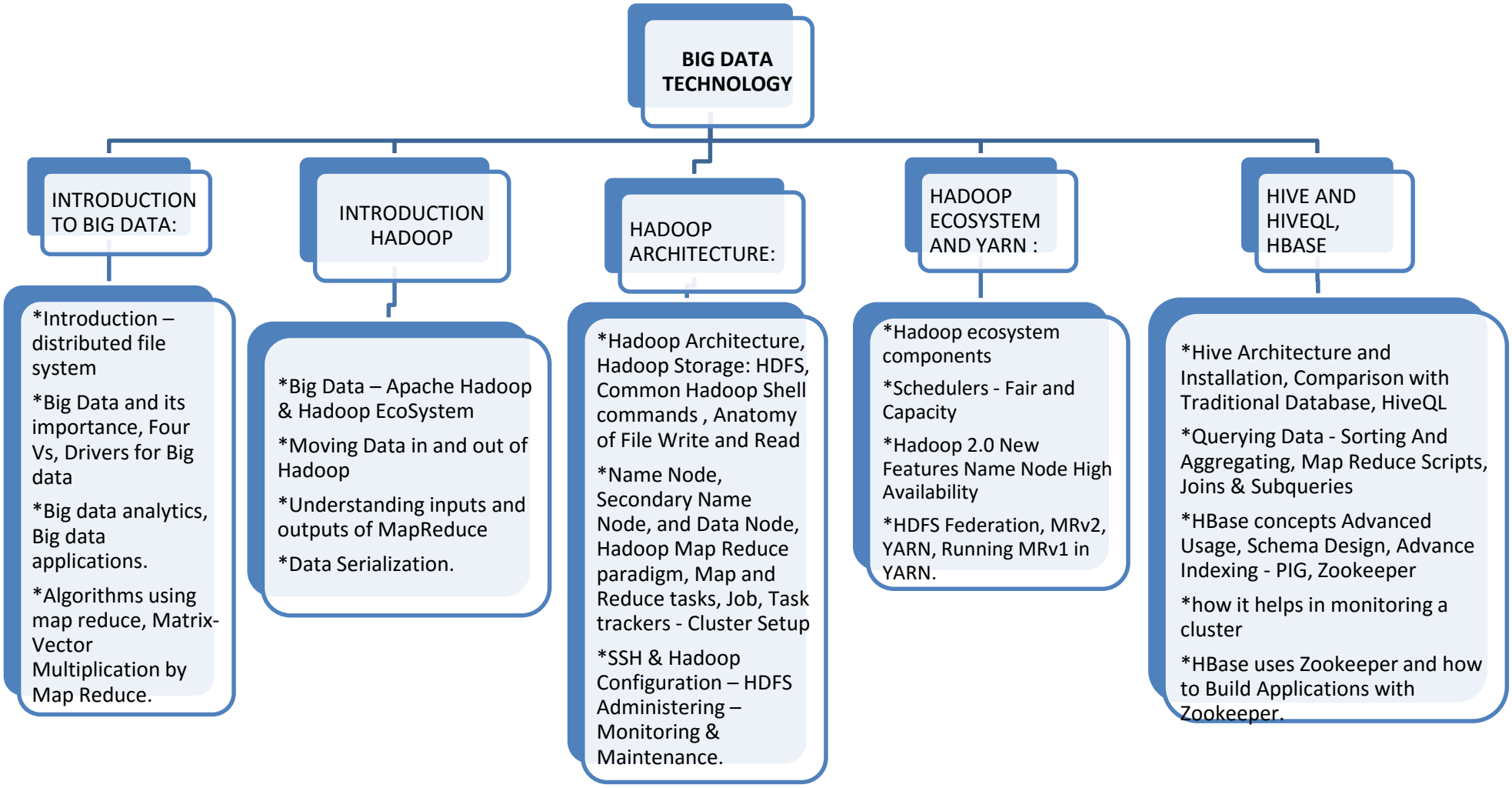
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	M									
CO2		L			S			S		
CO3			M			M				M
CO4									M	
CO5				L		M	M			

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


BIG DATA TECHNOLOGY
INTRODUCTION TO BIG DATA:
*Introduction – distributed file system
*Big Data and its importance, Four Vs, Drivers for Big data
*Big data analytics, Big data applications.
*Algorithms using map reduce, Matrix-Vector Multiplication by Map Reduce.
INTRODUCTION HADOOP
*Big Data – Apache Hadoop & Hadoop EcoSystem
*Moving Data in and out of Hadoop
*Understanding inputs and outputs of MapReduce
*Data Serialization.
HADOOP ARCHITECTURE:
*Hadoop Architecture, Hadoop Storage: HDFS, Common Hadoop Shell commands , Anatomy of File Write and Read
*Name Node, Secondary Name Node, and Data Node, Hadoop Map Reduce paradigm, Map and Reduce tasks, Job, Task trackers - Cluster Setup
*SSH & Hadoop Configuration – HDFS Administering – Monitoring & Maintenance.
HADOOP ECOSYSTEM AND YARN :
*Hadoop ecosystem components
*Schedulers - Fair and Capacity
*Hadoop 2.0 New Features Name Node High Availability
*HDFS Federation, MRv2, YARN, Running MRv1 in YARN.
HIVE AND HIVEQL, HBASE
*Hive Architecture and Installation, Comparison with Traditional Database, HiveQL
*Querying Data - Sorting And Aggregating, Map Reduce Scripts, Joins & Subqueries
*HBase concepts Advanced Usage, Schema Design, Advance Indexing - PIG, Zookeeper
*how it helps in monitoring a cluster
*HBase uses Zookeeper and how to Build Applications with Zookeeper.

Syllabus

Unit I – **Introduction to Big Data:** Introduction- Distributed file system – Big Data and its importance, Four Vs, Drivers for Big data, Big data analytics, Big data applications. Algorithms using map reduce, Matrix-Vector Multiplication by Map Reduce. **(12hrs)**

Unit II – Introduction Hadoop: Big Data – Apache Hadoop & Hadoop Eco System – Moving Data in and out of Hadoop – Understanding inputs and outputs of Map Reduce - Data Serialization. **(12hrs)**

Unit- III Hadoop Architecture: Hadoop Architecture, Hadoop Storage: HDFS, Common Hadoop Shell commands , Anatomy of File Write and Read., Name Node, Secondary Name Node, and Data Node, Hadoop Map Reduce paradigm, Map and Reduce tasks, Job, Task trackers - Cluster Setup – SSH &Hadoop Configuration – HDFS Administering –Monitoring & Maintenance. **(12hrs)**

Unit-IV Hadoop Ecosystem and Yarn : Hadoop ecosystem components - Schedulers - Fair and Capacity, Hadoop 2.0 New Features Name Node High Availability, HDFS Federation, MRv2, YARN, Running MRv1 in YARN. **(10hrs)**

Unit-V HIVE AND HIVEQL, HBASE : Hive Architecture and Installation, Comparison with Traditional Database, HiveQL - Querying Data - Sorting And Aggregating, Map Reduce Scripts, Joins &Subqueries, HBase concepts Advanced Usage, Schema Design, Advance Indexing - PIG, Zookeeper - how it helps in monitoring a cluster, HBase uses Zookeeper and how to Build Applications with Zookeeper. **(14hrs)**

Total (60hrs)

Reference Books:

1. Boris lublinsky, Kevin t. Smith, Alexey Yakubovich, “Professional Hadoop Solutions”, Wiley, ISBN: 9788126551071, 2015.
2. Chris Eaton, Dirk deroos et al., “Understanding Big data”, McGraw Hill, 2012.
3. Tom White, “HADOOP: The definitive Guide”, O Reilly 2012. 6 IT2015 SRM (E&T)
4. VigneshPrajapati, “Big Data Analytics with R and Haoop”, Packet Publishing 2013.
5. Tom Plunkett, Brian Macdonald et al, “Oracle Big Data Handbook”, Oracle Press, 2014.
6. http://www.bigdatauniversity.com/
7. JyLiebowitz, “Big Data and Business analytics”,CRC press, 2013.

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**INTRODUCTION TO BIG DATA:**	
1.1	Introduction – distributed file system	2
1.2	Big Data and its importance, Four Vs, Drivers for Big data	2
1.3	Big data analytics, Big data applications.	2
1.4	Algorithms using map reduce, Matrix-Vector Multiplication by Map Reduce.	2
2	**INTRODUCTION HADOOP**	
2.1	Big Data – Apache Hadoop&HadoopEcoSystem	2
2.2	Moving Data in and out of Hadoop	3
2.3	Understanding inputs and outputs of MapReduce	2
2.4	Data Serialization.	1
3	**HADOOP ARCHITECTURE:**	
3.1	Hadoop Architecture, Hadoop Storage: HDFS, Common Hadoop Shell commands , Anatomy of File Write and Read	3
3.2	Name Node, Secondary Name Node, and Data Node, Hadoop Map Reduce paradigm, Map and Reduce tasks, Job, Task trackers - Cluster Setup	3
3.3	SSH &Hadoop Configuration – HDFS Administering –Monitoring & Maintenance.	2
4	**HADOOP ECOSYSTEM AND YARN :**	
4.1	Hadoop ecosystem components	1
4.2	Schedulers - Fair and Capacity	2
4.3	Hadoop 2.0 New Features Name Node High Availability	2
4.4	HDFS Federation, MRv2, YARN, Running MRv1 in YARN.	1
5	**HIVE AND HIVEQL, HBASE**	
5.1	Hive Architecture and Installation, Comparison with Traditional Database, HiveQL	1
5.2	- Querying Data - Sorting And Aggregating, Map Reduce Scripts, Joins &Subqueries	1
5.3	HBase concepts Advanced Usage, Schema Design, Advance Indexing - PIG, Zookeeper	2
5.4	how it helps in monitoring a cluster	1
5.5	HBase uses Zookeeper and how to Build Applications with Zookeeper.	1

ANDROID MOBILE APPLICATION DEVELOPMENT	**L**	**T**	**P**	**C**
	3			**3**

Preamble

The mobile application development landscape uses Android as the platform.The basics of the Android platform, Android application components, Activities and their lifecycle, UI design, Multimedia, 2D graphics and networking support in Android.

Prerequisite

- Nil

Course Outcomes

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

Course Outcomes		Level
CO1	Learn the basic elements in module computing	Apply
CO2	Know the concepts of android	Understanding
CO3	Understand the android activities and GUI design concepts	Understanding
CO4	Know the advanced UI programming	Understanding
CO5	Learn toast, menu dialog, list and adapters	Understanding

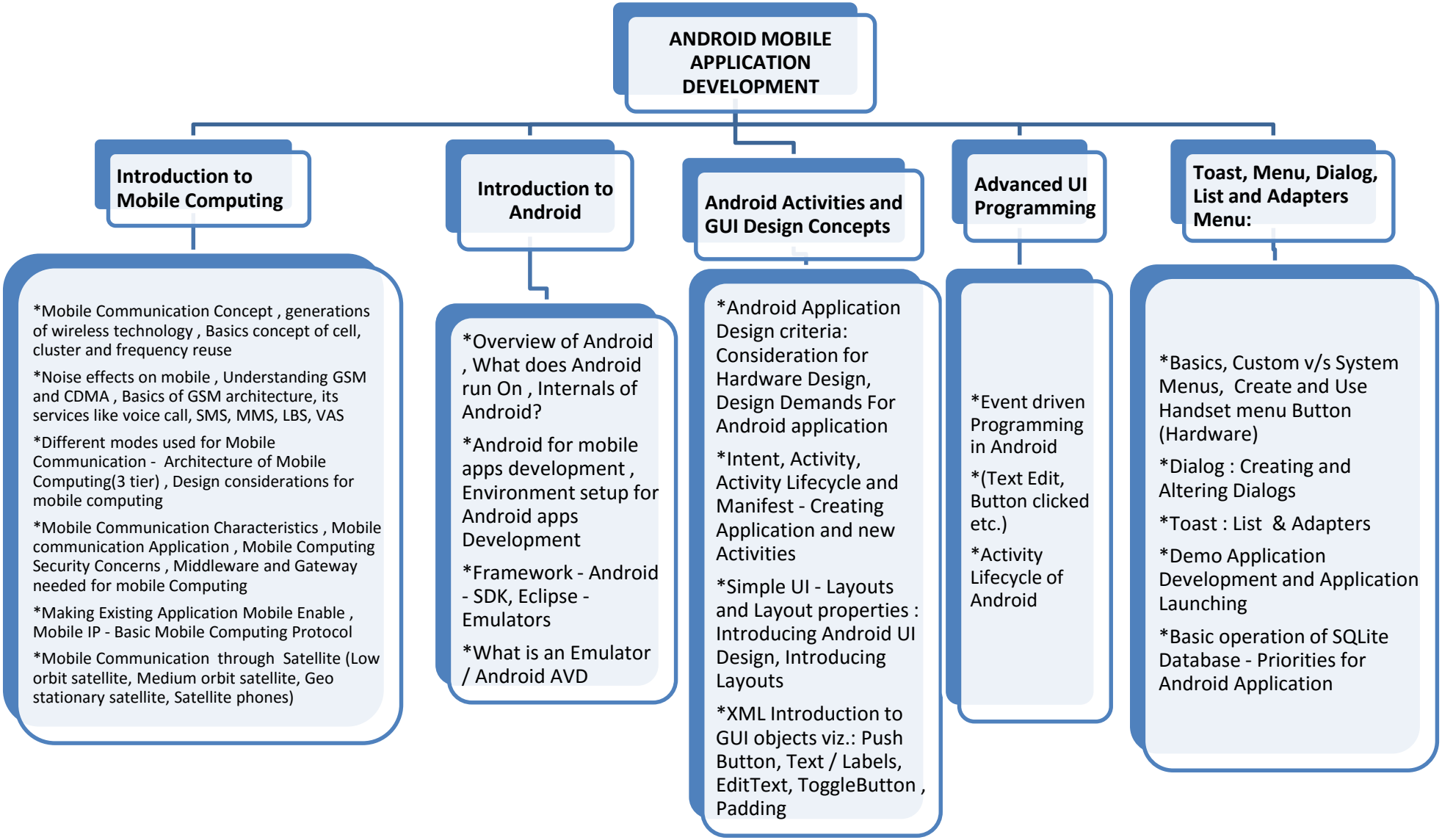
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	M	M								S
CO2								L		
CO3		M		S	L				L	
CO4						M				
CO5			S							

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


ANDROID MOBILE APPLICATION DEVELOPMENT
Introduction to Mobile Computing
*Mobile Communication Concept , generations of wireless technology , Basics concept of cell, cluster and frequency reuse
*Noise effects on mobile , Understanding GSM and CDMA , Basics of GSM architecture, its services like voice call, SMS, MMS, LBS, VAS
*Different modes used for Mobile Communication - Architecture of Mobile Computing(3 tier) , Design considerations for mobile computing
*Mobile Communication Characteristics , Mobile communication Application , Mobile Computing Security Concerns , Middleware and Gateway needed for mobile Computing
*Making Existing Application Mobile Enable , Mobile IP - Basic Mobile Computing Protocol
*Mobile Communication through Satellite (Low orbit satellite, Medium orbit satellite, Geo stationary satellite, Satellite phones)
Introduction to Android
*Overview of Android , What does Android run On , Internals of Android?
*Android for mobile apps development , Environment setup for Android apps Development
*Framework - Android - SDK, Eclipse - Emulators
*What is an Emulator / Android AVD
Android Activities and GUI Design Concepts
*Android Application Design criteria: Consideration for Hardware Design, Design Demands For Android application
*Intent, Activity, Activity Lifecycle and Manifest - Creating Application and new Activities
*Simple UI - Layouts and Layout properties : Introducing Android UI Design, Introducing Layouts
*XML Introduction to GUI objects viz.: Push Button, Text / Labels, EditText, ToggleButton , Padding
Advanced UI Programming
*Event driven Programming in Android
*(Text Edit, Button clicked etc.)
*Activity Lifecycle of Android
Toast, Menu, Dialog, List and Adapters Menu:
*Basics, Custom v/s System Menus, Create and Use Handset menu Button (Hardware)
*Dialog : Creating and Altering Dialogs
*Toast : List & Adapters
*Demo Application Development and Application Launching
*Basic operation of SQLite Database - Priorities for Android Application

Syllabus

UNIT –I Introduction to Mobile Computing Mobile Communication Concept - generations of wireless technology – Basics concept of cell, cluster and frequency reuse - Noise effects on mobile - Understanding GSM and CDMA - Basics of GSM architecture, its services like voice call, SMS, MMS, LBS, VAS - Different modes used for Mobile Communication - Architecture of Mobile Computing(3 tier) - Design considerations for mobile computing - Mobile Communication Characteristics - Mobile communication Application - Mobile Computing Security Concerns - Middleware and Gateway needed for mobile Computing - Making Existing Application Mobile Enable - Mobile IP - Basic Mobile Computing Protocol - Mobile Communication through Satellite (Low orbit satellite, Medium orbit satellite, Geo stationary satellite, Satellite phones) **(14hrs)**

UNIT–II Introduction to Android Overview of Android - What does Android run On - Internals of Android? - Android for mobile apps development - Environment setup for Android apps Development - Framework - Android - SDK, Eclipse - Emulators –What is an Emulator / Android AVD **(10hrs)**

UNIT –III Android Activities and GUI Design Concepts Android Application Design criteria: Consideration for Hardware Design, Design Demands For Android application, Intent, Activity, Activity Lifecycle and Manifest - Creating Application and new Activities - Simple UI - Layouts and Layout properties : Introducing Android UI Design, Introducing Layouts - XML Introduction to GUI objects viz.: Push Button, Text / Labels , EditText, Toggle Button , Padding **(13hrs)**

UNIT –IV Advanced UI Programming Event driven Programming in Android - (Text Edit, Button clicked etc.) - Activity Lifecycle of Android **(11hrs)**

UNIT –V Toast, Menu, Dialog, List and Adapters Menu: Basics, Custom v/s System Menus, Create and Use Handset menu Button (Hardware) - Dialog : Creating and Altering Dialogs - Toast : List & Adapters - Demo Application Development and Application Launching - Basic operation of SQLite Database - Priorities for Android Application **(12hrs)**

Total (60hrs)

Books:

1J.F.De Marzio, Android –A Programmer's Guide, McGraw Hill Pub, 2008.
2. Building Android Apps IN EASY STEPS McGraw - Hill Education
3.Professional Android 2 Application Development by Reto Meier, Wiley India Pvt Ltd.,2012
4.Beginning Android by Mark L Murphy,Wiley India Pvt Ltd.,2015
5. Pro Android, by Sayed Y Hashimi and SatyaKomatineni Wiley India Pvt Ltd., 2015

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**Introduction to Mobile Computing**	
1.1	Mobile Communication Concept , generations of wireless technology , Basics concept of cell, cluster and frequency reuse	2
1.2	Noise effects on mobile , Understanding GSM and CDMA , Basics of GSM architecture, its services like voice call, SMS, MMS, LBS, VAS	2
1.3	Different modes used for Mobile Communication - Architecture of Mobile Computing(3 tier) , Design considerations for mobile computing	2
1.4	Mobile Communication Characteristics , Mobile communication Application , Mobile Computing Security Concerns , Middleware and Gateway needed for mobile Computing	2
1.5	Making Existing Application Mobile Enable , Mobile IP - Basic Mobile Computing Protocol	1
1.6	Mobile Communication through Satellite (Low orbit satellite, Medium orbit satellite, Geo stationary satellite, Satellite phones)	1
2	**Introduction to Android**	
2.1	Overview of Android , What does Android run On , Internals of Android?	2
2.2	Android for mobile apps development , Environment setup for Android apps Development	2
2.3	Framework - Android - SDK, Eclipse - Emulators	2
2.4	What is an Emulator / Android AVD	1
3	**Android Activities and GUI Design Concepts**	
3.1	Android Application Design criteria: Consideration for Hardware Design, Design Demands For Android application	3
3.2	Intent, Activity, Activity Lifecycle and Manifest - Creating Application and new Activities	2
3.3	Simple UI - Layouts and Layout properties : Introducing Android UI Design, Introducing Layouts	2
	XML Introduction to GUI objects viz.: Push Button, Text / Labels, EditText, ToggleButton , Padding	1
4	**Advanced UI Programming**	
4.1	Event driven Programming in Android	1
4.2	(Text Edit, Button clicked etc.)	2
4.3	Activity Lifecycle of Android	2
5	**Toast, Menu, Dialog, List and Adapters Menu:**	
5.1	Basics, Custom v/s System Menus, Create and Use Handset menu Button (Hardware)	1
5.2	Dialog : Creating and Altering Dialogs	1
5.3	Toast : List & Adapters	2
5.4	Demo Application Development and Application Launching	1
5.5	Basic operation of SQLite Database - Priorities for Android	1

	Application	

Fundamentals of Research Methods and Statistical Applications	**L**	**T**	**P**	**C**
	3			**3**

Preamble

Statistics is the science of collecting, analyzing and making inference from data. Statistics is a particularly useful branch of mathematics that is not only studied theoretically by advanced mathematicians but one that is used by researchers in many fields to organize, analyze, and summarize data.

Prerequisite

- Nil

Course Outcomes

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

Course Outcomes		Level
CO1	Learn the concepts of research methods and statistical applications	Understanding
CO2	Understand the research formulation	Understanding
CO3	Study the research design and methods	Understanding
CO4	Learn data collection and analysis	Understanding
CO5	Know the structure of reporting and thesis writing	Understanding

Mapping with Programme Outcomes

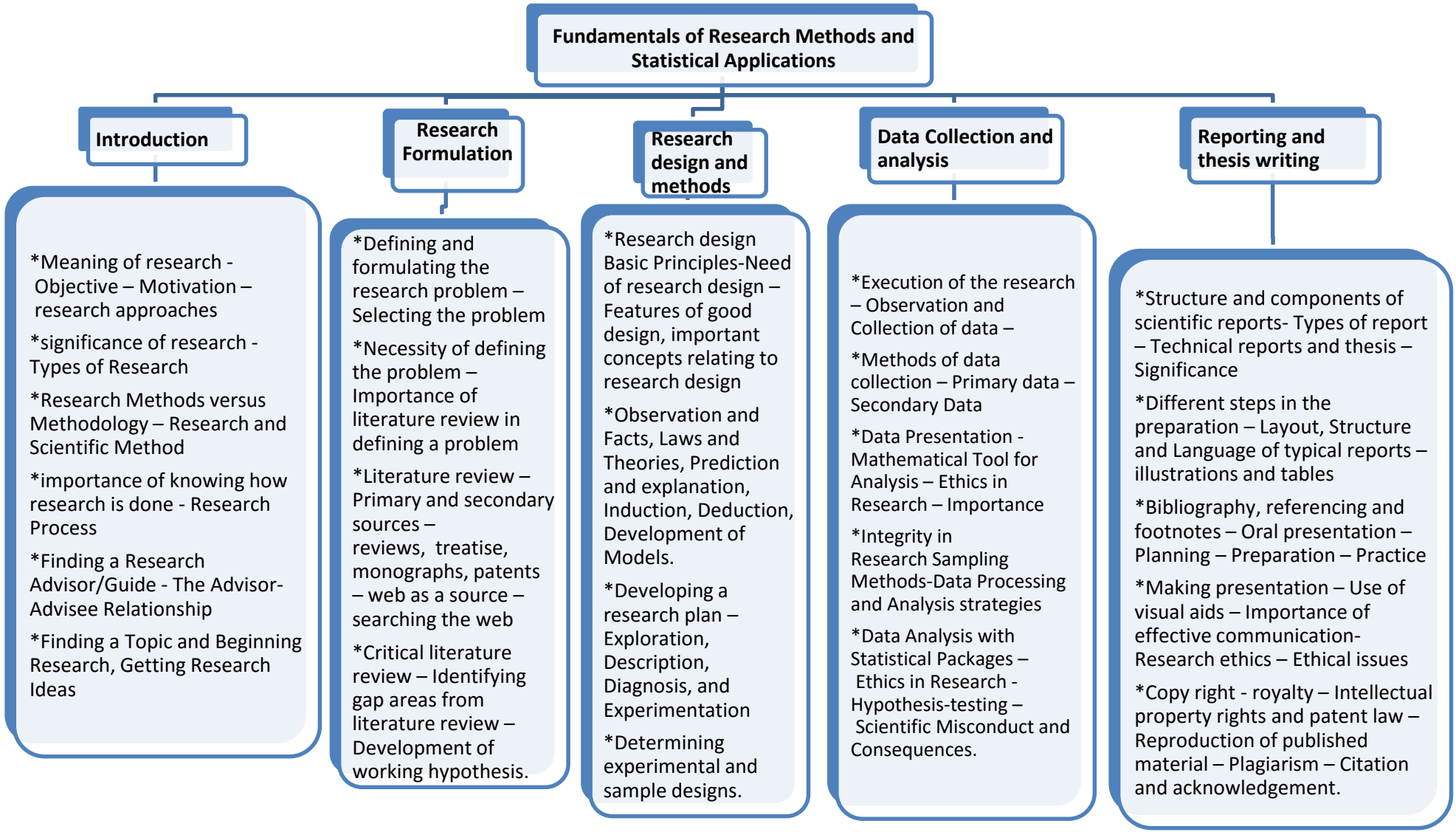
Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	M									
CO2				M						
CO3		L	M							L
CO4					L			M		
CO5							L			

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map

-


Fundamentals of Research Methods and Statistical Applications
Introduction
*Meaning of research - Objective – Motivation – research approaches
*significance of research - Types of Research
*Research Methods versus Methodology – Research and Scientific Method
*importance of knowing how research is done - Research Process
*Finding a Research Advisor/Guide - The Advisor-Advisee Relationship
*Finding a Topic and Beginning Research, Getting Research Ideas
Research Formulation
*Defining and formulating the research problem – Selecting the problem
*Necessity of defining the problem – Importance of literature review in defining a problem
*Literature review – Primary and secondary sources – reviews, treatise, monographs, patents – web as a source – searching the web
*Critical literature review – Identifying gap areas from literature review – Development of working hypothesis.
Research design and methods
*Research design Basic Principles-Need of research design – Features of good design, important concepts relating to research design
*Observation and Facts, Laws and Theories, Prediction and explanation, Induction, Deduction, Development of Models.
*Developing a research plan – Exploration, Description, Diagnosis, and Experimentation
*Determining experimental and sample designs.
Data Collection and analysis
*Execution of the research – Observation and Collection of data –
*Methods of data collection – Primary data – Secondary Data
*Data Presentation - Mathematical Tool for Analysis – Ethics in Research – Importance
*Integrity in Research Sampling Methods-Data Processing and Analysis strategies
*Data Analysis with Statistical Packages – Ethics in Research - Hypothesis-testing – Scientific Misconduct and Consequences.
Reporting and thesis writing
*Structure and components of scientific reports- Types of report – Technical reports and thesis – Significance
*Different steps in the preparation – Layout, Structure and Language of typical reports – illustrations and tables
*Bibliography, referencing and footnotes – Oral presentation – Planning – Preparation – Practice
*Making presentation – Use of visual aids – Importance of effective communication- Research ethics – Ethical issues
*Copy right - royalty – Intellectual property rights and patent law – Reproduction of published material – Plagiarism – Citation and acknowledgement.

Syllabus

Unit I - Introduction – Meaning of research - Preamble – Motivation – research approaches - significance of research - Types of Research – Research Methods versus Methodology – Research and Scientific Method – importance of knowing how research is done - Research Process – Finding a Research Advisor/Guide - The Advisor-Advisee Relationship - Finding a Topic and Beginning Research, Getting Research Ideas **(12hrs)**

Unit-II – Research Formulation – Defining and formulating the research problem – Selecting the problem – Necessity of defining the problem – Importance of literature review in defining a problem – Literature review – Primary and secondary sources – reviews, treatise, monographs, patents – web as a source – searching the web- Critical literature review – Identifying gap areas from literature review – Development of working hypothesis. **(12hrs)**

Unit-III – Research design and methods – Research design Basic Principles-Need of research design – Features of good design – important concepts relating to research design – Observation and Facts, Laws and Theories, Prediction and explanation, Induction, Deduction, Development of Models. Developing a research plan – Exploration, Description, Diagnosis, and Experimentation, Determining experimental and sample designs. **(12hrs)**

Unit-IV – Data Collection and analysis- Execution of the research – Observation and Collection of data – Methods of data collection – Primary data – Secondary Data – Data Presentation - Mathematical Tool for Analysis – Ethics in Research – Importance – Integrity in Research Sampling Methods-Data Processing and Analysis strategies – Data Analysis with Statistical Packages – Ethics in Research - Hypothesis-testing – Scientific Misconduct and Consequences . **(11hrs)**

Unit-V – Reporting and thesis writing – Structure and components of scientific reports- Types of report – Technical reports and thesis – Significance – Different steps in the preparation – Layout, Structure and Language of typical reports – illustrations and tables – Bibliography, referencing and footnotes – Oral presentation – Planning – Preparation – Practice – Making presentation – Use of visual aids – Importance of effective communication-Research ethics – Ethical issues – Copy right - royalty – Intellectual property rights and patent law – Reproduction of published material – Plagiarism – Citation and acknowledgement. **(12hrs)**

Total (60hrs)

Books:

1. "Engineering Research Methodology: A Computer Science and Engineering and Information and Communication Technologies Perspective", KrishnanNallaperumal, https://www.researchgate.net/publication/259183120_Engineering_Research_Methodology_A_Computer_Science_and_Engineering_and_Information_and_Communication_Technologies_Perspective
2. Kothari, C.R, 2014. *Research Methodology*: Methods and Techniques, New age International, 3rdEdition.
3. KavadiaGerg, Agarwal&Agarwal, 2002, Introduction to *Research Methodology*, RBSA Publishers.
4. Agarwal, B.L., 2015, Comprehensive *Research Methodology*, New age International, 1st edition.

5. Mukul Gupta, Deepa Gupta, 2011, *Research Methodology,* PHI publisher

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**Introduction**	
1.1	Meaning of research - Objective – Motivation – research approaches	2
1.2	significance of research - Types of Research	1
1.3	Research Methods versus Methodology – Research and Scientific Method	1
	importance of knowing how research is done - Research Process	2
	Finding a Research Advisor/Guide - The Advisor-Advisee Relationship	1
	Finding a Topic and Beginning Research, Getting Research Ideas	1
2	**Research Formulation**	
2.1	Defining and formulating the research problem – Selecting the problem	2
2.2	Necessity of defining the problem – Importance of literature review in defining a problem	2
2.3	Literature review – Primary and secondary sources – reviews, treatise, monographs, patents – web as a source – searching the web	2
2.4	Critical literature review – Identifying gap areas from literature review – Development of working hypothesis.	1
3	**Research design and methods**	
3.1	Research design Basic Principles-Need of research design – Features of good design, important concepts relating to research design	2
3.2	Observation and Facts, Laws and Theories, Prediction and explanation, Induction, Deduction, Development of Models.	2
3.3	Developing a research plan – Exploration, Description, Diagnosis, and Experimentation	2
	Determining experimental and sample designs.	1
4	**Data Collection and analysis-**	
4.1	Execution of the research – Observation and Collection of data –	1
4.2	Methods of data collection – Primary data – Secondary Data	2
4.3	Data Presentation - Mathematical Tool for Analysis – Ethics in Research – Importance	2
	Integrity in Research Sampling Methods-Data Processing and Analysis strategies	1
	Data Analysis with Statistical Packages – Ethics in Research - Hypothesis-testing – Scientific Misconduct and Consequences.	2
5	**Reporting and thesis writing**	
5.1	Structure and components of scientific reports- Types of report – Technical reports and thesis – Significance	1
5.2	Different steps in the preparation – Layout, Structure and Language of typical reports – illustrations and tables	1
5.3	Bibliography, referencing and footnotes – Oral presentation – Planning – Preparation – Practice	2
5.4	Making presentation – Use of visual aids – Importance of effective communication-Research ethics – Ethical issues	1
5.5	Copy right - royalty – Intellectual property rights and patent law – Reproduction of published material – Plagiarism – Citation and acknowledgement.	1

Mobile And Digital Forensics	Category	L	P	Credit
	PE	3	0	3

Preamble

Mobile device forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions. The phrase mobile device usually refers to mobile phones; however, it can also relate to any digital device that has both internal memory and communication ability, including PDA devices, GPS devices and tablet computers.

Prerequisite

- Introduction to Digital Forensics

Course Outcomes

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

Course Outcomes		Level
CO1	Learn concepts of wireless technologies	Understanding
CO2	Study the security framework for mobile systems	Apply
CO3	Know the mobile phone forensics	Understanding
CO4	Understand the basis in digital forensics	Apply
CO5	Understand the analysis of digital forensic techniques	Apply

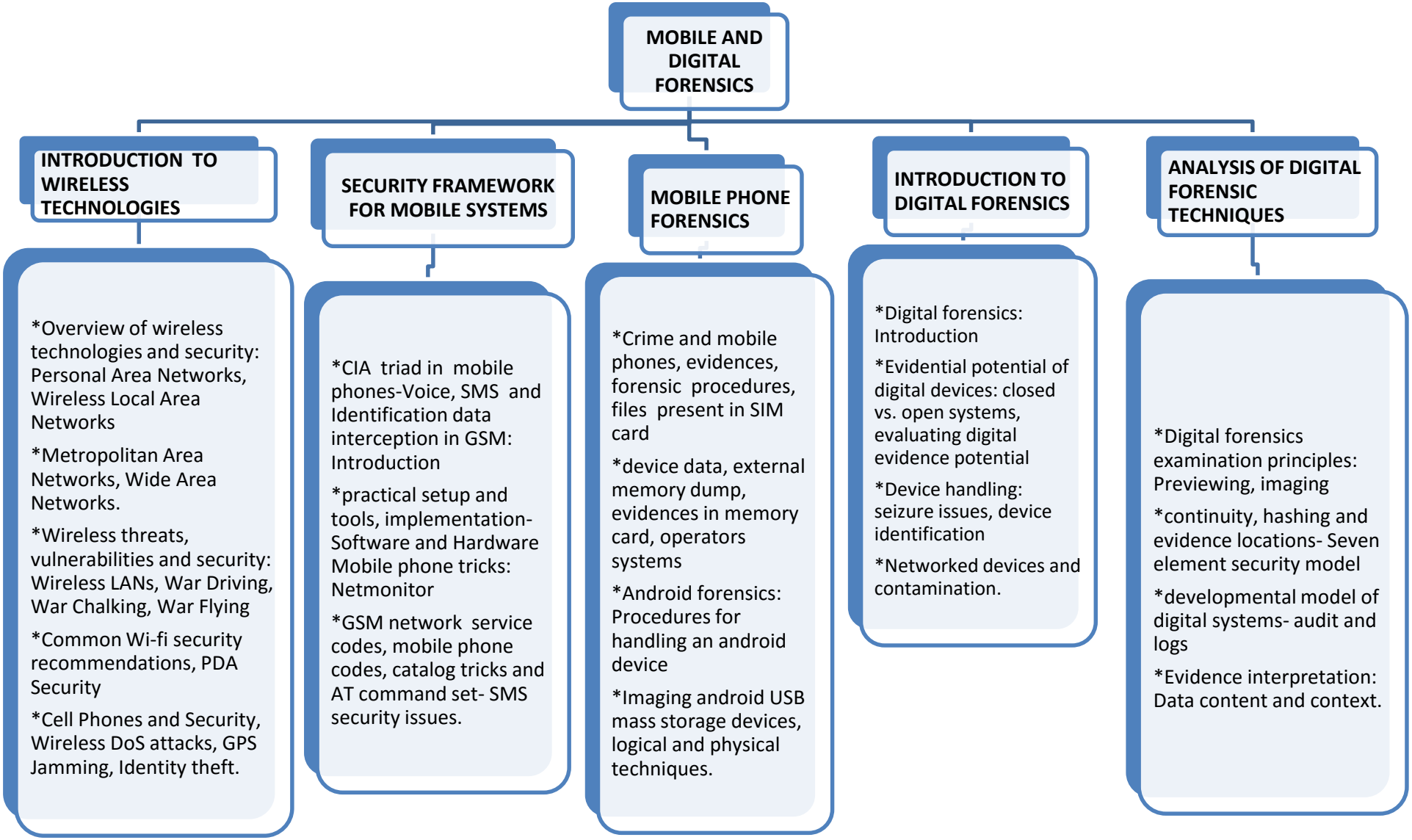
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1					S		M			
CO2										L
CO3				M		L		M		
CO4	M	L								
CO5										S

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


MOBILE AND DIGITAL FORENSICS
INTRODUCTION TO WIRELESS TECHNOLOGIES
*Overview of wireless technologies and security: Personal Area Networks, Wireless Local Area Networks
*Metropolitan Area Networks, Wide Area Networks.
*Wireless threats, vulnerabilities and security: Wireless LANs, War Driving, War Chalking, War Flying
*Common Wi-fi security recommendations, PDA Security
*Cell Phones and Security, Wireless DoS attacks, GPS Jamming, Identity theft.
SECURITY FRAMEWORK FOR MOBILE SYSTEMS
*CIA triad in mobile phones-Voice, SMS and Identification data interception in GSM: Introduction
*practical setup and tools, implementation-Software and Hardware Mobile phone tricks: Netmonitor
*GSM network service codes, mobile phone codes, catalog tricks and AT command set- SMS security issues.
MOBILE PHONE FORENSICS
*Crime and mobile phones, evidences, forensic procedures, files present in SIM card
*device data, external memory dump, evidences in memory card, operators systems
*Android forensics: Procedures for handling an android device
*Imaging android USB mass storage devices, logical and physical techniques.
INTRODUCTION TO DIGITAL FORENSICS
*Digital forensics: Introduction
*Evidential potential of digital devices: closed vs. open systems, evaluating digital evidence potential
*Device handling: seizure issues, device identification
*Networked devices and contamination.
ANALYSIS OF DIGITAL FORENSIC TECHNIQUES
*Digital forensics examination principles: Previewing, imaging
*continuity, hashing and evidence locations- Seven element security model
*developmental model of digital systems- audit and logs
*Evidence interpretation: Data content and context.

Syllabus

UNIT – I INTRODUCTION TO WIRELESS TECHNOLOGIES: Overview of wireless technologies and security: Personal Area Networks, Wireless Local Area Networks, Metropolitan Area Networks, Wide Area Networks. Wireless threats, vulnerabilities and security: Wireless LANs, War Driving, War Chalking, War Flying, Common Wi-fi security recommendations, PDA Security, Cell Phones and Security, Wireless DoS attacks, GPS Jamming, Identity theft. **(13hrs)**

UNIT – II SECURITY FRAMEWORK FOR MOBILE SYSTEMS : CIA triad in mobile phones-Voice, SMS and Identification data interception in GSM: Introduction, practical setup and tools, implementation- Software and Hardware Mobile phone tricks: Netmonitor, GSM network service codes, mobile phone codes, catalog tricks and AT command set- SMS security issues. **(12hrs)**

UNIT – III MOBILE PHONE FORENSICS : Crime and mobile phones, evidences, forensic procedures, files present in SIM card, device data, external memory dump, evidences in memory card, operators systems- Android forensics: Procedures for handling an android device, imaging android USB mass storage devices, logical and physical techniques. **(11hrs)**

UNIT – IV INTRODUCTION TO DIGITAL FORENSICS : Digital forensics: Introduction – Evidential potential of digital devices: closed vs. open systems, evaluating digital evidence potential- Device handling: seizure issues, device identification, networked devices and contamination. **(12hrs)**

UNIT – V ANALYSIS OF DIGITAL FORENSIC TECHNIQUES : Digital forensics examination principles: Previewing, imaging, continuity, hashing and evidence locations- Seven element security model- developmental model of digital systems- audit and logs- Evidence interpretation: Data content and context. **(12hrs)**

Total (60hrs)

Books:

1. Gregory Kipper, "Wireless Crime and Forensic Investigation", Auerbach Publications, 2007.
2. Iosif I. Androulidakis, " Mobile phone security and forensics: A practical approach", Springer publications, 2012.
3. Andrew Hoog, "Android Forensics: Investigation, Analysis and Mobile Security for Google Android", Elsevier publications, 2011.
4. Angus M.Marshall, " Digital forensics: Digital evidence in criminal investigation", John – Wiley and Sons, 2008.

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**INTRODUCTION TO WIRELESS TECHNOLOGIES**	
1.1	Overview of wireless technologies and security: Personal Area Networks, Wireless Local Area Networks	3
1.2	Metropolitan Area Networks, Wide Area Networks.	1
1.3	Wireless threats, vulnerabilities and security: Wireless LANs, War Driving, War Chalking, War Flying	3
	Common Wi-fi security recommendations, PDA Security	2
	Cell Phones and Security, Wireless DoS attacks, GPS Jamming, Identity theft.	1
2	**SECURITY FRAMEWORK FOR MOBILE SYSTEMS**	
2.1	CIA triad in mobile phones-Voice, SMS and Identification data interception in GSM: Introduction	2
2.2	practical setup and tools, implementation- Software and Hardware Mobile phone tricks: Netmonitor	2
2.3	GSM network service codes, mobile phone codes, catalog tricks and AT command set- SMS security issues.	3
3	**MOBILE PHONE FORENSICS**	
3.1	Crime and mobile phones, evidences, forensic procedures, files present in SIM card	2
3.2	device data, external memory dump, evidences in memory card, operators systems	2
3.3	Android forensics: Procedures for handling an android device	2
	Imaging android USB mass storage devices, logical and physical techniques.	2
4	**INTRODUCTION TO DIGITAL FORENSICS**	
4.1	Digital forensics: Introduction	1
4.2	Evidential potential of digital devices: closed vs. open systems, evaluating digital evidence potential	2
4.3	Device handling: seizure issues, device identification	2
4.4	Networked devices and contamination.	1
5	**ANALYSIS OF DIGITAL FORENSIC TECHNIQUES**	
5.1	Digital forensics examination principles: Previewing, imaging	1
5.2	continuity, hashing and evidence locations- Seven element security model	1
5.3	developmental model of digital systems- audit and logs	2
5.4	Evidence interpretation: Data content and context.	1

Data Mining And Warehousing	Category	L	P	Credit
	PE	3	0	3

Preamble

Collections of databases that work together are called data warehouses. This makes it possible to integrate data from multiple databases. Data mining is used to help individuals and organizations make better decisions.

Prerequisite

- database management

Course Outcomes

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

Course Outcomes		Level
CO1	Learn data mining concepts	Understanding
CO2	Study the steps in knowledge discovery process	Understanding
CO3	Learn the data warehouse architecture	Understanding
CO4	Understand the hardware and operational design of data warehouse	Understanding
CO5	Know the planning, tuning and testing	Apply

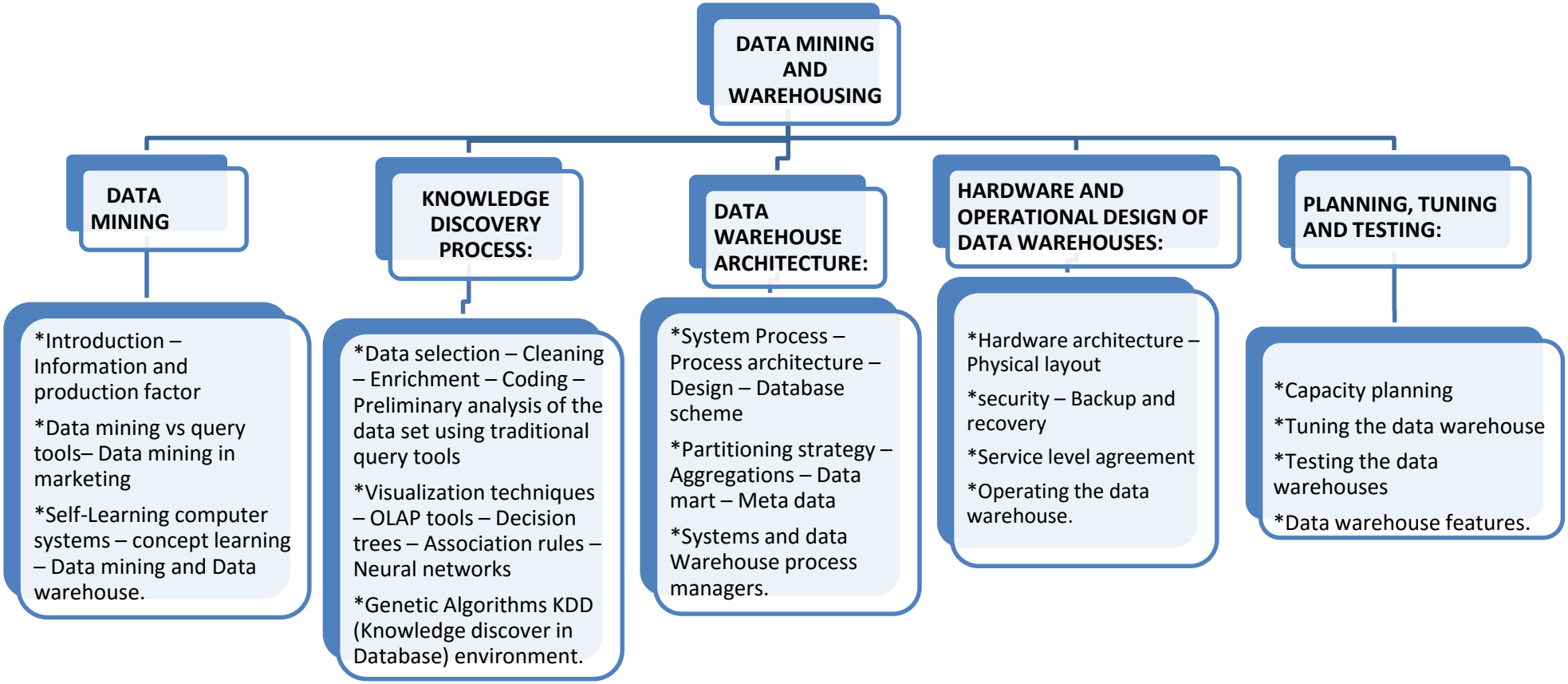
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1									L	
CO2			M		S					
CO3		M					L			
CO4								S		
CO5	L									

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


DATA MINING AND WAREHOUSING
DATA MINING
*Introduction – Information and production factor
*Data mining vs query tools– Data mining in marketing
*Self-Learning computer systems – concept learning – Data mining and Data warehouse.
KNOWLEDGE DISCOVERY PROCESS:
*Data selection – Cleaning – Enrichment – Coding – Preliminary analysis of the data set using traditional query tools
*Visualization techniques – OLAP tools – Decision trees – Association rules – Neural networks
*Genetic Algorithms KDD (Knowledge discover in Database) environment.
DATA WAREHOUSE ARCHITECTURE:
*System Process – Process architecture – Design – Database scheme
*Partitioning strategy – Aggregations – Data mart – Meta data
*Systems and data Warehouse process managers.
HARDWARE AND OPERATIONAL DESIGN OF DATA WAREHOUSES:
*Hardware architecture – Physical layout
*security – Backup and recovery
*Service level agreement
*Operating the data warehouse.
PLANNING, TUNING AND TESTING:
*Capacity planning
*Tuning the data warehouse
*Testing the data warehouses
*Data warehouse features.

Syllabus

UNIT I Data Mining : Introduction – Information and production factor – Data mining vs query tools– Data mining in marketing – Self learning computer systems – concept learning – Data mining and Data warehouse. **(12hrs)**

Unit II Knowledge discovery process: Data selection – Cleaning – Enrichment – Coding – Preliminary analysis of the data set using traditional query tools – Visualization techniques – OLAP tools – Decision trees – Association rules – Neural networks – Genetic Algorithms KDD (Knowledge discover in Database) environment. **(13hrs)**

Unit III Data warehouse Architecture: System Process – Process architecture – Design – Database scheme – Partitioning strategy – Aggregations – Data mart – Meta data – Systems and data Warehouse process managers. **(12hrs)**

Unit IV Hardware and operational design of data warehouses – Hardware architecture – Physical layout – security – Backup and recovery – Service level agreement – operating the data warehouse. **(12hrs)**

Unit V Planning, Tuning and Testing: Capacity planning – Tuning the data warehouse – Testing the data warehouses – Data warehouse features. **(12hrs)**

Total (60hrs)

Books:

1. Pieter Adriaans, DolfZantinge, Data Mining, Addison Wesley 1996
2. Sam Anahory, Dennis Muray, Data Warehousing in the real world, Addison Wesley 1996
3. Sean Kelly, Data WareHousing in Action, John Wiley 1997.

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**DATA MINING**	
1.1	Introduction – Information and production factor	3
1.2	Data mining vs query tools– Data mining in marketing	1
1.3	Self-Learning computer systems – concept learning – Data mining and Data warehouse.	3
2	**KNOWLEDGE DISCOVERY PROCESS:**	
2.1	Data selection – Cleaning – Enrichment – Coding – Preliminary analysis of the data set using traditional query tools	3
2.2	Visualization techniques – OLAP tools – Decision trees – Association rules – Neural networks	2
2.3	Genetic Algorithms KDD (Knowledge discover in Database) environment.	3
3	**DATA WAREHOUSE ARCHITECTURE:**	
3.1	System Process – Process architecture – Design – Database scheme	2
3.2	Partitioning strategy – Aggregations – Data mart – Meta data	2
3.3	Systems and data Warehouse process managers.	2
4	**HARDWARE AND OPERATIONAL DESIGN OF DATA WAREHOUSES:**	
4.1	Hardware architecture – Physical layout	2
4.2	security – Backup and recovery	2
4.3	Service level agreement	2
4.4	Operating the data warehouse.	2
5	**PLANNING, TUNING AND TESTING:**	
5.1	Capacity planning	2
5.2	Tuning the data warehouse	2
5.3	Testing the data warehouses	2
5.4	Data warehouse features.	1

Big Data Security	Category	L	P	Credit
	PE	3	0	3

Preamble

Big Data security is the processing of guarding data and analytics processes, both in the cloud and on-premise, from any number of factors that could compromise their confidentiality.

Prerequisite

- Information security

Course Outcomes

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

Course Outcomes		Level
CO1	Know the big data privacy, ethics and security	Understanding
CO2	Study the security, compliance, auditing and protection of data	Understanding
CO3	Learn hadoop security design	Apply
CO4	Understand hadoop ecosystem security	Apply
CO5	Know data security and event logging	Understanding

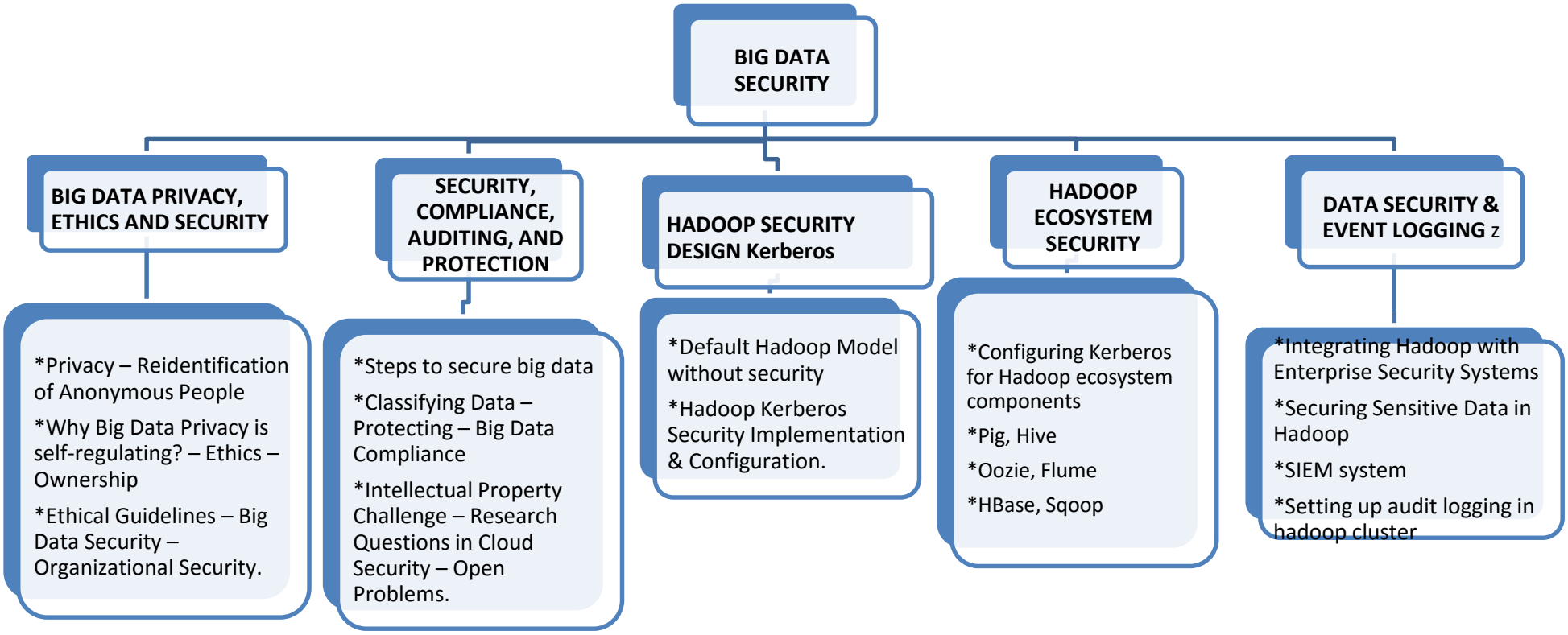
Mapping with Programme Outcomes

Cos	PSO1	PSO2	PSO3	PSO4	PSO5	PSO6	PSO7	PSO8	PSO9	PSO10
CO1	M									
CO2		L				M				
CO3		L		M				M		
CO4										S
CO5					L					

Assessment Pattern

Category	Continuous Assessment Tests (25)			Terminal Examination (75)
Remember	5	5	5	20
Understand	10	10	10	20
Apply	5	5	5	10
Analyze	5	5	5	10
Evaluate				5

Concept Map


BIG DATA SECURITY
BIG DATA PRIVACY, ETHICS AND SECURITY
*Privacy – Reidentification of Anonymous People
*Why Big Data Privacy is self-regulating? – Ethics – Ownership
*Ethical Guidelines – Big Data Security – Organizational Security.
SECURITY, COMPLIANCE, AUDITING, AND PROTECTION
*Steps to secure big data
*Classifying Data – Protecting – Big Data Compliance
*Intellectual Property Challenge – Research Questions in Cloud Security – Open Problems.
HADOOP SECURITY DESIGN Kerberos
*Default Hadoop Model without security
*Hadoop Kerberos Security Implementation & Configuration.
HADOOP ECOSYSTEM SECURITY
*Configuring Kerberos for Hadoop ecosystem components
*Pig, Hive
*Oozie, Flume
*HBase, Sqoop
DATA SECURITY & EVENT LOGGING z
*Integrating Hadoop with Enterprise Security Systems
*Securing Sensitive Data in Hadoop
*SIEM system
*Setting up audit logging in hadoop cluster

Syllabus

UNIT I – BIG DATA PRIVACY, ETHICS AND SECURITY Privacy – Reidentification of Anonymous People – Why Big Data Privacy is self-regulating? – Ethics – Ownership – Ethical Guidelines – Big Data Security – Organizational Security. **(12hrs)**

UNIT II - SECURITY, COMPLIANCE, AUDITING, AND PROTECTION Steps to secure big data – Classifying Data – Protecting – Big Data Compliance – Intellectual Property Challenge – Research Questions in Cloud Security – Open Problems. **(12hrs)**

UNIT III – HADOOP SECURITY DESIGN Kerberos – Default Hadoop Model without security - Hadoop Kerberos Security Implementation & Configuration. **(12hrs)**

UNIT IV – HADOOP ECOSYSTEM SECURITY Configuring Kerberos for Hadoop ecosystem components – Pig, Hive, Oozie, Flume, HBase, Sqoop. **(12hrs)**

UNIT V – DATA SECURITY & EVENT LOGGING Integrating Hadoop with Enterprise Security Systems - Securing Sensitive Data in Hadoop – SIEM system – Setting up audit logging in hadoop cluster **(12hrs)**

TOTAL (60hrs)

Books:

1. Mark Van Rijmenam, "Think Bigger: Developing a Successful Big Data Strategy for Your Business", Amazon, 1 edition, 2014.
2. Frank Ohlhorst John Wiley & Sons, "Big Data Analytics: Turning Big Data into Big Money", John Wiley & Sons, 2013.
3. SherifSakr, "Large Scale and Big Data: Processing and Management", CRC Press, 2014.
4. Sudeesh Narayanan, "Securing Hadoop", Packt Publishing, 2013.
5. Ben Spivey, Joey Echeverria, "Hadoop Security Protecting Your Big Data Problem", O'Reilly Media, 2015.
1. Top Tips for Securing Big Data Environments: e-book (http://www.ibmbigdatahub.com/whitepaper/top-tips-securing-big-data-environments-ebook)
2. http://www.dataguise.com/?q=securing-hadoop-discovering-and-securing-sensitive-Datahadoop-data-stores
8. Gazzang for Hadoophttp: // www.cloudera.com/ content/cloudera/ en/ solutions/ Enterprise solutions / security-for-hadoop.html
9. eCryptfs for Hadoop https://launchpad.net/ecryptfs.
10. Project Rhino - https://github.com/intel-hadoop/project-rhino/

Course Contents and Lecture Schedule

S.No.	Topic	No. of Lectures
1	**BIG DATA PRIVACY, ETHICS AND SECURITY**	
1.1	Privacy – Reidentification of Anonymous People	3
1.2	Why Big Data Privacy is self-regulating? – Ethics – Ownership	3
1.3	Ethical Guidelines – Big Data Security – Organizational Security.	3
2	**SECURITY, COMPLIANCE, AUDITING, AND PROTECTION**	
2.1	Steps to secure big data	3
2.2	Classifying Data – Protecting – Big Data Compliance	2
2.3	Intellectual Property Challenge – Research Questions in Cloud Security – Open Problems.	3
3	**HADOOP SECURITY DESIGN Kerberos**	
3.1	Default Hadoop Model without security	2
3.2	Hadoop Kerberos Security Implementation & Configuration.	2
4	**HADOOP ECOSYSTEM SECURITY**	
4.1	Configuring Kerberos for Hadoop ecosystem components	2
4.2	Pig, Hive	2
4.3	Oozie, Flume	2
4.4	HBase, Sqoop	2
5	**DATA SECURITY & EVENT LOGGING**	
5.1	Integrating Hadoop with Enterprise Security Systems	2
5.2	Securing Sensitive Data in Hadoop	2
5.3	SIEM system	2
5.4	Setting up audit logging in hadoop cluster	1

NCYP41	Dissertation and Viva Voce	

Preamble of this course is to facilitate transfer of knowledge acquired by a student to a field of his chosen specialization for application to solving a problem. The Co-ordinator of Students' Project works from the department shall coordinate this course. Student is expected to collect and study relevant material under mentorship of a Project Supervisor, identify a suitable problem and propose methodology towards its solution. Alternately a student can explore hardware / software implementation of existing solution(s).

The student will be tested for his understanding of basic principles of the core Specializations. The internal assessment will be made by Project Supervisor. The Project Supervisor will conduct three reviews in each level of progress. On completion of the work, a thesis report should be prepared in the prescribed format and submitted to the department. The end-semester university examination will have a thesis presentation and Viva-Voce examination conducted by a committee of one external examiner and one internal examiner appointed by the HOD/Professor/ Co-ordinator of Students' Project works.