M.Sc. Cyber Security

Syllabus
(With effect from 2021 -22)

Program Code:

DEPARTMENT OF COMPUTER SCIENCE
Bharathiar University
(A State University Accredited with "a" by NAAAC and
13th Rank among Indian Universities by MHRD-NIRF)
Coimbatore 641046, INDIA

MISSION

- ✓ To develop IT professionals with ethical and human values.
- ✓ To organize, connect, create and communicate mathematical ideas effectively, through industry 4.0.
- ✓ To provide a learning environment to enhance innovations, problem solving abilities, leadership potentials, team-spirit and moral tasks.
- ✓ To nurture the research values in the developing areas of Computer Science and interdisciplinary fields.
- ✓ Promote inter-disciplinary research among the faculty and the students to create state of art research facilities.
- ✓ To promote quality and ethics among the students.
- ✓ Motivate the students to acquire entrepreneurial skills to become global leaders.

Programme Educational Objectives (PEOs)	
The M.Sc. Cyber Security program describe accomplishments that graduates are expected to attain within five to seven years after graduation.	
PEO1	Expertise with the knowledge on cyber offenses and law.
PEO2	Exhibit high standards with regard to application of Digital Cyber Security in protecting data in the digital device and server.
PEO3	Proficiency in various techniques to moderate the difficulties associated with information security in the server.
PEO4	To analytically educate the necessity to understand the impact of cybercrimes and threats with solutions in a global context.

Programme Specific Outcomes (PSOs)	
After the successful completion of M.Sc Cyber Security program the students are expected to	
PSO1	Impart education with domain knowledge effectively and efficiently in par with the expected quality standards for Cyber Security professional.
PSO2	Ability to apply the mathematical, technical and critical thinking skills in the discipline of Cyber Security in digital information.
PSO3	Ability to engage in life-long learning and adopt fast changing technology to prepare for professional development.
PSO4	Expose the students to learn the important Cyber Security such as Cyber Policing, Web Application Security, Server Security, firewalls, Malware Analysis, so that they can opportunity to be a part of industry 5.0 applications irrespective of domains.
PSO5	Inculcate effective communication skills combined with professional & ethical attitude.

Programme Outcomes (POs)	
On successful completion of the M.Sc. Cyber Security	
PO1	Exhibit good **domain knowledge** and completes the assigned responsibilities effectively and efficiently in par with the expected quality standards.
PO2	Apply **analytical and critical thinking** to identify, formulate, analyze, and solve complex problems in order to reach authenticated conclusions
PO3	**Design and develop research based solutions** for complex problems with specified needs through appropriate consideration for the public health, safety, cultural, societal, and environmental concerns.
PO4	Establish the ability to **Listen, read, proficiently communicate and articulate complex ideas** with respect to the needs and abilities of diverse audiences.
PO5	**Deliver innovative ideas to instigate new business ventures** and possess the qualities of a good entrepreneur
PO6	Acquire the qualities of a **good leader and engage in efficient decision-making.**
PO7	Graduates will be able to undertake any responsibility as an **individual/member of multidisciplinary teams and have an understanding of team leadership**
PO8	Function as s**ocially responsible individual** with ethical values and accountable to ethically validate any actions or decisions before proceeding and actively contribute to the societal concerns.
PO9	Identify and **address own educational needs i**n a changing world in ways sufficient to maintain the competence and to allow them to contribute to the advancement of knowledge
PO10	**Demonstrate knowledge and understanding of management principles a**nd apply these to one own work to manage projects and in multidisciplinary environment.

BHARATHIAR UNIVERSITY : : COIMBATORE 641 046

M. Sc. Cyber Security (Affiliated Colleges)

(Effective For the candidates admitted during the academic year -2021 – 2022 & onwards)

REVISED SCHEME OF EXAMINATIONS – CBCS PATTERN

Course Code	Title of the Course	Credits	Hours		Maximum marks		
			Theory	Practical	CIA	ESE	Total
FIRST SEMESTER							
	Paper 1: Foundation of Information Security	4	5		50	50	100
	Paper 2: Network Technology and Security	4	5		50	50	100
	Paper 3: Ethical Hacking for Cyber Security	4	5		50	50	100
	Paper 4: Python Programming	4	5		50	50	100
	Practical I: Python Programming lab	4		5	50	50	100
	Practical II: Information Security Lab	4		5	50	50	100
	Total	**24**	**20**	**10**	**300**	**300**	**600**
SECOND SEMESTER							
	Paper 5: Introduction to Cyber Crime	4	4		50	50	100
	Paper 6: Web and Database Security	4	4		50	50	100
	Paper 7:Digital Forensic and Best Practices	4	4		50	50	100
	Paper 8: Cloud Fundamentals and Cloud Security	4	4		50	50	100
	ELETIVE I	4	4		50	50	100
	Practical III: Ethical Hacking and Digital Forensics Lab	4		5	50	50	100
	Practical IV: Web and Database Security Lab	4		5	50	50	100
	Total	**28**	**20**	**10**	**350**	**350**	**700**
THIRD SEMESTER							
	Paper 9: Network security and Cryptography	4	4		50	50	100
	Paper 10: Security Standards and Compliance	4	4		50	50	100
	Paper 11: Mobile and Wireless Security	4	4		50	50	100
	Paper 12: Evolving Technologies and Threats	4	4		50	50	100

	ELECTIVE II	4	4		50	50	100
	Practical V:Advance Digital Forensics Lab	4		4	50	50	100
	Practical VI: Network Security & Cryptography Lab	4		4	50	50	100
	Practical VII: Case studies of Cyber Security	2		2	25	25	50
	Total	**30**	**20**	**10**	**375**	**375**	**750**
FOURTH SEMESTER							
	Project Work and viva voce (200 Marks)	8		-	-	-	200*
	Total	**8**					**200**
	Grand Total	**90**	**60**	**30**	**1025**	**1025**	**2250**
	ONLINE COURSES						
	#Swayam / MOOC/ Spoken English Tutorial	**2**					
	#Job Oriented Certificate Course	**2**					

*Project Report – 100 Marks and Viva voce – 100 Marks

During II and III Semester (Optional)

SEMESTER –1

Course Code		FOUNDATIONS OF INFORMATION SECURITY	L	T	P	C
Core/elective/Supportive		Core	5	0	0	4
Pre - requisite		• Basic knowledge in Computers Security	Syllabus version		I	

Course Objectives

The main objectives of this course are to:
1. To understand the fundamental functioning of security patterns.
2. To understand the security Attack and Preventions.
3. To understand the need for Authentication, Access controls, Security operations.

Expected Course Outcomes

1	Understand the conceptual foundation of information security awareness.	K2
2	Study the physical and logical perimeters of information assets and its security.	K2
3	Analysis the risk events, treatment plans, assessment	K4
4	Examining the access controls, monitoring, management, and review process	K5
5	Detail evaluation of information classification, roles, and responsibilities	K5

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

UNIT I	FOUNDATION OF SECURITY	12

Overview of Security, Security Taxonomy, General Security Resources, Security Patterns - The History of Security Patterns, Scope of Pattern Characteristics of Security Patterns, Sources for Security Pattern Mining and Types of Patterns

UNIT II	SECURITY ATTACK	11

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

UNIT III	SECURITY OPERATIONS AND ADMINISTRATION	12

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

UNIT IV	NETWORKS AND TELECOMMUNICATIONS	12

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

UNIT V	MALICIOUS CODE AND ATTACK PREVENTION TOOLS	13

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

Total Lecture Hours		**60 Hours**
Text Book(s)		
1	Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, Peter Sommerlad,"Security Patterns: Integrating Security and Systems Engineering", Wiley Publications, 2013	
2	Fundamentals of information systems security- Dividkim | Michael G.solomon - 3rd edition.	
REFERENCE BOOK(S):		
1	Matt Bishop, "Computer Security Art and Science", Pearson/PHI, 2002.	
2	Michael E Whiteman and Herbert J Mattord; "Principles of Information Security", Vikas Publishing House, New Delhi, 2003.	
RELATED ONLINE CONTENTS (MOOC, SWAYAM,NPTEL, WEBSITES ETC)		
1	**https://nptel.ac.in/courses/106/106/106106129/**	
2	**https://www.digitalocean.com/community/tech_talks/foundations-of-computer-security**	
Course Designed by :		

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**
CO1	**S**	**S**	**S**	**S**	**M**	**M**	**M**	**L**	**L**	**L**
CO2	**S**	**S**	**M**	**M**	**M**	**L**	**L**	**L**	**L**	**L**
CO3	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**	**L**
CO4	**S**	**S**	**M**	**L**	**L**	**M**	**L**	**L**	**L**	**L**
CO5	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		NETWORK TECHNOLOGY AND SECURITY	L	T	P	C
Core/elective/Supportive		Core	5	0	0	4
Pre - requisite		• Basic knowledge in Network and Cryptography	Syllabus version		I	

Course Objectives

The main objectives of this course are to:

1. To understand the basics of network security in the computer systems
2. To understand the type's protocols and reference models.
3. To discuss about the network security attacks and network security assessment
4. To know about assessment of network security and remote Information Services

Expected Course Outcomes

1	Understand network security and identify protocols	K2
2	Remember the basics of computer networks and hardware	K3
3	Explain Network Security Assessment and RIS and Demonstrate about Cryptography algorithms	K3, K5
4	Explain the Reference Models (OSI and TCP/IP)	K4, K5
5	Illustrate the Security Attacks	K5

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

UNIT I	INTRODUCTION TO COMPUTER NETWORKS	12

Overview of Computer Networks: Introduction – Business and Home Applications – Mobile Users – Social Applications. Network Hardware: PAN – LAN – MAN – WAN. Reference Models: OSI – TCP/IP - Comparisons of OSI and TCP/IP. Example Networks: Internet – Arpanet – NSFNET – Mobile Phone Networks – Wireless LAN – RFID and Sensor Networks.

UNIT II	PROTOCOLS TYPES AND USAGE	11

Protocols: Network Security Technologies and Protocols -TCP/IP– VOIP – WAN – LAN – MAN– SAN – ISO Protocols in OSI –other protocols. Internet Security: Network Access Control and Cloud Security –Transport Level Security – Wireless Network Security – Email Security – IP Security – Remote User Authentication. Firewalls: Need – Characteristics – Types – Basing – Location and Configuration

UNIT III	CHALLENGES OF SECURITY ATTACKS	12

Security Attacks: Challenges of Securing Information – Threat Actors – Defending against Attacks. Attacking using Malware – Social Engineering Attacks. Basic Cryptography – Cryptography Algorithms – Cryptographic Attacks. Networking based attacks - Server Attacks. Wireless Network Security Attacks and solutions. Types of mobile devices – mobile device risks – securing mobile devices – embedded systems and Internet of Things

UNIT IV	ASSESSMENT OF NETWORK SECURITY AND REMOTE INFORMATION SERVICES	12

Network Security Assessment: Assessment Standards – Network Security Assessment and Platform. Assessing IP VPN Services: IPsec VPNs – Attacking IPsec VPNs. Assessing Remote Information

Services: Remote Information Services – DNS – Finger – Auth – NTP – SNMP – LDAP – rwho – RPC risers – Remote Information Services Countermeasures		
UNIT V	**BASICS OF CRYPTOGRAPHY ALGORITHMS**	**13**
Overview of Cryptography: Computer Security Concepts – OSI Security Architecture – Security Attacks – Security Services – Security Mechanisms. Symmetric Ciphers: Traditional Block Cipher Structure – DES – AES. Asymmetric Ciphers: Public Key Cryptography and RSA. Hash Functions: – SHA – SHA 3. Message Authentication: Requirements – Functions – codes - CCM and GCM. Digital Signatures and Scheme: (EDSS &SDSS) - Algorithms - NIST – ECDS – RSA-PSS.		
Total Lecture Hours		**60 Hours**
Text Book(s)		
1	Computer Networks (5th Edition), Andrew S.Tanenbaum David J. Wetherall, 2014.	
2	Network Protocols Handbook (2nd Edition), Javvin Technologies Inc, 2004.	
REFERENCE BOOK(S):		
1	Cryptography and Network Security: Principles and Practice (6th Edition), William Stallings, Prentice Hall Press, 2013.	
2	Network Security Assessment (2nd Edition), Chris McNab, O‟REILLY, 2008	
RELATED ONLINE CONTENTS (MOOC, SWAYAM, NPTEL, WEBSITES ETC)		
1	https://onlinecourses.swayam2.ac.in/ugc19_hs25/preview	
2	https://www.coursera.org/learn/introduction-cybersecurity-cyber-attacks	
Course Designed by :		

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**M**	**M**	**M**	**M**	**M**	**L**	**S**	**L**
CO2	**S**	**S**	**M**	**M**	**S**	**L**	**L**	**M**	**L**	**L**
CO3	**S**	**S**	**M**	**S**	**M**	**L**	**M**	**L**	**S**	**S**
CO4	**S**	**S**	**M**	**L**	**L**	**M**	**L**	**L**	**S**	**L**
CO5	**S**	**M**	**M**	**M**	**M**	**L**	**M**	**M**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		ETHICAL HACKING FOR CYBER SECURITY	L	T	P	C
Core/elective/Supportive		Core: 3	5	0	0	4
Pre - requisite		• Basic knowledge in Computer network, firewall, Hacking and cyber security terminology	Syllabus version		I	

Course Objectives

The main objectives of this course are to:

1. To understand Information Security, Cyber threats, attacks, web security.
2. To know about different modes of hacking tools and phases of penetration tests and Methodologies.

Expected Course Outcomes

1	Understand the basics of information security, threats, and its attacks	K1,K2
2	Understand the fundamentals of ethical hacking with the hacking methodologies	K1,K2
3	Understand the vulnerabilities and use the frameworks to identify vulnerabilities by service scan	K2
4	Understand the web security issues with the fundamentals of OWASP	K2
5	Analyze the phases of the penetration test with the methods	K3,K4

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

UNIT I	FUNDAMENTALS OF ETHICAL HACKING	12

Overview of Cyber threats – Data and Network Security Attacks – Threats: MAC spoofing – Access control Network protocol and services–Hacking terms - Ethical Hacking overview –Modes of Ethical Hacking – Ethics and Legality.

UNIT II	HACKING METHODOLOGY INVESTIGATION	11

Foot printing: Reconnaissance - Foot printing theory – Penetration test – Phases of Penetration test - Methods of Foot printing – Network Information gathering process – Terminologies of Foot printing –Foot printing through search engine directives – Who is tool –NetCraft – Extract Information from DNS - Foot printing from Email servers -Social Engineering.

UNIT III	SCANNING AND ENUMERATION	12

Scanning: Concept of Nmap - - Port scanning with Nmap – Subnet - Scanning IPs with Nmap Pings and Ping sweeps – Port - Three way handshake – NmapSyn scanning – Nmap TCP Scan – Nmap UDP Scan - Bypass of IPS and IDS – Nmap Script Engine Enumeration: Service Fingerprinting – Vulnerability Scanners – Basic Banner Grabbing – Common Network services – SMTP – DNS – RPCBIND Enumeration – SMB – NetBIOS

UNIT IV	SYSTEM AND NETWORK VULNERABILITY	12

Metasploit – Penetration testing with framework Metasploit – Scan services to identify vulnerabilities – Scan FTP services – Scan HTTP services – Exploitation – Post exploitation techniques – Meterpreter – Rootkit – Backdoor – Password hashes.

UNIT V	SOFTWARE VULNERABILITY	13

Fundamentals of OWASP Zed Attack Proxy (ZAP) – Web app vulnerability scan - Code Injection

Attacks – Broken Authentication – Sensitive Data Exposure – XML External Entities – Broken Access Control – Security misconfiguration – Website pen testing - Cross Site Scripting (XSS) – Insecure Deserialization – Using Components with known vulnerabilities – Insufficient logging and monitoring		
Total Lecture Hours		**60 Hours**
Text Book(s)		
1	McClure, S., Scambray, J. and Kurtz, G., 2012. Hacking Exposed 7Network Security Secrets and Solutions. New York: McGraw-Hill.	
2	Engebretson, P., 2013. The Basics Of Hacking And Penetration Testing. Amsterdam: Syngress, an imprint of Elsevier	
REFERENCE BOOK(S):		
1	Zaid Sabih, Learn Ethical Hacking from Scratch, 2018, PACKT publishing, ISBN: 978-1-78862-205-9	
2	Harsh Bothra, Hacking be a hacker with ethics, Khanna Publishing, 2016, ISBN: 978-03-86173-05-8	
RELATED ONLINE CONTENTS (MOOC, SWAYAM, NPTEL, WEBSITES ETC)		
1	**https://nptel.ac.in/courses/106/105/106105217/**	
2	**https://www.guru99.com/ethical-hacking-tutorials.html**	
Course Designed by :		

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**M**	**M**	**M**	**M**	**M**	**L**	**L**	**L**
CO2	**S**	**S**	**M**	**M**	**S**	**L**	**L**	**M**	**L**	**L**
CO3	**S**	**S**	**M**	**S**	**M**	**L**	**L**	**L**	**L**	**L**
CO4	**S**	**S**	**S**	**L**	**L**	**M**	**L**	**L**	**S**	**L**
CO5	**S**	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		PYTHON PROGRAMMING	L	T	P	C
Core/elective/Supportive		Core	5	0	0	4
Pre - requisite		• Basic knowledge in Object Oriented Programming and Network.	Syllabus version			I

Course Objectives

The main objectives of this course are:

1. Understand different Data Structures of Python.
2. To understand the basics of Python programming and Ethical Hacking from Scratch.
3. To strengthen fundamental skills in Network security and penetration testing.

Expected Course Outcomes

1	To understand the Python programming basics and data types.	K1, K2
2	To describe the environment setup and data structures.	K2
3	To demonstrate modular programming and to explain network concepts	K2, K3
4	To design working environment of virtual environment and understand various library in python	K4, K5
5	To create a test cases for the penetration testing with suitable techniques.	K6

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

UNIT I	**PYTHON – AN OVERVIEW**	**12**

Python – Introduction – History of Python – Python Features - Python Interpreter – Installation and Setup: Windows – Linux – macOS – Installing/Updating Python Packages - Basic Data Types – Python Built-in Functions – IDEs – Text Editors - Importing and Exporting Files: CSV File – JSON File – txt File- Excel File – Xml File – Delimited Formats.

UNIT II	**PYTHON DATA STRUCTURE**	**11**

Data Structures: Introduction – NumPy Package - Python List: Introduction – List Manipulation – List Operations - Python Tuples: Creating Tuples - Operation in Tuples – Accessing and Functions in Tuples – Python Dictionary: Accessing – Functions in Dictionary – Functions – Indexing – Slicing – Arrays Functions – Exception Handling -Global and Local Variables

UNIT III	**MODULAR PROGRAMMING**	**12**

Modular Programming - TCP Server- Client – UDP Server- Client – HTTP Server- Retrieving hostname IP – Banner grabbing - Socket Server Framework – Scapy: Syn Flood attack Scapy – Ping Sweep – Sniffing with Scapy – Buffer Overflow – exploit writing**.**

UNIT IV	**PYTHON ENVIRONMENT SETUP**	**12**

Python Environment Setup - Introduction –Virtual Environment - Setting Up Virtual Box – Setting Up VMWare –Kali Linux Installation -Networking Setup: Introduction – Basic Socket Library – Urllib Library: Access URL Resources/Download Files – ftplib Library: Develop an FTP Client - smtplib Library: SMTP Client.

UNIT V	**PENETRATION TESTING**	**13**

Penetration Test Introduction – Categories – Pen-testing Process – Use Cases: Developing Ethical Hacking Tools: Automating Information Gathering – Keylogger.		
Total Lecture Hours		**60 Hours**
Text Book(s)		
1	Mark Lutz, "Learning Python", O'Reilly, Fifth Edition, 2013.	
2	Behrouz A. Forouzan, "Data communication and Networking", Tata McGraw-Hill, 2004.	
3	Wesley J. Chun, "Core Python Programming", 2nd Edition, Pearson Education.	
REFERENCE BOOK(S):		
1	Andrew S. Tanenbaum, "Computer Networks", PHI, Fourth Edition, 2003	
2	Allen B. Downey, "Think Python: How to Think Like a Computer Scientist" 2nd edition, Updated for Python 3, Shroff/O,,Reilly Publishers, 2016 2 Guido van Rossum and Fred L. Drake Jr, ―An Introducti	
RELATED ONLINE CONTENTS (MOOC, SWAYAM, NPTEL, WEBSITES ETC)		
1	**https://nptel.ac.in/courses/106/106/106106182/**	
2	**https://www.programiz.com/python-programming**	
Course Designed by :		

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**S**	**S**	**M**	**M**	**M**	**L**	**L**	**L**
CO2	**S**	**S**	**M**	**S**	**S**	**L**	**L**	**M**	**L**	**L**
CO3	**S**	**S**	**M**	**S**	**M**	**L**	**L**	**L**	**L**	**L**
CO4	**S**	**S**	**M**	**L**	**L**	**L**	**L**	**L**	**L**	**L**
CO5	**S**	**M**	**M**	**M**	**L**	**L**	**L**	**L**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		PYTHON PROGRAMMING LAB	L	T	P	C
Core/elective/Supportive		Core Lab	0	0	5	4
Pre - requisite		• Basic knowledge in Object oriented Programming.	Syllabus version			I

Course Objectives

The main objectives of this course are to:
1. To understand the basic data structures like tuple, List, Dictionary.
2. To understand the applications of the data structures using various techniques
3. To Learn the python performance in many cybersecurity functions, including malware analysis, scanning, and penetration testing functions

Expected Course Outcomes

1	Understand the concepts of object oriented	K2
2	Implementation of data structures like Stack, Queue, Tree , List	K3
3	Evaluate the object oriented skills with functions and packages	K5
4	To Create a basic penetration testing programs	K6

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

LIST OF PROGRAMS	**10**
1. Write a python Program for list, tuples and dictionary.	
2. Program using conditional statement of python	
3. Programs using exception handling	
4. Programs using different packages in python	
5. Programs using functions 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	
10. Program for network scanning	
Total Lecture Hours	**45 Hours**

Course Designed by :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	S	M	L	L	L	L	L	L	L	L
CO2	S	M	M	L	L	L	L	L	L	L
CO3	S	S	S	L	L	L	L	L	L	L

*S-Strong; M-Medium; L-Low

Course Code		INFORMATION SECURITY LAB	L	T	P	C
Core/elective/Supportive		Core Lab	0	0	5	4
Pre - requisite		• Basic knowledge in Computer network	Syllabus version		I	

Course Objectives

The main objectives of this course are to:
1. To understand the fundamental functioning of security patterns.
2. To understand the security Attack and Preventions.
3. To understand the need for Authentication, Access controls, Security operations.

Expected Course Outcomes

1	Understand the concepts of network	K2
2	To demonstrate the concepts of files in Windows	K4
3	To Evaluate the skills for server client process	K5
4	To evaluate the packet tracking over LAN	K5

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

LIST OF PROGRAMS	10
To Demonstrate the User Identity and Access Management	
To Demonstrate the Account Authorization in windows operating system	
To Demonstrate the Access and Privilege Management in Directories	
To Demonstrate the System and Network Access Control	
To Demonstrate the Operating Systems Access Controls	
To Demonstrate the process of access Monitoring Systems with windows	
To Demonstrate the Website blocking with browser	
To demonstrate the IP Allocation for the computers.	
To demonstrate the Trouble shooting for the hardware devices	
To demonstrate the event logging	
To demonstrate the ICMP tracing packets over the network	
Total Lecture Hours	**45 Hours**

Course Designed by :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	S	S	S	M	M	L	L	L	L	L
CO2	S	S	M	M	L	L	L	L	L	L
CO3	S	S	M	M	L	L	L	L	L	L
CO4	S	S	M	L	L	L	L	L	L	L

*S-Strong; M-Medium; L-Low

SEMESTER – 2

Course Code		Introduction to Cyber Crime	L	T	P	C
Core/elective/Supportive		Core	4	0	0	4
Pre - requisite		Basic knowledge in Internet and data crimes.	Syllabus version		I	

Course Objectives		
The main objectives of this course are to: 1. To explain the concept of cybercrime and various types of attacks 2. To explain the impact of cybercrime on society		
Expected Course Outcomes		
1	Understand the concept of cybercrime and emerging crime threats and attacks in cyberspace	K2
2	Classify the main typologies, characteristics, activities, actors and forms of cybercrime, including the definitional, technical and social aspects.	K3
3	Evaluate behavioral aspects of the various type of attacks in cyberspace.	K4
4	Analyze the impact of cybercrime crime on businesses and individuals and discuss the impact of cybercrime on society	K4
K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create		

UNIT I	Cyber Crime - Overview	18
Cyber Crime- Overview, Internal and External Attacks, Attack Vectors. Cybercrimes against Individuals – E-mail spoofing and online frauds, Phishing and its forms, Spamming, Cyber-defamation, Cyber stalking, Cyber Bullying and harassment, Computer Sabotage, Pornographic offenses, Password Sniffing. Key loggers and Screen loggers. Cyber Crimes against Women and Children.		
UNIT II	**Cybercrime against organization**	**18**
Cybercrime against organization – Unauthorized access of computer, Password Sniffing, Denial-of-service (DOS) attack, Backdoors and Malwares and its types, E-mail Bombing, Salami Attack, Software Piracy, Industrial Espionage, Intruder attacks. Banking Trojans: An Overview-Executive Summary – Introduction - Stages of Attack. - Techniques and Malicious Code Evolution		
UNIT III	**Security policies violations**	**17**
Security policies violations, Crimes related to Social Media, ATM, Online and Banking Frauds. Intellectual Property Frauds. Cyber Crimes against Women and Children. General Data Protection Regulations Personal Data Protection Bill and its Compliance, Data Protection Principles, Data Protection Officer		
UNIT IV	**Global perspective on cybercrimes**	**19**
A global perspective on cybercrimes, Phases of cyber-attack – Reconnaissance, Passive Attacks, Active Attacks, Scanning, Gaining Access, Maintaining Access, Lateral movement and Covering Tracks. Detection Avoidance, Types of Attack vectors, Zero-day attack, Overview of Network based attacks.		

UNIT V	Cybercrime and cloud computing	18
Cybercrime and cloud computing, Different types of tools used in cybercrime, Password Cracking – Online attacks, Offline attacks, Remote attacks, Random Passwords, Strong and weak passwords. Viruses and its types. Ransomware and Crypto currencies. DoS and DDoS attacks and their types. Cybercriminal syndicates and nation state groups.		
	Total Lecture Hours	**90 Hours**
Text Book(s)		
1	Nina Godbole and SunitBelapore; "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley Publications, 2011.	
2	Shon Harris, "All in One CISSP, Exam Guide Sixth Edition", McGraw Hill, 2013.	
3	Bill Nelson, Amelia Phillips and Christopher Steuart; "Guide to Computer Forensics and Investigations" – 3rd Edition, Cengage, 2010 BBS.	
Reference Book(s)		
1	William Stallings; "Cryptography and Network Security: Principles and Practices", Fifth Edition, Prentice Hall Publication Inc., 2007.	
2	Atul Jain; "Cyber Crime: Issues, Threats and Management", 2004.	
3	Majid Yar; "Cybercrime and Society", Sage Publications, 2006.	
4	Michael E Whiteman and Herbert J Mattord; "Principles of Information Security", Vikas Publishing House, New Delhi, 2003. 8. Matt Bishop, "Computer Security Art and Science", Pearson/PHI, 2002	
	Related Online Contents (MOOC, SWAYAM,NPTEL, Websites etc)	
1	**https://onlinecourses.swayam2.ac.in/aic20_sp06/preview**	
2	**https://onlinecourses.swayam2.ac.in/arp19_ap79/preview**	
Course Designed by :		

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**
CO2	**M**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**
CO3	**S**	**M**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**
CO4	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		WEB AND DATABASE SECURITY	L	T	P	C
Core/elective/Supportive		Core	4	0	0	4
Pre - requisite		• Basic knowledge in Cyber Security	Syllabus version		I	

Course Objectives

The main objective of the course is:

1. To Understand an Overview of information security
2. To Understand an overview of Access control of relational databases

Expected Course Outcomes

1	Understand the Web architecture and applications	K2
2	Understand client side and service side programming	K2
3	Analyze how common mistakes can be bypassed and exploit the application	K3,K4
4	Evaluate the common application vulnerabilities	K5

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

UNIT I	**Web Security**	**12**

The Web Security Problem, Risk Analysis and Best Practices Cryptography and the Web: Cryptography and Web Security, Working Cryptographic Systems and Protocols, Legal Restrictions on Cryptography, Digital Identification.

UNIT II	**Web Privacy**	**11**

The Web's War on Your Privacy, Privacy-Protecting Techniques, Backups and Antitheft, Web Server Security, Physical Security for Servers, Host Security for Servers, Securing Web Applications, Web Application Proxies, Information Gathering: whois, nsLookup, netcraft, web server fingerprinting, subdomain enumeration,

UNIT III	**Database Security**	**12**

Recent Advances in Access Control, **Auditing** , **Authentication** , **Integrity controls**, **Backups,** Access Control Models for XML, Database Issues in Trust Management and Trust Negotiation, Security in Data Warehouses and OLAP Systems

UNIT IV	**Security Re-engineering for Databases**	**12**

Security Re-engineering for Databases Concepts and Techniques, Database Watermarking for Copyright Protection, Trustworthy Records Retention, Damage Quarantine and Recovery in Data Processing Systems, Hippocratic Databases: Current Capabilities.

UNIT V	**Future Trends Privacy in Database Publishing**	**13**

A Bayesian Perspective, Privacy-enhanced Location-based Access Control, **Database driven websites** Efficiently Enforcing the Security and Privacy Policies in a Mobile Environment.

Total Lecture Hours	**60 Hours**

Text Book(s)

1	Web Security, Privacy and Commerce, Simson G. Arfinkel, Gene Spafford, O' Reilly	
2	Handbook on Database security applications and trends, Michael Gertz, Sushil Jajodia	
REFERENCE BOOK(S):		
1	"Web applications security" By Andrew Hoffman, O'Reilly	
2	"Database and Applications Security" Bhavani Thuraisingham, Auerbach Publications	
RELATED ONLINE CONTENTS (MOOC, SWAYAM, NPTEL, WEBSITES ETC)		
1	**https://nptel.ac.in/noc/courses/noc15/SEM1/noc15-cs03/**	
2	**https://www.tutorialspoint.com/db2/db2_database_security.htm**	
Course Designed by :		

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**
CO1	**S**	**S**	**M**	**M**	**M**	**L**	**L**	**L**	**L**	**L**
CO2	**S**	**S**	**M**	**M**	**M**	**L**	**L**	**L**	**L**	**L**
CO3	**S**	**S**	**M**	**M**	**M**	**M**	**M**	**L**	**S**	**S**
CO4	**S**	**S**	**M**	**M**	**M**	**M**	**L**	**L**	**S**	**L**

*S-Strong; M-Medium; L-Low

Course Code		DIGITAL FORENSICS AND BEST PRACTICES	L	T	P	C
Core/elective/Supportive		Core	4	0	0	4
Pre - requisite		None			I	

Course Objectives

The main objective of this courses are:

1. To introduce the principle and concepts of digital forensic
2. To detail about the various investigation procedures like data acquisition nd evidence gathering

Expected Course Outcomes

1	Explain the principles of network ,mobile and cyber forensic science	K2
2	Illustrate the cyber-crime investigation procedures	K2
3	Apply the cyber-crime techniques to data acquisition and evidence collection	K3
4	Analyzing the digital evidences and arriving at conclusions	K4
5	Examine the Volatile and Non-volatile Digital Evidence	K4

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

UNIT I	Basics of Digital Forensics	11

Digital Forensics- Introduction, Objective and Methodology, Rules of Digital Forensics, Good Forensic Practices, Daubert's Standards, Principles of Digital Evidence. Overview of types of Computer Forensics – Network Forensics, Mobile Forensics, Social Media Forensics and E-mail Forensics. Services offered by Digital Forensics. First Responder – Role, Toolkit and Do's and Don'ts

UNIT II	Cyber Crime Investigation	12

Introduction to Cyber Crime Investigation, Procedure for Search and seizure of digital evidences in cyber-crime incident- Forensics Investigation Process- Presearch consideration, Acquisition, Duplication & Preservation of evidences, Examination and Analysis of evidences, Storing of Evidences, Documentation and Reporting, Maintaining the Chain of Custody.

UNIT III	Data Acquisition and Evidence Gathering	12

Data Acquisition of live system, Shutdown Systems and Remote systems, servers. E-mail Investigations, Password Cracking. Seizing and preserving mobile devices. Methods of data acquisition of evidence from mobile devices. Data Acquisition and Evidence Gathering from Social Media. Performing Data Acquisition of encrypted systems. Challenges and issues in cyber-crime investigation.

UNIT IV	Analysis of Digital Evidences	13

Search and Seizure of Volatile and Non-volatile Digital Evidence, Imaging and Hashing of Digital Evidence, Introduction to Deleted File Recovery, Steganography and Steganalysis, Data Recovery Tools and Procedures, Duplication and Preservation of Digital Evidence, Recover Internet Usage Data, Recover Swap files/Temporary Files/Cache Files. Software and Hardware tools used in cyber-crime investigation – Open Source and Proprietary tools. Importance of Log Analysis in forensic

analysis. Understanding Storage Formats for Digital Evidence – Raw Format, Proprietary Formats, Advanced Forensic Formats.		
UNIT V	**Windows and Linux Forensics**	**12**
Windows Systems Artifacts: File Systems, Registry, Event logs, Shortcut files, Executables. Alternate Data Streams (ADS), Hidden files, Slack Space, Disk Encryption, Windows registry, startup tasks, jump lists, Volume Shadow, shell bags, LNK files, Recycle Bin Forensics (INFO, $i, $r files). Forensic Analysis of the Registry – Use of registry viewers, Regedit. Extracting USB related artifacts and examination of protected storages. Linux System Artifact: Ownership and Permissions, Hidden files, User Accounts and Logs.		
Total Lecture Hours		**90 Hours**
Text Book(s)		
1	Nina Godbole and Sunit Belapore; "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley Publications,2011.	
2	Bill Nelson, Amelia Phillips and Christopher Steuart; "Guide to Computer Forensics and Investigations" – 3rd Edition, Cengage, 2010 BBS.	
3	Shon Harris; "All in One CISSP Guide, Exam Guide Sixth Edition", McGraw Hill, 2013.	
Reference Book(s)		
1	LNJN National Institute of Criminology and Forensic Science, "A Forensic Guide for Crime Investigators – Standard Operating Procedures", LNJNNICFS, 2016.	
2	Peter Hipson; "Mastering Windows XP Registry", Sybex, 2002.	
	Related Online Contents (MOOC, SWAYAM,NPTEL, Websites etc)	
1	**https://onlinecourses.swayam2.ac.in/aic20_sp06/preview**	
2	**https://onlinecourses.swayam2.ac.in/arp19_ap79/preview**	
Course Designed by :		

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**
CO2	**M**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**
CO3	**S**	**M**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**
CO4	**S**	**S**	**M**	**L**	**L**	**L**	**L**	**L**	**L**	**L**
CO5	**S**	**S**	**S**	**L**	**L**	**L**	**L**	**L**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		CLOUD FUNDAMENTALS AND CLOUD SECURITY	L	T	P	C
Core/elective/Supportive		Core	4	0	0	4
Pre - requisite		• Basic knowledge in cloud computing and architecture.	Syllabus version		I	

Course Objectives

The main objective of this courses are:

1. To understand the various issues in cloud computing.
2. To understand the security issues in the grid and the cloud environment.
3. To gain expertise in server, network and cloud service management.

Expected Course Outcomes

1	To understand the Basic concepts in Cloud computing	K2
2	To understand the Different Infrastructure Security in Cloud	K3
3	To apply the Data lifecycle and encryption, architecture	K3
4	To evaluate the virtualization in the cloud security	K5
5	To Analyze the Various Cloud Security Architecture	K4

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

UNIT I	INTRODUCTION TO CLOUD COMPUTING	12

Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vsprivateclouds, role of virtualization in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture. Application availability, performance, security and disaster recovery; next generation Cloud Applications.

UNIT II	CLOUD SERVICES MANAGEMENT	11

Reliability, availability and security of services deployed from the cloud. Performance and scalability of services, tools and technologies used to manage cloud services deployment; Cloud Economics: Cloud Computing infrastructures available for implementing cloud based services. Economics of choosing a Cloud platform for an organization, based on application requirements, economic constraints and business needs. Discuss industry cases including open sources.

UNIT III	SECURING THE CLOUD	12

Securing The Cloud: Security Concepts - Confidentiality, privacy, integrity, authentication, nonrepudiation, availability, access control, defence in depth, least privilege- how these concepts apply in the cloud and their importance in PaaS, IaaS and SaaS. e.g. User authentication in the cloud

UNIT IV	VIRTUALIZATION SECURITY	12

Virtualization Security: Multi-tenancy Issues: Isolation of users/VMs from each other- How the cloud provider can provide this- Virtualization System Security Issues: e.g. ESX and ESXi Security, ESX file system security- storage considerations, backup and recovery- Virtualization System Vulnerabilities.

UNIT V	SECURING THE CLOUD	13
Securing The Cloud: Security Concepts - Confidentiality, privacy, integrity, authentication, nonrepudiation, availability, access control, defence in depth, least privilege- how these concepts apply in the cloud and their importance in PaaS, IaaS and SaaS. e.g. User authentication in the cloud		
Total Lecture Hours		**60 Hours**
Text Book(s)		
1	Rittinghouse, J.W. & Ransome, J.F. (2010). Cloud Computing: Implementation, Management, and Security. CRC Press.	
2	Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", O'Reilly Media; 1 edition, [ISBN: 0596802765], 2009.	
REFERENCE BOOK(S):		
1	Ronald L. Krutz, Russell Dean Vines, "Cloud Security", Wiley [ISBN: 0470589876], , 2010.	
2	Vacca, J. (2016). Cloud Computing Security: Foundations and Challenges. CRC Press	
RELATED ONLINE CONTENTS (MOOC, SWAYAM, NPTEL, WEBSITES ETC)		
1	**https://www.javatpoint.com/what-is-cloud-security**	
2	**https://nptel.ac.in/courses/106/105/106105167/**	
Course Designed by :		

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**M**	**M**	**M**	**M**	**M**	**L**	**S**	**L**
CO2	**S**	**S**	**M**	**M**	**S**	**L**	**L**	**M**	**L**	**L**
CO3	**S**	**S**	**M**	**S**	**M**	**L**	**M**	**L**	**L**	**L**
CO4	**S**	**S**	**M**	**L**	**L**	**M**	**L**	**L**	**S**	**L**
CO5	**S**	**S**	**M**	**M**	**M**	**L**	**M**	**M**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		ETHICAL HACKING AND DIGITAL FORENSICS LAB	L	T	P	C
Core/elective/Supportive		Core Lab	0	0	5	4
Pre - requisite		Types of Computer File Systems and computer Networks basics.	Syllabus version			I

Course Objectives

The main objectives of this course are to:

1. To understand the basics of network and ethical hacking.
2. To understand the digital forensic laboratory tools.
3. To Learn about Secure the system in networks.

Expected Course Outcomes

1	To understand about various investigation strategies	K2
2	Will help to know about the working and functioning of Forensic science laboratories	K4
3	Will learn the Police science its role in criminal investigation and Prevention of crime	K4
4	To evaluate various hacking, cracking and attacks.	K5

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

LIST OF PROGRAMS	10

Ethical Hacking:

1. Perform network scanning to identify live and vulnerable machines in a network.
2. Perform OS banner grabbing, service, and user enumeration
3. Perform port scanning to identify live vulnerability in machines over network
4. Perform password Hacking and dictionary attack
5. Perform penetration testing of applications

Digital forensics:

1. Explore and exploit the various computer forensic tools for evidence collection and analysis used in File analysis.
2. Collect and analyze browser information, including browser history, cookies, proxy settings, web forms, bookmarks, cache, add-ons, saved passwords, etc
3. Collect digital evidence from mobile phones and cloud services used on phones (Android)
4. Preparing and processing of investigations. Try to examine and identify the evidences from the drives.
5. Extracting of files that has deleted in the disk.

Total Lecture Hours	45 Hours

Course Designed by :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**
CO2	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**	**L**
CO3	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**	**L**
CO4	**S**	**S**	**M**	**L**	**L**	**L**	**L**	**L**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		**WEB AND DATABASE SECURITY LAB**	**L**	**T**	**P**	**C**
Core/elective/Supportive		**Core Lab**	**0**	**0**	**5**	**4**
Pre - requisite		Basic knowledge about Database Management Systems, Practical exposure on Commercial Database Management Systems and Web Security	**Syllabus version**		**I**	

Course Objectives

The main objectives of the courses are to:

1. The protection of data against threats such as accidental or intentional loss, destruction or misuse.
2. To establish and preserve **database** confidentiality, integrity, and availability.

Expected Course Outcomes

1	Design of access control methods for secure web & database application development	K3
2	Analyse and Classify the vulnerabilities in the Web and Database applications	K4
3	Design & implementation various methods for web & database intrusion detection.	K6
4	Design and Implementation security audit methods.	K6

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

LIST OF PROGRAMS **9**

1. Creation and manipulation of database using SQL scripts and graphical interfaces
2. Implementing DAC: Implementation of database security policies using DAC in oracle 10g/SQL server
3. Implementing of MAC to ensure confidentiality and control information flow using either Oracle 10g or SQL server. This provides exposure to understand the concepts of MAC and Trojan hose
4. Implementation of Virtual Private Database using View using Oracle 10g or SQL server
5. Design a method to simulate the HTML injections and cross-site scripting (XSS) to exploit the attackers
6. Determine HTML injection bugs and possible measures to prevent HTML injection exploits.
7. Implement Secure coding for buffer flow heap attacks
8. Implementation of Design methods to break authentication schemes
9. Implementation of methods for abusing Design Deficiencies against web sites.

Total Lecture Hours	**45 Hours**
Course Designed by :	

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**
CO2	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**	**L**
CO3	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**	**L**
CO4	**S**	**S**	**M**	**L**	**L**	**L**	**L**	**L**	**L**	**L**

*S-Strong; M-Medium; L-Low

SEMESTER – 3

Course Code		NETWORK SECURITY AND CRYPTOGRAPHY	L	T	P	C
Core/elective/Supportive		Core	4	0	0	4
Pre - requisite		Basics of Networks & its Security	Syllabus version		I	

Course Objectives

The main objectives of this course are to:

1. Enable students to learn the Introduction to Cryptography, Web Security and Case studies in Cryptography.
2. To gain knowledge on classical encryption techniques and concepts of modular arithmetic and number theory.
3. To explore the working principles and utilities of various cryptographic algorithms including secret key cryptography, hashes and message digests, and public key algorithms.

Expected Course Outcomes

1	Understand the process of the cryptographic algorithms	K1,K2
2	Compare and apply different encryption and decryption techniques to solve problems related to confidentiality and authentication	K2,K3
3	Apply and analyze appropriate security techniques to solve network security problem	K3,K4
4	Explore suitable cryptographic algorithms	K4,K5
5	Analyze different digital signature algorithms to achieve authentication and design secure applications	K5,K6

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

UNIT I	**INTRODUCTION**	**12**

Introduction to Cryptography – Security Attacks – Security Services –Security Algorithm- Stream cipher and Block cipher - Symmetric and Asymmetric-key Cryptosystem Symmetric Key Algorithms: Introduction – DES – Triple DES – AES – IDEA – Blowfish – RC5.

UNIT II	**CRYPTO SYSTEM**	**11**

Public-key Cryptosystem: Introduction to Number Theory - RSA Algorithm – Key Management - Diffie-Hell man Key exchange – Elliptic Curve Cryptography Message Authentication and Hash functions – Hash and Mac Algorithm – Digital Signatures and Authentication Protocol.

UNIT III	**NETWORK SECURITY**	**12**

Network Security Practice: Authentication Applications – Kerberos – X.509 Authentication services and Encryption Techniques. E-mail Security – PGP – S / MIME – IP Security.

UNIT IV	**WEB SECURITY**	**12**

Web Security - Secure Socket Layer – Secure Electronic Transaction. System Security - Intruders and Viruses – Firewalls– Password Security

UNIT V	**CASE STUDY**	**13**

Case Study: Implementation of Cryptographic Algorithms – RSA – DSA – ECC (C / JAVA Programming). Network Forensic – Security Audit - Other Security Mechanism: Introduction to: Stenography – Quantum Cryptography – Water Marking - DNA Cryptography		
Total Lecture Hours		**60 Hours**
Text Book(s)		
1	William Stallings, "Cryptography and Network Security", PHI/PearsonEducation.	
2	Bruce Schneir, "Applied Cryptography", CRC Press.	
REFERENCE BOOK(S):		
1	A.Menezes, P Van Oorschot and S.Vanstone, "Hand Book ofApplied Cryptography", CRC Press, 1997	
2	AnkitFadia,"Network Security",MacMillan.	
RELATED ONLINE CONTENTS (MOOC, SWAYAM, NPTEL, WEBSITES ETC)		
1	https://nptel.ac.in/courses/106/105/106105031/	
2	http://www.nptelvideos.in/2012/11/cryptography-and-network-security.html	
Course Designed by :		

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**S**	**S**	**S**	**M**	**M**	**L**	**S**	**L**
CO2	**S**	**S**	**M**	**M**	**S**	**L**	**L**	**M**	**L**	**L**
CO3	**S**	**S**	**S**	**S**	**M**	**M**	**M**	**L**	**L**	**L**
CO4	**S**	**S**	**M**	**L**	**L**	**M**	**L**	**L**	**L**	**L**
CO5	**S**	**M**	**M**	**M**	**M**	**L**	**M**	**M**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		SECURITY STANDARDS AND COMPLIANCE	L	T	P	C
Core/elective/Supportive		Core	4	0	0	4
Pre - requisite		Basic knowledge of Policy, Process, Standard, Procedure and Compliance	Syllabus version		I	

Course Objectives

The main objectives of this course are to:

1. To understand the risk management process for all organizations.
2. To understand the security standards, compliance, security controls and access controls.
3. To learn what PCI DSS is and understand how it applies to the organizations.
4. To understand the technologies referenced by PCI DSS
5. To understand how to building and maintaining a Secure Network

Expected Course Outcomes

1	Understand the risk management process for all organizations	K2
2	Understand the security standards, security controls and control libraries.	K2
3	Understand what PCI DSS is and understand how it applies to the organizations.	K2
4	Understand how to building and maintaining a Secure Network	K2
5	Develop a case study for organization using PCI DSS.	K3

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

UNIT I	SECURITY RISK MANAGEMENT	12

Organizational Security Risk Management: Risk is Inevitable – Strategic Governance and Risk Management – Elements of Risk Management – Risk Types and Risk Handling Strategies – Overview of the Risk Management Process. Existing Risk Management Frameworks: Standard Best Practice – Formal Architecture – General Shape of the RMF Process – RMF Implementation – Other Frameworks and Models for Risk Management – International Organization for Standardization

UNIT II	SECURITY CONTROLS AND CONTROL LIBRARY	11

Select Security Controls: Understanding Control Selection - Federal Information Processing Standard Publication 200 – Document Collection and Relationship Building - Control Libraries: Control Objectives for Information and Related Technologies – CIS Critical Security Controls – Industrial Automation and Control Systems Security Life Cycle – ISO/IEC 27001

UNIT III	PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)	12

PCI Introduction – Electronic Card Payment Ecosystem – Compliance Deadlines – Compliance and Validation – History of PCI DSS – PCI Council – QSAs, PFIs, PCIPs, QIRs, ASVs – PCI Requirements – PCI DSS and Risk – Benefits of Compliance – Case Study.

UNIT IV	PCO SCOPE AND SECURE NETWORK	12

Determining and Reducing the PCI Scope: Basics – Scope Reduction Tips – Planning PCI Project.

Building and Maintaining a Secure Network: Establishing Firewall Configuration Standards – Tools and Best Practices – Common Mistakes and Pitfalls – Case Study.		
UNIT V	**STRONG ACCESS CONTROLS**	**13**
Principles of Access Control – Limitations of User Access – Authentication Basics – Windows and PCI Compliance – POSIX Access Control – CISCO and PCI Requirements – CISCO Enforce Session Timeout – Physical Security – Random Password for Users – Common Mistakes and Pitfalls – Case Study.		
Total Lecture Hours		**60 Hours**
Text Book(s)		
1	Anne Kohnke, Ken Sigler, Dan Shomaker, "Implementing Cybersecurity: A Guide to the National Standards and Technology Risk Management Framework" CRC Press, 2017.	
2	Branden R. Williams, Anton A. Chuvakin, "PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance", Fourth Edition, Syngress, 2015.	
REFERENCE BOOK(S):		
1	Barry L. Williams "Information Security Policy Development for Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0", CRC Press, 2013	
RELATED ONLINE CONTENTS (MOOC, SWAYAM, NPTEL, WEBSITES ETC)		
1	https://nptel.ac.in/courses/106/106/106106129/	
2	https://www.akamai.com/us/en/resources/security-compliance.jsp	
Course Designed by :		

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**M**	**M**	**M**	**M**	**M**	**L**	**S**	**L**
CO2	**S**	**S**	**M**	**M**	**S**	**L**	**L**	**M**	**L**	**L**
CO3	**S**	**S**	**M**	**S**	**M**	**L**	**M**	**L**	**S**	**S**
CO4	**S**	**S**	**M**	**L**	**L**	**M**	**L**	**L**	**S**	**L**
CO5	**S**	**M**	**M**	**M**	**M**	**L**	**M**	**M**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		MOBILE AND WIRELESS SECURITY	L	T	P	C
Core/elective/Supportive		Core	4	0	0	4
Pre - requisite		Basic knowledge in wireless standards and Network Security.	Syllabus version		I	

Course Objectives

The main objective of the courses are to:

To ensure effective, automated wireless threat protection, companies and government organizations should implement a complete wireless security solution covering assets across the enterprise that enables them to discover vulnerabilities, assess threats, prevent attacks, and ensure ongoing compliance.

Expected Course Outcomes

1	Understanding security and privacy for mobile and wireless networks	K2
2	Understand the securing wireless networks	K3
3	Apply the concepts in mobile security	K3,K5
4	Analyze the ADHOC network security concept	K4, K5
5	Evaluate the RFID security system	K5

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

UNIT I	INTRODUCTION	**12**

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.

UNIT II	MOBILE SECURITY	**11**

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.

UNIT III	SECURING WIRELESS NETWORKS	**12**

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 .

UNIT IV	ADHOC NETWORK SECURITY	**12**

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

UNIT V	RFID SECURITY	13
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, RFID: an anti-counterfeiting tool.		
Total Lecture Hours		**60 Hours**
Text Book(s)		
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.	
REFERENCE BOOK(S):		
1	NoureddineBoudriga,"Security of Mobile Communications", ISBN 9780849379413, 2010.	
2	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.	
RELATED ONLINE CONTENTS (MOOC, SWAYAM, NPTEL, WEBSITES ETC)		
1	https://nptel.ac.in/courses/106/105/106105160/	
2	https://www.tutorialspoint.com/wireless_security/index.htm	
Course Designed by :		

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**M**	**M**	**M**	**M**	**M**	**L**	**L**	**L**
CO2	**S**	**S**	**M**	**M**	**S**	**L**	**L**	**M**	**L**	**L**
CO3	**S**	**S**	**M**	**S**	**M**	**L**	**M**	**L**	**L**	**L**
CO4	**S**	**S**	**M**	**L**	**L**	**M**	**L**	**L**	**L**	**L**
CO5	**S**	**M**	**M**	**M**	**M**	**L**	**L**	**L**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		EVOLVING TECHNOLOGIES AND THREATS	L	T	P	C
Core/elective/Supportive		Core: 1	4	0	0	4
Pre - requisite		Current and Future Technology Trends	Syllabus version		I	

Course Objectives

The main objectives of this course are to:

1. To understand Web Technology, Robotics and Autonomous Systems
2. To analyze security problems associated with big data
3. To analyze and Build Big data Applications

Expected Course Outcomes

1	Understand the security in web technology	K2
2	Analyze the security problems associated with big data	K4
3	Apply the secure techniques in Big data Applications	K3
4	Understand the security violations in Robotics	K2
5	Understand the security violations in Autonomous Systems	K2

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

UNIT I	ADVANCES IN WEB TECHNOLOGIES	12

Improving Security in Web Sessions- Special Management of Cookies, Proposed mechanism for web session, management, Implementation and experiments. Leveraging Semantic Web Technologies for Access Control- Implementing RBAC with ontologies, semantically extending the XACML attribute model, Ontology-based context awareness.

UNIT II	COMPLEX & DISTRIBUTED IT INFRASTRUCTURE	11

Fundamental Concepts, Definitions, Statistics, Data Privacy Attacks, Data linking and profiling, access control models, role based access control, privacy policies, their specifications, languages and implementation, privacy policy languages, privacy in different domains- medical, financial, Medical privacy legislation, policies and best practices, examination of privacy matters specific to the World Wide Web, Protections provided by the Freedom of Information Act or the requirement for search warrants.

UNIT III	PRIVACY AND IDENTITY THEFT	12

Fundamental Concepts, Definitions, Statistics, Data Privacy Attacks, Data linking and profiling, access control models, role based access control, privacy policies, their specifications, languages and implementation, privacy policy languages, privacy in different domains- medical, financial, etc Medical privacy legislation, policies and best practices, Examination of privacy matters specific to the World Wide Web.

UNIT IV	THREATS OF BIG DATA	12
An Approach to Facilitate Security Assurance for Information Sharing and Exchange in BigData: Applications, UML extensions for XML security, Extensions for policy modeling and integration, Integrating local security policies into a global security policy, Real-time Network Intrusion Detection Using Hadoop-Based Bayesian Classifier, Overview on Hadoop based technologies, Survey of Intrusion Detection Systems, Hadoop-based real-time Intrusion Detection: System architecture, Practical application scenario and system evaluation.		
UNIT V	**ROBOTICS & AUTONOMOUS SYSTEMS**	**13**
Emerging Security Challenges in Cloud Computing, from Infrastructure-Based Security to Proposed Provisioned Cloud Infrastructure - Infrastructure security, Cloud service models, Provisioned access control infrastructure (DACI).		
	Total Lecture Hours	**60 Hours**
Text Book(s)		
1	Babak Akhgar Hamid Arabnia, "Emerging Trends in ICT Security", Morgan Kaufmann, 2013	
2	Divya Gupta Chowdhry, Rahul Verma, Manisha Mathur, "The Evolution of Business in the Cyber Age: Digital Transformation, Threats, and Security", CRC Press, 2020	
REFERENCE BOOK(S):		
1	Seema Acharya, SubhashniChellappan, "Big Data Analytics", Wiley, 2015.	
2	Vladlena Benson John McAlaney, " Emerging Cyber Threats and Cognitive Vulnerabilities, Academic Press,2019	
RELATED ONLINE CONTENTS (MOOC, SWAYAM, NPTEL, WEBSITES ETC)		
1	https://nptel.ac.in/courses/110/105/110105148/	
2	https://www.tutorialspoint.com/emerging-technologies-of-2017	
Course Designed by :		

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**M**	**M**	**M**	**M**	**M**	**L**	**S**	**L**
CO2	**S**	**S**	**M**	**M**	**S**	**L**	**L**	**M**	**L**	**L**
CO3	**S**	**S**	**M**	**S**	**M**	**L**	**M**	**L**	**S**	**S**
CO4	**S**	**S**	**M**	**L**	**L**	**M**	**L**	**L**	**S**	**L**
CO5	**S**	**M**	**M**	**M**	**M**	**L**	**M**	**M**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		NETWORK SECURITY AND CRYPTOGRAPHY LAB	L	T	P	C
Core/elective/Supportive		Core Lab	0	0	4	4
Pre - requisite		Basic knowledge in data structure and network security.	Syllabus version		I	

Course Objectives

The main objectives of this course are to:

1. To understand the simple client/server model.
2. To understand the insecurity of default passwords, printed passwords and password transmitted in plain text.
3. To learn the skills for developing the own cryptography algorithms.

Expected Course Outcomes

1	To understand the Encryption technique for protecting information and communication.	K2
2	To apply the knowledge in **cryptographic** techniques such as MAC and digital signatures.	K3
3	To evaluate the algorithm development skill for secure the data.	K4, K5
4	To Analyze the skills in wireless network data secure.	K4

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

LIST OF PROGRAMS	10

1. Implement the following SUBSTITUTION TECHNIQUES concepts:
   a) Caesar Cipher b) Play-fair Cipher c) Hill Cipher
2. Implement the Rail fence – row & Column Transformation
3. Implement the DES algorithms
4. Implement the RSA Algorithm
5. Implement the MD5 Algorithm
6. Implement the SHA-1 Algorithm
7. Implement the Signature Scheme - Digital Signature Standard
8. Setup a honey pot and monitor the honeypot on network
9. Perform wireless audit on an access point or a router and decrypt WEP and WPA.
10. Demonstrate Intrusion Detection System (IDS) using any tool.

Total Lecture Hours	45 Hours

Course Designed by :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**
CO2	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**	**L**
CO3	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**	**L**
CO4	**S**	**S**	**M**	**L**	**L**	**L**	**L**	**L**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		ADVANCE DIGITAL FORENSIC LAB	L	T	P	C
Core/elective/Supportive		Core Lab : 4	0	0	4	4
Pre - requisite		Basic knowledge in Disc file structure of NTFS, FAT and Forensic Tools.	Syllabus version		I	

Course Objectives

The main objectives of this course are to:

1. To understand the cyber security related activities in real world.
2. To learn the skills for data carving and data hiding
3. To understand the methodology for data carving from any electronic devices.

Expected Course Outcomes

1	To understand the basic skills for Digital evidence collection from crime scene.	K2
2	To apply the mathematical and analytical skills for finding the evidence.	K3
3	To Evaluate the skills set for data carving from the digital evidence.	K5
4	To Evaluate the skills for advanced file system data carving in slack.	K5

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

LIST OF PROGRAMS	10

1. Create an image file from the any storage devices (Disc, secondary memory, memory card).
2. Find the hash values for avoiding data duplication.
3. Find the information form the disc with FAT File system.
4. Find the information form the disc with NTFS file system.
5. Collect log details form running machines.
6. Find the network data transmission with any network forensic tools
7. Find the image form SIM cards by using any mobile forensic tools.
8. To recover the electronic evidence from mobile phone and Tablets.
9. Search a binary image of embedded files in .exe code.
10. Perform memory analysis for windows operating system.

Total Lecture Hours	45 Hours

Course Designed by :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**
CO2	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**	**L**
CO3	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**	**L**
CO4	**S**	**S**	**M**	**L**	**L**	**L**	**L**	**L**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		**CASE STUDIES OF CYBER SECURITY**	**L**	**T**	**P**	**C**
Core/elective/Supportive		**Core Lab**	**0**	**0**	**2**	**2**
Pre - requisite		Basic knowledge in cyber Security	**Syllabus version**		**I**	

Course Objectives

The main objectives of this course are to:

1. To learn the real-world use cases outlining the enterprise has need to defend the perimeter against cyber threats.

Expected Course Outcomes

1	Analyze the reality of the cyber security	K4
2	Analyze the case using relevant theoretical concepts from security	K4
3	Compare the analyzed strategies of the Related case.	K5
4	Create a report for the analyzed case	K6

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

LIST OF PROGRAMS	**10**
Each students have to do 2 Case studies and subject the report concern guides.	
Total Lecture Hours	**30 Hours**

Course Designed by :

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**S**	**S**	**S**	**L**	**L**	**M**	**M**	**L**
CO2	**S**	**S**	**S**	**S**	S	**L**	**L**	**M**	**L**	**L**
CO3	**S**	**S**	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**
CO4	**S**	**S**	**S**	**S**	**L**	**L**	**M**	**M**	**L**	**L**

*S-Strong; M-Medium; L-Low

SEMESTER 4

Course Code		Project Work Lab	L	T	P	C
Core/elective/Supportive		Core - 13				8
Pre - requisite		Students should have the strong knowledge in analytical skills and any one of the programming languages in this course.	Syllabus version		I	

Course Objectives

The main objectives of this course are to:

1. To understand and select the task based on their core skills.
2. To get the knowledge about analytical skill for solving the selected task.
3. To get confidence for implementing the task and solving the real time problems.
4. Express technical and behavioral ideas and thought in oral settings.
5. Prepare and conduct oral presentations

Expected Course Outcomes

On the successful completion of the course, student will be able to:

1	Formulate a real world problem and develop its requirements develop a design solution for a set of requirements	K3
2	Test and validate the conformance of the developed prototype against the original requirements of the problem	K5
3	Work as a responsible member and possibly a leader of a team in developing software solutions	K3
4	Express technical ideas, strategies and methodologies in written form. Self-learn new tools, algorithms and techniques that contribute to the software solution of the project	K1-K4
5	Generate alternative solutions, compare them and select the optimum one	K6

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

Aim of the project work

1. The aim of the project work is to acquire practical knowledge on the implementation of the programming concepts studied.
2. Each student should carry out individually one project work and it may be a work using the software packages that they have learned or the implementation of concepts from the papers studied or implementation of any innovative idea focusing on application-oriented concepts.
3. The project work should be compulsorily done in the college only under the supervision of the department staff concerned.

Viva Voce

1. Viva-Voce will be conducted at the end of the year by both Internal (Respective Guides) and

External Examiners, after duly verifying the Annexure Report available in the College, for a total of 200 marks at the last day of the practical session.
2. Out of 200 marks, 160 marks for project report and 40 marks for Viva Voce.

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**S**	**S**	**M**	**L**	**L**	**L**	**L**	**L**
CO2	**S**	**S**	**S**	**S**	**M**	**L**	**L**	**L**	**L**	**L**
CO3	**S**	**S**	**S**	**S**	**M**	**M**	**M**	**L**	**L**	**L**
CO4	**S**	**S**	**S**	**S**	**M**	**M**	**M**	**L**	**L**	**L**
CO5	**S**	**S**	**S**	**S**	**M**	**M**	**M**	**L**	**L**	**L**

*S-Strong; M-Medium; L-Low

ELECTIVE COURSES

Course Code		INTRODUCTION TO BIG DATA SECURITY	L	T	P	C
Core/elective/Supportive		Electives	4	0	0	4
Pre - requisite		Basic knowledge in Information security	Syllabus version			I

Course Objectives

The main objectives of the course are:

1. To conceptualization and summarization of big data and machine learning, trivial data versus big data, big data computing technologies, machine-learning techniques, and scaling up machine learning approaches.
2. To learn the Application of big data computing technologies.

Expected Course Outcomes

1	Understand the HADOOP security design	K2
2	Understand the security, compliance, auditing and protection of data	K2
3	Analyze the big data privacy, ethics and security	K3,K5
4	Analyze the HADOOP ecosystem security	K4, K5
5	Evaluate the data security and event logging in the system	K5

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

UNIT I	**BIG DATA PRIVACY**	**12**

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

UNIT II	**SECURITY, COMPLIANCE, AUDITING, AND PROTECTION**	**11**

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.

UNIT III	**HADOOP SECURITY DESIGN**	**12**

HADOOP SECURITY DESIGN Kerberos – Default Hadoop Model without security - Hadoop Kerberos Security Implementation & Configuration.

UNIT IV	**HADOOP ECOSYSTEM SECURITY**	**12**

HADOOP ECOSYSTEM SECURITY Configuring Kerberos for Hadoop ecosystem components – Pig, Hive, Oozie, Flume, HBase, Sqoop.

UNIT V	**DATA SECURITY & EVENT LOGGING**	**13**

DATA SECURITY & EVENT LOGGING Integrating Hadoop with Enterprise Security Systems - Securing Sensitive Data in Hadoop – SIEM system – Setting up audit logging in hadoop cluster

Total Lecture Hours	**60 Hours**

Text Book(s)

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.	
REFERENCE BOOK(S):		
1	SherifSakr, “Large Scale and Big Data: Processing and Management”, CRC Press, 2014	
2	Sudeesh Narayanan, “Securing Hadoop”, Packt Publishing, 2013.	
RELATED ONLINE CONTENTS (MOOC, SWAYAM, NPTEL, WEBSITES ETC)		
1	https://www.cloudera.com/content/cloudera/en/solutions/ Enterprise solutions/security-for-hadoop.html	
2	https://nptel.ac.in/courses/106/104/106104189/	
Course Designed by :		

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**
CO1	**S**	**S**	**M**	**M**	**M**	**M**	**M**	**L**	**L**	**L**
CO2	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**	**L**
CO3	**S**	**S**	**M**	**S**	**M**	**L**	**M**	**L**	**L**	**L**
CO4	**S**	**S**	**M**	**L**	**L**	**M**	**L**	**L**	**L**	**L**
CO5	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		**ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING**	**L**	**T**	**P**	**C**
Core/elective/Supportive		**Electives**	**4**	**0**	**0**	**4**
Pre - requisite		Basics of AI & an Introduction about ML	**Syllabus version**			**I**

Course Objectives

The main objectives of this course are to:
1. Enable the students to learn the basic functions of AI, Heuristic Search Techniques.
2. Provide knowledge on concepts of Representations and Mappings and Predicate Logic.
3. Introduce Machine Learning with respect Data Mining, Big Data and Cloud.
4. Study about Applications & Impact of ML.

Expected Course Outcomes

1	Demonstrate AI problems and techniques	K2
2	Understand machine learning concepts	K3

3	Apply basic principles of AI in solutions that require problem solving, inference, perception, knowledge representation, and learning	K3, K5
4	Analyze the impact of machine learning on applications	K4, K5
5	Analyze and design a real world problem for implementation and understand the dynamic behavior of a system	K5
K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create		
UNIT I	**INTRODUCTION**	**12**
Introduction: AI Problems - Al techniques - Criteria for success. Problems, Problem Spaces, Search: State space search - Production Systems - Problem Characteristics - Issues in design of Search.		
UNIT II	**SEARCH TECHNIQUES**	**11**
Heuristic Search techniques: Generate and Test - Hill Climbing- Best-First, Problem Reduction, Constraint Satisfaction, Means-end analysis. Knowledge representation issues: Representations and mappings -Approaches to Knowledge representations -Issues in Knowledge representations - Frame Problem.		
UNIT III	**PREDICATE LOGIC**	**12**
Using Predicate logic: Representing simple facts in logic - Representing Instance and Isa relationships - Computable functions and predicates - Resolution - Natural deduction. Representing knowledge using rules: Procedural Vs Declarative knowledge - Logic programming - Forward Vs Backward reasoning - Matching - Control knowledge.		
UNIT IV	**MACHINE LEARNING**	**12**
Understanding Machine Learning: What Is Machine Learning?-Defining Big Data-Big Data in Context with Machine Learning-The Importance of the Hybrid Cloud-Leveraging the Power of Machine Learning-The Roles of Statistics and Data Mining with Machine Learning-Putting Machine Learning in Context-Approaches to Machine Learning.		
UNIT V	**APPLICATIONS OF MACHINE LEARNING**	**13**
Looking Inside Machine Learning: The Impact of Machine Learning on Applications - Data Preparation-The Machine Learning Cycle.		
	Total Lecture Hours	**60 Hours**
Text Book(s)		
1	Elaine Rich and Kevin Knight," Artificial Intelligence", Tata McGraw Hill Publishers company Pvt Ltd, Second Edition, 1991.	
2	George F Luger, "Artificial Intelligence",4th Edition, Pearson Education Publ,2002.	
REFERENCE BOOK(S):		
1	Machine Learning For Dummies®, IBM Limited Edition by Judith Hurwitz, Daniel Kirsch.	
RELATED ONLINE CONTENTS (MOOC, SWAYAM, NPTEL, WEBSITES ETC)		
1	https://www.ibm.com/downloads/cas/GB8ZMQZ3	

2	https://www.javatpoint.com/artificial-intelligence-tutorial	
Course Designed by :		

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**M**	**M**	**M**	**M**	**M**	**L**	**L**	**M**
CO2	**S**	**S**	**M**	**M**	**M**	**M**	**L**	**L**	**L**	**L**
CO3	**S**	**S**	**M**	**S**	**M**	**L**	**M**	**M**	**L**	**L**
CO4	**S**	**S**	**M**	**M**	**M**	**M**	**L**	**L**	**M**	**L**
CO5	**S**	**M**	**M**	**L**	**L**	**L**	**M**	**L**	**M**	**L**

*S-Strong; M-Medium; L-Low

Course Code		**INTERNET OF THINGS**	**L**	**T**	**P**	**C**
Core/elective/Supportive		**Electives**	**4**	**0**	**0**	**4**
Pre - requisite	• Basic knowledge in Computer Hardware and Protocols.		**Syllabus version**			**I**

Course Objectives

The main objective of this courses are:

1. To understand the fundamentals of Internet of Things
2. To learn about the basics of IOT protocols
3. To build a small low cost embedded system using Raspberry Pi.
4. To apply the concept of Internet of Things in the real world scenario.

Expected Course Outcomes

1	Understand various protocols for IoT	K2
2	Analyze applications of IoT in real time scenario	K4
3	Deploy an IoT application and connect to the cloud.	K5
4	Develop web services to access/control IoT devices.	K6
5	Design a portable IoT using Rasperry Pi	K6

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

UNIT I	**INTRODUCTION TO IoT**	**12**

Introduction to IoT: Evolution of IoT – Definition & Characteristics of IoT - Architecture of IoT – Technologies for IoT – Developing IoT Applications – Applications of IoT – Industrial IoT – Security in IoT- IoT and M2M - IoT System Management with NETCONF-YANG- IoT Platforms Design Methodology

UNIT II	**IoT ARCHITECTURE**	**11**

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		
UNIT III	**IoT PROTOCOLS**	**12**
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		
UNIT IV	**BUILDING IoT WITH RASPBERRY PI & ARDUINO**	**12**
Building IOT with RASPERRY PI- IoT Systems - Logical Design using Python – IoT Physical Devices & Endpoints - IoT Device -Building blocks -Raspberry Pi -Board - Linux on Raspberry Pi - Raspberry Pi Interfaces -Programming Raspberry Pi with Python - Other IoT Platforms - Arduino.		
UNIT V	**REAL-WORLD APPLICATIONS AND CASE STUDIES**	**13**
Real world design constraints - Applications - Asset management, Industrial automation, smart grid, Commercial building automation, Smart cities - participatory sensing - Data Analytics for IoT – Software & Management Tools for IoT Cloud Storage Models & Communication APIs - Cloud for IoT - Amazon Web Services for IoT.		
Total Lecture Hours		**60 Hours**
Text Book(s)		
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.	
REFERENCE BOOK(S):		
1	Olivier Hersent, David Boswarthick, Omar Elloumi , ―The Internet of Things – Key applications and Protocols‖, Wiley, 2012	
2	Honbo Zhou, ―The Internet of Things in the Cloud: A Middleware Perspective‖, CRC Press, 2012.	
RELATED ONLINE CONTENTS (MOOC, SWAYAM, NPTEL, WEBSITES ETC)		
1		
2		
Course Designed by :		

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**M**	**M**	**M**	**M**	**M**	**L**	**S**	**L**
CO2	**S**	**S**	**M**	**M**	**S**	**L**	**L**	**M**	**L**	**L**
CO3	**S**	**S**	**M**	**S**	**M**	**L**	**M**	**L**	**S**	**S**
CO4	**S**	**S**	**M**	**L**	**L**	**M**	**L**	**L**	**S**	**L**
CO5	**S**	**M**	**M**	**M**	**M**	**L**	**M**	**M**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		MALWARE ANALYSIS	L	T	P	C
Core/elective/ Supportive		Electives	4	0	0	4
Pre - requisite		Operating System, Basics of Malware, Security Concepts and Algorithms	Syllabus version			I

Course Objectives

The main objectives of this course are to:

1. To understand the nature of malware, its capabilities, and how it is combated through detection and classification.
2. To able apply the tools and methodologies used to perform static and dynamic analysis on unknown executable.
3. To understand the social, economic, and historical context in which malware occurs.

Expected Course Outcomes

1	Understand the nature of malware, its capabilities, and how it is combated through detection and classification	K2
2	Understand the social, economic, and historical context in which malware occurs	K2
3	Analyze malicious in windows programs	K4
4	Apply the tools and procedures used to perform analysis on unknown executable.	K4
5	Apply techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples.	K4, K5

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

UNIT I	MALWARE ANALYSIS OVERVIEW	12

Introduction: Definition of Malware – Goals of .Malware Analysis– Malware Analysis Techniques - Types of Malware Analysis – General Rules for Malware Analysis. Analyzing malicious windows programs: Windows API – Windows Registry – Networking APIs – Following Running Malwares – Kernel vs User Mode- Native API.

UNIT II	BASIC ANALYSIS	11

Basic Static Techniques – Antivirus Scanning – Hashing – Finding Strings – Packed and Obfuscated Malware – Portable Executable File Format – Linked Libraries and Function – Static Analysis in Practice – PE File Headers and Sections. Basic Dynamic Analysis: Quality and Dirty Approach – Running Malware – Monitoring with Process Monitor – Viewing Process with Process Explorer: The Process Explorer Display, Using the Verify Option, Comparing Strings, Using Dependency Walker, Analyzing Malicious Documents – Comparing Registry Snapshots with Regshot – Faking a Network

UNIT III	ADVANCED ANALYSIS	12

x86 Architecture: Memory, instructions, opcodes, operands, registers, functions, stack. IDA Pro Inference – Cross Reference – Analysing Functions – Using Graphing Options – Enhancing Disassembly – Extending IDA with Plug-ins.

UNIT IV	ADVANCED DYNAMIC ANALYSIS	12

Source-Level vs Assembly Level Debuggers –Kernel vs User-Mode Debugging – Using

Debugger – Exceptions – Modifying Execution with a Debugger. OllyDbg: Loading Malware – OllyDbg Interface – Memory Map Viewing Threads and Stacks – Executing Code – Breakpoints – Loading DLLs – Tracing – Exception Handling – Patching – Analyzing Shellcode.		
UNIT V	**ANTI-DISASSEMBLY AND ANTI-DEBUGGING**	**13**
Anti-Disassembly: Understanding Anti-Disassembly – Defeating Disassembly Algorithm – Anti-Disassembly Techniques – Obscuring Flow Control – Thwarting Stack-Frame Analysis. Anti-Debugging: Windows Debugger Detection – Identifying Debugger Behaviour – Defeat Malware.		
Total Lecture Hours		**60 Hours**
Text Book(s)		
1	Michael Sikorski, Andrew Honig, "Practical Malware Analysis", No Strach Press, 2012	
2	Michael Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard "Malware Analyst"s Cookbook and DVD: Tools and Techniques for Fighting Malicious Code", Wiley Publishing Inc, 2011	
REFERENCE BOOK(S):		
1	Eldad Eilam, "Reversing: Secrets of Reverse Engineering", Wiley Publishing Inc, 2005	
2	Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters, "The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory", Wiley, 2014	
RELATED ONLINE CONTENTS (MOOC, SWAYAM, NPTEL, WEBSITES ETC)		
1	**https://www.cse.iitk.ac.in/pages/CS698M.html**	
2	https://www.elearnsecurity.com/course/malware_analysis_professional	
Course Designed by :		

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**S**	**S**	**M**	**M**	**L**	**L**	**S**	**L**
CO2	**S**	**S**	**S**	**M**	**S**	**M**	**L**	**L**	**L**	**L**
CO3	**S**	**S**	**M**	**S**	**M**	**L**	**M**	**L**	**L**	**L**
CO4	**S**	**S**	**M**	**M**	**M**	**M**	**L**	**L**	**L**	**L**
CO5	**S**	**M**	**M**	**M**	**M**	**L**	**L**	**L**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		APPLICATIONS & SYSTEMS SECURITY	L	T	P	C
Core/elective/ Supportive		Electives	4	0	0	4
Pre - requisite		• Basic knowledge in Network and Cryptography	Syllabus version			I

Course Objectives

The main objectives of the course are:

1. **To learn about security** measures at the **application** level.
2. to prevent data or code within the app from being stolen or hijacked.
3. To learn about Professional monitoring services

Expected Course Outcomes

1	Apply relevant methods for **security** modelling and analysis of software **applications** and information **systems**	K2
2	Analyses relevant professional and research ethical problems related to securing information **system** and software	K3
3	Analyze and evaluate the cyber security needs of an organization	K3,K5
4	Determine and analyze software vulnerabilities and security solutions to reduce the risk of exploitation	K4, K5
5	Measure the performance and troubleshoot cyber security systems	K5

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

UNIT I	**PROTECTION & SECURITY**	**12**

Protection & Security: Goals of Protection, Domain of protection, Security Problem, Authentication, One Time Password, Program Threats, System Threats, Threat Monitoring, Encryption

UNIT II	**SOFTWARE AND SYSTEM SECURITY**	**11**

Software and System Security: Control Hijacking Attacks – Buffer Overflow, Integer Overflow, Bypassing Browser Memory Protection, Sandboxing and Isolation, Tools and Techniques for Writing, Robust Application Software, Security Vulnerability Detection Tools, and Techniques. Program Analysis, Privilege, Access Control, and Operating System Security, Exploitation Techniques and Fuzzing, Operating System Mechanisms, Unix, Windows, Qmail, Chromium and Android

UNIT III	**SECURITY IN MOBILE PLATFORMS**	**12**

Security in Mobile Platforms: Android, Security mode, threat models, information tracking, rootkits, Threats in Mobile Applications, Analyzer for Mobile Apps to discover security vulnerabilities, viruses, Spywares, Keyloggers and Malware Detection

UNIT IV	**HARDWARE SECURITY, SUPPLY CHAIN SECURITY**	**12**

Hardware Security, Supply Chain Security: Threats of hardware Trojans and Supply chain Security, Side Channel Analysis based Threats, and attacks.

UNIT V	**INFRASTRUCTURE SECURITY**	**13**

Infrastructure Security: IT Infrastructure Management Services, Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement. Data Centre Management: Introduction to DCM, Data Center design, Data Center Security Procedure, Server Security, Storage area network, Virtualization, Introduction of Virtual Private Cloud (VPC), Cloud Logging and monitoring.		
Total Lecture Hours		**60 Hours**
Text Book(s)		
1	Principles of Computer Security: W.A.Coklin, G.White, Fourth Edition, McGrawHill	
2	Cryptography and Network Security Principles and Practices,William Stallings,Seventh Edition,Pearson	
REFERENCE BOOK(S):		
1	Web Technologies: TCP/IP, Web/Java Programming, and Cloud Computing Achyut S. Godbole,Tata McGraw-Hill Education, 2013	
2	Principles of Computer Security: W.A.Coklin, G.White, Fourth Edition, McGrawHill	
RELATED ONLINE CONTENTS (MOOC, SWAYAM, NPTEL, WEBSITES ETC)		
1	https://nptel.ac.in/courses/106/106/106106199/	
2	https://www.edureka.co/blog/application-security-tutorial/	
Course Designed by :		

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**
CO2	**S**	**S**	**S**	**M**	**S**	**M**	**L**	**L**	**L**	**L**
CO3	**S**	**S**	**M**	**S**	**M**	**L**	**M**	**L**	**L**	**L**
CO4	**S**	**S**	**S**	**M**	**M**	**M**	**L**	**L**	**L**	**L**
CO5	**S**	**S**	**S**	**M**	**M**	**L**	**L**	**L**	**L**	**L**

*S-Strong; M-Medium; L-Low

Course Code		**ROBOTIC PROCESS AUTOMATION FOR BUSINESS**	**L**	**T**	**P**	**C**
Core/elective/ Supportive		**Electives**	**4**	**0**	**0**	**4**
Pre - requisite		• Basic knowledge in Network and Cryptography	**Syllabus version**			**I**
Course Objectives						
The main objectives of this course are to:						

1. Learn the concepts of RPA, its benefits, types and models.
2. Gain the knowledge in application of RPA in Business Scenarios.
3. Identify measures and skills required for RPA

	Expected Course Outcomes	
1	Understand the Automation cycle and its techniques	K1, K2
2	Demonstrate the benefits and ethics of RPA	K3
3	Draw inferences and information processing of RPA	K3,K5
4	Implement & Apply RPA in Business Scenarios	K6
5	Analyze on Robots & leveraging automation	K4

K1 – Remember K2 – Understand K3 – apply K4- Analyze K5 – evaluate K6- Create

UNIT I	**INTRODUCTION**	**12**

Introduction to RPA - Overview of RPA - Benefits of RPA in a business environment - Industries & domains fit for RPA - Identification of process for automation - Types of Robots - Ethics of RPA & Best Practices - Automation and RPA Concepts - Different business models for implementing RPA - Centre of Excellence – Types and their applications - Building an RPA team - Approach for implementing RPA initiatives

UNIT II	**AUTOMATION**	**11**

Role of a Business Manager in Automation initiatives - Skills required by a Business Manager for successful automation - The importance of a Business Manager in automation - Analyzing different business processes - Process Mapping frameworks - Role of a Business Manager in successful implementation – Part 1 - Understanding the Automation cycle – First 3 automation stages and activities performed by different people.

UNIT III	**AUTOMATION IMPLEMENTATION**	**12**

Evaluating the Automation Implementation Detailed description of last 3 stages and activities performed by different people - Role of a Business Manager in successful completion – Part 2 - Activities to be performed post-implementation - Guidelines for tracking the implementation success - Metrics/Parameters to be considered for gauging success - Choosing the right licensing option - Sending emails - Publishing and Running Workflows.

UNIT IV	**ROBOT**	**12**

Ability to process information through scopes/systems - Understand the skill of information processing and its use in business - Leveraging automation - Creating a Robot - New Processes. Establish causality by variable behavior - Understand the skill of drawing inference or establishing causality by tracking the behavior of a variable as it varies across time/referenced variable - Leveraging automation for this skill - Robot & new process creation.

UNIT V	**ROBOT SKILL**	**13**

Inference from snapshots of curated terms – Omni-source data curation - Multisource trend tracking - Understand the skill of drawing inference from the behavior of curated terms by taking snapshots across systems in reference to time/variable(s) - Leveraging automation for this skill – Robot creation and new process creation for this skill.

Total Lecture Hours	**60**

		Hours
Text Book(s)		
1	Alok Mani Tripathi" Learning Robotic Process Automation: Create Software robots and automate business processes with the leading RPA tool" Packt Publishing Limited March 2018	
2	Tom Taulli "The Robotic Process Automation Handbook" Apress , February 2020.	
REFERENCE BOOK(S):		
1	Steve Kaelble" Robotic Process Automation" John Wiley & Sons, Ltd., 2018	
RELATED ONLINE CONTENTS (MOOC, SWAYAM, NPTEL, WEBSITES ETC)		
1	https://nptel.ac.in/courses/112/105/112105249/	
2	https://www.uipath.com/blog/learning-robotic-process-automation-through-video-tutorials	
Course Designed by :		

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	**S**	**S**	**M**	**M**	**M**	**M**	**M**	**L**	**S**	**L**
CO2	**S**	**S**	**M**	**M**	**S**	**L**	**L**	**M**	**L**	**L**
CO3	**S**	**S**	**M**	**S**	**M**	**L**	**M**	**L**	**S**	**S**
CO4	**S**	**S**	**M**	**L**	**L**	**M**	**L**	**L**	**S**	**L**
CO5	**S**	**M**	**M**	**M**	**M**	**L**	**M**	**M**	**L**	**L**

*S-Strong; M-Medium; L-Low

BHARATHIAR UNIVERSITY : : COIMBATORE 641046

DEPARTMENT OF COMPUTER SCIENCE

MISSION

1. To keep pace with emerging technologies and concepts, students are thrown open to the ever changing arena, meeting the industry requirements and standards, with the necessary knowledge and skill sets.
2. Are trained to explore more, at their own pace, knowing the demands of the IT world.
3. Apart from all the technical stuff, to inculcate the students about the Human Values and Professional ethics and to play a vital role in the society. Imparting them not only as world class Professionals, but also as tech savvy human beings to serve mankind.

ELECTIVE I:

1. Introduction to Big Data Security
2. Artificial Intelligence and Machine Learning.
3. Internet of Thing

ELECTIVE II:

1. Malware Analysis
2. Applications & Systems Security
3. Robotic Process Automation for Business