SRI VENKATESWARA COLLEGE OF ENGINEERING
(An Autonomous Institution, Affiliated to Anna University, Chennai)
SRIPERUMBUDUR TK. - 602 117
DEPARTMENT OF INFORMATION TECHNOLOGY
M.Tech Cyber Forensics and Information Security
CURRICULUM & SYLLABUS

SEMESTER I

Sl. No.	Course Code	Course Title	Category	Contact Period	L	T	P	C	Pre-Requisite	F/ M
1	MA18187	Mathematical Foundations For Information Security	FC	4	3	1	0	4	-	F
2	CF18101	Foundations of Cyber Security	PC	4	3	1	0	4	-	F
3	CF18102	Advanced Operating Systems	PC	3	3	0	0	3	-	F
4	CF18103	Network Principles and Security	PC	3	3	0	0	3	-	F
5	CF18104	Computer Forensics and Digital Evidence	PC	3	3	0	0	3	-	F
6	CF18111	Network Design and Security Laboratory	PC	3	0	0	3	2	-	F
7	CF18112	Ethical Hacking Essentials Laboratory	PC	3	0	0	3	2	-	F
				23	15	2	6	21		

SEMESTER II

Sl. No.	Course Code	Course Title	Category	Contact Period	L	T	P	C	Pre-Requisite	F/ M
1	CF18201	Fundamentals to Security in Biometrics	PC	3	3	0	0	3	Foundations of Cyber Security	M
2	CF18202	Digital Forensics and Digital Investigations	PC	4	3	1	0	4	-	M
3	CF18203	Blockchain for Security	PC	3	3	0	0	3	-	F
4	CF18204	Internet of Things and Security	PC	4	3	1	0	4	-	F
5		Professional Elective I	MC	3	3	0	0	3	-	F
6	CF18211	IoT and Blockchain Laboratory	PC	3	0	0	3	2	-	F
7	CF18212	Digital Forensics Laboratory	PC	3	0	0	3	2	-	F
8	CF18213	Case Study I – Forensic Investigations	EEC	2	0	0	2	1	-	F
				25	15	2	8	22		

SEMESTER III

SL. No.	Course Code	Course Title	Category	Contact Period	L	T	P	C	Pre-Requisite	F/ M
1	CF18301	Penetration and Application Testing	PC	4	3	1	0	4	Network Principles and Security	F
2		Professional Elective II	PE	3	3	0	0	3	-	M
3		Professional Elective III	PE	3	3	0	0	3	-	M
4		Professional Elective IV	PE	3	3	0	0	3	-	M
5	CF18311	Project Phase 1	EEC	12	0	0	12	6	-	F
				25	12	1	12	19		

SEMESTER IV

Sl. No.	Course Code	Course Title	Category	Contact Period	L	T	P	C	Pre-Requisite	F/ M
1.	CF18411	Project Phase 2	EEC	24	0	0	24	12	Project Phase I	F
				24	0	0	24	12		

Total Credits : 74

PROFESSIONAL ELECTIVES

Sl. No	Course Code	Course Title	Contact Period	L	T	P	C
1	CF18001	Applied Cryptography	3	3	0	0	3
2	CP18105	Machine Learning Techniques (Common to CP,NW&CFIS)	3	3	0	0	3
3	CF18002	Data Mining Techniques	3	3	0	0	3
4	CF18003	Intrusion Detection and Prevention Systems	3	3	0	0	3
5	CP18016	Social Network Analysis (Common to CP, NW & CFIS)	3	3	0	0	3
6	CF18004	Principles of Secure Coding	3	3	0	0	3
7	CF18005	Trust Management in E – Commerce	3	3	0	0	3
8	CF18006	Biometric Image Processing	3	3	0	0	3
9	CF18007	Cyber Security Management and Cyber Laws	3	3	0	0	3
10	NW18010	Network Virtualization (Common to NW & CFIS)	3	3	0	0	3
11	CP18011	Cloud Computing Technologies (Common to CP, NW & CFIS)	3	3	0	0	3
12	CF18008	Energy Aware Computing	3	3	0	0	3
13	NW18007	Advanced Infrastructure Management (Common to NW & CFIS)	3	3	0	0	3
14	CF18009	Malware Analysis and Reverse Engineering	3	3	0	0	3
15	NW18009	Data Analytics and Business Intelligence (Common to NW & CFIS)	3	3	0	0	3
16	CF18010	Wireless Security	3	3	0	0	3

Total Credits (From Sem I to IV): 74

MA18187	MATHEMATICAL FOUNDATIONS FOR INFORMATION SECURITY	L	T	P	C
		3	1	0	4

Course Objectives:

The students will be able to

- To understand the concepts of number theory which play an important role in computer science and cryptography
- To understand basic concepts of various algebraic structures used in computer science
- To understand the concepts of advanced algebraic structures used in computer science
- To understand the basic mathematical principles and functions that form the foundation for coding theory
- To understand basics of elliptic curves and pseudo random numbers and its usage

Unit I Number Theory **12**

Introduction - Divisibility - Greatest common divisor - Prime numbers - Fundamental theorem of arithmetic - Fermat numbers - Euclidean algorithm - Fermat's theorem - Euler totient function - Euler's theorem. Congruences - Definition - Basic properties of congruences - Residue classes - Chinese remainder theorem.

Unit II Algebraic Structures I **12**

Groups – Cyclic groups, Cosets, Modulo groups - Primitive roots - Rings – Sub rings, ideals and quotient rings.

Unit III Algebraic Structures II **12**

Integral domains, Fields – Finite fields - Classification - Structure of finite fields.

Unit IV Coding Theory **12**

Introduction - Basic concepts - Codes, minimum distance, equivalence of codes, Linear codes - Generator matrices and parity - Check matrices - Hamming codes.

Unit V Elliptic Curves and Pseudorandom Number Generation **12**

Discrete Logarithm - Elliptic curves - Introduction to Pseudo random numbers.

Total Hours:60(L:45+T:15)

Course Outcomes:

At the end of the course, the students will be able

- Apply the concepts of number theory in cryptography
- Apply concepts of various algebraicstructures in computer science
- Enumerate the basic concepts of mathematicalprinciples and functions that form the foundation for coding theory
- Demonstrate discretelogarithms, elliptic curves and pseudo random numbers.

Text Books:

1. Kenneth H Rossen, Discrete Mathematics and its Applications, Seventh Edition, McGraw Hill, 2012.
2. Rudolf Lidl, Gunter Pilz, Applied Abstract Algebra, Second Edition, Springer, 1998.
3. D.S. Malik, J. Mordeson, M.K. Sen, Fundamentals of abstract algebra, McGraw Hill, 1997.
4. Joseph A. Gallian, Contemporary Abstract Algebra, Narosa, 1998.
5. L. Washington, Elliptic Curves: Number Theory and Cryptography, Chapman & Hall CRC, 2003.

References:

1. Niven, H.S. Zuckerman, H. L. Montgomery, An introduction to the theory of numbers, John Wiley and Sons, 2001.
2. Fraleigh J.B., A first course in abstract algebra, Pearson Education, 2005.
3. Douglas R Stinson, Cryptography: Theory and Practice, CRC Press, 2015.

CF18101	FOUNDATIONS OF CYBER SECURITY	L	T	P	C
		3	1	0	4

Course Objectives:

The students will be able to

- Understand various block cipher and stream cipher models
- Describe the principles of public key cryptosystems, hash functions and digital signature
- To get a firm knowledge on Cyber Security Essentials

Unit I Introduction to Security **12**

Data Encryption Standard-Block cipher principles-block cipher modes of operation-Advanced Encryption Standard (AES)-Triple DES-Blowfish-RC5 algorithm

Unit II Public Key Cryptography and Hash Algorithms **12**

Principles of public key cryptosystems-The RSA algorithm-Key management - Diffie Hellman Key exchange- Hash functions-Hash Algorithms (MD5, Secure Hash Algorithm)

Unit III Fundamentals of Cyber Security **12**

How Hackers Cover Their Tracks- Fraud Techniques- Threat Infrastructure- Techniques to Gain a Foothold (Shellcode, SQL Injection, Malicious PDF Files)- Misdirection, Reconnaissance, and Disruption Methods

Unit IV Planning for Cyber Security **12**

Privacy Concepts -Privacy Principles and Policies -Authentication and Privacy - Data Mining - Privacy on the Web - Email Security - Privacy Impacts of Emerging Technologies

Unit V Cyber Security Management **12**

Security Planning - Business Continuity Planning - Handling Incidents - Risk Analysis - Dealing with Disaster – Legal Issues – Protecting programs and Data – Information and the law – Rights of Employees and Employers - Emerging Technologies - The Internet of Things - Cyber Warfare

Total Hours:60(L:45+T:15)

Course Outcomes:

At the end of the course, the students will be able to,

- Implement basic security algorithms required by any computing system
- Analyze the vulnerabilities in any computing system and hence be able to design a security solution
- Analyze the possible security attacks in complex real time systems and their effective countermeasures
- Enumerate various governing bodies of cyber laws
- Impart various privacy policies for an organization

References

1. William Stallings, “Cryptography and Network Security”, Pearson Education, 6th Edition, 2013.
2. Charles P. Pfleeger Shari Lawrence Pfleeger Jonathan Margulies, Security in Computing, 5th Edition , Pearson Education , 2015.
3. Graham, J. Howard, R., Olson, R., Cyber Security Essentials, CRC Press, 2011.
4. George K.Kostopoulous, Cyber Space and Cyber Security, CRC Press, 2013.

CF18102	ADVANCED OPERATING SYSTEMS	L	T	P	C
		3	0	0	3

Course Objectives:

The students will be able to

- Have a detailed knowledge on Operating system concepts
- Understand the need for operating system security
- Administer an open source Operating System

Unit I Operating Systems: Overview 9

Operating System structure and operations - Process Management- Memory Management – Storage Management - Protection and Security– Process Scheduling – Inter process communication- Multi threading models- Semaphores – Monitors - Deadlocks- Mutexes- Critical Section problem

Unit II Memory Management in Operating System 9

Swapping – Contiguous Memory Allocation – Segmentation – Paging – Virtual Memory: Demand Paging – Page Replacement – Allocation of Frames – Thrashing – Allocating Kernel Memories

Unit III Linux System Administration 9

Requirements for a Linux Administrator – Server Requirements – Logging in Remotely – Network configuration – Providing DNS – Adding Relational DB – Configuring mail securely – Adding FTP services – Synchronizing the system clock – Installing perl modules

Unit IV Operating Systems: Trust Model 9

Security Goals – Trust and Threat Model – Protection System – Reference Monitor – Secure Operating System – Assessment Criteria – Mutics History – Multics System and Security

Unit V Operating Systems Security 9

System History – Unix and Windows History – Unix Security – Windows Security – Verifiable Security Goals – Security Kernels – Securing Commercial Operating Systems

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Enumerate the basic functionalities of operating system
- Demonstrate Linux system administration
- Formulate Security features for an operating system
- Perform memory management in OS
- Implement Trust model for Multics system

References

1. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, “Operating System Concepts”,

John Wiley & Sons ,Inc., 9th Edition, 2012.

2. Trent Jaeger, “Operating Systems Security”, Morgan & Claypool Publishers, 2008.
3. Tom Adelstein and Bill Lubanovic, “Linux System Administration”, O'Reilly Media, Inc., 1st Edition, 2007.
4. William Stallings, “Operating System: Internals and Design Principles”, Prentice Hall, 7th Edition, 2012.

CF18103	NETWORK PRINCIPLES AND SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

The students will be able to

- Identify the basic networking principles
- Understand the need for network security
- Expose themselves to security at various network layers

Unit I Fundamentals of Networks **9**

Networking Technology – Connecting Devices - The OSI Model - TCP/IP Model - Threats to Network communications - Wireless Network Security – Denial of Service – Distributed Denial of Service

Unit II Cryptography in Network Security **9**

Malicious vs Non Malicious code – Counter Measures – Authentication – Access Control – Network and Browser Encryption – Firewalls – IDS – Network Management

Unit III Network and Transport Layer Security **9**

Network Layer: IPSec Protocol – IP Authentication Header – IP ESP – VPN - Key Management Protocol for IPSec – Transport Layer: SSL Protocol – TLS Protocol

Unit IV E – mail and Web Security **9**

Pretty Good Privacy – MIME – S/MIME - Enhanced Security Services for S/MIME - SET for E-commerce Transactions

Unit V Cloud and Wireless Network Security **9**

Cloud Computing – Cloud Security Risks and Counter Measures – Cloud Security as a Service – Wireless Network Security: Wireless Security – Mobile Device Security – WLAN Security

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Classify and secure various layers of networks
- Understand the concept of Network Layer Security
- Develop protocols for Web and Mail security
- Apply various password management techniques for system security
- Develop measures for cloud and wireless network security

References

1. Man Young Rhee, “Internet Security: Cryptographic Principles”, “Algorithms and Protocols”, Wiley Publications, 2003.
2. Charles Pfleeger, ”Security in Computing”, Prentice Hall, 4th Edition, 2006.

3. William Stallings, “Cryptography and Network Security”, Pearson Education, 6th Edition, 2013.
4. Charlie Kaufman, Radia Perlman, Mike Speciner, “Network Security”, Prentice Hall, 2nd edition , 2002.

CF18104 COMPUTER FORENSICS & DIGITAL EVIDENCE

L	T	P	C
3	0	0	3

Course Objectives:

The students will be able to

- Study the procedure for forensic investigation
- Audit and analyze the computer systems for data extraction
- Understand the process of cloud and mobile device forensics

Unit I Computer Forensics Fundamentals **9**

Introduction to Computer Forensics – Computer Forensics Services – Benefits of Professional Forensics Methodology – Steps taken by Computer Forensics Specialists – Types of Computer Forensics System: IDS, Firewall – PKI – Wireless Network Security – Identity Management Security System – Identity Theft.

Unit II Computer Forensics Technology **9**

Types of Military, Business and Law Enforcement Computer Forensic Technology – Specialized Forensics Techniques – Hidden Data and How to Find it – Spyware and Adware – Encryption Methods – Internet Tracing Methods – Avoiding Pitfalls with Firewall – Biometric Security Systems.

Unit III Data Acquisition and Processing Crime Scenes **12**

Understanding Storage Formats for Digital Evidence - Determining the Best Acquisition Method - Using Acquisition Tools - Validating Data Acquisitions - Performing RAID Data Acquisitions - Identifying Digital Evidence - Collecting Evidence in Private-Sector Incident Scenes - Processing Law Enforcement Crime Scenes - Preparing for a Search - Securing a Computer Incident or Crime Scene - Seizing Digital Evidence at the Scene - Obtaining a Digital Hash.

Unit IV Network and E – mail Forensics **9**

Performing Live Acquisitions - Network Forensics Overview - Exploring the Role of E-mail in Investigations - Exploring the Roles of the Client and Server in E-mail - Investigating E-mail Crimes and Violations - Understanding E-mail Servers - Using Specialized E-mail Forensics Tools.

Unit V Cloud and Mobile Device Forensics **6**

An Overview of Cloud Computing - Legal Challenges in Cloud Forensics - Technical Challenges in Cloud Forensics - Acquisitions in the Cloud - Tools for Cloud Forensics - Understanding Mobile Device Forensics - Understanding Acquisition Procedures for Mobile Devices.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Plan and prepare for all stages of an investigation
- Explore web server attacks, DNS and router attacks
- Identify various evidences of cyber crime

- Examine network traffic and identify illicit servers
- Acquire data from mobile devices and crime scenes securely

References

1. Bill Nelson, Amelia Phillips, Christopher Steuart, "Guide to Computer Forensics andInvestigations: Processing Digital Evidence", 5th edition, Cengage Learning, 2015.
2. John R.Vacca, "Computer Forensics", Cengage Learning, 2005.
3. Nelson, Phillips, Enfinger, Steuart, "Computer Forensics and Investigations", CengageLearning, India Edition, 2008.
4. Marjie T.Britz, "Computer Forensics and Cyber Crime: An Introduction", 3rd Edition,Prentice Hall, 2013.

CF18111 NETWORK DESIGN AND SECURITY LABORATORY

L	T	P	C
0	0	3	2

Course Objectives:

The students will be able to

- Understand the basics of Networking
- Learn network programming in Linux using C/Python

List of Exercises

I Network Design using CISCO Packet Tracer

1. Configure a LAN with a switch/hub with minimum 3 PCs
2. Configure a internetwork with 2 routers and two or more LANs using static routes
3. Establish a dynamic routing based internetwork with 2 routers and two or more LANs using RIP/OSPF
4. Analyze the performance of various TCP variants using an FTP application for the given network

II Network Programming using C/Python

5. Develop a program for demonstrating inter process communication
6. Creation of TCP client/server application
7. Creation of UDP client/server application
8. Develop an Iterative UDP server with 2 or 3 clients
9. Develop a concurrent TCP server with 2 or 3 clients
10. Implement Digital Signature
11. Implement ARP and RARP
12. Create a Socket based application in Python
13. Intrusion Detection using Snort tool
14. Create an application that interacts with e-mail servers in python
15. Develop applications that work with remote servers using SSH, FTP etc in Python
16. Simulate PING and TRACEROUTE commands

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Design and Configure LAN's
- Create simple network applications using C/Python
- Demonstrate Interprocess communication
- Simulate IDPS
- Develop applications that work with remote servers

LIST OF EQUIPMENT FOR A BATCH OF 18 STUDENTS:

SOFTWARE:

Windows/Ubuntu/ Kali Linux with C/C++/Java/Python

Cisco Packet Tracer, Snort IDS, Eclipse or equivalent IDE

HARDWARE:

Standalone desktops - 18

CF18112	ETHICAL HACKING ESSENTIALS LABORATORY	L	T	P	C
		0	0	3	2

Course Objectives:

The students will be able to

- Understand the basics of Ethical Hacking
- Learn various Hacking tools

List of Exercise

1. Basic Linux Commands
2. Advanced Linux commands
3. Information Gathering
4. Vulnerability Analysis
5. Web Application Analysis
6. Database Assessment
7. Password Attacks
8. Wireless Attacks
9. Reverse Engineering
10. Exploitation tools
11. Sniffing & spoofing
12. VM-WARE

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Gather the information from various sources
- Assess the vulnerabilities in Database
- Analyse the vulnerabilities in Web application
- Enumerate various attacks and its counter measures
- Use different Exploitation tools

LIST OF EQUIPMENT FOR A BATCH OF 18 STUDENTS:

SOFTWARE:

Kali Linux and its Tools

HARDWARE:

Standalone desktops - 18

CF18201 FUNDAMENTALS TO SECURITY IN BIOMETRICS

L	T	P	C
3	0	0	3

Course Objectives:

The students will be able to

- Understand the functionalities of biometrics
- Discover the need of biometrics for an organization
- Learn to develop biometric based applications
- Emphasize the need of biometric security

Unit I Fundamentals of Biometrics **9**

Biometric System – Enrollment and recognition – Sensor modules – Feature extraction module - Database module – Matching module – Biometric functionalities – Biometric system errors – Design cycle of Biometrics – Security and Privacy issues.

Unit II Fingerprint Recognition **9**

Friction ridge pattern: Features and formation – Fingerprint Acquisition – Feature extraction – Matching – Fingerprint indexing – Fingerprint synthesis: Level 1 and Level 2 – Palmprint.

Unit III Face and Iris Recognition **9**

Psychology of face recognition – Facial features – Design – Image acquisition – Face detection – Feature extraction and matching – Face modelling – Iris Recognition: Design and Image acquisition – Image segmentation – Image normalization, Encoding and matching – Iris quality – Performance Evaluation.

Unit IV Signature and Keystroke Recognition **9**

Behavioural biometrics – Features and Classification – Signature Recognition: History of Handwriting Analysis - Automated Systems for Signature Recognition - Offline and Online Signatures - Types of Forgeries - Databases for Signature System Evaluation - Commercial Software – Signature Recognizers – Keystroke Dynamics: Keystroke Analysis - Authentication and Identification - Characteristics of Keystroke Dynamics - Approaches to Keystroke Dynamics.

Unit V Security in Biometrics **9**

Adversary Attacks – Insider and Infrastructure attack - Attacks at the User Interface – Impersonation – obfuscation – spoofing - Countermeasure: spoof detection - Attacks on Biometric Processing – System modules and interconnections - Attacks on the Template Database - Biometric template security.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Identify various biometric techniques
- Design biometric recognition systems
- Develop simple biometric based application

- Elucidate the need for biometric security
- Analyse the various attcks possible in Biometric system

References

1. James wayman,Anil k.Jain ,Arun A.Ross ,Karthik Nandakumar, “Introduction to Biometrics”, Springer, 2011.
2. Khalid saeed with Marcin Adamski, “New Directions in Behavioral Biometrics”, CRC Press 2017
3. Paul Reid "Biometrics For Network Security ", Person Education 2004.

CF18202 DIGITAL FORENSICS AND DIGITAL INVESTIGATIONS

L	T	P	C
3	0	0	3

Unit I Digital Forensics **9**

Foundations of Digital Forensics - Digital Evidence - Increasing Awareness of Digital Evidence - Digital Forensics: Past, Present, and Future - Principles and Challenges of Digital Forensics - Digital Forensics Research - Language of Computer Crime Investigation.

Unit II Digital Investigations **9**

Conducting Digital Investigations - Digital Investigation Process Models - Scaffolding for Digital Investigations - Applying the Scientific Method in Digital Investigations - Fundamental Principles - Preparing to Handle Digital Crime Scenes – Surveying and Preserving the Digital Crime Scene - Equivocal Forensic Analysis – Victimology - Crime Scene Characteristics.

Unit III Digital Evidence **9**

Violent Crime and Digital Evidence - Digital Evidence as Alibi - Investigating an Alibi – Time and Location as Alibi - Investigating Computer Intrusions - Forensic Preservation of Volatile Data - Investigation of Malicious Computer Programs – Cyberstalking.

Unit IV Computer basics for Digital Investigators **9**

Basic Operation of Computers - Representation of Data - File Systems and Location of Data - Dealing with Password Protection and Encryption - Applying Forensic Science to Computers - Digital Evidence on Windows Systems - Digital Evidence on UNIX Systems.

Unit V Forensic Science on Networks **9**

Digital Evidence on the Internet - Online Anonymity and Self-Protection - E-mail Forgery and Tracking - Usenet Forgery and Tracking - Digital Evidence on Physical and Data-Link Layers - Digital Evidence at the Network and Transport Layers.

Total Hours:45

Outcomes:

- Relate the fundamentals of computer forensics, laws, report writing and tools in digital investigations.
- Assess the investigative smart practices and applicability of concerned laws & investigative tools.
- Inspect the acquired data, recover the deleted data and manage a case .
- Select the correct method to handle the digital evidence and acquire appropriate certification to build the career in digital forensics.
- Create a method for gathering, assessing and applying new and existing legislation specific to the practice of digital forensics.

References

1. Eoghan Casey, “Digital Evidence and Computer Crime Forensic Science, Computers and the Internet”, Third Edition, Elsevier, 2011
2. Kevin Mandia, Chris Prosise, Matt Pepe, ―Incident Response and Computer Forensics ―, TataMcGraw -Hill, New Delhi, 2006.
3. Nelson Phillips and Enfinger Steuart, ―Computer Forensics and Investigations‖, Cengage Learning, New Delhi, 2009.
4. Cory Altheide and Harlan Carvey, ―Digital Forensics with Open Source Tools‖ Elsevier publication, April 2011

CF18203	BLOCKCHAIN FOR SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

The students will be able to

- Understand the cryptography basics of a blockchain
- Recognize the requirement of a simple blockchain application
- Study about the tools used for blockchain development

Unit I Crypto Fundamentals for Blockchain 12

Hash Functions – Digital Hash – Pre-image resistance – Second pre-image resistance – Message Digest – Secure Hash Algorithms – Distributed Hash Tables – Digital Signatures – Signcryption – Blind Signatures.

Unit II Features of Blockchain 9

History of Blockchain – Decentralization – Generic Elements of Blockchain – Addresses – Transaction – Block – Contents of a Block – Block Header - State Machine – Nodes– Types of Blockchain.

Unit III Consensus in Blockchain 9

Fault tolerance – Paxos – Consensus – Byzantine Agreement – Proof of Work – Proof of Stake – Proof of Elapsed Time – Proof of Importance – Practical Byzantine Fault Tolerance – CAP Theorem - Mining – How blockchain accumulates block.

Unit IV Hyperledger for Blockchain 9

Hyperledger as a protocol – Fabric – Sawtooth lake – Reference Architecture – Privacy and Confidentiality – Fabric Architecture – Components of the fabric – Blockchain services – API's and CLI's.

Unit V Applications of Blockchain 6

Bitcoin – Cryptocurrency – Smart Contracts – Financial Applications – IoT Blockchain Applications – Government Applications – Blockchain Security.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Elucidate the requirements of a blockchain
- Design a simple blockchain based application
- Implement Consensus mechanism in blockchain
- Deploy sample applications over Hyperledger
- Explain the requirement of mining in blockchain

References

1. Imran Bashir, “Mastering Blockchain”, Packt Publishing 2017.
2. Melanie Swan, “Blockchain - Blueprint for a New Economy”, O'Reilly Media, 2015
3. Roger Wattenhofer, “The science of the blockchain”, Inverted Forest Publishing, 2016
4. www.blockchain.io
5. www.blockchain.org

CF18204	INTERNET OF THINGS AND SECURITY	L	T	P	C
		3	1	0	4

Course Objectives:

The students will be able to

- Understand the fundamentals of Internet of Things
- Fabricate a low cost embedded system using Raspberry Pi or Arduino
- Apply IoT in Real world scenario

Unit I Fundamentals of IoT **12**

The flavour of the Internet – Technology of IoT – Enchanted objects – Design principles for connected device – Privacy – Webthinking – Affordance.

Unit II Internet Principles **12**

Internet Communications – IP, TCP – Protocol suite – UDP – IP Addresses – TCP and UDP ports – MAC Address – Application Layer Protocols.

Unit III Prototyping Embedded Devices **12**

Prototypes and production - Open source versus closed source - Tapping into the community – Electronics - Embedded computing basics – Arduino - Raspberry pi - electric imp – plug computing.

Unit IV Prototyping Physical and Online Components **12**

Preparation, sketch, iterate and explore - Non digital methods - Laser cutting - 3D printing – Getting started with API – Writing a new API – Real time reactions – Memory Management.

Unit V Prototype to Business Models **12**

Business model canvas – Models - Funding an internet of things startup – Scaling up Software – Ethics: Privacy – Control – Environment – Solutions.

Total Hours:60(L:45+T:15)

Course Outcomes:

At the end of the course, the students will be able to,

- Analyze various protocols of IoT
- Design a portable IoT application using Raspberry Pi or Arduino
- Deploy an IoT application to the cloud.
- Analyze applications of IoT in real time scenario
- Design Prototype for physical and online components

References

1. Adrian McEwen, Hakim Cassimally, Designing the Internet of Things, 1/e, Wiley publication, 2013
2. Charalampos Doukas , Building Internet of Things with the Arduino, Create space, 2002.
3. Dieter Uckelmann (et.al), Architecting the Internet of Things, Springer, 2011.

CF18211	IOT AND BLOCKCHAIN LABORATORY	L	T	P	C
		0	0	3	2

Course Objectives:

The students will be able to

- Understand the basics of Arduino/ Raspberry Pi programming
- Learn to develop simple blockchain applications.

Arduino and Raspberry Pi

1. Arduino programming to make the LED Blink with and without delay
2. Serial Communication in Arduino with Wireless Module and Programming
3. Bluetooth (HC-05) and ZigBee (TI -CC2500)
4. Programming the Raspberry Pi to make the LED Blink using Python
5. Integration of sensors/components with Raspberry Pi and Programming
6. Serial Communication Between Arduino and Raspberry Pi using Universal Serial Bus(USB)

Security in Arduino and Raspberry Pi

7. Implementation of MD5, SHA1, SHA256 in Arduino/Raspberry Pi using Hash Functions.
8. Implementation of DES and AES Algorithms in Arduino/Raspberry Pi using Arduino Cryptographic Library.

Blockchain Implementation

9. Implementation of basic Hash algorithms required for Blockchain
10. Developing simple applications using Hyperledger framework
11. Developing simple applications using Ethereum framework
12. Simulation of mining in Blockchain
13. Implementation of ethereum smart contracts

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Develop simple applications using Arduino/ Raspberry Pi
- Implement various security protocols
- Create simple applications using blockchain tools
- Simulate mining in blockchain
- Design application using Hyperledger/ethereum framework

LIST OF EQUIPMENT FOR A BATCH OF 18 STUDENTS:

SOFTWARE:

Windows/Ubuntu/ Kali Linux with C/C++/Java/Python

Cisco Packet Tracer, Snort IDS, Eclipse or equivalent IDE

HARDWARE:

Standalone desktops – 18 IoT kit -18

CF18212	DIGITAL FORENSICS LABORATORY	L	T	P	C
		0	**0**	**3**	**2**

Course Objectives:

The students will be able to

- Perform basic digital forensics.
- Demonstrate the use of simple digital forensics tools.
- Conduct a digital forensics exercise.

List of Exercises

Disk Imaging and Cloning

1. Use VMWare and modify device configuration in a VMWare system

Analyzing disk structure and file systems

2. The Sleuth Kit Tools

Search Word Filtering from Unallocated, Slack and Swap Space

Unix File Recovery – Data Unit Level

3. Review of unallocated space and extracting with dls

FILE RECOVERY: META DATA LAYER

4. Find meta data information for evidence found in a search list

Keyword Searches, Timelines, Hidden Data

Data Mining for Digital Forensics

5. Encryption and Password Recovery
6. Steganography Detection
7. File Extension Renaming and Signaturing
8. Application Analysis
9. Client and Web Analysis
10. Network Analysis

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Practice and gain basic knowledge about VMware and various file system
- Analyse disk structure and file system
- Perform file recovery
- Perform mining for digital forensics
- Apply steganography in digital forensics

LIST OF EQUIPMENT FOR A BATCH OF 18 STUDENTS:

SOFTWARE:

Ubuntu/ Kali Linux with C/C++/Java/Python

Sleuth Kit, Wireshark, VMWare, OWASP, DVWA

HARDWARE:

Standalone desktops - 18

CF18303	PENETRATION AND APPLICATION TESTING	L	T	P	C
		3	0	0	3

OBJECTIVES:

- To understand and analyse entire penetration testing process including planning, reconnaissance, scanning, exploitation, post-exploitation, and result reporting
- To understand the fundamental information associated with methods employed and insecurities identified
- To develop an excellent understanding of current cybersecurity issues and ways that user, administrator, and programmer errors can lead to exploitable insecurities.

UNIT I THE BASICS 9

Using Kali Linux – Linux File System – User Privilege – File permission – Data manipulation – Managing and Networking – Shell and python Scripting – Metasploit Framework

UNIT II ASSESSMENTS AND EXPLOITATION 9

Finding Vulnerabilities – Nmap scripting engine – Metasploit Scanner – Metasploit exploit check functions – Web application scanning – Using wireshark to capture traffic – SSL attacks and scripting – Exploiting WebDav credentials – Exploiting Open phpMyAdmin – Exploiting third party web appplications

UNIT III EXPLOIT DEVELOPMENT 9

Stack based buffer overflow in Linux – Memory Theory – Linux Buffer overflow - Stack based buffer overflow in Windows – Causing a crash – Locating EIP – Structured exception handler – Fuzzing programs – Porting public exploits – Writing metasploit modules – Exploitation mitigation techniques

UNIT IV POST EXPLOITATION 9

Client side exploitation – Bypassing filters – Client side attacks – Social Engineering – Bypassing Antivirus applications – Meterpreter – Local information gathering – Lateral movement – Pivoting – Persistence – Web Application testing – SQL injection – Xpath injection – Cross site scripting - Web application scanning with w3af.

UNIT V WIRELESS AND MOBILE HACKING 9

Monitoring mode – Wired equivalent privacy – WPA2 – Wifi protected setup – Smartphone pentest framework – Mobile attack vectors – Remote and Client side attacks – Malicious apps – Mobile post exploitation.

TOTAL : 45 PERIODS

OUTCOMES:

Upon successful completion of this course, a student will be able to:

- Demonstrate professional and ethical responsibility, communicate effectively, the impactof security practices in a global and societal context
- Elaborate vulnerabilities, mechanisms to identify vulnerabilities/threats/attacks
- Apply knowledge of engineering to security evaluations, design and conduct security assessmentexperiments
- Apply techniques and modern engineering tools necessary for computer security engineering practice

- Enumerate the technical workings of various penetration tests and produce reports based on them

References

1. Georgia Weidman, Penetration Testing – A hands-on introduction to hacking, No Scratch Press, 2014
2. Jon Erickson , Hacking: The Art of Exploitation, O'Reilly 2nd Edition
3. Rajat Khare, "Network Security and Ethical Hacking", Luniver Press, 2006
4. Ramachandran V, BackTrack 5 Wireless Penetration Testing Beginner's Guide (3rd ed.). Packt Publishing, 2011
5. Thomas Mathew, "Ethical Hacking", OSB publishers, 2003

CF18001	APPLIED CRYPTOGRAPHY	L	T	P	C
		3	0	0	3

Course Objectives:

The students will be able to

- Understand basic encryption methods and algorithms, he strengths and weaknesses of encryption algorithms.
- Understand encryption key exchange and management
- Gain knowledge on hashing and its applications

Unit I Cryptography and Computational Hardness 9

Introduction -Private Key Cryptography - Public Key Cryptography - Hash functions - Digital Signature - Multiplication, Primes, and Factoring - Hardness Amplification - Collections of One-Way Functions - Basic Computational Number Theory - Factoring-based Collection of OWF - Discrete Logarithm-based Collection

Unit II Indistinguishability and Pseudo-Randomness 9

RSA Collection - One-way Permutations - Trapdoor Permutations - Rabin collection - A Universal One Way Function - Computational Indistinguishability - Pseudo-random generators - Hard-Core Bits from Any OWF - Secure Encryption - An Encryption Scheme with Short Keys - Multi-message Secure Encryption - Pseudorandom Functions - Construction of Multi-message Secure Encryption - Public Key Encryption - El-Gamal Public Key Encryption scheme - A Note on Complexity Assumptions

Unit III Public Key and Private Key Cryptosystems 9

Chosen plaintext attack - Security against multi-key attacks - Building CPA secure ciphers - Nonce based encryption - Message integrity - Message integrity from Universal Hashing - Elliptic Curve cryptography and pairings - Analysis of number theoretic assumptions

Unit IV Protocols for Cryptography 9

Protocols for Identification and Login - Authenticated Encryption - Identification and signatures from sigma protocols - Combining Sigma protocols - Witness independence and applications - Proving properties in zero-knowledge

Unit V Protocols for Key Exchange 9

Authenticated Key exchange - HSM security - One-sided Authentication - Deniability - Password authenticated key exchange - Secure multi-party computation - Evaluating arithmetic circuits - Garbled circuits - Formal models for multiparty communication

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Design algorithms for constructing cryptographic computations
- Analyse the correctness of cryptographic protocols.
- Enumerate the methods used for encryption, authentication, integrity, certification and data privacy.

- Apply the complex protocols that involve many steps and computing agents, who donot trust each other.
- Simulate the electronic transactions

References

1. Rafael Pass and Abhi Shelat, “A Course in Cryptography”, Third edition: January 2010
2. Dan Boneh and Victor Shoup, “A Graduate Course in Applied Cryptography”, January 2020.
3. William Stallings, “Cryptography and Network Security: Principles and Practices”, Seventh Edition, Pearson Education, 2017.
4. Matt Bishop ,“Computer Security art and science ”, Second Edition, Pearson Education, 2002

CP18105	MACHINE LEARNING TECHNIQUES (Common to CP,NW,CFIS)	L	T	P	C
		3	0	0	3

Course Objectives:

The students will be able to

- To introduce students to the basic concepts and techniques of Machine Learning.
- To have a thorough understanding of the Supervised and Unsupervised learning techniques.
- To study the various probabilities based learning techniques.

Unit I Introduction to Machine Learning Techniques 9

Learning – Types of Machine Learning – Supervised Learning – The Brain and the Neuron – Design a Learning System – Perspectives and Issues in Machine Learning – Concept Learning Task – Concept Learning as Search – Finding a Maximally Specific Hypothesis – Version Spaces and the Candidate Elimination Algorithm – Linear Discriminants – Perceptron – Linear Separability – Linear Regression.

Unit II Linear Models 9

Multi-layer Perceptron – Going Forwards – Going Backwards: Back Propagation Error – Multilayer Perceptron in Practice – Examples of using the MLP – Overview – Deriving Back Propagation – Radial Basis Functions and Splines – Concepts – RBF Network – Curse of Dimensionality – Interpolations and Basis Functions – Support Vector Machines Virtual.

Unit III Tree and Probabilistic Models 9

Learning with Trees – Decision Trees – Constructing Decision Trees – Classification and Regression Trees – Ensemble Learning – Boosting – Bagging – Different ways to Combine Classifiers – Probability and Learning – Data into Probabilities – Basic Statistics – Gaussian Mixture Models – Nearest Neighbor Methods – Unsupervised Learning – K means Algorithms – Vector Quantization – Self Organizing Feature Map.

Unit IV Dimensionality Reduction and Evolutionary Models 9

Dimensionality Reduction – Linear Discriminant Analysis – Principal Component Analysis – Factor Analysis – Independent Component Analysis – Locally Linear Embedding – Isomap – Least Squares Optimization – Evolutionary Learning – Genetic algorithms – Genetic Offspring: - Genetic Operators – Using Genetic Algorithms – Reinforcement Learning – Overview – Getting Lost Example – Markov Decision Process.

Unit V Graphical Models 9

Markov Chain Monte Carlo Methods – Sampling – Proposal Distribution – Markov Chain Monte Carlo – Graphical Models – Bayesian Networks – Markov Random Fields – Hidden Markov Models – Tracking Methods.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Distinguish between, supervised, unsupervised and semi-supervised learning
- Apply the apt machine learning strategy for any given problem
- Suggest supervised, unsupervised or semi-supervised learning algorithms for given problem
- Design systems that uses the appropriate graph models of machine learning

References

1. Ethem Alpaydin, "Introduction to Machine Learning 3e (Adaptive Computation and Machine Learning Series)", Third Edition, MIT Press, 2014
2. Jason Bell, "Machine learning – Hands on for Developers and Technical Professionals", First Edition, Wiley, 2014
3. Peter Flach, "Machine Learning: The Art and Science of Algorithms that Make Sense of Data", First Edition, Cambridge University Press, 2012.
4. Stephen Marsland,"Machine Learning – An Algorithmic Perspective", Second Edition, Chapman and Hall, CRC Machine Learning and Pattern Recognition Series, 2014.

CF18002	DATA MINING TECHNIQUES	L	T	P	C
		3	0	0	3

Course Objectives:

The students will be able to

- Understand Data mining principles and techniques and Introduce DM as a cutting edge business intelligence
- Explore the concepts of Datawarehousing Architecture and Implementation
- Study the overview of developing areas – Web mining, Text mining and ethical aspects of Datamining
- Identify Business applications and Trends of Data mining

Unit I Introduction to Data Warehousing 9

Evolution of Decision Support Systems- Data warehousing Components – Building a Datawarehouse, Data Warehouse and DBMS, Data marts, Metadata, Multidimensional data model, OLAP vs OLTP, OLAP operations, Data cubes, Schemas for Multidimensional Database: Stars, Snowflakes and Fact constellations

Unit II Data Warehouse Process and Architecture 9

Types of OLAP servers, 3–Tier data warehouse architecture, distributed and virtual data warehouses. Data warehouse implementation, tuning and testing of data warehouse. Data Staging (ETL) Design and Development, data warehouse visualization, Data Warehouse Deployment, Maintenance, Growth, Business Intelligence Overview- Data Warehousing and Business Intelligence Trends - Business Applications- tools-SAS

Unit III Introduction to Data Mining 9

Data mining-KDD versus datamining, Stages of the Data Mining Process-task premitives, Data Mining Techniques -Data mining knowledge representation – Data mining query languages, Integration of a Data Mining System with a Data Warehouse – Issues, Data preprocessing – Data cleaning, Data transformation, Feature selection, Dimensionality reduction, Discretization and generating concept hierarchies-Mining frequent patterns- association-correlation

Unit IV Classification and Clustering 9

Decision Tree Induction - Bayesian Classification – Rule Based Classification – Classification by Backpropagation – Support Vector Machines – Associative Classification – Lazy Learners – OtherClassification Methods – Clustering techniques – , Partitioning methods- k-means-HierarchicalMethods – distance based agglomerative and divisible clustering, Density-Based Methods –expectation maximization -Grid Based Methods – Model-Based Clustering Methods – Constraint –Based Cluster Analysis – Outlier Analysis

Unit V Predictive Modeling Of Big Data and Trends In Datamining 9

Statistics and Data Analysis – EDA – Small and Big Data –Logistic Regression Model – Ordinary Regression Model-Mining complex data objects – Spatial databases – Temporal databases – Multimedia databases – Time series and sequence data – Text mining – Web mining – Applications in Data mining

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Design Multidimensional Intelligent model from typical system
- Explore the features of high dimensional system
- Implement various mining techniques on complex data objects
- Apply various Business Applications Tools
- Analyze various classification and clustering techniques

References

1. Jiawei Han and Micheline Kamber, Data Mining: Concepts and Techniques, Morgan Kaufmann Publishers, third edition2011, ISBN: 1558604898.
2. Alex Berson and Stephen J. Smith, " Data Warehousing, Data Mining & OLAP", Tata McGrawHill Edition, Tenth Reprint 2007.
3. G. K. Gupta, "Introduction to Data Min Data Mining with Case Studies", Easter Economy Edition, Prentice Hall of India, 2006.
4. Data Mining:Practical Machine Learning Tools and Techniques,Third edition,(Then Morgan Kufmann series in Data Management systems), Ian.H.Witten, Eibe Frank and Mark.A.Hall, 2011
5. Statistical and Machine learning –Learning Data Mining, techniques for better Predictive Modeling and Analysis to Big Data

CF18003	INTRUSION DETECTION AND PREVENTION SYSTEMS	L	T	P	C
		3	0	0	3

Course Objectives:

The students will be able to

- Understand the state of the art of intrusion detection system
- Design and implement Intrusion Detection System
- Understand the classes of attacks on computer systems
- Identify various types of IDS of signature based and anomaly based techniques to solve problems related to intrusion detection and prevention.

Unit I Introduction **9**

Understanding Intrusion Detection – Intrusion detection and prevention basics – IDS and IPS analysis schemes, Attacks, Detection approaches –Misuse detection – anamoly detection – specification based detection – hybrid detection-methodologies-Signature & Anomaly based Detection, Stateful protocol analysis Types of IDS, Information sources Host based information sources, Network based information sources.

Unit II Theoretical Foundations of Detection Technologies **9**

Taxonomy of anomaly detection system – fuzzy logic – Bayes theory – Artificial Neural networks – Support vector machine - IDS TECHNOLOGIES: Components & Architecture-Typical components, Network Architectures Security capabilities - Information gathering capabilities, logging capabilities, detection & prevention capabilities. Network protocol based IDS, Hybrid IDS, and Analysis schemes.

Unit III Network Based IDS **9**

Networking Overview- OSI layers. Components and Architecture - Typical components, Network architectures and sensor locations. Security capabilities Wireless IDPS - Wireless Networking overview- WLAN standards & components. Components Network Behaviour analysis system.

Unit IV Host Based IDS **9**

Components and Architecture-Typical components, Network architectures, Agent locations, host architectures. Security capabilities-Logging, detection, prevention and other capabilities. Using & Integrating multiple IDPS technologies-Need for multiple IDPS technologies, Integrating different IDPS technologies-Other technologies with IDPS capabilities, Anti - malware technologies, Firewalls and Routers, Honeypots.

Unit V Applications and Snort Tools **9**

Tool Selection and Acquisition Process - Bro Intrusion Detection – Prelude Intrusion Detection - Cisco Security IDS - Snorts Intrusion Detection – NFR security - Introduction to Snort, Working with Snort Rules, Snort configuration, Snort with MySQL, Running Snort on Multiple Network Interfaces.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Enumerate the need of anomaly detection and its types
- Analyze various IDS technologies
- Configure a network using IDS tools
- Configure a server and its hosts for realtime Intrusion Detection
- Select and install a IDS system such as Snort to secure the network

References

1. Carl Endorf, Eugene Schultz and Jim Mellander " Intrusion Detection & Prevention" , 1st Edition, Tata McGraw-Hill, 2006
2. Ali A. Ghorbani, Wei Lu, "Network Intrusion Detection and Prevention: Concepts and Techniques", Springer, 2010.
3. Karen Scarfone, Peter Mell," Guide to Intrusion Detection and Prevention Systems (IDPS)", NIST special publication, 2007.
4. Stephen Northcutt, Judy Novak : "Network Intrusion Detection", 3rd Edition, New Riders Publishing, 2002.
5. Paul E. Proctor, "The Practical Intrusion Detection Handbook ", Prentice Hall , 2001.
6. Rafeeq Rehman : " Intrusion Detection with SNORT, Apache,MySQL, PHP and ACID," 1st Edition, Prentice Hall , 2003

CP18016	SOCIAL NETWORK ANALYSIS (Common to CP,NW & CFIS)	L	T	P	C
		3	0	0	3

Course Objectives:

The students will be able to

- Understand the concepts of Social networks and Web Social Networks
- Appreciate the modelling and visualizing techniques associated with Social Networks

Unit I Social Network Analysis Fundamentals 9

Introduction to Web - Limitations of current Web – Development of Semantic Web – Emergence of the Social Web – Statistical Properties of Social Networks -Network analysis – Development of Social Network Analysis - Key concepts and measures in network analysis – Discussion networks - Blogs and online communities - Web-based networks.

Unit II Modeling and Visualization 9

Visualizing Online Social Networks - A Taxonomy of Visualizations - Graph Representation - Centrality- Clustering - Node-Edge Diagrams - Visualizing Social Networks with MatrixBased Representations- Node-Link Diagrams - Hybrid Representations - Modelling and aggregating social network data - RandomWalks and their Applications –Use of Hadoop and MapReduce - Ontological representation of social individuals and relationships.

Unit III Mining Communities 9

Aggregating and reasoning with social network data, Advanced Representations – Extracting evolution of Web Community from a Series of Web Archive - Detecting Communities in Social Networks - Evaluating Communities – Core Methods for Community Detection & Mining - Applications of Community Mining Algorithms - Node Classification in Social Networks.

Unit IV Evolution 9

Evolution in Social Networks – Framework - Tracing Smoothly Evolving Communities – Models and Algorithms for Social Influence Analysis - Influence Related Statistics - Social Similarity and Influence - Influence Maximization in Viral Marketing - Algorithms and Systems for Expert Location in Social Networks – Expert Team Formation - Link Prediction in Social Networks - Feature based Link Prediction - Bayesian Probabilistic Models - Probabilistic Relational Models.

Unit V Text and Opinion Mining 9

Text Mining in Social Networks -Opinion extraction – Sentiment classification and clustering - Temporal sentiment analysis - Irony detection in opinion mining - Wish analysis - Product review mining – Review Classification – Tracking sentiments towards topics over time.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Build a social network data set from existing social networking sites
- Identify the components of a web social network
- Identify the different data structures and graph algorithms that can be used for web social network mining
- Perform text and opinion mining in social network
- Design Models and Algorithms for Social Influence Analysis

References

1. Charu C. Aggarwal, "Social Network Data Analytics", Springer; 2011
2. Peter Mika, "Social Networks and the Semantic Web", Springer, 1st edition 2007.
3. Borko Furht, "Handbook of Social Network Technologies and Applications",Springer, 1st edition, 2010.
4. Guandong Xu , Yanchun Zhang and Lin Li, "Web Mining and Social Networking – Techniques and applications", Springer, 1st edition, 2011.

CF18004	PRINCIPLES OF SECURE CODING	L	T	P	C
		3	0	0	3

Course Objectives:

The students will be able to

- Explain security design principles
- Analyze and Design projects by applying security principles
- Implement projects using security primitives
- Utilize tools for security analysis

Unit I Introduction to Security **9**

Security goals- -Proactive Security development process, Secure Software Development Cycle (S-SDLC) , Security issues while writing SRS, Best Practices SD3 (Secure by design, default and deployment), Security principles and Secure Product Development Timeline, Security Design Principles.

Unit II Secure Programming Techniques **9**

Worms and other malware, Buffer overflows, client state manipulation, sql injection-password security-cross domain security in web applications.

Unit III Secure coding **9**

Safe initialization ,Access control, Input validation, buffer overflows, format String problems, Integer overflows, C++ catastrophes, Catching exceptions, command injection, information leakage, Race conditions, Poor usability executing code with too much privilege. Failure to, protect stored data.

Unit IV Database and Web-specific issues **9**

SQL Injection Techniques and Remedies, Race conditions, Time of Check Versus Time of Use and its protection mechanisms. Validating Input and Interprocess Communication, Securing Signal Handlers and File Operations. XSS scripting attack and its types – Persistent and Non persistent attack XSS Counter measures and Bypassing the XSS Filters.

Unit V Testing secure applications **9**

Testing Secure Applications: Security code overview, secure software installation. The Role of the Security Tester, Building the Security Test Plan. Testing HTTP-Based Applications, Testing File-Based Applications, Testing Clients with Rogue Servers

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Elucidate the principles required for securing an organization
- Create secure projects for an organization
- Deploy projects and their security features
- Design methodologies for secure software development
- Utilize the tools available for security and secure an organization

References

1. Foundations of Security, Daswani N., Kern C., Kesavan A., Apress
2. 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them by John Viega (Author), Matt Messier (Author)
3. Secure Programming Cookbook for C and C++,O'Reilly Media
4. Writing Secure Code, Michael Howard and David LeBlanc,Microsoft Press, 2nd Edition, 2004

CF18005	TRUST MANAGEMENT IN E-COMMERCE	L	T	P	C
		3	0	0	3

Course Objectives:

The students will be able to

- Ecommerce business models and Digital Payments systems
- Knowledge about Ecommerce security Environment
- To study about Ecommerce mechanisms and trusted computing Platform.

Unit I Introduction To E-Commerce **9**

Introduction to E-Commerce – Network and E-Commerce – Types of E-Commerce –E-commerce Business Models, Major Business to Consumer (B2C) business models, Major Business to Business (B2B) business models, Business models in emerging E-commerce areas, How the Internet and the web change business: strategy, structure and process, The Internet: Technology Background, The Internet Today, Internet II- The Future Infrastructure.

Unit II E-Commerce Security and Payment **9**

E-commerce security environment, Security threats in the e-commerce environment, Technology solution, Management policies, Business procedures, and public laws, Payment system, E-commerce payment system, Electronic billing presentment and payment.

Unit III Trust In E-Commerce **9**

Inter-organizational trust in E-Commerce: Need – Trading partner trust – Perceived benefits and risks of E-Commerce – Technology trust mechanism in E-Commerce – Perspectives of organizational, economic and political theories of inter-organizational trust – Conceptual model of inter-organizational trust in E-Commerce participation.

Unit IV Trusted Computing Platform **9**

Introduction to trusted computing platform: Overview – Usage Scenarios – Key components of trusted platform – Trust mechanisms in a trusted platform.

Unit V Trust Models **9**

Trusted platforms for organizations and individuals – Trust models and the E-Commerce domain.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Explain B2C,B2B,C2C,Business models
- Illustrate the Policies, Procedures and Laws and Security threats in E-Commerce environment.
- Analyze and explain the issues, risks and challenges in inter-organisational trust in Ecommerce
- Explain the Key components and Trust mechanisms of trusted computing platform.
- Describe the Trusted platforms for organizations and individuals

References

1. S. J. Joseph, E-Commerce: an Indian perspective, PHI
2. Kenneth C. Laudon and Carol Guercio Trave, ―E-Commerce Business Technology Society‖, 12th Edition Pearson Education, 2016.
3. Pauline Ratnasingam, ―Inter-Organizational Trust for Business-to-Business E- Commerce‖, IRM Press, 2005.
4. Siani Pearson, et al, ―Trusted Computing Platforms: TCPA Technology in Context‖ Prentice Hall PTR, 2002.

CF18006	BIOMETRIC IMAGE PROCESSING	L	T	P	C
		3	**0**	**0**	**3**

Course Objectives:

The students will be able to

- Understand the basics of Image processing
- Model and picture the transformation of image
- Understand the growth of object detection

Unit I Image Processing Essentials **9**

Human vision system – Computer vision system – Image formation – Fourier Transform – Sampling Criteria – Histograms – Point operators – Group operations – Statistical operations – Mathematical morphology.

Unit II Feature Extraction: Edge detection and Fixed shape matching **9**

Edge Detection- Phase congruency- Localized feature extraction- Describing image motion - Thresholding and subtraction - Template matching - Feature extraction by low-level features - Hough transform - Deformable shape analysis - Active contours (snakes).

Unit III Object Detection and Description **9**

Boundary descriptions - Region descriptors - Texture description – Classification – Segmentation - Moving object detection - Tracking moving features - Moving feature extraction and description.

Unit IV Voice and Hand Biometrics **9**

Voice biometric techniques - Acoustic analysis for robust speaker recognition - Distributed speaker recognition through UBM–GMM models – Hand Biometrics: Characterization by minutiae extraction – Sample Databases.

Unit V Multi biometrics and Visual Data Protection **9**

Different principles of multi biometrics - Fusion levels - Applications and illustrations - Biometrics using ECG - Biometrics using medical imaging – Parametric and Non-parametric approaches for classification - Visual data hiding Security.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Enumerate the necessity of image processing
- Enumerate various techniques for feature extraction
- Analyze various techniques for object detection
- Apply various tools for biometrics
- Design data protection techniques

References

1. Amine Nail -Ali and Regis Fournier "Signal and Image Processing for Biometrics" John Wiley and sons,2012
2. Mark S.Nixon, Alberto S.Aguado, Feature Extraction and image processing for computer vision, Third Edition, , Elsevier 2012.
3. Scott E Baugh "Digital Image Processing and analysis" 2nd Edition CRC Press 2010

CF18007	CYBER SECURITY MANAGEMENT AND CYBER LAWS	L	T	P	C
		3	0	0	3

Course Objectives:

The students will be able to

- Understand the need of Cyber Security
- Explore the laws governing Cyber Security
- Gain knowledge on Cyber Security Management

Unit I Fundamentals of Cyber Security **9**

Introduction-Cyber Security and its problem-Intervention Strategies: Redundancy, Diversity and Autarchy.

Unit II Issues in Cyber Security **9**

Private ordering solutions, Regulation and Jurisdiction for global Cyber security, Copy Right-source of risks, Pirates, Internet Infringement, Fair Use, postings, criminal liability, First Amendments, Data Loss.

Unit III Intellectual Property Rights **9**

Copy Right-Source of risks, Pirates, Internet Infringement, Fair Use, postings, Criminal Liability, First Amendments, Losing Data, Trademarks, Defamation, Privacy-Common Law Privacy, Constitutional law, Federal Statutes, Anonymity, Technology expanding privacy rights.

Unit IV Procedural Issues **9**

Duty of Care, Criminal Liability, Procedural issues, Electronic Contracts & Digital Signatures, Misappropriation of information, Civil Rights, Tax, Evidence.

Unit V Legal Aspects of Cyber Security **9**

Ethics, Legal Developments, Late 1990 to 2000, Cyber security in Society, Security in cyber laws case. studies, General law and Cyber Law-a Swift Analysis

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Enumerate ethical laws of computer for different countries
- Explore the needs on copy right issues of software
- Analyze the issues those are specific to amendment rights
- Demonstrate cyber security management skills
- Explore the various options with IPR

References

1. Jonathan Rosenoer,"Cyber Law: The law of the Internet", Springer-Verlag, 1997.
2. Mark F Grady, Fransesco Parisi, "The Law and Economics of Cyber Security", Cambridge University Press, 2006
3. Michael Graves, ―Digital Archaeology: The Art and Science of Digital Forensics, Addison-Wesley Professional, 2014

NW18010	NETWORK VIRTUALIZATION (Common to NW &CFIS)	L	T	P	C
		3	0	0	3

Course Objectives:

The students will be able to

- Understand the need for Virtualization
- Get a practical knowledge on VMWare tools

Unit I Virtualization Fundamentals 9

Virtualization-need, Virtualization Technologies :Server Virtualization, Hardware emulation, Storage Virtualization, Network-attached storage, Storage area networks, I/O Virtualization, Network Virtualization, Client Virtualization, Application virtualization, Desktop virtualization, Case study: Studying Server Consolidation, Development and Test Environments , Quality of Service, Simple failover High availability, Clustering ,Data mirroring, Data replication, IT Operational Flexibility, Load balancing, Server pooling, Helping with Disaster Recovery, Rethinking Virtualization in Business Terms : Rethinking Infrastructure Virtualization, Benefits of Virtualization.

Unit II VMWare Virtualization 9

Virtual machines, and vSphere components, server, network, and storage virtualization, vSphere. Create Virtual Machine VMware vCenter Server: Introduction to vCenter Server architecture and appliance, Virtual Machine Management: Deploy virtual machines using templates and cloning, Modify and manage virtual machines, Create and manage virtual machine snapshots, Perform VMware vSphere vMotion and Storage vMotion migrations, Create a vSpherevApp.

Unit III Access and Authentication Control 9

Control user access through roles and permissions, Configure and manage the ESXi firewall, Configure ESXi lockdown mode, Integrate ESXi with Active Directory, Introduce VMware vShield Zones.

Unit IV Installing VMWare Components 9

Introduce ESXi installation, Describe boot from SAN requirements, Introduce vCenter Server deployment options, Describe vCenter Server hardware, software, and database requirements, Install vCenter Server (Windows based).

Unit V Implement and Configure Window Server 2008 Hyper V 9

Configure Hyper V Virtual Networking, Configure and use Hyper V remote administration, Create and configure Virtual Hard Drives, Use Virtual Machine snapshots, Describe considerations for configuring Hyper-V servers for high availability, Virtual Machine Manager (VMM) features and use VMM to manage virtual machines.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Enumerate the features of network virtualization
- Demonstrate VMWare tools
- Configure the system using Virtualization tools
- Analyse the various requirements for VMware
- Experiment various roles in Access and authentication control

References

1. Virtualization: a beginner's guide - Danielle Ruest, Nelson Ruest , McGraw-Hill Prof Med, 2010.
2. Windows Server 2008 Hyper-V: Insiders Guide to Microsoft's Hypervisor By John Kelbley, Mike Sterling, Allen Stewart, Sybex; 1 edition (April 20, 2009).
3. Virtualization for Dummies - Bernard Golden, For Dummies; 1 edition (December 5, 2007).
4. Mastering Microsoft Virtualization - Tim Cerling, Jeffrey Buller, Jeffrey L. Buller, Sybex; 1 edition (December 21, 2009).

CP18011	CLOUD COMPUTING TECHNOLOGIES (Common to CP,NW &CFIS)	L	T	P	C
		3	0	0	3

Course Objectives:

The students will be able to

- Gain knowledge on the concept of virtualization that is fundamental to cloud computing
- Understand the various issues in cloud computing
- Be able to set up a private cloud

Unit I Virtualization In Cloud **9**

Basics of Virtual Machines - Process Virtual Machines – System Virtual Machines –Emulation –Interpretation – Binary Translation - Taxonomy of Virtual Machines. Virtualization – Management Virtualization — Hardware Maximization – Architectures – Virtualization Management – Storage Virtualization – Network Virtualization.

Unit II Virtualization Infrastructure **9**

Comprehensive Analysis – Resource Pool – Testing Environment –Server Virtualization – Virtual Workloads – Provision Virtual Machines – Desktop Virtualization – Application Virtualization - Implementation levels of virtualization – virtualization structure – virtualization of CPU, Memory and I/O devices – virtual clusters and Resource Management – Virtualization for data center automation.

Unit III Cloud Platform Architecture **9**

Cloud deployment models: public, private, hybrid, community – Categories of cloud computing: Everything as a service: Infrastructure, platform, software- A Generic Cloud Architecture Design – Layered cloud Architectural Development – Virtualization Support and Disaster Recovery – Architectural Design Challenges - Public Cloud Platforms : GAE,AWS – Inter-cloud Resource Management.

Unit IV Programming Model **9**

Introduction to Hadoop Framework - Mapreduce, Input splitting, map and reduce functions, specifying input and output parameters, configuring and running a job –Developing Map Reduce Applications - Design of Hadoop file system –Setting up Hadoop Cluster - Cloud Software Environments -Eucalyptus, Open Nebula, Open Stack, Nimbus.

Unit V Cloud Security **9**

Cloud Infrastructure security: network, host and application level – aspects of data security, provider data and its security, Identity and access management architecture, IAM practices in the cloud, SaaS, PaaS, IaaS availability in the cloud - Key privacy issues in the cloud –Cloud Security and Trust Management.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Examine the concepts of virtualization and virtual machines
- Integrate the knowledge on the concept of virtualization that is fundamental to cloud computing
- Interpret various security issues in Cloud Computing
- Develop a private cloud for different applications
- Inspect the security issues in the grid and the cloud environment

References

1. Danielle Ruest, Nelson Ruest, "Virtualization: A Beginner‟s Guide", McGraw-Hill Osborne Media, 2009.
2. Jim Smith, Ravi Nair , "Virtual Machines: Versatile Platforms for Systems and Processes", Elsevier/Morgan Kaufmann, 2005
3. John W.Rittinghouse and James F.Ransome, "Cloud Computing: Implementation, Management, and Security", CRC Press, 2010.
4. Kai Hwang, Geoffrey C Fox, Jack G Dongarra, "Distributed and Cloud Computing, From Parallel Processing to the Internet of Things", Morgan Kaufmann Publishers, 2012.

CF18008	ENERGY AWARE COMPUTING	L	T	P	C
		3	0	0	3

Course Objectives:

The students will be able to

- Understand the fundamentals of Energy Efficient Computing
- Understand the concept of Energy Efficient Storage Systems
- Introduce the various types of scheduling algorithms in energy efficient computing
- Introduce the concept of Green Networking
- Study Energy Aware Applications

Unit I Introduction **9**

Subreshold Computing – Energy Efficient Network-on-Chip Architectures for Multi-Core Systems-Energy-Efficient MIPS CPU Core with Fine-Grained Run-Time Power Gating –Low Power design of Emerging memory technologies.

Unit II Energy Efficient Storage **9**

Disk Energy Management-Power Efficient Strategies for Storage Systems-Dynamic thermal management for high performance storage systems- Energy-Saving Techniques for Disk Storage Systems.

Unit III Energy Efficient Scheduling Algorithms **9**

Algorithms and Analysis of Energy-Efficient Scheduling of Parallel Tasks- Dynamic Voltage Scaling- Speed Scaling - Processor optimization-Online job scheduling Algorithms.

Unit IV Green Networking **9**

Power-Aware Middleware for Mobile Applications -Energy Efficiency of Voice-over-IP Systems - Intelligent Energy-Aware Networks - Green TCAM-Based Internet Routers.

Unit V Energy Aware Computing Applications **9**

On-Chip Network-Video Codec Design-Energy Aware Surveillance Camera -Low Power Design Challenge in Biomedical Implant Electronics.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Design Power efficient architecture Hardware and Software
- Analyze the different types of Energy Efficient Storage systems.
- Design the algorithms for Energy Efficient Systems
- Identify the different types of Green Networking schemes in the energy efficient
- computing
- Explore the applications of Energy Aware Computing

References

1. Bob steiger wald ,Chris:Luero, Energy Aware computing, Intel Press,2012
2. Chong -Min Kyung, Sungioo yoo, Energy Aware system design Algorithms and Architecture, Springer, 2011.
3. Ishfaq Ah mad, Sanjay Ranka, Handbook of Energy Aware and Green Computing, CRC Press, 2012

NW18007 ADVANCED INFRASTRUCTURE MANAGEMENT (Common to NW&CFIS)

L	T	P	C
3	0	0	3

Course Objectives:

The students will be able to

- Understand the requirements of Infrastructure management
- Get a firm knowledge on various storage technologies
- Know the need for network and cloud management

Unit I Infrastructure Management Overview **9**

Infrastructure management activities, Preparing for Infrastructure Management Factors to consider in designing IT organizations and IT infrastructure, Determining customer's Requirements, Identifying System Components to manage, Exist Processes, Data, applications, Tools and their integration, Patterns for IT systems management, Introduction to the design process for information systems, Models, Information Technology Infrastructure Library (ITIL).

Unit II Different Storage Technologies and Virtualization **9**

Challenges in Data Storage and Management, Data Storage Infrastructure. Components of a Storage System Environment,Intelligent Storage System (ISS) and its components, Introduction to Networked Storage: Evolution of networked storage, Architecture, Overview of FC-SAN, NAS, and IPSAN. Network-Attached Storage (NAS): Benefits of NAS, Components, Implementations, File Sharing, I/O operations, Content Addressed Storage (CAS): CAS Architecture, Storage and Retrieval, Examples. Storage Virtualization: Forms, Taxonomy, Configuration, Challenges, Types of Storage Virtualizations.

Unit III Network Infrastructure **9**

Implementing, Managing and Maintaining IP Addressing; Configure TCP/IP addressing on a server computer using DHCP; Implementing, Managing and Maintaining Name Resolution using DNS Server; Implementing, Managing and Maintaining Routing and Remote Access; Configure remote access authentication protocols; Implement secure access between private networks; Manage Routing and Remote Access routing interfaces; Maintaining a Network Infrastructure.

Unit IV Cloud Infrastructure **9**

Architectural Design of Compute and Storage Clouds, Layered Cloud Architecture Development, Design Challenges, Inter Cloud Resource Management, Resource Provisioning and Platform Deployment, Global Exchange of Cloud Resources. Administrating the Clouds, Cloud Management Products, Emerging Cloud Management Standards.

Unit V Case Study **9**

Devops Infrastructure Management, Container Infrastructure Management, Engine yard PaaS, Docker Infrastructure Management.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Examine the Infrastructure management activities
- Explore the different storage technologies
- Manage and Maintain Routing and Remote Access
- Develop Layered Cloud Architecture
- Explore Devops, Container and Docker Infrastructure Management

References

1. G. Somasundaram, Alok Shrivastava, EMC Educational Services, Information Storage and Management, Wiley India.
2. Robert Spalding, "Storage Networks: The Complete Reference", Tata McGraw Hill, Osborne, 2003.
3. Marc Farley, "Building Storage Networks", Tata McGraw Hill, Osborne, 2001.
4. Jan Van Bon, "Foundations of IT Service Management: based on ITIL", Van Haren Publishing, 2005.

CF18009 MALWARE ANALYSIS AND REVERSE ENGINEERING

L	T	P	C
3	0	0	3

Course Objectives:

The students will be able to

- Gain in-depth knowledge on fundamentals of malware analysis.
- Use JIT compilers for malware detection in legitimate code.
- Implement DNS filtering and apply reverse engineering.

Unit I Introduction to Malware Analysis **9**

Introduction to key MA tools and techniques, Understanding Malware Threats, Malware indicators, Malware Classification, Introduction to MA Sandboxes Capturing and Analyzing Network Traffic, Internet simulation using INetSim, Using Deep Freeze to Preserve Physical Systems, Using FOG for Cloning and Imaging Disks.

Unit II Reverse Engineering Malware **9**

Behavioural Analysis vs. Code Analysis, Resources for Reverse-Engineering Malware (REM) - Examining Clam AV Signatures, Creating Custom Clam AV Databases, Using YARA to Detect Malware Capabilities.

Unit III Malware Forensics **9**

Using TSK for Network and Host Discoveries, Using Microsoft Offline API to Registry Discoveries , Identifying Packers using PEiD, Registry Forensics with Reg Ripper Plugins:, Bypassing Poison Ivy's Locked Files, Bypassing Conficker's File System ACL Restrictions, Detecting Rogue PKI Certificates.

Unit IV Malware and Kernel Debugging **9**

Opening and Attaching to Processes, Configuration of JIT Debugger for Shellcode Analysis, Controlling Program Execution, Setting and Catching Breakpoints, Debugging with Python Scripts and Py Commands, DLL Export Enumeration, Execution, and Debugging, Debugging a VMware Workstation Guest (on Windows), Debugging a Parallels Guest (on Mac OS X).

Unit V Memory Forensics and Volatility **9**

Memory Dumping with MoonSols Windows Memory Toolkit, Accessing VM Memory Files Overview of Volatility, Investigating Processes in Memory Dumps, Code Injection and Extraction, Detecting and Capturing Suspicious Loaded DLLs, Finding Artifacts in Process Memory, Identifying Injected Code with Malfind and YARA.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Apply the concept of malware and reverse engineering.
- Implement tools and techniques of malware analysis.
- Perform Malware and kernel debugging
- Perform forensics on memory
- Experiment with proactive and defensive measures to deter and repel potential threats

References

1. Michael Sikorski, Andrew Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software publisher William Pollock, 2012.
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, 1st Edition, 2014.

NW18009 DATA ANALYTICS AND BUSINESS INTELLIGENCE

L	T	P	C
3	0	0	3

Course Objectives:

The students will be able to

- Understand linear and logistic regression models
- Understand simulation using regression models
- Understand data collection and model understanding

Unit I Linear Regression **9**

Introduction to data analysis – Statistical processes – statistical models – statistical inference – review of random variables and probability distributions – linear regression – one predictor – multiple predictors – prediction and validation – linear transformations – centering and standardizing – correlation – logarithmic transformations – other transformations – building regression models – fitting a series of regressions.

Unit II Logistic and Generalized Linear Models **9**

Logistic regression – logistic regression coefficients – latent-data formulation – building a logistic regression model – logistic regression with interactions – evaluating, checking, and comparing fitted logistic regressions – identifiability and separation – Poisson regression – logistic-binomial model – Probit regression – multinomial regression – robust regression using t model – building complex generalized linear models – constructive choice models.

Unit III Simulation and Causal Inference **9**

Simulation of probability models – summarizing linear regressions – simulation of non-linear predictions – predictive simulation for generalized linear models – fake-data simulation – simulating and comparing to actual data – predictive simulation to check the fit of a time-series model – causal inference – randomized experiments – observational studies – causal inference using advanced models – matching – instrumental variables.

Unit IV Multilevel Regression **9**

Multilevel structures – clustered data – multilevel linear models – partial pooling – group-level predictors – model building and statistical significance – varying intercepts and slopes – scaled inverse-Wishart distribution – non-nested models – multi-level logistic regression – multi-level generalized linear models.

Unit V Data Collection and Model Understanding **9**

Design of data collection – classical power calculations – multilevel power calculations – power calculation using fake-data simulation – understanding and summarizing fitted models – uncertainty and variability – variances – R2 and explained variance – multiple comparisons and statistical significance – analysis of variance – ANOVA and multilevel linear and general linear models – missing data imputation.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- .Demonstrate logistic and Generalized Linear Models
- .Develop simulation using regression models
- .Perform casual inference from data
- .Build multilevel regression models
- Inspect data collection and variance analysis.

References

1. Andrew Gelman and Jennifer Hill, "Data Analysis using Regression and multilevel/Hierarchical Models", Cambridge University Press, 2006.
2. Philipp K. Janert, "Data Analysis with Open Source Tools", O'Reilley, 2010.
3. Davinderjit Sivia and John Skilling, "Data Analysis: A Bayesian Tutorial, Second Edition, Oxford University Press, 2006.
4. Robert Nisbelt, John Elder, and Gary Miner, "Handbook of statistical analysis and data mining applications", Academic Press, 2009.

CF18010	WIRELESS SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

The students will be able to

- Gain in-depth knowledge on wireless and mobile network security and its relation to the new security based protocols.
- Apply proactive and defensive measures to counter potential threats, attacks and intrusions.
- Design secured wireless and mobile networks that optimise accessibility whilst minimising vulnerability to security risks.

Unit I Introduction **9**

Uniqueness of wireless- Wireless Information Warfare- Taxonomies of Wireless Communication Networks-Information Theory-Decision Theory-A Model for cost effective risk management-Performance measures.

Unit II Security in WLAN **9**

Wireless Transmission Media, WLAN Products and standards- securing WLAN - countermeasures-WAP-WTLS-Bluetooth-VoIP.

Unit III Security in cellular Networks **9**

Threats, Hacking and Viruses in mobile communications- Access control and Authentication in mobile communications.

Unit IV Security in Adhoc Networks **9**

Ad hoc Networking-Major Routing Protocol in Adhoc Networks- Attacks against Ad Hoc Networks, Securing Ad hoc Networks- Authentication in Ad hoc Networks – key Management – Intrusion Detection in Ad hoc Networks

Unit V Security in RFID **9**

Multi tag RFID systems-Attacking RFID systems-RFID Relay attacks-Physical privacy and security in RFID systems- Authentication Protocol in RFID systems-Lightweight Cryptography for Low-Cost RFID tags.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

- Enumerate advanced security and privacy issues in wireless systems, includingcellular and wireless LAN
- Analyze state-of-the-art technologies and protocols of wireless network security
- Identify and investigate in-depth both early and contemporary threats to mobile and wireless networks security
- Analyze the various aspects of security in RFID
- Apply proactive and defensive measures to deter and repel potential threats, attacks and intrusions

References

1. Nichols, Randall K. ; Lekkas, Panos, “Wireless Security : Models, Threats, And Solutions”, McGraw Hill Professional, 2002.
2. Yan Zhang and Paris Kitsos, “Security in RFID and Sensor Networks”, CRC PRESS, 2009.
3. Noureddine Boudriga, ”Security of Mobile Communications”, ISBN 9780849379413, 2010.