NATIONAL ENGINEERING COLLEGE

(An Autonomous Institution – Affiliated to Anna University, Chennai)

K.R.NAGAR, KOVILPATTI – 628 503

www.nec.edu.in

REGULATIONS – 2015

DEPARTMENT OF

INFORMATION TECHNOLOGY

CURRICULUM AND SYLLABI OF
M.Tech. (IT) – INFORMATION AND CYBER WARFARE

SEMESTER – I

S. No.	Course Category	Course Code	Course Title	L	T	P	C	Question pattern$^{\oplus}$
THEORY COURSES								
1.	SFC	15IC11C	Quantization and Number theory	2	2	0	3	B
2.	PCC	15IC12C	Information security and Cryptography	3	0	0	3	B
3	SFC	15IC13C	Vulnerability Assessment	3	0	0	3	B
4.	PCC	15IC14C	Data and Cloud Security	3	2	0	4	B
5.	PCC	15IC15C	Advanced Databases	3	0	0	3	B
6.	PCC	15IC16C	Biometric Security Analysis	3	0	0	3	B
PRACTICAL COURSES								
7.	PCC	15IC17C	Vulnerability Assessment Laboratory	0	0	4	2	
			Total	**17**	**4**	**4**	**21**	

SEMESTER – II

S. No.	Course Category	Course Code	Course Title	L	T	P	C	Question pattern$^{\oplus}$
THEORY COURSES								
1.	PCC	15IC21C	Network and Wireless Security	3	2	0	4	B
2.	PCC	15IC22C	Cyber laws and Security Policies	3	0	0	3	B
3.	PCC	15IC23C	Mobile Application Development	3	0	0	3	B
4.	PCE		Elective-I	3	0	0	3	
5.	PSE		Elective –II	3	0	0	3	
PRACTICAL COURSES								
6.	PCC	15IC24C	Network and Wireless Security Laboratory	0	0	4	2	
7.	PCC	15IC25C	Mobile Application Development Laboratory	0	0	4	2	
8.	PCC	15IC26C	Research Paper and Patent Review – Technical Seminar	0	0	4	2	
			Total	**15**	**2**	**12**	**22**	

SFC – Specific Foundation Course, CFC - Common Foundation Course, PCC – Programme Core Course, PCE – Programme Core Elective Course, PSE – Programme Specific Elective Course, OEC – Open Elective Course

SEMESTER – III

S. No.	Course Category	Course Code	Course Title	L	T	P	C	Question pattern⊕
THEORY COURSES								
1.	PSE		Elective -III	3	0	0	3	
2.	PSE		Elective –IV	3	0	0	3	
3.	PCE		Elective –V	3	0	0	3	
4.	OEC		Elective – VI	3	0	0	3	
PRACTICAL COURSES								
5.	PCC	15IC31C	Project Work Phase-I	0	0	12	6	
			Total	**12**	**0**	**12**	**18**	

SEMESTER – IV

S. No.	Course Category	Course Code	Course Title	L	T	P	C	Question pattern⊕
PRACTICAL COURSES								
1.	PCC	15IC41C	Project Work Phase-II	0	0	24	12	
			TOTAL	**0**	**0**	**24**	**12**	

TOTAL CREDITS TO BE EARNED FOR THE AWARD OF THE DEGREE - 73

SFC – Specific Foundation Course, CFC - Common Foundation Course, PCC – Programme Core Course, PCE – Programme Core Elective Course, PSE – Programme Specific Elective Course, OEC – Open Elective Course

PROGRAMME ELECTIVE COURSES

S. No.	Course Category	Course Code	Course Title	L	T	P	C	Question pattern$^{\oplus}$
PROGRAMME CORE ELECTIVE COURSES								
1.	PCE	15IC01E	Soft Computing	3	0	0	3	B
2.	PCE	15IC02E	Machine Learning	3	0	0	3	B
3.	PCE	15IC03E	Computational Statistics and Data Mining	3	0	0	3	B
4.	PCE	15IC04E	Information Ethics for Computer Professionals	3	0	0	3	B
5.	PCE	15IC05E	Pattern Recognition	3	0	0	3	B
6.	PCE	15IC06E	Digital watermarking and Steganography	3	0	0	3	B
7.	PCE	15IC07E	Social Network Security	3	0	0	3	B
8.	PCE	15IC08E	Big Data Security	3	0	0	3	B
9.	PCE	15IC09E	Intellectual Property Rights	3	0	0	3	B
10.	PCE	15IC10E	Digital Forensics	3	0	0	3	B
PROGRAMME SPECIFIC ELECTIVE COURSES								
11.	PSE	15IC11E	Risk Assessment and Security Audit	3	0	0	3	B
12.	PSE	15IC12E	Forensics and Incident Response	3	0	0	3	B
13.	PSE	15IC13E	Distributed System Security	3	0	0	3	B
14.	PSE	15IC14E	E – Commerce Security	3	0	0	3	B
15.	PSE	15IC15E	Global Cyber Warfare	3	0	0	3	B
16.	PSE	15IC16E	Web Application Security	3	0	0	3	B
17.	PSE	15IC17E	Operating System Security	3	0	0	3	B
18.	PSE	15IC18E	IOT Security	3	0	0	3	B
19.	PSE	15IC19E	Malware Security	3	0	0	3	B
20.	PSE	15IC20E	Enterprise and Perimeter Security	3	0	0	3	B
21.	PSE	15IC21E	Secure Coding Practices	3	0	0	3	B

15IC11C QUANTIZATION AND NUMBER THEORY

L	T	P	C
2	2	0	3

COURSE OUTCOMES

Upon completion of this course, the students will be able to
CO 1: explain the basic concepts of quantization. (K2)
CO 2: grasp the concepts of vector quantization theory. (K2)
CO 3: acquire the basic concepts of Number theory. (K2)
CO 4: analyze the inter relation between varies arithmetical functions. (K2)
CO 5: describe the concept of quadratic residues. (K2)

UNIT I QUANTIZATION 12

Quantization - Max Lloyed Quantizer - Uniform Quantizer - Properties of optimum Mean square quantizers - Non Uniform Quantization.

UNIT II VECTOR QUANTIZATION 12

Vector Quantization - Relationship between transformation stage and quantization stage-Codebook design and k-means algorithm.

UNIT III ARITHMETIC AND CONGRUENCES 12

Introduction – Divisibility- Greatest common divisor - Prime numbers - The fundamental theorem of arithmetic- Definition and basic properties of congruences - Residue classes and complete residue systems - Linear congruences.

UNIT IV ARITHMETICAL FUNCTIONS 12

The Mobius function μ(n)– The Euler totient function φ(n)– A relation connecting φ and μ – A product formula for φ(n) – properties of φ(n) –Multiplicative functions– completely multiplicative function.

UNIT V QUADRATIC RECIPROCITY 12

Quadratic Residues – Legendre’s symbol and its properties – Evaluation of (-1|p) and (2|p) – Gauss’ lemma – The Quadratic Reciprocity law – Applications – The Jacobi symbol.

L: 30 T: 30 TOTAL: 60 PERIODS

REFERENCES

1. Allen Gersho, Robert M.Gray, “Vector Quantization and Signal Compression”, Springer Science + Business Media, LLC, New York, Eighth Printing 2012.
2. Bernard Widrow, Istvain Kollar, “Quantization Noise”, Cambridge University Press, 2008.
3. Tom M.Apostol, “Introduction to Analytic Number Theory”, Springer International Student Edition, Narosa Publishing House, New Delhi, 2013.
4. G.A.Jones & J.M.Jones, “Elementary Number Theory”, Springer publications, 2005.

15IC12C INFORMATION SECURITY AND CRYPTOGRAPHY

L	T	P	C
3	0	0	3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: define key terms and critical concepts of information security. (K1)
CO2: explain risk management and professional issues in Information security (K1)
CO3: describe the various security technologies and security tools. (K2)
CO4: explain the basic principles of cryptography and algorithms. (K2)
CO5: describe technical strategies and models for implementing a project plan. (K2)

UNIT I NEEDS FOR SECURITY 9

Information Security: Introduction- Components of Information System - Approaches to Information Security Implementation - The Security Systems Development Life Cycle-Security professionals and organization –Needs for Security: Threats, Attacks, Secure Software development.

UNIT II PROFESSIONAL ISSUES IN INFORMATION SECURITY & RISK MANAGEMENT 9

Law & Ethics in Information Security - Risk Management: Risk Identification-Risk Assessment-Risk Control Strategies- Planning for security: Information Security planning and Governance-Information Security Policy, Standards, and Practices.

UNIT III SECURITY TECHNOLOGIES 9

Security Technologies: Firewall and VPNs – Intrusion Detection -Prevention systems – Security tools.

UNIT IV CRYPTOGRAPHY 9

Cryptology Terminology - Cipher methods – Cryptographic Algorithms – Cryptographic tools – Protocol for secure communications - Attacks on cryptosystems - Physical Security.

UNIT V IMPLEMENTATION OF INFORMATION SECURITY 9

Implementing Information Security: Information Security Project Management – Technical and Non-Technical Aspects of Implementation - Security Certification and Accreditation - Security and personnel: Credentials of Information Security Professionals – Employment Policy and Practices.

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Michael E. Whitman, Herbert J. Mattord, “Principles of Information Security”, Fourth Edition, Cengage Learning, 2012.
2. William Stallings, “Cryptography and Network Security”, Fourth Edition, Pearson Education, 2011.
3. ForouzanMukhopadhyay, “Cryptography and Network Security”, Fourth Edition, McGraw Hill, 2010
4. C K Shyamala, N Harini, Dr T R Padmanabhan, “Cryptography and Network Security”, First Edition, Wiley, India
5. Bernard Menezes, “Network Security and Cryptography”, First Edition, Cengage Learning, 2010.

15IC13C VULNERABILITY ASSESSMENT

L	T	P	C
3	0	0	3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: explain the features of Vulnerability and security tools.(K1)
CO2: outline the importance of Assessment methodology and risk analysis. (K2)
CO3: gain knowledge on Vulnerability Management Tools and configuration management. (K2)
CO4: discuss various threats, attacks and countermeasure in software elements. (K2)
CO5: explain various risks involved in regulating Assessments and Vulnerability management methodology. (K2)

UNIT I WINDOWS OF VULNERABILITY AND TOOLS 9

Introduction- Vulnerability Assessment- Understanding the Risks Posed by Vulnerabilities-Detecting Vulnerabilities via Security Technologies- Deciphering VA Data- Leveraging Configuration Tools to Assess Vulnerabilities- Features of vulnerability Assessment Tool-Classifying networks- Scanning networks.

UNIT II NETWORK VULNERABILITY ASSESSMENT 9

Project Scoping-Assessing Vulnerability assessment timeline-NVAT-Prioritizing risks and threats-Assessment Methodology-Top down and Bottom Up Examination-Case study with assessment report.

UNIT III VULNERABILITY AND CONFIGURATION MANAGEMENT 9

Vulnerability Management Plan- Six Stages of Vulnerability Management- Vulnerability Management Tools- eEye Digital Security- Symantec (BindView)- Still Secure- Open Source and Free Vulnerability Management Tools- Configuration and Patch Scanning- Patch Management-Patch Distribution and Deployment- Configuration Management.

UNIT IV VULNERABILITY THREATS 9

Threats-attacks-Impersonation-Identification versus authentication-Biometrics countermeasure-Recurring threads and Usability-Flaw in space craft software-Race condition-Time of check and time of use-Countermeasure-secure software elements.

UNIT V REGULATING ASSESSMENTS AND PEN TESTS 9

Introduction- The Payment Card Industry (PCI) Standard- The Health Insurance Portability-Drafting an Information Security Program- The Sarbanes-Oxley Act of 2002 (SOX)– HIPAA-Vulnerability Management Methodology-Categorizing, Baseline scan and penetration testing-Remediate Vulnerabilities and Risk- Vulnerability Assessment Schedule- Monitor for New Risks.

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Steve Manzuik, Andre Gold, Chris Gatford, “Network Security Assessment from Vulnerability to Patch”, Syngress Publishing Incorporation, 2007.
2. Thomas R. Peltier, Justin Peltier ,john A.Blackeley, “Managing A Network Vulnerability Assessment”, Auerbach Publications, CRC Press,2003.
3. Charles P. Pfleeger, Shari Lawrence Pfleeger, “Analyzing Computer Security: A Threat / Vulnerability / Countermeasure Approach”, First Edition, Kindle Edition, 2012.

4. Mary Lynn Garcia, “Vulnerability Assessment of Physical Protection Systems”, Elsevier Butterworth-Heinemann Publisher, 2006.
5. John McDonald, Mark Down, Justin Schuh, “The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities”, Pearson Education, 2007.

15IC14C	**DATA AND CLOUD SECURITY**	**L T P C**
		3 2 0 4

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: describe the fundamentals of cloud computing and its security. (K2)
CO2: analyze risk issues and legal aspects in cloud computing. (K3)
CO3: illustrate various data security methods in cloud computing. (K2)
CO4: explore security controls and monitoring in cloud computing. (K2)
CO5: investigate security and evaluation criteria in internal and external cloud. (K3)

UNIT I INTRODUCTION TO CLOUD COMPUTING ARCHITECTURE AND SECURITY 12

Understanding Cloud Computing –The IT foundation for Cloud – A Brief Primer on Security – Security Architecture – Cloud Reference Architecture - Control over Security in the Cloud Model – Making sense of Cloud Deployment – Real world Cloud Usage Scenarios

UNIT II SECURITY CONCERNS RISK ISSUES AND LEGAL ASPECTS 12

Cloud Computing: Security Concerns - Assessing your risk tolerance in Cloud Computing – Legal and Regulatory issues - Securing the Cloud: Architecture – Security Requirements for the Architecture - Security Patterns and Architectural elements – Cloud Security Architecture - Planning Key Strategies for Secure Operation

UNIT III DATA SECURITY 12

Overview of Data Security in Cloud Computing - Data Encryption: Applications and Limits – Cloud Data Security: Sensitive Data Categorization - Cloud Data Storage

UNIT IV KEY STRATEGIES AND BEST PRACTICES 12

Overall Strategy: Effectively Managing Risk - Overview of Security Controls - Limits of Security Controls - Security Monitoring

UNIT V SECURITY AND EVALUATION CRITERIA 12

Building an Internal Cloud - Private Clouds: Motivation and Overview - Security Criteria for Ensuring a Private Cloud – Selecting an External Cloud Provider - Evaluating Cloud Security: An Information Security Framework –Checklists for Evaluating Cloud Security

L: 45 T: 30 TOTAL: 75 PERIODS

REFERENCES

1. J.R. ("Vic") Winkler, “Securing the Cloud: Cloud Computer Security Techniques and Tactics”, Syngress, 2011.
2. Greg Schulz, “Cloud and Virtual Data Storage Networking”, CRC Press, 2012.
3. Ronald L. Krutz, Russell Dean Vines, “Cloud Security – A Comprehensive Guide to Secure Cloud Computing”, Wiley Publishiing, 2010.
4. Tim Mather, Subra Kumaraswamy, ShahedLatif, “Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance”, O’Reilly Media, First edition, 2009.
5. Lee Newcombe, “Securing Cloud Services”, IT Governance Publishing, 2012.

15IC15C ADVANCED DATABASES

L T P C
3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: Acquire knowledge on parallel and distributed databases and its applications.(k1)
CO2: Explain the usage and applications of Object Oriented databases (k1)
CO3: Describe the principles of intelligent databases (k1)
CO4: Explain the usage of advanced data models (k1)
CO5: Learn emerging databases such as XML, Cloud and Big Data (k1)

UNIT I PARALLEL AND DISTRIBUTED DATABASES 9

Database System Architectures: Centralized and Client-Server Architectures – Server System Architectures – Parallel Systems- Distributed Systems – Parallel Databases: I/O Parallelism – Inter and Intra Query Parallelism – Inter and Intra operation Parallelism – Design of Parallel Systems- Distributed Database Concepts - Distributed Data Storage – Distributed Transactions – Commit Protocols – Concurrency Control – Distributed Query Processing – Case Studies

UNIT II OBJECT AND OBJECT RELATIONAL DATABASES 9

Concepts for Object Databases: Object Identity – Object structure – Type Constructors – Encapsulation of Operations – Methods – Persistence – Type and Class Hierarchies – Inheritance – Complex Objects – Object Database Standards, Languages and Design: ODMG Model – ODL – OQL – Object Relational and Extended – Relational Systems: Object Relational features in SQL/Oracle – Case Studies.

UNIT III INTELLIGENT DATABASES 9

Active Databases: Syntax and Semantics (Starburst, Oracle, DB2)- Taxonomy- Applications- Design Principles for Active Rules- Temporal Databases: Overview of Temporal Databases- TSQL2- Deductive Databases: Logic of Query Languages – Data log- Recursive Rules-Syntax and Semantics of Datalog Languages- Implementation of Rules and Recursion- Recursive Queries in SQL- Spatial Databases- Spatial Data Types- Spatial Relationships- Spatial Data Structures- Spatial Access Methods- Spatial DB Implementation.

UNIT IV MOBILE DATABASES 9

Mobile Databases: Location and Handoff Management - Effect of Mobility on Data Management - Location Dependent Data Distribution - Mobile Transaction Models -Concurrency Control - Transaction Commit Protocols- Multimedia Databases- Information Retrieval.

UNIT V EMERGING TECHNOLOGIES 9

XML Databases: XML-Related Technologies-XML Schema- XML Query Languages- Storing XML in Databases-XML and SQL- Native XML Databases- Web Databases- Geographic Information Systems- Biological Data Management- Cloud Based Databases: Data Storage Systems on the Cloud- Cloud Storage Architectures-Cloud Data Models- Query Languages- Introduction to Big Data-Storage-Analysis.

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Henry F Korth, Abraham Silberschatz, S. Sudharshan, “Database System Concepts”, Sixth Edition, McGraw Hill, 2011.

2. R. Elmasri, S.B. Navathe, “Fundamentals of Database Systems”, Sixth Edition, Pearson Education/Addison Wesley, 2010.
3. Carlo Zaniolo, Stefano Ceri, Christos Faloutsos, Richard T.Snodgrass, V.S.Subrahmanian, Roberto Zicari, “Advanced Database Systems”, Morgan Kaufmann publishers,2006.
4. Vijay Kumar, “Mobile Database Systems”, John Wiley & Sons, 2006.
5. C.J.Date, A.Kannan, S.Swamynathan, “An Introduction to Database Systems”, Eighth Edition, Pearson Education, 2006

15IC16C BIOMETRIC SECURITY ANALYSIS

L	T	P	C
3	0	0	3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO 1: explain the key issues and importance of biometric systems for security concerns. (K2)
CO 2: recognize physical and behavior biometric characteristics. (K2)
CO 3: describe the security and privacy aspects of biometric systems. (K2)
CO 4: identify different authentication services along with biometric verification mechanisms. (K2)
CO 5: explain various biometric template protection schemes. (K2)

UNIT I INTRODUCTION 9

Biometrics- Introduction- benefits of biometrics over traditional authentication systems -benefits of biometrics in identification systems-selecting a biometric for a system –Applications - Key biometric terms and processes - biometric matching methods -Accuracy in biometric systems.

UNIT II BIOMETRIC RECOGNITION 9

Fingerprint quality assessment-segmentation based metrics-Hand vein patterns-optical methods-PCAnet deep learning-Multispectral palm print-ear recognition-ear biometrics-Data analysis-Case study.

UNIT III BIOMETRIC SECURITY 9

Introduction - AES Encryption and Decryption - ECG Identification - Hardware Implementation.

UNIT IV BIO METRIC VERIFICATION 9

Classification: Logistic Regression (LR) - Random Forests - Generalized Linear Models - Evaluation Metrics.

UNIT V BIOMETRIC TEMPLATE PROTECTION 9

Evolution of Biometric Template Protection Schemes - Systematic Literature Review Technique - Classification of Approaches for BTP - Biometric Cryptosystems - Homomorphic Encryption - Research Implications and Future Directions.

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Richard Jiang, Somaya Al-maadeed, Ahmed Bouridane, Danny Crookes, Azeddine Beghdadi Editors, “Biometric Security and Privacy”, Springer International Publishing Switzerland, 2017.
2. Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnapalli, Niranjan Varadarajan, Srinivas Padmanabhuni and Srikanth Sundarrajan, “Distributed Systems Security: Issues, Processes and Solutions”, Wiley publications, 2009.
3. Rachid Guerraoui and Franck Petit, “Stabilization, Safety, and Security of Distributed Systems”, Springer, 2010.

15IC17C	VULNERABILITY ASSESSMENT LABORATORY	L T P C
		0 0 4 2

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: investigate the various forensics in the detection of crime in disk, network and device.(K2)

CO2: identify and analyse the stages an ethical hacker requires to take in order to compromise a target system. (K2)

CO3: critically evaluate security techniques used to protect system and user data in windows and web based forum. (K3)

LIST OF EXPERIMENTS

1. Disk Forensics, Network Forensics, Device Forensics
2. Web Based Email Attacks & Security
3. Windows OS Hacking
4. Malwares Working and Detection
5. Networking Attacks and Security
6. Web Server Attacks and Security
7. VOIP and Mobile hacking
8. Penetration Testing and justification of penetration testing through risk analysis

SUGGESTED SOFTWARE TOOLS/UTILITIES

1. CyberCheck 4.0 - Academic Version
2. CyberCheckSuite
3. MobileCheck
4. Network Session Analyser
5. Win-LiFT
6. TrueImager
7. TrueTraveller
8. PhotoExaminerVer 1.1
9. CDRAnalyzer

P: 60 TOTAL: 60 PERIODS

15IC21C	**NETWORK AND WIRELESS SECURITY**	**L T P C**
		3 2 0 4

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: describe the fundamentals of wireless networks. (K2)
CO2: analyze the security issues in wireless LAN and MAN. (K4)
CO3: explain the security architecture and protocols in Bluetooth and VANET. (K2)
CO4: describe the security vulnerabilities in wireless mesh network. (K3)
CO5: analyze the security architecture and routing protocols for wireless sensor networks. (K4)

UNIT I SECURE WIRELESS NETWORK 12

Overview of security issues in wireless networks - Security architecture of cellular communication networks- Security technique in GSM, 3G, LTE networks - Security issues in femto cell - Mobile devices.

UNIT II SECURITY IN WIRELESS LAN AND WIRELESS MAN 12

Introduction to wireless LAN -current state of WLAN security- communication security- Access point security- other issues- Introduction to wireless man- Wimax- Security goals and solutions - Security vulnerabilities, Threads and counter measures.

UNIT III SECURITY IN BLUERTOOTH AND VANET 12

Bluetooth- Introduction- primer-security solutions-security vulnerabilities, threads and counter measures- VANET- introduction - Security architecture framework- Secure communication protocol-Privacy enhancing and secure positioning.

UNIT IV SECURITY IN WIRELESS MESH N/W AND RFID 12

Wireless mesh networks- characteristics- security vulnerabilities-defense mechanisms-security standards and products- RFID- network primer-security requirements- hardware and protocol based solutions- Advanced protocol based security- Commercial security.

UNIT V SECURITY IN WIRELESS SENSOR NETWORKS 12

Introduction- key management- secure routing protocol- location privacy protection- Secure data aggregation- security architecture- cryptographic approach- Trust management- location privacy.

L: 45 T: 30 TOTAL: 75 PERIODS

REFERENCES

1. Lei Chen"Wireless Network Security-Theories and Applications" Springer, 2013.
2. Andrea Goldsmith, Wireless Communications, Cambridge University Press, 2007.
3. William Stallings, "Wireless Communications and networks" Pearson / Prentice Hall of India, Second Edition, 2007.
4. Simon Haykin & Michael Moher, "Modern Wireless Communications", Pearson Education, 2007.
5. Behrouz A. Fourcuzan ," Cryptography and Network security" Tata McGraw-Hill, 2008

15IC22C	CYBER LAWS AND SECURITY POLICIES	L T P C 3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: explain the basic information on cybercrime. (K1)
CO2: describe cyber laws for various crime activities. (K2)
CO3: identify the security policies for cyber issues. (K2)
CO4: analyze the role of organization for securing cyberspace. (K4)
CO5: explain the need for security in organizations. (K1)

UNIT I INTRODUCTION TO CYBER CRIME 9

Introduction, Forgery, Hacking, Software Piracy, Computer Network intrusion - Category of Cybercrime - Cybercrime Mobile & Wireless devices - Tools and Methods used in Cybercrime - Phishing & Identity Theft.

UNIT II CYBER LAW 9

Power of Arrest without Warrant under the IT act, 2000: A Critique - Cyber Crime and Criminal Justice: Penalties, Adjudication and Appeals – Jurisdiction in the cyber world – Battling Cyber Squatters and Copyright Protection – E-Commerce taxation – Digital signatures, certifying authorities and E-Governance – Indian Evidence Act – Protection of Cyber Consumers in India

UNIT III CYBER AND INFORMATION SECURITY POLICY 9

Cyber governance issues – Cyber user issues – Cyber conflict issues – Cyber management issues – Cyber infrastructures issues - Introduction - Corporate policies - Tier 1, Tier 2 and Tier3 policies - process management - planning and preparation - developing policies - asset classification policy - developing standards.

UNIT IV SECURING CYBERSPACE 9

The private sector role in securing cyberspace - National governments and their role in securing cyberspace - International law's role in securing cyberspace - Privacy, surveillance and the law Cyber War and Strategy - Authentication and Identity - Current legislative and policy initiatives

UNIT V ORGANIZATIONAL AND HUMAN SECURITY 9

Organizational and Human Security: Adoption of Information Security Management Standards, Human Factors in Security - Role of information security profession

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Reich, Pauline C, "Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization", IGI Global, 2012.
2. Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, Marcus H. Sachs, Jeffrey Schmidt, "Cyber Security Policy Guidebook", John Wiley & Sons, 2012.
3. VivekSood, "Cyber Law Simplified", Tata Mcgraw Hill, 2001.
4. Kenneth J. Knapp, "Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions", IGI Global, 2009.
5. Jonathan Rosenoer, "Cyber law: the Law of the Internet", Springer - verlag, 1997.

15IC23C	MOBILE APPLICATION DEVELOPMENT	L T P C
		3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: Explore the differences between mobile based application and conventional application (K1)
CO2: Design UI in the context of mobile application (K2)
CO3: Develop mobile applications for Android (K2)
CO4: Write Android application involving integration of sensors, connectivity to database, etc. (K2)
CO5: Write simple App for IOS, blackberry and Windows phone (K2)

UNIT I INTRODUCTION 8

Brief History of Mobile Software Development - Mobile Web Vs. Mobile App - Hardware and Software for different Mobile frameworks - Difference between Mobile and Desktop applications

UNIT II USER INTERFACE DESIGN 9

Mobile Application users - Basic Design principles - Mobile Information Design - Mobile Platforms: Android, IOS, Blackberry OS, Windows Phone

UNIT III APPLICATION DEVELOPMENT FOR ANDROID-I 10

Android Platform - Different SDKs and their growth - Android Architecture - Android Development Environment Setup - Anatomy of Android Application - Views & Layouts - List View - Adapters - HTTP Connection initiation

UNIT IV APPLICATION DEVELOPMENT FOR ANDROID-II 10

Database Integration - Android Preferences - Broadcast Receivers - Content providers - Usage of different sensors – Services - intent filters

UNIT V OTHER MOBILE FRAMEWORKS 8

IOS - Objective C Basics - a simple App in IOS - Windows Phone basics - Simple Application in Windows Phone - Blackberry basics - Simple Application in Blackberry - Introduction to Cross-platform Mobile Application development.

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Jeff Mc Wherter and Scott Gowell, "Professional Mobile Application Development", Wrox, 2012
2. Joseph Annuzzi, Jr.,LaurenDarcey, Shane Conder “Introduction to Android™ Application Development, Addision-Wesley, Fourth Edition, 2014
3. Charlie Collins, Michael Galpin and Matthias Kappler, “Android in Practice”, Dream Tech, 2012
4. Professional Cross-Platform Mobile Development in C#, By Scott Olson, John Hunter, Ben Horgen, Kenny Goers, wrox, 2012
5. Zigurd Mednieks, Laird Dornin, G, Blake Meike and Masumi Nakamura, “Programming Android”, O‟Reilly, 2011.
6. Reto Meier, Wrox Wiley, “Professional Android 2 Application Development”, 2010.
7. Alasdair Allan, “iPhone Programming”, O’Reilly, 2010
8. Wei-Meng Lee, “Beginning iPhone SDK Programming with Objective-C”, Wrox Wiley, 2010.

15IC24C NETWORK AND WIRELESS SECURITY LABORATORY

L	T	P	C
0	0	4	2

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: design and implementation of a simple client/server model, VPN and running application using sockets and TCP/IP. (K2)

CO2: evaluate application response time in the presence and absence of a firewall. (K4)

CO3: implement the security policies and management. (K2)

CO4: implement the routing protocols like RIP and OSPF. (K2)

LIST OF EXPERIMENTS

1. Eavesdropping Attacks and its prevention using SSH.
2. Isolating WLAN Traffic using Separate Firewall for VPN Connection.
3. Virtual Private Network Over WAN.
4. Managing Security in Small Business Network.
5. Security Group Policies Management.
6. ICMP Ping.
7. Subnetting and OSI Model.
8. Firewalls.
9. Routing Information Protocol (RIP).
10. Open Shortest path first (OSPF).
11. Virtual Private Network (VPN).

P: 60 TOTAL: 60 PERIODS

15IC25C	MOBILE APPLICATION DEVELOPMENT LABORATORY	L	T	P	C
		0	0	4	2

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: Design and develop mobile applications for Android and IOS. (K2)

LIST OF EXPERIMENTS

1. Develop Android Programs using Layout
2. Android Programs using views
3. Develop Android Programs with intent filters, broadcast receivers
4. Develop Android Programs with data integration
5. Develop an Android App for multimedia applications
6. Develop an android App for Email and SMS applications
7. Simple applications in IOS, Windows and cross platforms

P: 60 TOTAL: 60 PERIODS

		L	T	P	C
15IC26C	**RESEARCH PAPER AND PATENT REVIEW – TECHNICAL SEMINAR**	**0**	**0**	**4**	**2**

The student will make at least two technical presentations on current topics related to the specialization. The same will be assessed by a committee appointed by the department. The students are expected to submit a report at the end of semester covering the various aspects of his/her presentation.

P: 60 TOTAL: 60 PERIODS

15IC01E SOFT COMPUTING

L	T	P	C
3	0	0	3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO 1: apply fuzzy logic and reasoning to handle uncertainty and solve engineering problems (K3)
CO 2: implement neural networks to pattern classification and regression problems. (K3)
CO 3: apply genetic algorithms to combinatorial optimization problems.(K4)
CO 4: effectively use of existing software tools to solve real problems using a soft computing approach (K5)

UNIT I FUZZY SYSTEMS 9

Fuzzy Sets – Operations on Fuzzy Sets – Fuzzy Relations – Membership Functions- Fuzzy Rules and Fuzzy Reasoning – Fuzzy Inference Systems –Fuzzy Decision Making - Fuzzy Tool box in Matlab.

UNIT II ARTIFICIAL NEURAL NETWORKS 9

Machine Learning Using Neural Network, Adaptive Networks – Feed forward Networks – Supervised Learning Neural Networks – Radial Basis Function Networks –Unsupervised Learning Neural Networks – NNTool in Matlab.

UNIT III NEURO - FUZZY MODELING 9

Adaptive Neuro-Fuzzy Inference Systems – Coactive Neuro-Fuzzy Modeling – Classification and Regression Trees – Data Clustering Algorithms – Rulebase Structure Identification – ANFIS Applications using Matlab.

UNIT IV GENETIC ALGORITHMS 9

Evolutionary Computation – Genetic Algorithms – Terminologies and Operators of GA –Ant Colony Optimization – Particle Swarm Optimization – GATool using Matlab.

UNIT V APPLICATIONS 9

Fuzzy Classification – Fuzzy Pattern Recognition – Applications of Neural Networks: Bio informatics, Knowledge Extraction, Security Systems, Natural Landmark Recognition Task - Applications of Genetic Algorithm: Machine Learning, Image Processing, Data Mining and Wireless Networks.

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Timothy J.Ross, “Fuzzy Logic with Engineering Applications”, Third Edition, Wiley, 2010.
2. Jyh-Shing Roger Jang, Chuen-Tsai Sun, Eiji Mizutani, “Neuro-Fuzzy and Soft Computing”, First Edition, Prentice-Hall of India, 2003.
3. S.N.Sivanandam, S.N.Deepa, “Introduction to Genetic Algorithms”, First edition, Springer, 2007.
4. S. N. Sivanandam, S. Sumathi and S. N. Deepa, “Introduction to Fuzzy Logic using MATLAB”, First Edition, Springer, 2007.
5. Simon Haykin, “Neural Networks and Learning Machines”, Third Edition, Pearson Education, 2008.

15IC02E	MACHINE LEARNING	L T P C
		3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: explain theory for underlying machine learning (K2)
CO2: construct algorithms to learn linear and non-linear models (K3)
CO3: implement data clustering algorithms (K3)
CO4: construct algorithms to learn tree and rule-based models (K3)
CO5: apply reinforcement learning techniques (K3)

UNITI FOUNDATIONS OF LEARNING 9

Components of learning – learning models – geometric models – probabilistic models – logicmodels – grouping and grading – learning versus design – types of learning – supervised – unsupervised – reinforcement – theory of learning – feasibility of learning – error and noise – training versus testing – theory of generalization – generalization bound – approximationgeneralizationtradeoff – bias and variance – learning curve

UNIT II LINEAR MODELS 9

Linear classification – univariate linear regression – multivariate linear regression – regularized regression – Logistic regression – perceptrons – multilayer neural networks – learning neuralnetworks structures – support vector machines – soft margin SVM – going beyond linearity generalization and overfitting – regularization – validation

UNIT III DISTANCE-BASED MODELS 9

Nearest neighbor models – K-means – clustering around medoids – silhouttes – hierarchicalclustering – k-d trees – locality sensitive hashing – non-parametric regression – ensemble learning– bagging and random forests – boosting – meta learning

UNIT IV TREE AND RULE MODELS 9

Decision trees – learning decision trees – ranking and probability estimation trees – regression trees – clustering trees – learning ordered rule lists – learning unordered rule lists – descriptive rule learning – association rule mining – first-order rule learning

UNIT V REINFORCEMENT LEARNING 9

Passive reinforcement learning – direct utility estimation – adaptive dynamic programming temporal-difference learning – active reinforcement learning – exploration – learning an actionutilityfunction – Generalization in reinforcement learning – policy search – applications in gameplaying – applications in robot control

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Y. S. Abu-Mostafa, M. Magdon-Ismail, and H.-T. Lin, “Learning from Data”, AMLBook Publishers, 2012.
2. P. Flach, “Machine Learning: The art and science of algorithms that make sense of data”, Cambridge University Press, 2012.
3. K. P. Murphy, “Machine Learning: A probabilistic perspective”, MIT Press, 2012.
4. C. M. Bishop, “Pattern Recognition and Machine Learning”, Springer, 2007.

5. D. Barber, “Bayesian Reasoning and Machine Learning”, Cambridge University Press, 2012.
6. M. Mohri, A. Rostamizadeh, and A. Talwalkar, “Foundations of Machine Learning”, MIT Press, 2012.
7. T. M. Mitchell, “Machine Learning”, McGraw Hill, 1997.
8. S. Russel and P. Norvig, “Artificial Intelligence: A Modern Approach”, Third Edition, Prentice Hall, 2009

15IC03E COMPUTATIONAL STATISTICS AND DATA MINING **L T P C**
3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1:explain the fundamental concepts in machine learning (K1)
CO2: analyze the functionalities of various clustering and association approaches. (K4)
CO3: outline the estimation methods for regression and time series in mining.(K2)
CO3: gain knowledge on various computational statistical methods.(K2)
CO4: discuss the evaluation procedure for statistical analysis. (K4)

UNIT I INTRODUCTION TO MACHINE LEARNING 9

Basic concepts in machine learning and data mining. Bayesian and modelling, model selection. Linear regression and regularization.Linear discriminant analysis and logistic regression. Bagging and boosting. Splines, generalized additive models, trees, and random forests. Kernel smoothers and support vector machines.

UNIT II CLUSTERING AND ASSOCIATION ANALYSIS 9

Principles and tools for dividing objects into groups and discovering relationships hidden in large data sets. Partitional methods and hierarchical clustering. Cluster evaluation. Association analysis using item sets and association rules.Evaluation of association patterns.

UNIT III REGRESSION AND TIME SERIES 9

Classical Linear Regression Model-OLS method of estimation; tests of hypotheses- Use of dummy variables in regression-residuals and fitted values-Variable selection- Validation of assumptions using graphical techniques- Logistic regression; odds ratio, concordance-discordance measures.

UNIT IV COMPUTATIONAL STATISTICS 9

Computer arithmetic-Random number generation and simulation techniques-Markov Chain Monte Carlo methods-Numerical linear algebra-Optimization methods in statistics-MCMC methods: Metropolis-Hastings and Gibbs sampling.

UNIT V STATISTICAL EVIDENCE EVALUATION 9

Probabilistic reasoning and likelihood theory- Bayesian hypothesis testing- Bayesian belief networks.Statistical decision theory and influence diagrams- Elements of forensic theory-Sensitivity analysis.

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Jiawei Han &MichelineKamber, “Datamining – Concepts and Techniques”, Morgan Kaufmann Publishers, Elsevier, Third Edition, 2011.
2. James, G., Witten, D. Hastie, T. and Tibshirani, R. “An Introduction to Statistical Learning”, Springer, 2014.
3. C.P. Robert and G. Casella,“Introducing Monte Carlo Statistical Methods with R”, Springer, 2010
4. T. Hastie, R. Tibshirani, J. Friedman,“The Elements of Statistical Learning”, Second Edition, Springer, 2009.

15IC04E INFORMATION ETHICS FOR COMPUTER PROFESSIONALS

L	T	P	C
3	0	0	3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO 1: analyze the asymptotic performance of algorithms. (K3)
CO 2: explain linear data structures for solving computing problems. (K2)
CO 3: choose the concepts and algorithms of tree structure for solving problems.(K2)
CO 4: implement algorithms of various sorting and hashing techniques. (K3)
CO 5: solve computing problems using graph data structures. (K3)

UNIT I OVERVIEW OF COMPUTER ETHICS 9

Reason, Relativity and responsibility in Computer Ethics – Ethical problems in IT – Ethical Decision Making – Informatics and Professional Responsibility

UNIT II ISSUES IN COMPUTER ETHICS 9

Informational Privacy: Concepts Theories and Controversies – Online Anonymity – Ethical Isses in Computer Security: Hacking, Hacktivism and Counterhacking

UNIT III PROFESSIONAL ISSUES 9

Information Ethics in Library profession – Ethical issues in free and Open source software – Internet Research Ethics – Health Information Technology – Ethical Issues of Information and Business

UNIT IV RESPONSIBILITY ISSUES AND RISK ASSESSMENT 9

Responsibilities for information on the Internet – Virtual reality and Computer Simulation – Genetic Information:Epistemological and Ethical Issues – The Ethics of Cyber conflict – Case Study : A practical Mechanism for Ethical Risk Assessment – A SoDIS Inspection

UNIT V REGULATORY ISSUES AND CHALLENGES 9

Regulation and Governance of the Internet – Information Overload – Email Spam – The matter of Plagarism – Intellectual Property: Legal and Moral Challenges of Online File Sharing

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Kenneth E.Himma, Herman T.Tavani, “The Handbook of Information and Computer Ethics”, John Wiley & Sons Inc, 2008.
2. Terrell Ward Bynum, Simon Rogerson, “Computer Ethics and Professional Responsibility”, BlackWell Publishing ltd, 2004.
3. Herman T.Tavani, “Ethics and Technology Controversies, Questions, and Stratergies for Ethical Computing”, Fourth Edition, John Wiley & Sons Inc, 2008.
4. Deborah G. Johnson, “Computer Ethics”, Fourth Edition, John Wiley & Sons Inc, 2008.
5. Robert Plotkin, “Computer Ethics – Computers, Internet and Society”, First Edition, Checkmark Books, 2011.

15IC05E	**PATTERN RECOGNITION**	**L T P C**
		3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO 1: apply the mathematical foundations for recognition of patterns. (K3)

CO 2: identify the pattern Recognition models. (K1,K6)

CO 3: apply the non parametric techniques and clustering techniques in pattern Recognition in real time applications. (K3)

UNIT I INTRODUCTION 8

Introduction: Basics of pattern recognition – Design principles of pattern recognition system – Learning and adaptation – Pattern recognition approaches. Mathematical foundations: Linear algebra – Probability theory – Expectation – Mean and Covariance – Normal distribution – Multivariate normal densities – Chi square test of hypothesis.

UNIT II STATISTICAL PATTERN RECOGNITION 7

Statistical Patten Recognition: Bayesian Decision Theory – Classifiers – Normal density and discriminant functions.

UNIT III MODELS 10

Parameter estimation methods: Maximum-Likelihood estimation – Bayesian Parameter estimation – Dimension reduction methods – Principal Component Analysis (PCA) – Fisher Linear discriminant analysis – Expectation – maximization (EM) – Hidden Markov Models (HMM) – Gaussian mixture models.

UNIT IV NON PARAMETRIC TECHNIQUES 10

Nonparametric Techniques: Density Estimation – Parzen Windows – K-Nearest Neighbor Estimation – Nearest Neighbor Rule – Fuzzy classification.

UNIT V CLUSTERING TECHNIQUES 10

Unsupervised Learning and Clustering: Criterion functions for clustering – Clustering Techniques: Iterative square – Error partitional clustering – K-Means – agglomerative hierarchical clustering – Cluster validation.

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Richard O. Duda, Peter E. Hart and David G. Stork, “Pattern Classification”, Second Edition, John Wiley, 2006.
2. Bishop, Christopher M., “Pattern Recognition and Machine Learning”, First Edition, Springer, 2009.
3. S. Theodoridis, K. Koutroumbas, “Pattern Recognition”, Fourth Edition, Academic Press, 2009.
4. Keinosuke Fukunaga, “Introduction to Statistical Pattern Recognition”, Second Edition, Academic Press, 2003.
5. Sergios Thedoridis, Konstantinos Koutroumbas, “Pattern Recognition”, Fourth Edition, Academic Press, 2009.

15IC06E DIGITAL WATERMARKING AND STEGANOGRAPHY **L T P C**
3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO 1: Describe the basics of watermarking techniques and importance of Steganography.K2)
CO 2: Explain different types of watermarking applications and frameworks. (K2)
CO 3: Analyze the models of watermarking (K3)
CO 4: Discuss the concepts of steganography and steganalysis. (K3)
CO 5: Build self-learning and skills to deal with watermarking and steganography (K4)

UNIT I INTRODUCTION 9

Information Hiding, Steganography, and Watermarking. History of Watermarking. History of Steganography, Importance of Digital Watermarking. Importance of Steganography.

UNIT II APPLICATIONS AND PROPERTIES OF WATERMARKING AND STEGANOGRAPHY 9

Applications of watermarking - Applications of steganography – Properties of Watermarking Systems - Evaluating Watermarking Systems - Properties of Steganographic and Steganalysis Systems - Evaluating and Testing Steganographic Systems.

UNIT III MODELS OF WATERMARKING 9

Notation – Communications – Communication Based Models of Watermarking - Geometric Models of Watermarking - Modeling Watermark Detection by Correlation.

UNIT IV STEGANALYSIS 9

Steganographic Communication - Notation and Terminology - Information-Theoretic Foundations of Steganography - Practical Steganographic Methods - Minimizing the Embedding Impact - Steganalysis Scenarios - Some Significant Steganalysis Algorithms.

UNIT V APPLICATIONS 9

Applications of Watermarking, Broadcast Monitoring, Owner Identification ,Proof of Ownership, Transaction Tracking, Content Authentication, Copy Control, Device Control, Legacy Enhancement.Applications of Steganography, Steganography for Dissidents, Steganography for Criminals

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker, “Digital Watermarking and Steganography”, Morgan Kaufmann Publishers, Second Edition, 2008.
2. Frank Y. Shih., “Digital Watermarking and Steganography: Fundamentals and Techniques”, CRC Press.
3. Stefan Katzenbeisser, Fabien, A.P. Petitcolas., “Information Hiding Techniques for Steganography and Digital Watermarking”, Artech House.
4. Neil F. Johnson; Zoran Duric; Sushil Jajodia, “Information Hiding: Steganography and Watermarking - Attacks and Countermeasures”, Springer.
5. Gregory Kipper, “Investigator’s Guide to Steganography”, Auerbach Publications.

15IC07E SOCIAL NETWORK SECURITY L T P C
3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1:describe the significance of security in online social networks (K1)
CO2: outline the trust management policies in achieving security (K2)
CO3: gain knowledge on information sharing and identity management actions (K2)
CO4: analyze various privacy and terrorism issues on Online Social Networks (K4)

UNIT I ONLINE SOCIAL NETWORKS AND SECURITY ISSUES 9

Introduction- Social Networks: The Meaning of Community –Evolution of Online Social Networks – Trust Management – Controlled Information Sharing – Identity Management

UNIT II TRUST MANAGEMENT IN ONLINE SOCIAL NETWORKS 9

Trust, Policies and Reputation Systems – Trust properties – Trust Components – Social trust and Social Capital – Trust Evaluation Model

UNIT III INFORMATION SHARING IN ONLINE SOCIAL NETWORKS 9

Access control in Data Management System – Access control Models – Relationship – based Access control – Privacy settings in Commercial Online Social Networks – Existing Access control approaches

UNIT IV IDENTITY MANAGEMENT IN ONLINE SOCIAL NETWORKS 9

Digital Identity – Identity Management Models – Self-Presentation – Identity Disclosure – Identity Theft

UNIT V NETWORK ANALYSIS, PRIVACY AND TERRORISM 9

Privacy in Online Social Networks – Privacy Threats and Defenses – Terrorism Threats and Defenses

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Barbara Carminati, Elena Ferrari,MarcoViviani, "Security and Trust in Online Social Networks", Morgan & Claypool, 2013.
2. Richard Chbeir, Bechara Al Bouna, "Security and Privacy Preserving in Social Networks", Springer- VerlagWein, 2013..
3. YanivAltshuler, Yuval Elovici, Armin. B.Cremers, NadavAharony, Alex Pentland, "Security and Privacy in Social Networks", Springer Science Business Media, New York, 2013.

15IC08E	**BIG DATA SECURITY**	**L T P C** **3 0 0 3**

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: describe the significance of privacy and ethics in big data environment (K1)
CO2: analyze the steps to secure big data (K4)
CO3: build security in Hadoop environment and its ecosystem. (K3)
CO4: analyze data security and event logging in hadoop environment (K4)

UNIT I BIG DATA PRIVACY, ETHICS AND SECURITY 9

Privacy – Reidentification of Anonymous People –Big Data Privacy– Ethics – Ownership – Ethical Guidelines – Big Data Security – Organizational Security.

UNIT II SECURITY, COMPLIANCE, AUDITING, AND PROTECTION 9

Steps to secure big data – Classifying Data – Protecting – Big Data Compliance – Intellectual Property Challenge – Research Ques

UNIT III HADOOP SECURITY DESIGN 9

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

UNIT IV HADOOP ECOSYSTEM SECURITY 9

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

UNIT V DATA SECURITY & EVENT LOGGING 9

Integrating Hadoop with Enterprise Security Systems - Securing Sensitive Data in Hadoop – SIEMsystem – Setting up audit logging in hadoop cluster.

L: 45 TOTAL: 45 PERIODS

REFERENCES

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

15IC09E INTELLECTUAL PROPERTY RIGHTS **L T P C**
3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: describe the basic terminologies Intellectual property (K1)
CO2: Explain about trade marks in Intellectual property (K1)
CO3: Describe the Law of copy rights and Law of patents (K1)
CO4: Explain about trade secrets in Intellectual property (K1)
CO5: Describe the new development of intellectual property (K1)

UNIT – I INTRODUCTION 9

Introduction to Intellectual property: Introduction, types of intellectual property, international organizations, agencies and treaties, importance of intellectual property rights.

UNIT – II TRADE MARKS 9

Purpose and function of trademarks, acquisition of trade mark rights, protectable matter, selecting and evaluating trade mark, trade mark registration processes.

UNIT – III LAW OF COPY RIGHTS AND LAW OF PATENTS 9

Fundamental of copy right law, originality of material, rights of reproduction, rights to perform the work publicly, copy right ownership issues, copy right registration, notice of copy right, international copy right law.Foundation of patent law, patent searching process, ownership rights and transfer

UNIT – IV TRADE SECRETS 9

Trade secrete law, determination of trade secrete status, liability for misappropriations of trade secrets, protection for submission, trade screte litigation. Unfair competition: Misappropriation right of publicity, False advertising.

UNIT - V NEW DEVELOPMENT OF INTELLECTUAL PROPERTY 9

New developments in trade mark law; copy right law, patent law, intellectual property audits.
International overview on intellectual property, international - trade mark law, copy right law, international patent law, international development in trade secrets law.

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Siva Vaidhyanathan, Intellectual Property: A Very Short Introduction, Oxford University Press, 2017
2. Deborah, E. Bouchoux, Intellectual Property : The Law of Trademarks, Copyrights, Patents and Trade Secrets, 4 th Edition, Imprint : Delmar, 2013.
3. Intellectual property right - Unleashing the knowledge economy, prabuddha ganguli, Tata Mc Graw Hill Publishing Company Ltd, 2001

15IC10E	**DIGITAL FORENSICS**	**L T P C**
		3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO 1: explain the role of digital forensics in the business and private world (K2)
CO 2: identify potential sources of electronic evidence and explain the importance. (K2)
CO 3: recognize current techniques and tools for forensic investigations. (K2)
CO 4: explain and perform forensic analysis in various fields. (K2)
CO 5: describe the procedures for virtual, network and mobile device forensics. (K2)

UNIT I INTRODUCTION TO DIGITAL FORENSICS 9

Overview of Digital Forensics –Digital Evidence preparation – Private Sector High tech investigation – Data recovery Workstation and software – Conducting an investigation

UNIT II DIGITAL FORENSIC ACQUISITION AND AUTHENTICATION 9

Storage formats for digital evidence – Image acquisition – acquisition tools – authenticating data acquisition – RAID data acquisition – Remote Network acquisition tools

UNIT III CURRENT DIGITAL FORENSICS TOOLS 9

Software Tools: Command-Line – Linux - Other GUI – Hardware Tools: Workstations - Write-Blocker - Validating and Testing Forensics Software

UNIT IV DIGITAL FORENSIC ANALYSIS AND VALIDATION 9

Principles of Digital Forensic Data collection and Analysis - Validating Forensic Data - Addressing Data-Hiding Techniques – Case Studies

UNIT V VIRTUAL, NETWORK AND MOBILE DEVICE FORENSICS 9

Overview of Virtual Machine Forensics - Network Forensics: Securing a Network- Procedures for Network Forensics - Examining the Honeynet Project - Mobile Device Forensics: Understanding Mobile Device Forensics - Acquisition Procedures for Mobile Devices

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Bill Nelson, Amelia Phillips, Christopher Steuart, “Guide to Computer Forensics and Investigations”,Cengage Learning, Fifth Edition, 2016.
2. Eoghan Casey, “Handbook of digital forensics and investigation”, Elsevier Academic Press, First Edition, 2009
3. Eoghan Casey, “Digital Evidence and Computer Crime: Forensics Science, Computers and the Internet”, Elsevier Academic Press, Second Edition, 2004.

15IC11E RISK ASSESSMENT AND SECURITY AUDIT **L T P C**
3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: gain the knowledge about Information Risk. (K2)
CO2: discover knowledge in collecting data about organization. (K3)
CO3: explain various data analysis on Information Risk Assessment. (K1)
CO4: describe about IT audit and its activities. (K1)

UNIT I INTRODUCTION 9

Introduction toRisk –Information Security Risk Assessment Overview- Drivers, Laws and Regulations- Risk Assessment Frame work – Practical Approach.

UNIT II DATA COLLECTION 9

The Sponsors- The Project Team- Data Collection Mechanisms- Executive Interviews- Document Requests- IT Assets Inventories- Profile & Control Survey- Consolidation.

UNIT III DATA ANALYSIS 9

Compiling Observations- Preparation of catalogs- System Risk Computation- Impact Analysis Scheme- Final Risk Score.

UNIT IV RISK ASSESSMENT 9

System Risk Analysis- Risk Prioritization- System Specific Risk Treatment- Issue Registers- Methodology- Result- Risk Registers- Post Mortem.

UNIT V SECURITY AUDIT PROCESS 9

Pre-planning audit- Audit Risk Assessment- Performing Audit- Internal Controls- Audit Evidence- Audit Testing- Audit Finding- Follow-up activities.

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Mark Talabis Jason Martin, “Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis”, Kindle Edition. ISBN: 978-1-59749-735-0, 2012.
2. David L. Cannon, Brian T. O'Hara, Allen Keele, “CISA Certified Information Systems Auditor Study Guide”, Fourth Edition, SYBEX Publication. ISBN: 978-0-470-23152-4, 2016.

15IC12E FORENSICS AND INCIDENT RESPONSE **L T P C**
3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: summarize the activities of initial and incident responses. (K2)
CO2: investigate web server attacks, DNS attacks and router attacks. (K3)
CO3: describe the techniques related to system investigation. (K2)

UNIT I INCIDENT AND INCIDENT RESPONSE 9

Introduction to Incident - Incident Response Methodology – Steps - Activities in Initial Response Phase after detection of an incident

UNIT II INITIAL RESPONSE AND FORENSIC DUPLICATION 9

Initial Response & Volatile Data Collection from Windows system - Initial Response & Volatile Data Collection from Unix system - Forensic Duplication: Forensic duplication: Forensic Duplicates as Admissible Evidence, Forensic Duplication Tool Requirements, Creating a Forensic Duplicate / Qualified Forensic Duplicate of a Hard Drive

UNIT III STORAGE AND EVIDENCE HANDLING 9

File Systems-FAT, NTFS - Forensic Analysis of File Systems - Storage Fundamentals-Storage Layer, Hard Drives Evidence Handling-Types of Evidence, Challenges in evidence handling, Overview of evidence handling procedure

UNIT IV NETWORK FORENSICS 9

Collecting Network Based Evidence - Investigating Routers - Network Protocols - Email Tracing - Internet Fraud.

UNIT V SYSTEMS INVESTIGATION AND ETHICAL ISSUES 9

Data Analysis Techniques - Investigating Live Systems (Windows & UNIX) - Investigating Hacker Tools - Ethical Issues – Cybercrime.

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Kevin Mandia, Chris Prosise, “Incident Response and computer forensics”, Tata McGrawHill, 2006.
2. Peter Stephenson, “Investigating Computer Crime: A Handbook for Corporate Investigations”, Sept 1999.
3. Eoghan Casey, "Handbook Computer Crime Investigation's Forensic Tools and Technology", Academic Press, First Edition, 2001.
4. Skoudis. E., Perlman. R. Counter Hack: “A Step-by-Step Guide to Computer Attacks and Effective Defenses”, .Prentice Hall Professional Technical Reference. 2001.
5. Norbert Zaenglein, “Disk Detective: Secret You Must Know to Recover Information From a Computer”, Paladin Press, 2000.
6. Bill Nelson, Amelia Philips and Christopher Steuart, “Guide to computer forensics and investigations”, course technology, Cengage Learning; Fourth edition, ISBN: 1-435-49883-6, 2009.

15IC13E DISTRIBUTED SYSTEM SECURITY

L	T	P	C
3	0	0	3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: describe the basics of distributed systems security. (K1)

CO2: define the concepts of security engineering. (K1)

CO3: explain the threats, vulnerabilities and its solutions in distributed systems security. (K2)

CO4: apply the distributed systems security concepts with various case studies. (K4)

UNIT I INTRODUCTION 9

Introduction - Distributed Systems - Distributed Systems Security

UNIT II SECURITY ENGINEERING 9

Secure Development Lifecycle Processes Overview - A Typical Security Engineering Process - Important Security Engineering Guidelines and Resources - Common Security Issues and Technologies - Security Issues - Common Security Techniques

UNIT III THREATS AND VULNERABILITIES 9

Host-level threats and vulnerabilities - Infrastructure-level threats and vulnerabilities - Application-level threats and vulnerabilities - Service-level threats and vulnerabilities

UNIT IV SOLUTIONS 9

Host-level solutions - Infrastructure-level solutions - Application-level solutions - Service-level solutions

UNIT V CASE STUDIES 9

SOX Compliance - SOX Security Solutions - Multilevel Policy-Driven Solution Architecture - The Financial Application - Security Requirements Analysis - Final Security Architecture

L: 45 TOTAL: 45 PERIODS

REFERENCE

1. Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnapalli, Niranjan Varadarajan, SrinivasPadmanabhuni, SrikanthSundarrajan, “Distributed Systems Security: Issues, Processes and Solution”, 2009.

15IC14E E – COMMERCE SECURITY L T P C 3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: explain the basic concepts, theories, and business models underlying e- commerce. (K2)

CO2: analyze the importance of security and trust in e-commerce, and be able to realize techniques to foster the process of doing business on the Web. (K4)

CO3: explain the added value, risks and barriers in the adoption of e-Business & e-Commerce (K1)

CO4: comprehend the important issues in design and development, such as website effectiveness, usability, brand strategy, and personalizing the user experience. (K2)

CO5: apply necessary tools and information to design and build systems that take advantage of trusted computing. (K3)

UNIT I INTRODUCTION TO E-COMMERCE 9

Network and E-Commerce – Types of E-Commerce – E-Commerce Business Models: B2C, B2B, C2C, P2P and M-commerce business models – Ecommerce

UNIT II PAYMENT SYSTEMS & SECURITY 9

Types of payment system – Credit card E-Commerce transactions– B2C E-Commerce Digital payment systems – B2B payment system.

E-Commerce Security Environment – Security threats in E-Commerce environment – Policies, Procedures and Laws.

UNIT III INTER-ORGANIZATIONAL TRUST IN E-COMMERCE 9

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 INTRODUCTION TO TRUSTED COMPUTING PLATFORM 9

Overview – Usage Scenarios – Key components of trusted platform – Trust mechanisms in a trusted platform

UNIT V PLATFORMS & MODELS 9

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

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Gary Schneider, “Electronic Commerce”, Course Technologies, Sixth Edition, 2006.
2. Kenneth C. Laudon and Carol Guercio Trave, “E-Commerce Business Technology Society”, Pearson Education, 2005.
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.

15IC15E	GLOBAL CYBER WARFARE	L T P C
		3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: explain the warfare domain and Cyber act (K2)
CO2: gain knowledge on non-state actors in cyber conflicts between nation states (K2)
CO3: describe various modes of attack that have been used in cyber warfare (K2)
CO4: examine the military doctrines for cyber warfare developed by federations (K1)
CO5: explain the warfare framework used by Russia and US. (K2)

UNIT I OPERATIONAL HISTORY OF CYBER WARFARE 9

Cyberspace as a Warfare Domain -Purpose, Plausibility -Limits of Cyberwar - Netcentricity– Operational Cyberwar - A Conceptual Framework - Act of War - Relationship to IO- Cyber Crime - Future Threats - Rise of Nonstate Hacker - Noteworthy Events - Gaza Cyber war

UNIT II RESPONDING TO INTERNATIONAL CYBER ATTACKS 9

Law of War- Nonstate actors and Law of War -Analysing Cyber Attacks - Technological Limitations - Issues -Intelligence Component of Cyber Warfare-Korean DDOS Attacks-One year after RU-GE War -Ingushetia Conflict - Predictive Role of Intelligence - Nonstate Hackers and Social Web - Dark side of Social Networks-TwitterGate - Automating Process- False Identities - Components of Bulletproof Networks - SORM-2 - Kremlin and Russian Internet.

UNIT III WEAPONIZING MALWARE 9

Introduction - New Threat Landscape - StopGeogia.ru Malware Discussions - Twitter as DDoS Command Post against Iran, Social Engineering - Channel Consolidation - Adversary's Look at LinkedIn - BIOS Based Rootkit Attack - Malware for Hire - Targeted Attacks Against Military Brass and Government Executives. Organized Crime in Cyber space - Subtle Threat - Atrivo/Interchange -EST Domains- McColo- Russian Organized Crime and Kremlin

UNIT IV ROLE OF CYBER IN MILITARY DOCTRINE 9

Introduction- Russian Federation- FEP -Information wars- RF Military Policy- Art of Misdirection China Military Doctrine -Anti-access Strategies - 36 Stratagems - US Military Doctrine - Advice for Policymakers -Shoot the Hostage - Use Active Defenses to Defend Critical Information Systems - Scenarios and Options to Responding to Cyber Attacks- Nation Cyber Security.

UNIT V INFORMATION WARFARE FRAMEWORK 9

Russian Government Policy- Laws and Amendments - Government Structures - Russian Military of Defense - Administrative Changes - Electronic Warfare Troops - Military Units - Russian Federation Ministry ofCommunications and Mass Communications - US Department of Defense Cyber Command - Organizational Structure.Active Defense for Cyber - Covert Action - Cyber Active Defense under International Law -Cyber Active Defenses as Cover Action under International Law - Cyber Attacks Under International Law Nonstate Actors

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Jeffrey Carr, “Inside Cyber Warfare: Mapping the Cyber Underworld”, published by O,ReillyMedia,Inc.second edition 2012.
2. Martin C. LibickiJohnVacca , “Cyberdeterrence and Cyberwar”, published by RAND Corporation ,2009

3. Brandon Valeriano, RyanC.Maness “Cyberwar versus Cyber realities: conflict in the internation system”,Oxford University Press, 2015.

15IC16E **WEB APPLICATION SECURITY** **L T P C**
3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: describe the principles and techniques associated with the cyber security Practices (K1)

CO2: evaluate techniques used to break into an insecure web application and identify relevant Counter measures (K4)

CO3: integrate approaches to secure networks, intrusion detection and prevention systems(K3)

CO4: analyze the various security threats in maintaining secure database and counter measures.(K4)

UNIT I WEB APPLICATION INSECURITY AND DEFENCE MECHANISM 9

The Evolution of Web Applications, Web Application Security ,Key Problem Factors , Handling User Access , Handling User Input, Handling Attackers, HTTP Protocol, Web Functionality, Encoding Schemes

UNIT II HACKING AUTHENTICATION & SESSION MANAGEMENT 9

Authentication Technologies, Design Flaws in Authentication, Implementation Flaws in Authentication, Securing Authentication. The Need for State, Weaknesses in Token Generation, Weaknesses in Session Token Handling ,Securing Session Management

UNIT III ATTACKING ACCESS CONTROLS & DATA STORES 9

Common Vulnerabilities ,Attacking Access Controls, Securing Access Controls. Injecting into Interpreted Contexts, Injecting into SQL, Injecting into NoSQL, Injecting into XPath, Injecting into LDAP

UNIT IV ACCESSING BACK-END COMPONENTS 9

Injecting OS Commands, Manipulating File Paths, Injecting into XML Interpreters, Injecting into Back-end HTTP Requests, injecting into Mail Services.

UNIT V ANALYZING APPLICATION LOGIC 9

The Nature of Logic Flaws, Real-World Logic Flaws, Fooling a Password Change Function Breaking the Bank, Cheating on Bulk Discounts, Invalidating Input Validation, Racing Against the Login ,Avoiding Logic Flaws

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Dafydd Stuttard, Marcus Pinto, “The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws”, Second Edition, 2011.
2. Joel Scambray, Vincent Liu and Caleb Sima, “Hacking Exposed Web Applications”, Third Edition, 2010.
3. Ryan C. Barnett and Jeremiah Grossman, “Web Application Defender's Cookbook: Battling Hackers and Protecting Users”, 2012.

15IC17E OPERATING SYSTEM SECURITY

	L	T	P	C
	3	0	0	3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO 1: analyze the access control procedures. (K1)
CO 2: explain security and authorization mechanisms in operating system. (K3)
CO 3: describe the information flow models and transmission channel. (K2)
CO 4: explain various kernel methods involved in virtual machine system. (K3)
CO 5: Illustrate security based real time applications. (K3)

UNIT I INTRODUCTION AND ACCESS CONTROL FUNDAMENTALS 9

Introduction – Secure operating system-Goals-Trust model-Threat model- Protection system-Assessment criteria. Case study: Role based access control (RBAC).

UNIT II SECURITY IN OPERATING SYSTEM 9

Multics system-Unix security – Windows security - Authorization and security analysis-Vulnerabilities. Case Study: Building secure operating system for Linux.

UNIT III INFORMATION FLOW 9

Information flow secrecy models-Information flow integrity models-Covert channel-Security kernel-Secure communication processor- Gemini secure operating system.

UNIT IV SECURE VIRTUAL MACHINE SYSTEM 9

Separation kernels-VAX VMM security kernel-Security in other virtual machine systems- System assurance.

UNIT V SECURITY APPLICATIONS 9

Firewall and border security-Web, remote access and VPN security- E-mail security-Security through disaster recovery.

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Trent Jaeger, “Operating System Security”, Morgan &Claypool publisher, 2008.
2. Michael Palmer, “Guide to Operating Systems Security”, Information security professionals, 2003.

15IC18E IOT SECURITY L T P C
3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO 1: describe the basics of securing Internet of Things. (K2)
CO 2: explain architecture and threats in IoT. (K2)
CO 3: analyze various privacy schemes related to IoT (K3)
CO 4: describe the authentication mechanisms for IoT security and privacy. (K3)
CO 5: explain security issues for various applications using case studies (K4)

UNIT I INTRODUCTION: SECURING THE INTERNET OF THINGS 9

Introduction – Security Requirements in IoT architectures – Security in Enabling Technologies – IoT Security Life Cycle – Cryptographic Fundamentals for IoT Security Engineering - Security Concerns in IoT Applications – Basic Security Practices.

UNIT II SECURITY ARCHITECTURE IN THE INTERNET OF THINGS 9

Introduction – Security Requirements in IoT – Insufficient Authentication/Authorization – Insecure Access Control – Threads to Access Control, Privacy, and Availability – Attacks Specific to IoT – Malware Propagation and Control in Internet of Things.

UNIT III PRIVACY PRESERVATION 9

Privacy Preservation Data Dissemination - Privacy Preservation for IoT used in Smart Building – Exploiting Mobility Social Features for Location Privacy Enhancement in Internet of Vehicles – Lightweight and Robust Schemes for Privacy Protection in Key personal IOT Applications: Mobile WBSN and Participatory Sensing.

UNIT IV TRUST, AUTHENTICATION AND DATA SECURITY 9

Trust and Trust Models for IoT – Emerging Architecture Model for IoT Security and Privacy – preventing Unauthorized Access to Sensor Data – Authentication in IoT – Computational Security for the IoT – Secure Path Generation Scheme for real-Time Green IoT – Security Protocols for IoT Access Networks

UNIT V SOCIAL AWARENESS AND CASE STUDIES 9

User Centric Decentralized Governance Framework for Privacy and Trust in IoT – Policy Based Approach for Informed Consent in IoT - Security and Impact of the IoT on Mobile Networks – Security Concerns in Social IoT – Security for IoT Based Healthcare – Smart cities.

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Shancang Li, Li Da Xu, “Securing the Internet of Things,” Syngress (Elsevier) publication, 2017, ISBN: 978-0-12-804458-2.
2. Fei Hu, “Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations,” CRC Press (Taylor & Francis Group), 2016, ISBN:978-1-4987-23190.
3. Arshdeep Bahga, Vijay Madisetti, “Internet of Things – A Hands-on approach,” VPT Publishers, 2014, ISBN: 978-0996025515.
4. Alasdair Gilchris, “Iot Security Issues,” Walter de Gruyter GmbH & Co, 2017.
5. Sridipta Misra, Muthucumaru Maheswaran, Salman Hashmi, “Security Challenges and Approaches in Internet of Things,” Springer, 2016.
6. Brian Russell, Drew Van Duren, “Practical Internet of Things Security,” Packet Publishing Ltd, 2016.

15IC19E	MALWARE SECURITY	L T P C 3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO 1 Analyze the malware security issues related to software. (K3)
CO 2: Estimate the distributed, Stealthy malware detection and defense mechanism.(K3)
CO 3: Describe the malware preservation techniques (K2)
CO 4: Analyze the different coding techniques for variety of applications. (K3)

UNIT I SOFTWARE ANALYSIS AND ASSURANCE 9

Static disassembly and code analysis - Properties of malicious code: Behavioral- Structural- SQL injection attack- Detection – prevention - Next generation platform for analyzing executable.

UNIT II DISTRIBUTED MALWARE DETECTION AND DEFENSE 9

Very fast containment of scanning worms, revisited- Sting: An End-to-End- Self – Healing - Defending against Internet Worms - An insider looks at botnets - Co operative intrusion detectors-Challenge the base rate fallacy.

UNIT III STEALTHY AND TARGETED MALWARE DETECTION AND DEFENSE 9

Composite hybrid techniques - Defending against targeted attacks - Stealthy malware detection - Verifying code integrity - Enforcing untampered code execution - legacy systems - Secure information flow analysis.

UNIT IV MALWARE PRESERVATION TECHNIQUES 9

Infection mechanism – Targets - Virus propagation mechanism - Defending against virus – Malware – Self preservation techniques- Wrap stars - Trojan Software Distribution Sites - poisoning the source.

UNIT V MALICIOUS CODE 9

Mobile Code- Browser scripts - Active X control - java applets - Mobile code in e- Mail clients - distributed application and mobile code - Additional defense against malicious mobile code - User mode root kits: Windows - Unix.

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Mahai christodorescu, et al, “Malware detection-Advances in information security“,Springer, 2007.
2. Ed skoudis and lenny zeltser, “malware – fighting malicious code” prentice hall international, 2004.
3. Mehadi masud, latifur khan, Bhavani Thuraisingam, “Data mining tool for malware detection”, Taylor and Francis group, CRC press, 2012.

15IC20E ENTERPRISE AND PERIMETER SECURITY

L T P C
3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: explain the Enterprise security architecture and models. (K2)
CO2: describe the usage of firewalls and system integration. (K2)
CO3: outline the importance of encryption and system monitoring in enterprise management. (K2)
CO4: describe the usage of Packet filtering techniques and network proxy security in enterprise (K2)
CO5: explain the VPN network protocols, Intrusion detection and host defense mechanism. (K2)

UNIT I ENTERPRISE SECURITY OVERVIEW 9

The façade of Enterprise security-Pitfalls-Road map to secure Enterprise-Security architectures-third party services-Security architecture models-Trust model-Enterprise trust models-Micro and data centric architectures-Security policy and standards.

UNIT II SECURING THE NETWORK AND SYSTEMS 9

Next generation firewalls-Threat detection and mitigation-Network Segmentation-security architecture in DMZ-System classification-application white listing-host firewall-policy enforcement.

UNIT III SECURING ENTERPRISE DATA AND MONITORING 9

Data classification-Data Loss prevention-Encryption and Hashing-Securing wireless networks and implementation-Monitoring strategies-Privileged user access-system monitoring-Building the incident response team.

UNIT IV THE ESSENTIALS OF NETWORK PERIMETER SECURITY 9

Perimeter security fundamentals-packet filtering-IP Chains-Packet filtering devices-Egress filtering-Problems with filters-Stateful firewalls-application level traffic and state-Statefull filtering and inspection-Proxy firewalls-types of proxies-Tools for proxies.

UNIT V FORTIFYING THE SECURITY PARAMETER 9

Virtual private networks-VPN protocol -Network intrusion detection-sensor placement-host hardening-host defense components-Host based firewalls-Challenges of host based defense.

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Aaron Woody, “Enterprise Security: A Data-Centric Approach to Securing the Enterprise”, Packt Publishing,2013.
2. Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent, Ronald W. Ritchey, “Inside Network Perimeter Security”, Second Edition, Sams Publishing, 2005.
3. Van haren, “Open Enterprise Security Architecture (O-Esa): A Framework And Template For Policy-Driven Security”, The Open Group publishing, 2011.
4. John Sherwood, Andrew Clark, David Lynas,**”**Enterprise Security Architecture: A Business-Driven Approach”, CRC Press, Taylor and Francis group,2005
5. Daniel Minoli, “Enterprise Architecture A to Z: Frameworks, Business Process Modeling, SOA, and Infrastructure Technology”, Auerbach Publications, 2008.
6. Don Murdoch, “Blue Team Handbook: A Condensed Field Guide for the Cyber Security Incident Responder”, GSE Publishers, 2014.
7. Stephen Northcutt ,”Network Intrusion Detection: An Analyst's Handbook”, New Riders Professional Library, 1999.

15IC21E SECURE CODING PRACTICES **L T P C**
3 0 0 3

COURSE OUTCOMES

Upon completion of this course, the students will be able to

CO1: describe the need for secure coding and proactive development process. (K1)
CO2: explain and demonstrate secure coding practices. (K2)
CO3: enumerate input issues related to database and web. (K2)
CO4: explain fundamental principles of software security engineering. (K2)

UNIT I INTRODUCTION 9

Need for secure systems- Proactive security development process - Security principles to live by and threat modeling

UNIT II SECURE CODING IN C 9

Character strings- String manipulation errors – String Vulnerabilities and exploits – Mitigation strategies for strings- Pointers – Mitigation strategies in pointer based vulnerabilities – Buffer Overflow based vulnerabilities

UNIT III SECURE CODING IN C++ AND JAVA 9

Dynamic memory management- Common errors in dynamic memory management- Memory managers- Double –free vulnerabilities –Integer security- Mitigation strategies

UNIT IV DATABASE AND WEB SPECIFIC INPUT ISSUES 9

Quoting the Input – Use of stored procedures- Building SQL statements securely- XSS related attacks and remedies

UNIT V SOFTWARE SECURITY ENGINEERING 9

Requirements engineering for secure software: Misuse and abuse cases- SQUARE process model- Software security practices and knowledge for architecture and design

L: 45 TOTAL: 45 PERIODS

REFERENCES

1. Michael Howard, David LeBlanc, “Writing Secure Code”, Microsoft Press, Second Edition, 2003.
2. Robert C.Seacord, “Secure Coding in C and C++”, Pearson Education, Second Edition, 2013.
3. Julia H. Allen, Sean J. Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, “Software Security Engineering: A guide for Project Managers”, Addison-Wesley Professional, 2008.