Hindi Vidya Prachar Samiti's

Ramniranjan Jhunjhunwala College of Arts, Science & Commerce

(Autonomous College)

Affiliated to

UNIVERSITY OF MUMBAI

Syllabus for Semester III

Program: M.Sc. Information Technology

Program Code: RJSPIT

(CBCS 2018-19)

SEMESTER III

Course Code	Unit	Topics	Credits	L / Week
RJSPIT301	Paper Title: Embedded Systems			
	I	• Introduction • The Typical Embedded System • Characteristics and quality attributes of Embedded System • Embedded product development life cycle	4	4
	II	• Hardware Software Co-design and Program Modeling • Embedded Hardware design and development • Embedded Firmware design and development • Real Time Operating System (RTOS)		4
	III	• Memories and Memory Subsystem		4
	IV	• Programming Concept and Embedded Programming in C/C++ and Java		4
	V	• Trends in the Embedded Industry		4

RJSPIT302	Paper Title: Information Security Management			
	I	• Security Risk Assessment and Management	4	4
	II	• Security Management of IT Systems		4
	III	• Key Management in Organizations		4
	IV	• Auditing and Business continuity Planning		4
	V	• Computer forensics: techniques and tools		4

RJSPIT303a	Paper Title: Virtualization			
	I	• Overview Of Virtualization	4	4
	II	• Server Consolidation		4
	III	• Network Virtualization		4
	IV	• Virtualizing Storage		4
	V	• Blades and Virtualization		4

RJSPIT303b	Paper Title: Artificial Neural Networks			
	I	• Basics of Neuroscience	4	4
	II	• Geometry of Binary Threshold Neurons and Their Networks • Supervised Learning		4
	III	• Neural Networks		4
	IV	• Dynamical Systems Review and Attractor Neural Networks		4
	V	• Fuzzy Systems		4

RJSPIT304a	Paper Title: Digital Image Processing			
	I	• Introduction to Image Processing • Visual Preliminaries	4	4
	II	• Intensity transformations • Spatial filtering		4
	III	• Colour Image Processing • Image compression		4
	IV	• Morphological Image Processing • Segmentation		4
	V	• Representation and Description • Object Recognition		4

RJSPIT304b	Paper Title: Ethical Hacking			
	I	• Introduction to Ethical Hacking • Foot printing and Reconnaissance • Scanning Networks • Enumeration	4	4
	II	• System Hacking		4
	III	• Social Engineering • Session Hijacking		4
	IV	• Hacking web applications • SQL Injections • Hacking Mobile platforms • Hacking wireless network		4
	V	• Evading IDS • Firewalls and Honeypots • Cryptography and penetration testing		4

Course Code	Topic Heading	Credit	L/Week
RJSPITP301	Embedded Systems	2	4
RJSPITP302	Information Security Management	2	4
RJSPITP303a	Virtualization	2	4
RJSPITP303b	Artificial Neural Networks	2	4
RJSPITP304a	Digital Image Processing	2	4
RJSPITP304b	Ethical Hacking	2	4

Theory semester III

Course Code	Title	Credits
RJSPIT301	Embedded Systems	4

Unit	Description
I	**Introduction** What is an Embedded System, Embedded System vs. General Computing System. **The Typical Embedded System** Core of Embedded System, Memory, Sensors and Actuators, Communication Interface, Embedded Firmware. **Characteristics and quality attributes of Embedded System** Characteristics of an Embedded System, Quality Attributes of Embedded System. **Embedded product development life cycle** What is EDLC, Why EDLC? Objectives of EDLC, Different Phases of EDLC.
II	**Hardware Software Co-design and Program Modeling** Fundamental Issues in Hardware Software Co-design, Computational Models in Embedded Design, Introduction to Unifies Modeling Language (UML), Hardware Software Tradeoffs. **Embedded Hardware design and development** Analog Electronic Components, Digital Electronic Components, Electronic Design Automation (EDA) Tools, The PCB Layout design. **Embedded Firmware design and development** Embedded Firmware Design Approaches Embedded Firmware Development Languages. **Real Time Operating System (RTOS)** Operating System Basics, Types of Operating Systems, Device Drivers, How to choose an RTOS.
III	**Memories and Memory Subsystem** Introduction, Classifying Memory, A general Memory Interface, ROM Overview, Static RAM, Overview, Dynamic RAM Overview, Chip Organization, A SRAM Design, A DRAM Design, The DRAM Memory Interface, The Memory Map, Memory Subsystem Architecture, Basic Concepts of Caching, Design a cache system, Dynamic Memory Allocation, Testing Memories.
IV	**Programming Concept and Embedded Programming in C/C++ and Java** Software programming in Assembly Language (ALP) and in High-level Language 'C', C program Elements: Header and Source Files and Pre-processor Directives, Program Elements: Macros and Functions, Program Elements : Types, Data Structures, Modifiers, Statements, Loops and Pointers, Object-Oriented Programming, Embedded Programming in C++, Embedded Programming in Java.
V	**Trends in the Embedded Industry** Processor trends in Embedded System, Embedded OS Trends, Development Language Trends, Introduction of PIC Family of Microcontrollers, Introduction of ARM Family of Microcontrollers, Introduction of AVR Family of Microcontrollers.

M.Sc. IT	Semester III Theory
RJSPIT301 Course I Embedded Systems	Course Outcomes 3.1 : 1. To provide in-depth knowledge about embedded processor, its hardware and software through the use of simulation software, real devices interfaced to a PC and with embedded devices, you will develop competence in microprocessor based digital system design and interfacing. 2. To explain real time operating systems, inter-task communication and an embedded software development tool. Learning outcomes : Students will be able to: ➢ Learn basic embedded system, its characteristics and attributes . ➢ Build firmware with s/w –h/w code design and program modeling. ➢ Learn real time operating systems (RTOS). ➢ Learn classification of memory subsystems and their architecture ➢ Implement programming concepts embedded programming using C, C++ and JAVA.

Course Code	Title	Credits
RJSPIT302	Information Security Management	4

Unit	Description
I	**Security Risk Assessment and Management** Introduction to Security Risk Management. Reactive and proactive approaches to Risk Management. Risk assessment, quantitative and qualitative approaches and asset classification – Security Assurance Approaches: introduction to OCTAVE and COBIT approaches.
II	**Security Management of IT Systems** Network Security Management, IDS, and IPS configuration management. Web and wireless security management. General server configuration guidelines and maintenance. Information Security Management Information classification. Access control models, role-based and lattice models. Mandatory and discretionary access controls. Linux and Windows case studies. Technical controls, for authentication and confidentiality. Password management and key management for users. Case study: Kerberos.
III	**Key Management in Organizations** Public-key Infrastructure. PKI Applications, secure email case study (S/MIME or PGP). Issues in public-key certificate issue and lifecycle management – Management of IT Security Infrastructure; Computer Security log management, malware handling and vulnerability management programs. Specifying and enforcing security policies.
IV	**Auditing and Business continuity Planning** Introduction to Information Security Audit and Principles of Audit. Business continuity planning and disaster recovery. Case study: 9/11 tragedy. Backup and

	recovery techniques for applications and storage.
V	**Computer forensics: techniques and tools** Audit tools: NESSUS and NMAP, Information Security Standards and Compliance: overview of ISO 17799 Standard. Legal and Ethical issues.

M.Sc. IT	Semester III Theory
RJSPIT302 Course II Information Security Management	Course Outcomes 3.2 : 1. The course will provide the student with an understanding of the principles of information security management that are commonly used in business. It will introduce the student to commonly used frameworks and methods and explore critically the suitability and appropriateness of these for addressing today's organizational security needs. Learning outcomes : Student will be able to : ➢ Have an understanding of the key themes and principles of information security management and be able to apply these principles in designing solutions to managing security risks effectively; ➢ Apply the principles of information security management in a variety of contexts; ➢ Have an appreciation of the interrelationship between the various elements of information security management and its role in protecting organizations. ➢ Develop a "security mindset:" learn how to critically analyze situations of computer and network usage from a security perspective, identifying the salient issues, viewpoints, and trade-offs.

Course Code	Title	Credits
RJSPIT303a	Virtualization	4

Unit	Description
I	**Overview Of Virtualization** Basics of Virtualization – Virtualization Types – Desktop Virtualization – Network Virtualization – Server and Machine Virtualization – Storage Virtualization – System –level or Operating Virtualization – Application Virtualization – Virtualization Advantages – Virtual Machine Basics – Taxonomy of Virtual machines – Process Virtual Machines – System Virtual Machines – Hypervisor – Key Concepts.
II	**Server Consolidation** Hardware Virtualization – Virtual Hardware Overview – Server Virtualization – Physical and Logical Partitioning – Types of Server Virtualization – Business

	cases for Server Virtualization – Uses of Virtual server Consolidation – Planning for Development – Selecting server Virtualization Platform.
III	**Network Virtualization** Design of Scalable Enterprise Networks – virtualizing the Campus WAN Design – WAN Architecture – WAN Virtualization – Virtual Enterprise Transport virtualization – VLANs and Scalability – Theory Network Device Virtualization layer 2 – VLANs Layer 3 VRF. INSTANCES Layer2 – VFIs Virtual Firewall Contexts Network Device Virtualization – Data-Path Virtualization Layer 2 :802.1q – Trunking Generic Routing Encapsulation – IpsecL2TPv3 Label Switched Paths – Control-Plane Virtualization – Routing Protocols- VRF – Aware Routing Multi-Topology Routing.
IV	**Virtualizing Storage** SCSI- Speaking SCSI- Using SCSI buses – Fiber Channel – Fiber Channel Cables – Fiber Channel Hardware Devices – iSCSI Architecture – Securing iSCSI – SAN backup and recovery technique – RAID – SNIA Shared Storage Model – Host based Architecture – Storage based architecture – Network based architecture – Fault tolerance to SAN – Performing Backups – Virtual tape libraries.
V	**Blades and Virtualization –** Building Blocks for Next-Generation Data Centers, Evolution of Computing Technology – Setting the Stage , Evolution of Blade and Virtualization Technologies , Blade Architecture , Assessing Needs – Blade System Hardware Considerations.

M.Sc. IT	Semester III Theory
RJSPIT303a Course III Virtualization	Course Outcomes 3.3a : 1. This course will provide the student with a foundation in server and client virtualization. The student will install, configure and manage a server virtual environment. Virtual machines, live motion, monitoring, resource management, virtual networking, data recovery, high availability and fault tolerance are also covered in this course. Learning outcomes : Student will be able to : ➢ Implementing vmwareESXi for server virtualization ➢ Implementation XEN for server virtualization ➢ Implement Hyper-V sever virtualization ➢ Managing vmwareESXi with vCentre server ➢ Managing xen server Xen center ➢ Simulating SAN with navisphere/netapps

Course Code	Title	Credits
RJSPIT303b	Artificial Neural Networks	4

Unit	Description
I	The Brain Metaphor, Basics of Neuroscience, Artificial Neurons, Neural Networks and Architectures.
II	Geometry of Binary Threshold Neurons and Their Networks, Supervised Learning I: Perceptrons and LMS, Supervised Learning II: Back propagation and Beyond
III	Neural Networks: A Statistical Pattern Recognition Perspective, Statistical Learning Theory, Support Vector Machines and Radial Basis Function Networks.
IV	Dynamical Systems Review, Attractor Neural Networks, Adaptive Resonance Theory
V	Towards the Self-organizing Feature Map, Fuzzy Sets and Fuzzy Systems, Evolutionary Algorithms.

M.Sc. IT	Semester III Theory
RJSPIT303b Course III Artificial Neural Networks	Course Outcomes 3.3b : 1. Artificial neural networks use learning algorithms that are inspired by brain learning abilities. Various methods in neural networks have been developed for practical applications such as object recognition, image retrieval, pattern classification, function approximation and control. 2. The course will explain both the classical and the new techniques of neural networks in supervised, unsupervised and reinforcement learning schemes Learning outcomes : Student will be able to : ➢ Demonstrate working knowledge in Lisp in order to write simple Lisp programs and explore more sophisticated Lisp code on their own (a, c, i). ➢ Understand different types of AI agents ➢ Implement various AI search algorithms (uninformed, informed, heuristic, constraint satisfaction, genetic algorithms) ➢ build simple knowledge-based systems ➢ work knowledge of reasoning in the presence of incomplete and/or uncertain information ➢ apply knowledge representation, reasoning, and machine learning techniques to real-world problems ➢ carry out independent (or in a small group) research and communicate it effectively in a seminar setting

Course Code	Title	Credits
RJSPIT304a	Digital Image Processing	4

Unit	Description
I	**Introduction to Image Processing** Example of fields that uses image processing, steps of image processing, components, applications, Image sensors and Image formats. **Visual Preliminaries** Brightness adaptation and contrast, Acuity and contour, Texture and pattern discrimination, shape detection and recognition, perception of color, computational model of perceptual processing, Image sampling and quantization, Basic relationship between pixels.
II	**Intensity transformations** Introduction, Some basic intensity transformation functions, Histogram equalization, local histogram processing, using histogram statistics for image enhancement. **Spatial filtering** Fundamentals of spatial filtering, smoothing and sharpening spatial filters, combining spatial enhancement methods, using fuzzy techniques for intensity transformations and spatial filtering.
III	**Colour Image Processing** Colour fundamentals, colour models, pseudo colour image processing, basic of full-color image processing, colour transformations, smoothing and sharpening, image segmentation bases on colour, noise in colour images, colour image compression. **Image compression** Fundamentals, some basic methods, digital image watermarking, full motion video compression.
IV	**Morphological Image Processing** Introduction, Erosion and Dilation, Opening and closing, The Histor-Miss transformation, some basic morphological algorithms, Gray scale morphology. **Segmentation** Fundamentals, Point, Line and Edge detection, Thresholding, Region based segmentation, Segmentation using morphological watersheds, The use of motion in segmentation – Spatial techniques.
V	**Representation and Description** Representation, Boundary Descriptions, Regional Descriptors, Use of Principal components for Description, Relational Descriptors **Object Recognition** Patterns and patter classes, Recognition based on decision theoretic methods, structural methods

M.Sc. IT	Semester III Theory
RJSPIT304a	Course Outcomes 3.4a : 1. To study the image fundamentals and mathematical transforms

Course III Digital Image Processing	necessary for image processing. 2. To study the image enhancement techniques 3. To study image restoration procedures. To study the image compression procedures Learning outcomes : Student will be able to : ➢ Review the fundamental concepts of a digital image processing system. ➢ Analyze images in the frequency domain using various transforms. ➢ Evaluate the techniques for image enhancement and image restoration. ➢ Categorize various compression techniques. ➢ Interpret Image compression standards. ➢ Interpret image segmentation and representation techniques.

Course Code	Title	Credits
RJSPIT304b	Ethical Hacking	4

Unit	**Description**
I	Introduction to Ethical Hacking, Foot printing and Reconnaissance, Scanning Networks, Enumeration
II	System Hacking, Trojan and Backdoors, Viruses and Worms, Sniffing
III	Social Engineering, Denial of Service, Session Hijacking, Hacking Webservers
IV	Hacking Web Applications, SQL Injection, Hacking Wireless Networks, And Hacking Mobile Platforms.
V	Evading IDS, Firewalls and Honeypots, Buffer Overflows, Cryptography, Penetration Testing.

M.Sc. IT	Semester III Theory
RJSPIT304b Course IV Ethical Hacking	Course Outcomes 3.4b : 1. Introduces the concepts of Ethical Hacking and gives the students the opportunity to learn about different tools and techniques in Ethical hacking and security and practically apply some of the tools. Learning outcomes : Student will be able to : ➢ Use tools for whois, traceroute, email tracking, Google hacking, scanning network, IP fragmentation, war dialing countermeasures and cryptanalysis. ➢ Use NETBIOS Enumeration tool, SNMP Enumeration tool, LINUX/UNIX enumeration tools, NTP enumeration tool, DNS analyzing and enumeration tool. ➢ Use system hacking tools.

	➢ Know backdoors, Trojan, sniffing, denial of service attack, hijacking, webserver attack, SQL injection, security and web server tools. ➢ Know wireless hijacking tool.

Course Code	Practical Title	Credits
RJSPITP301	Embedded Systems	2

1. Study of hardware components
    a. 8051 microcontroller
    b. Resistors (color code, types)
    c. Capacitors
    d. ADC, DAC
    e. Operational Amplifiers
    f. Transistors, Diode, Crystal Oscillator
    g. Types of Relays
    h. Sensors
    i. Actuators
    j. Types of connectors
2. WAP to blink an LED.
3. WAP to serial data interface.
4. WAP for the keypad and LCD interface.
5. WAP to implement ADC0808 with 8051 microcontroller.
6. WAP to simulate elevator functions.
7. WAP to interface stepper motor controller.
8. WAP to simulate traffic signals.
9. WAP to generate waveforms using DAC.
10. WAP to use timer register to display binary counter on LED interface.

M.Sc. IT	Semester III Practical
RJSPITP301 Practical I Embedded Systems	Course Outcome: 1. To get familiar with the typical problems and constraints that arise when designing and developing embedded systems. 2. To find theoretical and practical solutions to these typical problems that the students are expected to master and be able to apply to realistic case studies. Learning outcomes : Student will be able to : ➢ design and implement an embedded systems

	➢ Perform rigorous analysis of a given problem, while taking into account the classical constraints of an embedded system ➢ Implement the designed system, according to the model.

Course Code	Practical Title	Credits
RJSPITP302	Information Security Management	2

1. Working with Sniffers for monitoring network communication (Ethereal).
2. Using open SSL for web server – browser communication.
3. Using GNU PGP.
4. Using IP TABLES on Linux and setting the filter rules.
5. Configuring S/MIME for e-mail communication.
6. Understanding the buffer overflow and format string attacks.
7. Using NMAP for ports monitoring.
8. Implementation of proxy based security protocols in C or C++ with features like confidentiality, integrity and authentication.
9. Socket programming.
10. Exposure to Client Server concept using TCP/IP, blowfish, Pretty Good Privacy

M.Sc. IT	Semester III Practical
RJSPITP302 Practical II Information Security Management	Course Outcome: 1. To learn various tools for providing security to information 2. To use GNUPGP , IP TABLES , ZENMAP tools 3. To use Wireshark software for monitoring network Learning outcomes : Students will be able to: ➢ Learn basic crypto graphics tools ➢ Know how to monitor network traffic and use filter

Course Code	Practical Title	Credits
RJSPITP303a	Virtualization	2

1. Implement vmwareESXi for server virtualization.
2. Implement XEN for server virtualization.
3. Implement Hyper-V server virtualization.
4. Manage vmwareESXi with vCentre server.
5. Manage Xen Server Xen center.
6. Understanding blade server with CISCO UCS/HP eva simulator.
7. Implement VLAN concept with L2/L3 switches/nexus virtual switching.

8. Simulating SAN with navisphere/netapps.

M.Sc. IT	Semester III Practical
RJSPITP303a Practical III Virtualization	Course Outcome: 1. To configure and implement server Virtualization 2. To manage server 3. To implement VLAN Learning outcomes : Students will be able to: ➢ Configure and implement server virtualization , managing server

Course Code	Practical Title	Credits
RJSPITP303b	Artificial Neural Networks	2

1. Show the functioning of Artificial Neural Network. (Implement all the Hidden Layer Functions).
2. Demonstrate that non separable two input perception cannot be classified using P=[-0.8, -0.8, 0.3, 1.0, 0.7; -0.8, 0.8, -0.4, -1.0, -0.7]; and Target T=[1 0 1 0 1]
3. Use perceptron learning rule to find final weights of a neural network using fixed input vectors and a fixed target vector.
4. Prediction using neural network.
5. Implement Radial Basis Function.
6. Implement Least Mean Square algorithm.
7. Implement Support Vector Machine Algorithm.
8. Create and train a feed forward back propagation network with a supplied input P and target T.
9. Design a Hopified network consisting of two neurons with two stable equilibrium points.
10. Perform defuzzication using the following methods
    a. Centroid
    b. Bisector
    c. Middle of maximum
    d. Smallest of maximum
    e. Largest of maximum

M.Sc. IT	Semester III Practical
RJSPITP303b	Course Outcome: 1. To study functioning of Artificial Neural Network

Practical III Artificial Neural Networks	2. Learn neural network 3. Learn implementation of various algorithms and functions Learning outcomes : Students will be able to: ➢ Implement all the Hidden Layer Functions ➢ Perform defuzzication using various methods

Course Code	Practical Title	Credits
RJSPITP304a	Digital Image Processing	2

1. WAP to study the effect of reducing the quantization values and spatial resolution
2. Image enhancement
    a. Thresholding
    b. Contrast adjustment
    c. Brightness adjustment
    d. Gray level slicing
3. Basic transformations
    a. Log transformations
    b. Power law transformations
    c. Negation
4. Different filters (LPF, HPF, Lapalcian, LOG etc).To generate mask for LOG use the following formula.

$$h_g(n_1, n_2) = e^{-(n_1^2 + n_2^2)/(2\sigma^2)}$$

$$h(n_1, n_2) = \frac{(n_1{}^2 + n_2{}^2 - 2\sigma^2) h_g(n_1, n_2)}{2\pi\sigma^6 \sum_{n_1} \sum_{n_2} h_g}$$

5.
    a. Write a program to apply a mask on the image.
6. Accept the size of mask from the user.
7. Check whether the mask is of odd size.
8. The program should work for any high pass and low pass mask.
9. Check the sum of all the elements of the mask. For low pass filter the sum should be one and zero for high pass filter.
10. Compare the output for different size of masks.
11.
    a. Write a program to plot a Histogram.
    b. Write a program to apply Histogram equalization.
12. Write a program to apply Gaussian filter on an image.
    a. Write a code to generate a Gaussian mask and then apply the mask on the image.
    b. Accept the size of mask and the sigma value from the user to generate a mask.
    c. Use the formula to generate Gaussian mask.

$$h_g(n_1, n_2) = e^{-(n_1^2 + n_2^2)/(2\sigma^2)}$$

$$h(n_1, n_2) = \frac{h_g(n_1, n_2)}{\sum_{n_1}\sum_{n_2} h_g}$$

13.
   a. Apply following morphological operations on the image:
      i. Opening
      ii. Closing
      iii. Morphological gradient
      iv. Top-hat transformation
   b. Write a program for boundary detection.
14.
   a. WAP to show RGB planes
   b. WAP to convert
      i. RGB to NTSC
      ii. RGB to YCbCr
      iii. RGB to CMY
      iv. RGB to HIS
15. WAP to achieve Pseudo coloring

M.Sc. IT	Semester III Practical
RJSPITP304a Practical IV Digital Image Processing	Course Outcome: 1. Introduce fundamental technologies for digital image, compression, analysis, and processing. Learning outcomes : Students will be able to: ➢ Gain understanding of algorithm, analytical tools, and practical implementations of various digital image applications ➢ Learn practical skills and analytical background for building digital image and its application

Course Code	Practical Title	Credits
RJSPITP304b	Ethical Hacking	2

1. Using the tools for who is, traceroute, email tracking, google hacking.
2. Using the tools for scanning network, IP fragmentation, war dialing countermeasures, SSL Proxy, Censorship circumvention.
3. Using NETBIOS Enumeration tool, SNMP enumeration tool, LINUX/UNIX.enumeration tools, NTP Enumeration tool, DNS analyzing and enumeration tool.

4. Using system hacking tools.
5. Study of backdoors and Trojan tools.
6. Study of sniffing tools.
7. Study of Denial of Service attack tools.
8. Study of Hijacking tools.
9. Study of webserver attack tools.
10. Study of SQL injection and web server tools.
11. Study of wireless hacking tools.
12. Using cryptanalysis tools.
13. Study of different security tools.

M.Sc. IT	Semester III Practical
RJSPITP304b Practical IV Ethical Hacking	Course Outcome: 1. Make technical foundation of ethical hacking 2. Know aspects of security, importance of data gathering, foot printing and system hacking 3. evaluate computer security 4. re-enforce and apply theory to encourage an analytical and problem based approach to ethical hacking Learning outcomes : Students will be able to: ➢ Identify and analyse the stages an ethical hacker requires to take in order to compromise a target system. ➢ Identify tools and techniques to carry out a penetration testing. ➢ Critically evaluate security techniques used to protect system and user data. ➢ Demonstrate systematic understanding of the concepts of security at the level of policy and strategy in a computer system.

References

1. Introduction to Embedded Systems, Shibu K.V. 2nd Edition, Tata McGraw Hill.
2. Embedded System Architecture, Programming and Design, , Raj Kamal, 2nd Edition, Tata McGraw Hill.
3. Embedded Systems: A Contemporary Design Tool, James .k. Peckol, 1st Edition, Wiley edition.
4. IT Security and Risk Management (Main reference), Slay,J and Koronios, A , 2006 Edition. Wiley .

5. Incident Response and Computer Forensics, Chris Prosise and Kevin Mandia, 2003 Edition. McGraw-Hill
6. Information Systems Security- Security Management, Metrics, Frameworks and Best Practices. , Nina Godbole , Wiley ,2009
7. Information Security Policies, Procedures and Standards: Guidelines for Effective Information Security Management (Paperback), 1st Edition, Auerbach,2001
8. Mastering _VMware_vSphere_5.5, Sybex Publication.
9. Configuring Windows Server Virtualization , Microsoft Press.
10. Citrix.XenServer.6.0.Administration.Essential.Guide, Feb.2007, Packtpub
11. Blade Server and Virtualization, Wiley.
12. Virtualization : A Beginner's Guide .
13. Professional Xen Virtualization , William von Hagen, January 2008, Wrox Publications.
14. Virtualization: From the Desktop to the Enterprise , Chris Wolf, Erick M. Halter, 2005, A Press.
15. VMware and Microsoft Platform in the Virtual Data Center, 2006, Auerbach.
16. Network Virtualization, Kumar Reddy, Victor Moreno, July2006, Cisco Press. Publications
17. Neural Networks, A Classroom Approach, Satish Kumar, 2nd Edition, McGraw Hill
18. Artificial Neural Networks , Robert Schalkoff, McGraw Hill.
19. Introduction to Neural Networks using MATLAB, Sivanandam, S Sumathi, McGraw Hill.
20. Digital Image Processing , Gonzalez and Woods, 3rd Edition, Pearson Education
21. Digital Image Processing and Analysis, Bhabatosh Chanda, Dwijesh Dutta Majumder, 2nd Edition, PHI.
22. Fundamentals of Digital Image Processing, Anil K Jain, 1st Edition, PHI.
23. Ethical Hacking Review Guide, Kimberly Graves, Wiley Publishing.
24. Ethical Hacking, Ankit Fadia, 2nd Edition, Macmillan India Ltd., 2006.
25. Insider Computer Fraud, Kenneth C, Brancik, 2008, Auerbach Publications.