Indira Gandhi Delhi Technical University for Women

(Established by Govt. of Delhi vide Act 09 of 2012)

Kashmere Gate, Delhi - 110006

Scheme of Examination
&
Detailed Syllabus
(w.e.f. Academic Year 2013-2014 onwards)

For

Masters of Technology
(Information Technology – Information Security Management)

Department of Information Technology

PROGRAMME OUTCOMES

PO1. An understanding of the theoretical foundations and the limits of secure computing.

PO2. An ability to design, develop and evaluate new computer based systems for novel cyber security applications which meet the desired needs of industry and society.

PO3. Understanding and ability to use advanced cyber security techniques and tools.

PO4. An ability to undertake original research at the cutting edge of cyber security& its related areas.

PO5.To prepare graduates who will perform both as an individual and in a team through good analytical, design and implementation skills.

PO6. To prepare graduates who will be lifelong learners through continuous professional development.

PROGRAMME SPECIFIC OUTCOMES

PSO1.To develop students into an ethical Cyber Security Professional.

PSO2.To impart interdisciplinary technical knowledge & skills needed to protect computer systems from vulnerabilities, detect & respond to security breaches and cyber threats of all kinds

PSO3.To produce post graduates who can perform cyber security risk assessment, troubleshoot performance issues, offer information assurance which can be applied immediately in their workplace or research areas viz.

FIRST SEMESTER

Paper Code	Paper Title	L	P	Credit
THEORY				
MIS -501	Secure Coding and Security Engineering	4	-	4
MIS -503	Advanced Data Structure	4	-	4
MIS -505	Cyber Security and Forensics	4	-	4
MMC -507	Advanced Network Technologies	4	-	4
MIS -509	Network Security and Management	4	-	4
PRACTICALS				
MIS -511	Secure Coding and Security Engineering Lab	-	2	1
MIS -513	Advanced Data Structure Lab	-	2	1
MIS -515	Cyber forensics and Incident Handling Management Lab	-	2	1
MIS-517	Technical Report Writing*	-	2	2
	TOTAL	**20**	**8**	**25**

SECOND SEMESTER

Code	Course Title	L	P	Credit
THEORY				
MIS -502	Cryptographic Protocols and Algorithms	4	-	4
MIS-504	OS Hardening	4	-	4
MIS-506	Cloud Computing Architecture	4	-	4
ELECTIVES (Choose any two) **				
MIS -508	Secure Wireless Networks	4	-	4
MIS -510	Web Application and its security management	4	-	4
MIS -512	Security Testing and Risk Management	4	-	4
MIS-514	Big Data and Business Analytics	4	-	4
MIS -516	Distributed Systems	4	-	4
MIS -518	IT Act 2000 and Cyber Laws	4	-	4
MIS -520	Digital Image Processing and Steganography	4	-	4
MIS-522	Intellectual Property Rights	4	-	4
MIS-524	Open Ended Research Topic	4	-	4
PRACTICALS				
MIS -526	Cryptographic Protocols and Algorithms Lab	-	2	1
MIS -528	OS Hardening Lab	-	2	1
MIS-530	Lab based on elective(s)	-	2	1
MIS-532	Term Paper*	-	2	2
	TOTAL	**20**	**8**	**25**

*NUES (Non University Examination System)

** Any of these subjects may be chosen in distance learning mode such as Massive Open Online Courses (MOOC's) and supervised by internal faculty-in –charge.

THIRD SEMESTER

Code	Course Title	L	P	Credit
THEORY				
MIS-601	Information Security Audit and Security Management	4	-	4
MIS-603	Advanced Database Management and information retrieval	4		4
ELECTIVES(Choose any one) **				
MIS-605	Security Architecture for Computational Grids	4	-	4
MIS -607	Ethical Hacking	4	-	4
MIS-609	Biometric Systems	4	-	4
MIS-611	Enterprise Information Security Management	4	-	4
MIS -613	E-Commerce and M-Commerce	4	-	4
PRACTICALS				
MIS-615	Information Security Audit and Security Management Lab	-	2	1
MIS -617	Advance Database Management and information retrieval Lab	-	2	1
MIS -619	Minor Project	-	8	12
	TOTAL	**12**	**12**	**26**

FOURTH SEMESTER

Code	Paper	L	P	Credit
MIS -602	Dissertation	-	30	24
MIS -604	Seminar and Progress Report*	-	04	04
	TOTAL		**34**	**28**

***NUES (Non University Examination System)**

** Any of these subjects may be chosen in distance learning mode such as Massive Open Online Courses (MOOC's) and supervised by internal faculty-in –charge.

1. The total number of credits of the Programme M. Tech. = 104.
2. Each student shall be required to appear for examination in all courses. However, for the award of the degree a student shall be required to earn the minimum of 100.

Paper Code: MIS-501	L	P	C
Paper Title: Secure Coding and Security Engineering	4	0	4

Introduction: Security breaches in software are costing companies large fines and regulatory burdens. Developing software, that is reliable in its functionality, resilient against attackers, and recoverable when the expected business operations are disrupted, is a must have. The assurance of confidentiality, integrity and availability is becoming an integral part of software development. This course is being introduced to integrate security principles and secure programming with Software development to reduce effort in removing basic vulnerabilities and risk thereby. The course is effective in enabling students to learn and develop software that is reliable and resilient to software attacks.

Course Objectives:

- To learn Secure Software Development Guidelines and Best Practices.
- To learn secure programming practices so as to build secure software resilient to cyber attacks.
- To learn secure configuration of various tiers and layers involved in Software Development.

Prerequisite: Basic Knowledge of Programming Language (s), Database Management, Network, Server

Course Outcomes: Upon successful completion of this course, students will be able to:

CO1: Acquire security requirements with respect to software development.

CO2: Design and implement software development with minimum software vulnerabilities.

CO3: Write and test software code with respect to security testing and remove security flaws.

Pedagogy: Lectures will be imparted along with hands on lab sessions and latest real world case studies about software vulnerabilities reported, prevention and patching techniques.

UNIT 1

Buffer Overrun, Format String Problems, Integer Overflow, and Software Security Fundamentals, SQL Injection, Command Injection, Failure to Handle Errors, and Security Touchpoints, Cross Site Scripting, Magic URLs, Weak Passwords, Failing to Protect Data, Weak random numbers, improper use of cryptography.

(10 Hrs)

UNIT 2

Information Leakage, Race Conditions, Poor Usability, Not Updating Easily, Executing with too much privilege, Failing to protect network traffic, improper use of PKI, trusting network name resolution, Failing to protect network traffic, improper use of PKI, trusting network name resolution, bonus topics, final project time.

(10 Hrs)

UNIT 3

Technical engineering basics — cryptography, protocols, access controls, cryptography hardware and software implementations. Types of attack — web exploits, card fraud, hardware hacks, electronic warfare , tampering, side-channels, malicious hardware. Specialized protection mechanisms- biometrics, seals, smartcards, RFID, alarms, and DRM, and how they fail. Security economics- why companies build insecure systems, why it's tough to manage security projects, and how to cope.

(10 Hrs)

UNIT IV

Security psychology — the privacy dilemma, what makes security too hard to use, and why deception will keep increasing. Ethics — vulnerability disclosure. Policy — why governments waste money on security, why societies are vulnerable to terrorism, and what to do about it. How to explore, read, critique, present and extend a wide variety of research literature in security engineering and related fields. How to plan, execute and report aresearch project Projects will probably involve one of the following: 1) simulation, 2) implementation, 3) comparison, 4) vulnerability analysis. Projects should also consider at least one multi-disciplinary aspects such as Psychology, Economics, Policy, Ethics, etc.

(10 Hrs)

References:

1. Howard, LeBlanc, and Viega, "24 Deadly Sins of Software Security", 1st edition,2005, The McGraw-Hill
2. Ross Anderson, "Security Engineering - A Guide to Building Dependable DistributedSystems", 2nd edition, 2008, Wiley Interscience.
3. Robert C. Seacord, "Secure Coding in C and C++", 2nd edition, 2013, SEI Series inSoftware Engineering .
4. Michael Howard and David LeBlanc, "Writing Secure Code", 2nd edition, 2003,Microsoft Press

	L	P	C
Paper Code: MIS-503			
Paper Title: Advanced Data Structure	4	0	4

Introduction: This course is about teaching of various data structure designs & its implementations, analyzing the various algorithm strategies and designing of new algorithms for various classes of problems. It is intended to be a gentle introduction to how we specify data structure, algorithms, some of the design strategies, and many of the fundamental ideas used in algorithm analysis throughout the syllabus.

Course Objective:

- To build an understanding on the basics of core and advance data structure.
- To impart a thorough understanding of linear data structures such as stacks, queues and their applications.
- To teach the selection of data structure for a particular problem
- To impart familiarity with various sorting, searching and hashing techniques and their performance comparison
- To teach students, how to write complex program using dynamic data structures.

Pre-requisite: Students should have some programming experience. In particular, they should understand recursive procedures and simple data structures such as arrays and linked lists.Students should have some facility with proofs by mathematical induction.

Course Outcome: After studying this course, students will be able to:

CO1: Compare different programming methodologies and define asymptotic notations to analyze performance of algorithms. Use appropriate data structures like arrays, linked list, stacks and queues to solve real world problems efficiently

CO2:. Represent and manipulate data using nonlinear data structures like trees and graphs to design algorithms for various applications.

CO3: Illustrate and compare various techniques for searching and sorting.

CO4: Compare Greedy and Dynamic Programming approaches and will be able to choose data structures for various complex problems

Pedagogy: The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Students would be encouraged to develop an understanding of the subject. Use of ICT and web based sources will be adopted.

UNIT I

Review of Elementary data structures: Arrays, Linked list, Stacks, Queues, Binary Trees, Hashing, Sorting and Searching techniques, Sparse matrices: Properties of sparse matrices, linked list representation of sparse matrices, Analyzing algorithms.

(10 Hrs)

UNIT 2

Definition Operations on B Trees, B+ trees, B* trees, Weight Balanced Trees (HuffmanTrees), 2-3 Trees and Red-Black Trees. Augmenting Red-Black Trees to Dynamic Order Statics and Interval Tree Applications. Operations on Disjoint sets and its union find problem Implementing Sets. Dictionaries, Priority Queues and Concatenable Queues using 2-3 Trees.

(10 Hrs)

UNIT 3

Binomial heaps, Fibonacci heaps, Union Find Data Structures, Amortization, Self-adjusting and persistent data structures. Definitions for Graphs, Algorithms for Connectedness, Findingall Spanning Trees in a Weighted Graph and Planarity Testing Breadth First and Depth First Search, Topological Sort, Strongly Connected Components and Articulation Point. Single source shortest path and all pair shortest path algorithms.

(10 Hrs)

UNIT 4

Greedy Method: General Method, Knapsack problem, Single source shortest path. Dynamic Programming: General method, 0/1 Knapsack problem, All pair shortest path. Backtracking: Sum of subsets, 8-queens problem, and Hamiltonian cycles.

(10 Hrs)

References:

1. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, "Introduction toAlgorithms", 1st edition, 2005, MIT Press.
2. Ellis Horowitz, Sartaj Sahni Sanguthevar Rajasekaran, "The Design and Analysis ofComputer Algorithms", 2nd edition, 2007, Galgotia
3. Aho, Hopcraft & Ulman, The Design and Analysis of Computer algorithms", 1stedition, 1974, Addison Wesley.
4. Tannenbaum, "Data Structures", 2nd edition, 2007, PHI
5. R.E. Tarjan, "Data Structures and Network algorithms", 1st edition, 2005, SIAMRegional Conference series in applied mathemetics..
6. Rajeev Motwani and Prabhakar Raghavan, "Randomized Algorithms", 1st edition, 1995, Cambridge University Press.
7. Dexter C. Kozan, "The Design & Analysis of Algorithms", 1st edition, 1991,Springer-Verlag.

Paper Code: MIS-505	L	P	C
Paper Title: Cyber Security and Forensics	4	0	4

Introduction: Cyber Security and Forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. This course provides for a broad introduction of cyber security and forensics concepts, industry best practices for information security and key security concepts that will protect an organization against fraud, data breaches and other vulnerabilities. It enables the students to gain in-depth knowledge in the field of Computer forensics & Cyber Crime.

Course Objective:

- To maintain an appropriate level of awareness, knowledge and skill to allow students to minimize the occurrence and severity of information security incidents.
- To learn techniques used to detect, respond and prevent network intrusions.
- To identify and apply appropriate forensics tools to acquire, preserve and analyze system image.
- To protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability.
- Identify sources of evidentiary value in various evidence sources including network logs, network traffic, volatile data.

Prerequisite: Knowledge of Computer Networking, Linux, UNIX, Understanding of Web Application Architecture and HTTP/HTTPS communication.

Course Outcomes: After completion of the course the students will be able to:

CO1: Understand the fundamentals of Cyber Security and comprehend the incident response process

CO2: Demonstrate the difference between data acquisition techniques

CO3: Apply forensic analysis tools to recover important evidence for identifying cyber-crime.

CO4: Apply investigation tools and techniques for analysis of data to identify evidence related to cyber-crime and use available digital forensics tools.

Pedagogy: The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Students would be encouraged to develop an understanding of the existing real life cyber security issues and how they are solved. Course will have a blend of theory and practice for the benefit of students. Use of ICT, web based sources as well as blackboard teaching will be adopted.

UNIT 1

Introduction to Incident Response Process Computer Security Incident, Goals of Incident response, Who is involved in Incident response, Incidence Response Methodology, Pre- incident preparation, Detection of Incidents,, Initial response, Formulate a response strategy, Investigate the incident, Reporting and Resolution.

(10 Hrs)

UNIT 2

Preparing for Incidence Response : preparing Individual Hosts, Recording of Cryptographic Checksum of critical files, enabling secure Audit Logging, Building Up your Hosts Defense, Preparing a Network : Installing Firewalls and IDS, User access control Lists, Establishing Appropriate Policies and procedures, creating a response tool Kit, Establishing an Incident Response Team, Incident handling After Detection of an Incident.

(10 Hrs)

UNIT 3

Fundamentals of Computer Forensics, Computer Forensics Technology, Live data collection from Windows systems, Live data Collection from Unix systems, Data Acquisition of digital evidence from electronic media, Evidence collection and preservation, Network Forensics, Email Investigations, Mobile device forensics, Computer Forensics Analysis and Validation, Macro Threats, Information Warfare.

(10 Hrs)

UNIT 4

Data analysis Techniques : Preparation for Forensic Analysis, Restoring a forensics Duplicate, Recovering deleted files on Windows systems, recovering Unallocated Space, Free Space and Slack space, Writing forensic Reports, Report Writing Guidelines.

(10 Hrs)

References:

1. K Mandla, C. Prosise , Matt Pepe, " Incident Response and Computer Forensics", 2nd Edition, 2003, TMH
2. John R. Vacca, "Computer Forensics", 2nd Edition, 2004, Firewall Media,.
3. Majid Yar, "Cybercrime and Society", 1st Edition, 2006, Sage Publications,.
4. Chad Steel, "Windows Forensics", 1st Edition, 2006, Wiley India,
5. R M Slade, " Software Forensics", 1st Edition, 2004, TMH

Paper Code: MMC-507	L	P	C
Paper Title: Advanced Network Technologies	4	0	4

Introduction: This advanced course develops knowledge about networks to understand their complexity and inform their future design. It seeks to discover and understand common principles and fundamental structures underlying networks and their behaviours. It makes students familiar with the foundations of computer networking, network protocol design and performance evaluation/analysis, and recent advances in network architecture and technology.

Course Objectives:

- To give the students an understanding of the principles behind the latest advances in computer network technology, from IPv6 extending to pervasive and ubiquitous computing
- To develop familiarity with current research problems and research methods in advance computer networks

Prerequisite: Computer Networks

Course Outcomes: On successful completion of this course, the students should be able to:

CO1: Illustrate reference models with layers, protocols and interfaces. Summarize functionalities of different Layers and High Speed Networks

CO2: Describe various Multi-access communication and delay models in Data networks, and how they are used to assist in network design.

CO3: Describe and Illustrate Congestion control and Traffic management techniques.

CO4: Differentiate between the various Internet Routing protocols and QoS and Resource reservation in IP networks.

Pedagogy: The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Students would be encouraged to develop an understanding of the subject. Use of ICT and web based sources will be adopted.

UNIT 1

Protocol and Network Fundamentals: Internet Evolution, Packet Switched Networks, TCP/IP Protocol Architecture, OSI Model, Internetworking, Overview of User Datagram Protocol and Internet Protocol. **High Speed Networks:** Frame Relay, Networks, ATM, High Speed LAN (10 Hrs)

UNIT 2

Delay Models In Data Networks: Characteristics of Queuing System, Little's Theorem, Queuing Models, Single Server Queues, Multi Server Queues, Priority Queuing, and Networks of Queues. **Multi-access Communication:** Aloha Modeling, Slotted Aloha Modeling, Carrier Sensing: CSMA/CA/CD, MACA, MACAW, 802.11 MAC Protocol. (10 Hrs)

UNIT 3

Congestion Control and Traffic Management: Congestion Control in Data Network andInternet, Link level flow control, Link level error control, TCP traffic control, Traffic and Congestion control in ATM Networks (10 Hrs)

UNIT 4

Internet Routing: Shortest Path Length Determination, Interior Routing Protocols: Distance Vector and Link State Protocol, Exterior Routing Protocol: BGP & IRDP, Multicasting. **Quality of Service and Resource Reservation in IP Networks:** Overview of QoS, Integrated Services, Differentiated Services, Random Early Detection (RED), Resource Reservation: RSVP, Multiprotocol Label Switching (MPLS). Real Time Transport Protocol.

(10 Hrs)

Text Books:

1. Dimitri Bersekas, Robert Gallager, "Data Networks", Second Edition, Pearson Education,2006.
2. William Stallings, "High Speed Networks and Internets", Second Edition, Pearson Education, 2010.

Reference Books:

1. James F. Kurose,Keith W.Ross, "Computer Networking: A Top-Down Approach Featuring the Internet", Third Edition, Pearson Education, 2007.
2. Nader F. Mir, "Computer and Communication Networks", Second Edition, Pearson Education, 2007.
3. Behrouz A. Forouzan, "Data Communications and Networking", Fourth Edition, Tata McGraw Hill, 2007
4. S.Keshav, "An Engineering Approach to Computer Networking", First Edition, Pearson Education, 1997.
5. Andrew S. Tanenbaum, "Computer Networks", Fourth Edition, Prentice Hall, 2003.

Paper Code: MIS-509	L	P	C
Paper Title: Network Security and Management	4	0	4

Introduction:

This course will introduce students to the basic building blocks of network security and management. The intent of this course is to familiarize students with security threats, cryptography, and application development in computer network protocols. The focus will be on how cryptography and its applications can maintain privacy and security in electronic communications and computer networks.

Course Objective:

- To understand the fundamentals of Cryptography.
- To acquire knowledge on standard algorithms used to provide confidentiality, integrity and authenticity.
- To explain and use modern cryptographic methods (symmetric encryption, public key encryption, hash functions, key management, digital signatures, certificates etc).
- To discuss various network security protocols.

Pre-requisite: None

Course Outcome: Upon successful completion of this course, students will be able to:

CO1: Understand the domain of security along with the knowledge of security attacks and models.
CO2: Apply the knowledge of the number theory in understanding the cryptosystems and designing the new cryptosystems with defined security requirements based on computationally hard problems.
CO3: Understand applied cryptographic basics and apply to real world problems.
CO4: Gain the knowledge of the algebraic structures that will enable them to work around in designing cryptosystems.

Pedagogy: The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Students would be encouraged to develop an understanding of the existing real life network security issues and how they are solved. Use of ICT, web based sources as well as blackboard teaching will be adopted.

UNIT 1
Security Taxonomy, Domain of information security, Security goals, security attacks, threats Vulnerabilities, Malicious Softwares, Virus, Trojan, Worms, spywares, Security services and Mechanism Security Techniques: Steganography, Digital watermarking, Security Models, Introduction to DB Security. Software vulnerabilities, Buffer and Stack over flow, Phishing. (10 Hrs)

UNIT 2
Mathematics of Cryptography, Integer Arithmetic, modular arithmetic, Linear congruences, Algebraic structures, GF(2n) Traditional Symmetric Key ciphers, Substitution, Transposition, Stream and Block Ciphers , Some Classical systems – Statistical theory of cipher systems-Complexity theory of crypto systems – Stream ciphers, Block ciphers. (10 Hrs)

UNIT 3
Modern Block Ciphers – DES and variant, modes of use of DES. Advanced Encryption Standard Transformations, Key expansion, Public Key Cryptography RSA, ECC, Web security, IP sec, Email Security (10 Hrs)

UNIT 4
Network management Architecture & Applications, Management standards and Models, Network Management Functions- Configurations Configuration Management, Fault management, Identification and Isolation, Management Protocols SNMP v1, SNMP v3,Network management Accounting & Performance Functions: accounting Management, Performance Management, Network Usage, Metrics.

(10 Hrs)

References:

1. William Stallings, "Cryptography and Network security Principles and Practices", 4th edition, 2005, PHI
2. Behrouz A. Forouzan , "Cryptography and Network Security", 1st Edition, 2007, TheMcGraw-Hill
3. J. Richard Burkle, "Network Management Concepts and Practice : A hands onapproach", 3rd Edition, 2000, Pearson education
4. Gollmann, Dieter, "Computer Security", 2nd edition, 2005, John Wiley & Sons Ltd.
5. Micki Krause, Harold F. Tipton, "Handbook of Information Security Management", 6th edition, 2011, Auerbach Publications
6. C P Pfleeger, S L Pfleeger, "Security in Computing", 4th edition, 2006, PHI
7. Ankit Fadia, " Network Security A Hackers Perspective", 2nd edition, 2002, Mc-Millan Publishing

Paper Code:MIS-511	L	P	C
Paper Title: Secure Coding and Security Engineering Lab	-	2	1

Experiments will be based on the subject Secure Coding and Security Engineering

Paper Code: MIS-513	L	P2	C1
Paper Title: Advanced Data Structure Lab	-		

Experiments will be based on the subject Advanced Data Structure

Paper Code: MIS-515	L	P	C
Paper Title: Cyber forensics and Incident Handling Management Lab-		2	1

Experiments will be based on the subject Cyber forensics and Incident Handling Management

Paper Code: MIS-517	L	P	C
Paper Title: Technical Report Writing	-	2	2

Technical reports describe the progress or results of scientific or technical research and development. The purpose of a technical report is to completely and clearly describe technical work, why it was done, result obtained and implications of those results. Technical report present facts and conclusions about designs and other projects. Typically, a technical report includes research about technical concepts as well as graphical depictions of designs and data. For guidelines of technical report writing, following website may be referred. www.theiet.org/students/resourees/technicalreport.com

Paper Code: MIS-502	L	P	C
Paper Title: Cryptographic Protocols and Algorithms	4	0	4

Introduction:

This advanced course will introduce students to the application of cryptography in real world. The intent of this course is to familiarize students with various classical and modern cryptographic protocols that are widely-used, heavily analysed and accepted as secure. The focus will be on how to design protocols that perform security related function by applying cryptographic methods and primitives and are robust and resistant to attacks

Course Objectives:

- To acquire knowledge on standard cryptographic protocols that are used to provide confidentiality, integrity and authenticity
- To explain and use modern cryptographic methods (hybrid encryption, key management, hybrid digital signatures, mutual authentication)
- To understand wide variety of cryptographic protocols that go beyond the traditional goals of data confidentiality, integrity, and authentication to also secure a variety of other desired characteristics of computer-mediated collaboration.

Prerequisite: Fundamentals of Information Security

Course Outcomes: On successful completion of this course, students will be able to:

CO1: Understand applied cryptographic basics and its applications.

CO2: Analyze advanced security concepts such as secret sharing, how to provide ownership without revealing personal credentials, how to prove data existed at a certain time, auditable voting systems, commitment protocols etc.

CO3: Develop interactive protocols that allow the signer to prove a forgery and limit who can verify the signature.

CO4: Apply the right algorithm, protocol, and systems to develop secure systems to protect digital assets in the cyber world.

Pedagogy: The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Students would be encouraged to develop an understanding of various cryptographic concepts. Course will have a blend of theory and practical for the benefit of students. Use of ICT, web based sources and blended teaching will be adopted.

UNIT 1

Protocol Building Blocks, Communication Using Symmetric Cryptography, One Way Hash Functions, Communication using Public Key Cryptography , digital signatures, signature with encryption, Random and Pseudo random sequence generation. (10 Hrs)

UNIT 2

Basic Protocols: key exchange, Authentication, Formal analysis of Authentication and Key exchange protocols, Multiple Key Public Key Cryptography, secret Splitting, Secret Sharing. (10 Hrs)

UNIT 3

Intermediate Protocols: time stamping services, subliminal channels, Undeniable Digitalsignatures, Proxy signatures, group signatures, Bit Commitment, fair coin flips, metal poker, key escrow. (10 Hrs)

UNIT 4

Advanced Protocols: Zero knowledge proofs, Zero knowledge proof for identity, blind signatures, identity based public key cryptography, Oblivious transfer, oblivious signatures, Simultaneous contact signing, Digital certified Mail, Esoteric protocols, secure elections. (10 Hrs)

References:

1. Bruce Schneier, Applied Cryptography, 2nd edition, 1996, Wiley
2. **Dong**, Ling, **Chen**, Kefei, , Security Analysis Based on Trusted Freshness, 1st edition2012, Springer
3. Bernard Menezes, "Network Security and Cryptography", 2nd edition, 2011, CenegeLearning
4. J A Buchman, " Introduction to Cryptography", 2nd Edition, 2009, Springer

Paper Code: MIS-504	L	P	C
Paper Title: OS Hardening	4	0	4

Introduction:
The objective of this course is to enable students to understand the principles and concepts of Network Security from the perspective of the Operating System (OS). It places emphasis on discovering the vulnerabilities of the standard Operating Systems (OS) to attacks and focuses on the methodologies and measures necessary to take a proactive and preventive stance to address security vulnerabilities. Students will examine the principles, practices, and policies related to hardening and securing Operating Systems so they are impervious to security threats. It focuses on the vulnerabilities and the related countermeasures of various Operating Systems and Network Devices.

Course Objectives:
- To list key concepts and terms associated with information systems security
- To identify risks, threats, and vulnerabilities associated with different operating systems
- To align security procedures and practices with protecting computer operating systems
- To design security controls to keep Windows and Linux computers secure
- To configure Windows and Linux controls to protect both server and client computers

Pre-requisites: Operating Systems, Computer Networks, Cyber Security Fundamentals
Course Outcomes: On successful completion of this course, students will be able to:
CO1: Describe the security fundamentals of Windows and Linux operating systems in general
CO2: Interpret issues relating to regulation and explain various facets of cyber-crimes pertaining to Network Operating Systems
CO3: Comprehend the Intellectual Property issues related to Proprietary Operating Systems
CO4: Distinguish between different attacks and vulnerabilities in Windows and Linux environment

Pedagogy: The teaching-learning of the course would be organized through lectures, assignments, projects/presentations and case studies. Students would be encouraged to develop an understanding of security threats, vulnerabilities and attacks in Operating Systems. Use of ICT and web-based sources by using blended mode will be adopted.

UNIT 1
Overview of Linux and Windows Operating system, Linux Kernel, Windows kernel, Networking , Secure booting, Boot loaders and Boot time services, Securing Virtual Terminals, Securing log in Screens, Users and Groups, Shadow Password, Groups, adding groups, Deleting Unnecessary users and Groups, Passwords, Password Aging, Process Accounting, Plugable Authentication Modules, , Hardening Kernel in Linux
(10 Hrs)

UNIT 2
Working of Linux Firewall, Tabls, Chains, Policies, Filtering Criteria, IP table Commands, Securing Connections and Remote Administrations, Public key encryptions, SSL,TLS, Open SSL, Remote administration, ssh, scp,sftp, ssh-agent, Agent forwarding, The sshd Daemon, Securing Files and File system, Access Permission, Imutable Files, Encrypting Files, Securely Mounting Files, Secring removal devices, Understanding Logging and log Monitoring, Syslog, Syslog-NG, Log anaysis and correlation, Hardening remote access to Email, Securing FTP server
(10 Hrs)

UNIT 3
Understanding Windows Kernel, Windows attacks, Automated Vs dedicated attackers, Virus, Trojan, Directory traversal, Password Cracking, Social engineering, Adware, spyware, spam, phishing and Farming, Conventional Defense mechanism, Unconventional defenses, Host based firewall, Use of Anti -virus , Anti-Spam software, and anti-spam softwares, HardeningTCP/IP stack, Securing Files and File system in Windows, NTFS permissions, Best practice recommendations.
(10 Hrs)

UNIT 4

Windows password authentication, Unicode password, Password Complexities, Strong Password, Windows password Hashes, Password Attacks, tools and techniques, Defensemechanism against password attacks, Disable LM password Hashes, Disable LM and NTLM authentication, Hardening File System, Protection of High Risk files, High risk windowsfiles, File Defenses, Methods to prevent unauthorised execution, Securing internet explorer

(10 Hrs)

References:

1. R A Grimes, "Professional Windows Desktop and server Hardening ", 1st edition,2006, Wiley India Edition
2. James Turnbull, " Hardening Linux", 1st edition , 2005, Apress publication
3. Scambray, Shema, and Sima, "Hacking Exposed Web Applications", 3rd edition ,2010, McGraw Hill.
4. Sander Van Vugt, " Red Hat Enterprise Linux 6 Administration", 1st edition, 2010,Wiley Inderscience

Paper Code: MIS-506	L	P	C
Paper Title: Cloud Computing Architecture	4	0	4

Introduction:
The course aims to familiarize the students with the advanced concepts of Cloud Computing Architecture and its Security Life Cycle. The prominent attributes of a secure cloud platform are data security, scalability, easy accessibility and sharing of data, zero maintenance, and easy data recovery. The course is designed for inculcating the research aptitude in graduate students, keeping the needs of Enterprise Cloud Computing in Industry 4.0 and the academic research.

Course Objectives:
- To comprehend importance of Enterprise Cloud Computing in Industry 4.0 and research
- To learn Cloud Computing architecture, its Security Requirements and Virtualization
- To understand Cloud Computing Life Cycle Management and Provisioning
- To identify current Security Challenges in Enterprise Cloud Computing.

Prerequisite: Basic understanding of Operating System, Network Security, Parallel and Distributed Computing, Computer Organization and Architecture

Course Outcomes: Upon Successful completion the students will be able to:
CO1: Conceptual clarity in Grid and Cloud Computing architecture.

CO2: Conceptual understanding of Virtualization at different levels

CO3: Logical insight for comprehending the Security Primitives in Cloud Computing.

CO4: A Research Case Study identifying Security Objectives and proposing a relevant solution

Pedagogy: The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Faculty members strive to make the classes interactive so that students can correlate the theories with practical examples for better understanding. Use of ICT, web-based resources as well as flipped classroom teaching will be adopted.

UNIT 1
The Evolution of Cloud Computing, Why Cloud Computing Matters, Advantages and Disadvantages of Cloud Computing, How Cloud Computing Works, Understanding Services and Applications by type, IaaS, PaaS, SaaS, IDaaS, CaaS, Cloud Computing for Everyone, Collaborating on Calendars and Schedule.

(10 Hrs)

UNIT 2
A Brief Primer on Cloud Security and Cloud Architecture, Security Architecture, Cloud Computing Architecture, Control over Security in Cloud Model, Security Concerns, Accessing Risk Tolerance in Cloud Computing, Legal and Regulatory Issues

(10 Hrs)

UNIT 3
Securing the Cloud: Architecture, Security requirements for the Architecture, Security Patterns and Architectural Elements, Cloud Security Architecture, Planning Key strategies forsecure operations, Overview of Data Security in Cloud Computing, Data Encryption, Cloud Data Storage, Cloud Lock-in.

(10 Hrs)

UNIT 4
Key strategies and Best Practices, Effectively Managing Risk, Overview and Limits of Security Controls, Security Monitoring, Building an Internal Cloud, Selecting an External Cloud, Evaluating Cloud Security, Operating a Cloud, Using Mobile Cloud.

(10 Hrs)

References:

1. Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, 1st edition, 2010, Wiley
2. Vic (J.R.) Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics, Syngress, 1st edition, 2011, Elseveir.
3. John W. Rittinghouse and Ames F. Ransome, "Cloud Computing Implementation, Management and Security", 2nd edition, 2010, CRC Press, Taylor & Francis Group, Boca Raton London New York.
4. Cloud Computing Bible, Barrie Sosinsky, 1st edition, 2011, Wiley-India
5. Miller Michael, Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online, 1st edition, 2008, Pearson Education India.

Paper Code: MIS-508	L	P	C
Paper Title: Secure Wireless Networks	4	0	4

Introduction: This course is about teaching of the fundamental concepts of wireless networks and imparting basic knowledge of the different types of ad-hoc networks and underlying protocols. Course will provide the understanding of the architecture of wireless networks for its various application setups.

Course Objectives:

- To understand the basics of wireless adhoc networks, mesh and sensor networks.
- To famiarize students with the challenges involved in wireless networks with respect to wired networks.
- To study about various types of wireless networks, i.e cellular networks, Bluetooth, Ad hoc networks, wireless mesh networks and wireless sensor networks.
- To discover about various design, security and privacy issues in wireless networks.

Prerequisite: Basic knowledge of wireless communication and computer networks.

Course Outcome: Upon successful completion of this course, students will be able to:
CO1: Understand the underlying technologies of wireless networks.
CO2: Describe the various Wireless Network Technologies with respect to security requirements and issues
CO3: Illustrate the secure design principles for wireless networks and various network security mechanisms.
CO4: Describe different ways to prevent and detect rogues in wireless network and its associated components.

Pedagogy: The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations and quizzes. Faculty members strive to make the classes interactive so that students can correlate the theories with practical examples for better understanding. Use of ICT, web-based resources as well as flipped class room teaching will be adopted.

UNIT 1

Wireless Networks, Wireless Network Architecture, Adhoc Networks, Sensor Networks,Wireless Devices, Access Points, PDA, Smart Phones, Wireless Standards, IEEE 802.11 a/b/g/n Emerging Wireless Technologies, SSID, BSSID, MAC Address, Beacons and Broadcasts, Associating and Authenticating.
(10 Hrs)

UNIT 2

WLAN Architecture, Frequency and Data rates, WLAN components, Security feature of 802.11 Problems With the IEEE 802.11 Standard, WEP, Problems in WEP, WPA, WPA2, Security Requirements and Threats, Loss of Confidentiality, Loss of Integrity, Risk Mitigation.
(10 Hrs)

UNIT 3

Secure Design Principles for Wireless Networks, Defense In Depth, Least Privilege, Network Segmentation, Wireless Assessments, Secure the Infrastructure, Rogue AP Detection, Physical Security, Firewalls, Routers, Switches, Intrusion Detection Systems and Intrusion Prevention Systems Wireless Intrusion Detection and Intrusion Prevention Systems,Honeypots, Web Authentication Gateways
(10 Hrs)

UNIT 4

Preventing Rogue Wireless Networks, Manually Detecting Rogue Wireless Networks, Tracing Malicious Rogue Access Points, Handling Rogue Access Points, Automated Detection of Rogue Wireless Networks, Other Wireless Technologies, Next-Gen Solutions, Lightweight Wireless Solutions, Cloud-based Wireless Solutions, Dedicated Wireless IDS, Client Protection
(10 Hrs)

References:

1. Tyler Wrightson , "Wireless Network Security: A Beginner's Guide", 1st edition,2012, McGraw-Hill
2. Security for mobile wireless sensor networks by Liu , Donggang, 1st edition, 2007,Springer
3. Wimax Standard & Security Ahson Syed, 1st edition, 2007, CRC Press (Taylor &Francis)
4. Wireless Security handbook Earle, Aaron E, 1st edition, 2006, Auerbac Publication(Taylor & Francis Group)
5. Yang Xiao, " Security in Sensor Networks", 1st edition, 2006, AuerBach Publications

Paper Code: MIS-510	L	P	C
Paper Title: Web Application and its Security Management	4	0	4

Introduction:

The course aims to familiarize the students with the advanced concepts of Web applications and the related security management. The course is designed to understand the security principles in developing a reliable web application and to identify and aid in fixing any security vulnerabilities during the web development process.

Course Objectives:

- To familiarize students about the Web Application architecture and its associated tools.
- To understand various security weaknesses associated with the web applications
- To learn usage of various tools to handle/mitigate security weaknesses

Prerequisite: Basic understanding of web application technology and concepts such as HTML, JavaScript and Cryptographic standards.

Course Outcomes: Upon successful completion of this course, students will be able to:

CO1: Understand web application architecture and tools handle its security problems.

CO2: Understand the concepts of profiling applications, and possible attacks. Use counter measure tools.

CO3: Understand security mechanisms that are applied for ensuring web application security and use of related tools.

CO4: Describe various SQL Injection attacks and use tools to handle/mitigate web application attacks.

Pedagogy:

The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations, and quizzes. Students would be encouraged to develop an understanding of the subject. The use of ICT and web-based sources will be adopted.

UNIT 1

History of web application- Introduction to web application architecture, Uniform Resource Locator (URL), HTTP- Introduction, HTTP Methods, WEBDAV methods, Request/Response analysis, Security problems with http, HTTPS- Handshake protocol, Record protocol, Proxy- Man in the middle attack, Tools: Burp proxy, Paros proxy, web scarab Encoding Techniques- URL Encoding, HTML Encoding, Unicode Encoding, Tools: Burp decoder

(10 Hrs)

UNIT II

Profiling Application - Spiders, crawlers, Search engine discovery, Banner Grabbing, Analysis of error codes, Tools: Http Print, netcraft Attacking Authentication- Authentication Types, Brute force attacks, Analyzing Auto complete options, Insecure credential transmission, Session puzzle attacks, Authentication bypass techniques, Shoulder surfing, CAPTCHA Rebinding attacks, Countermeasures, Tools: Bruter, Burp Repeater, Burp Intruder Attacking Authorization- Authorization types, Parameter tampering, Horizontal privilege escalation, Vertical privilege escalation , Referrer spoofing

(10 Hrs)

UNIT III

Cryptography weakness- Symmetric cryptography, Asymmetric cryptography, Substitution cipher, Stream cipher, Block cipher, Steganography, SSL cipher testing, Cracking hashes, Padding oracle attack, Cracking ECB encryption, Tools: SSLDigger, MD5 crack Attacking Session management- Introduction, Secure flag, HTTPOnly flag, Cookie Domain & Path, Session Token analysis, Session fixation , Cookie transmission mechanisms, Tools: Burp sequencer, Timeout issues

(10 Hrs)

UNIT IV

SQL injection- Error based SQLi, Blind SQLi, SQLi exploitation, Data extraction with UNION queries, Data extraction with inference techniques, Command execution with SQLi, Impact of SQLi, Remediation, Stored procedures Vs Parameterized queries, Tools: SQLMap, Absinthe URL Redirection attacks- Phishing attacks, Remediation HTTP Response splitting - Cache positioning Command execution Attacking Web Server- Denial of service attacks, Buffer over flows, Remediation

(10 Hrs)

References:

1. Scambray, Shema, and Sima, "Hacking Exposed Web Applications", 2nd edition,2006, McGraw Hill.
2. J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan "Improving Web Application Security: Threats and Countermeasures", 1st edition, 2003, Microsoft Corporation
3. Michael Howard, David LeBlanc, "Writing Secure Code", 2nd Edition, 2003, Microsoft Corporation
4. Simson Garfinkel,"Web Security, Privacy and Commerce", 2nd Edition, 2002,O'reilly
5. Michael Cross, "Developer's Guide to Web Application Security", 1st edition, 2007, Syngress publishing

Paper Code: MIS-512	L	P	C
Paper Title: Security Testing and Risk management	4	0	4

Introduction: This course is designed to enable students to recognize the need for Security Testing of software applications and assessing the risk associated. Design software with a security mindset and implementing security by writing secure code does not necessarily mean that the software is secure. It is imperative to validate and verify the functionality and security of software and this can be accomplished by quality assurance testing which should include testing for security functionality and security testing. Security testing is an integral process in the secure software development life cycle. Software that has undergone and passed validation of its security through testing is said to be of relative higher quality than software that hasn't. The course is effective in enabling students to learn Software Security testing techniques so as to develop software that is reliable and resilient to software attacks.

Course Objectives:

- To learn different types of functional and security testing and criteria that can be used to determine the type of security tests.
- To learn implementation of security patterns in removing the software and network vulnerabilities.
- To learn assessment and management of Risk through various risk assessment and management framework.

Prerequisite: Basic knowledge of Software applications, programming, Database, Network Concepts.

Course Outcomes: Upon successful completion of this course, students will be able to:

CO1: Learn what to test, which modules to test and how to test for software security issues.

CO2: Perform Security testing of software and web applications.
CO3: Detect Security vulnerabilities in software and network.

CO4: Develop a deep insight to the various state-of-the-art technologies of semantic search engine, semantic web browser and semantic recommender systems.

CO5: Assess, evaluate and analyse risk of a software applications using standard Risk assessment and Management Framework.

Pedagogy:
The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations, and quizzes. Students would be encouraged to develop an understanding of the subject. The use of ICT and web-based sources will be adopted.

UNIT 1
Role of Testing in SDLC: Review of software development models (Waterfall Models, SpiralModel, W Model, V Model) Agile Methodology and Its Impact on testing, Test Levels (Unit, Component, Module, Integration, System, Acceptance, Generic), Approaches to Testing – I: Dynamic Testing, Black Box Testing Equivalence Class Partitioning, Boundary Value Analysis, State Transition Test, Cause Effect Graphing and Decision Table Technique and Used Case Testing and Advanced black box techniques ,Statement Coverage, Branch Coverage, Test of Conditions, Path Coverage.

(10 Hrs)

UNIT 2
Fitting Security Testing into SDLC, Security requirements, Design vs implementation vulnerabilities, Common secure Design issues, poor use of cryptography, tracking users and their permissions, flawed input validation, weak structural security, programming language implementation isues, platform implementation issues, generic application security implementation issues

(10 Hrs)

UNIT 3

Directions for risk management development. Possibilities in six dimensions - what, when, why, which way, who, and wherewithal. Definitions of risk, threat, opportunity and uncertainty distinguished; relationship with performance objectives, implications for uncertainty management. Security Risk management, Risk leased security testing : information gathering, Run time inspection, Identfying threat paths, ranking the risks associated with vulnerabilities.

(10 Hrs)

UNIT 4

Objectives for risk management applications. Distinguishing benefits and objectives for risk management. Objectives for process, application, performance and strategic capability; links between these objectives. Planning the scope and purpose of a risk management application. Risk evaluation: The importance of risk-performance trade-offs, and risk efficiency as a key criterion in evaluating alternative course of action. Building capability in risk management. Assessing risk management capability (benchmarking, risk maturity). Nature and quality of risk management processes, Facilitators of risk management capability.

(10 Hrs)

References:

1. Elfriede Dustin, Luke Nelson and chris Wysopal, " The art of Software SecurityTesting", Addison-Wesley Professional, 1st edition, 2006
2. Wolf Halton, Alfred Basta, " Computer security and penetration Testing", delmerPublisher, 1st edition, 2007
3. Andreas Spillner, Tilo Linz, Hans Schaefer, "Software Testing Foundations", ShoffPublishers, 3rd edition, 2011
4. Srinivasan D and Gopalswamy R, " Software Testing: Principles and Practices",Pearson Ed, 1st edition, 2006
5. Aditya P. Mathur, " Foundations of Software Testing", Pearson Ed, 1st edition, 2000
6. Robert V Binder, " Testing Object Oriented Systems: models, patterns and tools",Addison Wesley, 1st edition, 1996
7. Roger S. Pressman , "Software Engineering – A practitioner's approach", 5th edition,2009, McGraw Hill
8. Jorion, Philippe, "Value at Risk: The New Benchmark for Managing Financial Risk",3rd edition, McGraw-Hill, 2007

Paper Code: MIS-514	L	P	C
Paper Title: Big Data and Business Analytics	4	0	4

Introduction:
This course is all about Business Analytics which gives exposure to various types of Business analytics, types of data, data sources, understanding of Big data and Business analytics. The course aims to Optimize business decisions and create competitive advantage with Big data analytics

Course Objectives:

- Understand the impact of big data for business decisions and strategy
- Gain hands-on experience on large-scale analytics tools to solve some open big data problems
- Optimize business decisions and create competitive advantage with Big data analytics

Prerequisite: Database Management System.

Course Outcomes: Upon successful completion of this course, students will be able to:
CO1: Understand the key issues in big data analytics and its associated applications in business analytics
CO2: Understand different business data classification techniques and their usage via case studies.
CO3: Describe business decision making process and usage of its tools via different case studies.
CO4: Demonstrate the concepts of various Big Data Analytics tools for application development.

Pedagogy: The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations, and quizzes. Students would be encouraged to develop an understanding of the subject. The use of ICT and web-based sources will be adopted.

UNIT 1
Big Data-Volume, Velocity, Variety, Varacity, types & sources of Big Data OLAP & RTAP, Data Exploration & Dimension Reduction : Data Summaries, Data Visualization, Correlation Analysis, Reducing no of categories in Categorial variables, principal component Analysis for classification & prediction, Accuracy measures, Cutoff, Oversampling & Asymetric Costs, Multiple Linear Regression,Transforming Data into Actionable Results.
(10 Hrs)
UNIT 2
Classification of Business data :- Naïve Bayes Classifier, k-Nearest Neighbour, Classification Tree, Generating Classification Rules from Trees, Discovering Association Rules in Transaction Databases, Business Case Studies for Data Classification.
(10 Hrs)
UNIT 3
Business Decision making process: Decision, Decision Process, Types of Decision, Kepher - Tregoe Decision making method, Decision Support Systems, Types of Decision Support Systems, DSS Architecture, DSS Hardware & Operating Systems, DSS Tools. Case studies for Developing Decision support Systems.
(10 Hrs)

UNIT 4

Tools for Big Data Analytics : No SQL, Hadoop, Mapreduce, Gephi, Association Rule Mining, Cluster Analysis, Genetic Algorithms, Fuzzy Logic & Uncertain Data Management, Unstructured Data, Web Data, Web communities, Crawlers, Social Networks, Blogs & Microblogs, Sentiment Analysis & Opinion mining, Document summarization technique, CASE STUDIES for Business Intelligence.

(10 Hrs)

References:

1. Shmueli, Patel & Bruce, "Data Mining for Business Intelligence", 2nd edition, 2010,Wiley Interscience Publications.
2. EG Mallach, "Decision Support Systems & Data warehousing Systems", 1st edition,2002, Tata McGraw Hill Publications.
3. R Roiger & M Geatz, "Data Mining – A Tutorial Based Primer", 2nd edition, PearsonEducation Asia.
4. Alex Berson & S J Smith, " Data Warehousing, Data Mining & OLAP", 1st edition,2004, Tata Mc Graw Hill Publishing Company.
5. J.C. Lee, "Social Networks Analysis", Springer Publications

Paper Code: MIS-516	L	P	C
Paper: Distributed Systems	4	0	4

Introduction: This course deals with distributed system architecture, enabling technologies for distributed systems, and the applications that can be built on distributed systems. It forms essential background for modern technology that puts computer networks to productive use, for example, service orientation, cloud and edge computing, NoSQL data bases, IoT middleware, and handling Big Data. The course shall introduce students to a selection of these areas through specific examples and situations

Course Objectives: At the end of the course students should demonstrate the ability to provide support for development of distributed systems and distributed applications

Pre-Requisites: Operating Systems, Computer Networks, Relational DBMS

Course Outcomes:
CO1: To provide hardware and software issues in modern distributed systems.
CO2: To get knowledge in distributed architecture, naming, synchronization, consistency and Replication, fault tolerance, security, and distributed file systems.
CO3: To analyze the current popular distributed systems such as peer-to-peer (P2P) systems.
CO4: To know about Shared Memory Techniques

Pedagogy: The course will be delivered in workshop mode with lecture material and problem-solving exercises suitably interspersed during lecture contact hours. Tutorial work shall be pen and paper problem solving as well as implementing/simulating components of distributed systems.

UNIT 1
Definition of Distributed System, Goals, Transparency, Openness Scalability, Hardware Concepts, Software Concepts: distributed operating system, Network operating System, Middle ware, The Client server model, Clients and servers, Application Layering, Client server architectures, Processes; distributed systems – hardware and software concepts, Client-server model; Communication – Lower-level protocols, transport protocols (10 Hrs)

UNIT II
higher level protocols, RMI Remote Object Invocation, Message oriented communication, Stream oriented communication Synchronization: Clock synchronization, Physical Clocks, Clock Synchronization Algorithms, Logical clocks, Lamport timestamp, Global state, Election algorithm, the Bully algorithm, A ring Algorithm (10 Hrs)

UNIT III
Consistency and replication, Data Centric Consistency Models, Strict Consistency, Sequential Consistency, Causal consistency, FIFO consistency, Wak and release Consistency, Distribution protocols, replca placement update propagation Epidemic Protocols, Fault tolerance, Reliable Group Communication, Distributed Commit, Two phase Commit, Three phase commit (10 Hrs)

UNIT IV
Distributed System Security: Security Threats, Policies and Mechanisms, design Issues, Secure Channel, Authentication, Secure Group Communication, Security Management, Key management, Secure Group Management Authentication Management, Kerberos, SESAME (10 Hrs)

References:

1. Tenenbaum, "Distributed Systems: Principles and Paradigms", 2nd edition, 2006,Pearson Education

2. Coloursist, "Distributed Systems: Concepts and design", 5th edition, 2011 PearsonEducation

Paper Code: MIS-518	L	P	C
Paper Title: IT Act 2000 and Cyber Laws	4	0	4

Introduction:

The objective of this course is to enable students to understand, explore, and acquire a critical understanding of cyber law. Develop competencies for dealing with frauds and deceptions (confidence tricks, scams) and other cybercrimes. It also covers overview of Intellectual Property Right and Cyber Laws in Indian and global perspectives.

Course Objectives:

- To introduce the cyber world and cyber law in general
- To explain about the various facets of cyber crimes
- To enhance the understanding of problems arising out of online transactions and provoke them to find solutions
- To clarify the Intellectual Property issues in the cyber space and the growth and development of the law in this regard
- To educate about the regulation of cyber space at national and international level

Pre-requisites: Cyber Security Fundamentals

Course Outcomes: On successful completion of this course, students will be able to:

CO1: Describe the fundamentals of cyber world and cyber law in general and technicalities of law in cyber world.

CO2: Interpret issues relating to regulation and explain various facets of cyber-crimes; and use different plagiarism tool.

CO3: Comprehend the Intellectual Property issues and E-Commerce in the cyber space.

CO4: Distinguish between different laws and regulations in cyber space at national and international level.

UNIT 1

Understanding Computers, Internet and Cyber Laws: Modern era: The Scene and problems, need for Cyber Laws, law and legal system, Jurisprudence of Indian Cyber Law, Evolution ofKey Terms and Concepts, Data, System, Network etc., Security threat to cyber space and e- commerce Evolution of Cyber Crime, Ranges of cybercrime, Indian IT act, amendments, Basics of PKI, Certification, Certifying authorities, The role of Certifying authority

(10 Hrs)

UNIT 2

Issues in Electronic Transaction, Issues, Authentication, The role of Electronic Signatures in E Commerce, Basic Laws of Digital and Electronic Signature, Authentication of signatures and Electronic Records, Protection of Intellectual property rights in Cyber spaces in India, Domain names in IPR, protection of Copy Rights, protection of Patents in India and associated laws, Patent as Intellectual Property, Plagiarism Issues, Tools to detect Plagiarism,Plagiarism Tools Turnitin, Viper

(10 Hrs)

UNIT 3

Penalties and Compensation and Adjudications of Violations of Provisions of IT act, penalty and compensation for damage to computer, compensation for failure to protect data, adjudications of disputes under the IT Act, Cyber Appellate Tribunal, Its Functions and Powers under the IT act, offenses under IT act in India, Obscenity and pornography on Cyberspace, hacking, punishment for violation of Privacy under It act

(10 Hrs)

UNIT 4

Indian evidence act, Examiner of Electronic evidence, amendments introduced in Indian evidence act, Indian CERT, Law regarding Electronic Cheques and truncated cheques, Ithe IT rules 2000, Ministerial Order on blocking of websites, Cyber laws in US, Cyber laws in Gobal Prospective

(10 Hrs)

References:

1. Harish Chander, "Cyber Laws and IT Protection", 1st edition, 2012, PHI
2. Dr. Jyoti Rattan, "Cyber Laws and Information Technology", Universal LawPublication.
3. Prof. Vimlendu Tayal "Cyber Law Cyber Crime Internet and E Commerce". Universal Law Publication.

Paper Code: MIS-620	L	P	C
Paper Title: Digital Image Processing and Steganography	4	0	4

Introduction: This course is an intensive study of the fundamentals of image processing, analysis and understanding. Topics to be covered include: a brief review of the necessary mathematical tools, human visual perception, sampling and quantization, image transformation, enhancement, restoration, compression, reconstruction, image geometric transformation, matching, segmentation, feature extraction, representation and description, recognition and interpretation, and so on.

Course Objectives:

- Cover the fundamental theory and algorithms that are widely used in digital image processing
- Expose students to current technologies and applications related to image processing
- Develop hands-on experience in using computers to process images
- Familiarize with MATLAB Image Processing Toolbox
- Develop creative thinking on solving problems of the state-of-the-art in image processing

Pre-requisites: Computer Graphics, Digital Signal Processing

Course Outcomes: On successful completion of this course, students will be able to:

CO1: Describe the fundamentals of Computer Graphics and Image Processing.

CO2: Interpret issues relating to security concerns in Computer Vision.

CO3: Comprehend the statistical analysis of the digital images from different sources.

CO4: Distinguish between different steganographic techniques.

Pedagogy: Lectures will be supported with case studies (driven by research papers) of privacy and security problems in Digital and Statistical Image Processing. Emphasis will be on practical system development by writing programs to collect, analyze and infer insights from digital images and videos.

UNIT 1

Light, Brightness adaption and discrimination, Pixels, coordinate conventions, Imaging Geometry, Perspective Projection, Spatial Domain Filtering, sampling and quantization. Intensity transformations, contrast stretching, histogram equalization, Correlation and convolution, Smoothing filters, sharpening filters, gradient and Laplacian. Hotelling Transform, Fourier Transforms and properties, FFT (Decimation in Frequency and Decimation in Time Techniques), Convolution, Correlation, 2-D sampling, Discrete Cosine Transform, Frequency domain filtering.

(10 Hrs)

UNIT 2

Basic Framework, Interactive Restoration, Image deformation and geometric transformations, image morphing, Restoration techniques, Noise characterization, Noise restoration filters, Adaptive filters, Linear, Position invariant degradations, Estimation of Degradationfunctions, Restoration from projections. Encoder-Decoder model, Types of redundancies, Lossy and Lossless compression, Entropy of an information source, Shannon's 1st Theorem, Huffman Coding, Arithmetic Coding, Golomb Coding, LZW coding.

(10 Hrs)

UNIT 3

Transform Coding, Sub-image size selection, blocking artifacts, DCT implementation using FFT, Run length coding, FAX compression (CCITT Group-3 and Group-4), Symbol-based coding, JBIG-2, Bit-plane encoding, Bit-allocation, Zonal Coding, Threshold Coding, JPEG, Lossless predictive coding, Lossy predictive coding, Motion Compensation, Expansion of functions, Multi-resolution analysis, Scaling functions, MRA refinement equation, Wavelet series expansion, Transform(DWT), Continuous Wavelet Transform, Fast Wavelet Transform, 2-D wavelet Transform, JPEG-2000 encoding, Digital Image Watermarking.

(10 Hrs)

UNIT 4

Bit plane slicing, Digital Watermarking, Secret-Key Stego-system, Pure stego-system, information-hiding capacity, Private Marking system, Public Marking system, Asymetric Marking system, phase space encryption, Wavelet transformation, Use of energy-based embedding using wavelet coefficients, Spread spectrum watermarking. Steganalysis

(10 Hrs)

References:

1. Rafael C Gonzalez and Richard E Woods, "Digital Image Processing", 3rd edition,2007, Pearson Education
2. A K Jain, " Fundamentals of Digital Image Processing", 1st edition, 1988, PHI

Paper Code: MIS-522	L	P	C
Paper Title: Intellectual Property Rights	4	0	4

Introduction:

The objective of this course is to enable students to understand, explore, and acquire a critical understanding of cyber law. Develop competencies for dealing with frauds and deceptions (confidence tricks, scams) and other cybercrimes. It also covers overview of Intellectual Property Right and Cyber Laws in Indian and global perspectives.

Course Objectives:

- To introduce the cyber world and cyber law in general
- To explain about the various facets of cyber crimes
- To enhance the understanding of problems arising out of online transactions and provoke them to find solutions
- To clarify the Intellectual Property issues in the cyber space and the growth and development of the law in this regard
- To educate about the regulation of cyber space at national and international level

Pre-requisites: Cyber Security Fundamentals

Course Outcomes: On successful completion of this course, students will be able to:

CO1: Describe the fundamentals of cyber world and cyber law in general and technicalities of law in cyber world.

CO2: Interpret issues relating to regulation and explain various facets of cyber-crimes; and use different plagiarism tool.

CO3: Comprehend the Intellectual Property issues and E-Commerce in the cyber space.

CO4: Distinguish between different laws and regulations in cyber space at national and international level.

UNIT 1

Introduction and the need for intellectual property right (IPR). IPR in India – Genesis and Development IPR in abroad, some important examples of IPR, Macro economic impact of the patent system Patent and kind of inventions protected by a patent. Legislation Covering IPRS in India.

(10 Hrs)

UNIT 2

Utility models Differences between a utility model and a patent, Trade secrets and know-howagreements, Copy Rights, Distinction between related rights and copyright, Rights coveredby copyright, Trademarks, Rights of trademark, signs used in trademarks, Types of trademark function, Protection of trademark, Registration of trademark, Domain name and how does it relate to trademarks , Plagiarism Issues, Tools to detect Plagiarism, Plagiarism Tools Turnitin, Viper

(10 Hrs)

UNIT 3

Geographical Indications, Protection of geographical indication, Reasons to protect geographical indication, Industrial Designs, Protection of an industrial design. Various kinds of protection provided by industrial designs. New Plant Varieties, Unfair Competitions. Plant Breeder and TRIPS agreement.

(10 Hrs)

UNIT 4

Enforcement of IPR, Infringement of intellectual property rights, Enforcement Measures, Emerging Issues, Overview of Biotechnology and Intellectual Property, Biotechnology Research and Intellectual Property Rights Management Licensing and Enforcing Intellectual Property Commercializing Biotechnology Invention Case studies of Biotechnology, Case studies
(10 Hrs)

References:

1. T. M Murray and M.J. Mehlman, Encyclopedia of Ethical, Legal and Policy issues inBiotechnology, John Wiley & Sons 2000
2. P.N. Cheremisinoff, R.P. Ouellette and R.M. Bartholomew, Biotechnology Applications and Research, Technomic Publishing Co., Inc. USA, 1985
3. D. Balasubramaniam, C.F.A. Bryce, K. Dharmalingam, J. Green and K. Jayaraman, Concepts in Biotechnology, University Press (Orient Longman Ltd.), 2002
4. Bourgagaize, Jewell and Buiser, Biotechnology: Demystifying the Concepts, WesleyLongman, USA, 2000.
5. Ajit Parulekar and Sarita D' Souza, Indian Patents Law – Legal & BusinessImplications; Macmillan India ltd , 2006
6. B.L.Wadehra; Law Relating to Patents, Trade Marks, Copyright, Designs &Geographical Indications; Universal law Publishing Pvt. Ltd., India 2000
7. P. Narayanan; Law of Copyright and Industrial Designs; Eastern law House, Delhi ,2010

Paper Code: MIS-524	L	P	C
Paper Title: Open Ended Research Topic	4	0	4

Paper Code: MIS-526	L	P	C
Paper Title: Cryptographic Protocols and Algorithms Lab	-	2	1

Experiments will be based on the subject Cryptographic Protocols and Algorithms

Paper Code: MIS-528	L	P	C
Paper Title: OS Hardening Lab	-	2	1

Experiments will be based on the subject OS Hardening

Paper Code: MIS-530	L	P	C
Paper Title : Lab based on elective(s)	-	2	1

Experiments will be based on the elective subject

	L	P	C
Paper Code: MIS-532			
Paper Title: Term Paper	-	2	2

Term papers are generally intended to describe an event, concepts or argue a point. The topic for the term paper may be based on the recent trends in technology / Industry or Academia research outcomes The guidelines for writing are same as that for technical report writing.

Paper Code: MIS-601	L	P	C
Paper Title: Information Security Audit and Security Management	4	0	4

Introduction:
The objective of this course is to enable students to understand, explore, and acquire a critical understanding of information security. Develop competencies for dealing with frauds and deceptions (confidence tricks, scams) and other cybercrimes. It also covers overview of Information Security Audit and Security Management in Indian and global perspectives.

Course Objectives:
- To introduce the information security management and audit in general
- To explain about the various facets of network security
- To enhance the understanding of problems arising out of online transactions and provoke them to find solutions
- To clarify the Security Audit issues in the cyber space and the growth and development of the law in this regard
- To educate about the regulation of security audit at national and international level

Pre-requisites: Cyber Security Fundamentals

Course Outcomes: On successful completion of this course, students will be able to:
CO1: Describe the fundamentals of cyber world and cyber law in general and technicalities of law in cyber world.

CO2: Interpret issues relating to regulation and explain various facets of cyber-crimes; and use different plagiarism tool.

CO3: Comprehend the Security Audit issues in the hyper-connected cyber space.

CO4: Distinguish between different laws and regulations in cyber space at national and international level.

Pedagogy:
The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations, and quizzes. Students would be encouraged to develop an understanding of the subject. The use of ICT and web-based sources will be adopted.

UNIT 1
Security Audit: Overview of the security audit, Architecture, Requirement, Characteristics, Recent trends, Challenges in the information security audit, Differences between an audit andan assessment, Cyber laws, Indian IT act, ISO standards **Process & Procedure:** Access Control, Cryptography, Telecomm and Network Security, Security Models and Architecture, Physical Security, Security Risk Management Practices, Physical Security, Disaster Recovery and Business Continuity, Law, Investigation, and Ethics, Application and Operations Security, IS Audit Process,, IT Governance, System and Infrastructure Life Cycle Management, IT Service Delivery and Support, Protection of Information Asset.
(10 Hrs)

UNIT 2
Security Investigation Phase: The history of and the need for security, A model for Internetwork security, Internet Standards and RFCs ,The Systems Development Life Cycle (SDLC),Differences between threats and attacks , Security Ethics, Security Attacks (Interruption, Interception, Modification and Fabrication),Security Services (Confidentiality, Authentication, Integrity, Non-repudiation, Availability) and Mechanisms, , Buffer overflow & format string vulnerabilities, TCP session hijacking, ARP attacks, route table modification. **Security Analysis:-** Risk Management & Discussion Points, Risk Assessment, Risk Identification, Risk Control Strategies and Mitigation Selection ,Risk Categories of Control, Risk Assessment in Real Life, Current Issues in Information Security Part 2, Social Engineering.

(10 Hrs)

UNIT 3

Security Architecture and Models: Introduction, Defining the Trusted Computing Base Protection Mechanisms in a Trusted Computing Base, System Security Assurance Concepts, Trusted Computer Security Evaluation Criteria, Information Technology Security Evaluation Criteria, Federal Criteria for Information Technology Security, Confidentiality and Integrity Models

(10 Hrs)

UNIT 4

Security Management: key distribution Approaches of Message Authentication, Secure Hash Functions and HMAC, Public key cryptography principles, public key cryptography algorithms, digital signatures, digital Certificates, Certificate Authority and key management Kerberos **Email privacy**: Pretty Good Privacy (PGP) and S/MIME **IP Security:** Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management, **Web Security:** Requirements, Secure SocketLayer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET).
(10 Hrs)

References:

1. William Stallings, "Network Security Essentials (Applications and Standards)", 4th edition, 2010, Pearson Education.
2. Eric Maiwald, " Hack Proofing your network by Fundamentals of Network Security",3rd edition, 2012, Dreamtech press
3. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security - PrivateCommunication in a Public World", 2nd edition, 2002, Pearson/PHI.
4. Whitman, "Principles of Information Security", 4th edition, 2011, Thomson.
5. Robert Bragg, Mark Rhodes, "Network Security: The complete reference", 2nd edition, 2013, TMH.

Paper Code: MIS-603	L	P	C
Paper Title: Advanced Database Management and Information Retrieval	4	0	4

Introduction:
This course builds upon the introductory courses in database management system. It introduces students to a number of highly efficient information retrieval techniques for solving data driven computational problems across a variety of areas.

Course Objectives:
- To impart knowledge of computational and advanced concepts of Database Management System.
- To understand concepts about searching and sorting algorithms for homogenous and heterogenous database.
- To understand about writing optimized query requests and sequential approach in solving information retrieval problems with advanced Database Management Systems.

Prerequisite: Knowledge of fundamentals of DBMS, Query Optimization and Information Analysis.

Course Outcomes: After studying this course student will be able to:
CO1: Define advanced highly efficient database management systems and their characteristic properties.

CO2: Understand the concept of space and time complexity and compare the efficiency of information retrieval algorithms.

CO3: Apply the advanced highly efficient No-SQL database to store and query complex information.

CO4: Design and employ information flow algorithms to solve real world problems.

Pedagogy:
The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations, and quizzes. Students would be encouraged to develop an understanding of the subject. The use of ICT and web-based sources will be adopted.

UNIT 1
Relational Model and its difficulties, Object Oriented Databases, Need for complex data types, Object Relational Systems, Data Storage and File Storage, Overview of Physical storage Media, Magnetic Disks, RAID, Tertiary Storage, Storage Access, File Organization, Organization of records in files, Data Dictionary Storage.
(10 Hrs)

UNIT 2
Indexing &Hashing, B+ Tree Index Files, B-Tree Index Files, Dynamic & Static Hashing, Query Processing, Measures of Query cost, Selection Operation, Sorting, Join operation, evaluation of expressions, Query Optimization, estimating statistics of expression results, transformation of Relational Expressions, Choice of evaluation plans, Materialized Views.
(10 Hrs)

UNIT 3
Distributed Databases, Homogeneous & Heterogeneous Databases, Distributed Data Storage, Distributed Transactions and their commit protocols, Concurrency Control in Distributed DataBases, Distributed Query Processing, Decision Support Systems, Data mining & Warehousing, Decision Analysis & OLAP, Multimedia Databases, Mobile Data bases.
(10 Hrs)

UNIT 4
Conversion of Data to information, Information Retrieval, Information Retrieval Models, Classical & Non Classical Models of Informational Retrieval Relation. Matching, Knowledge-based Approaches, Conceptual Graphs, Applications, Information Extraction, Automatic Text Summarization Systems, Question Answering

Systems.

(10 Hrs)

References:

1. Data base System Concepts, 5th Edition, 2005, Silberchatz, Korth, Sudershan Tata MC Graw Hills Publishing.
2. Database Management Systems, Ramez Elmasri & Shamkant Navathe, 6th Edition, 2010, Pearson Education Asia.
3. Information Retrieval, D.A Grossman, O.Frieder, 2nd edition, 2004, Springer Publication
4. Database Management Systems, Raghu Ramakrishnan, J.Gerkhe, 3rd Edition, 2003, Tata MC Gran Hill Publications
5. Information Sorage & management –Storing, Managing & Protecting Digital Information- G. Somasundaram, Alok Srivastava, 1st edition, 2009, wiley Publishng Inc.
6. Information Storage & Retrieval Systems :- Theory & Implementation 1st edition, 2000, G.J. Kowalski, M.T. Maybury

Paper Code: MIS-605	L	P	C
Paper Title: Security Architecture for Computational Grids	4	0	4

Introduction:
The course aims to familiarize the students with the advanced concepts of Security Architecture of Computational Grid and its Security Life Cycle. The prominent attributes of a secure grid platform are data security, scalability, easy accessibility and sharing of data, zero maintenance, and easy data recovery. The course is designed for inculcating the research aptitude in graduate students, keeping the needs of Enterprise Grid Computing in Industry 4.0 and the academic research.

Course Objectives:
- To comprehend importance of Enterprise Grid Computing in Industry 4.0 and research
- To learn Grid Computing architecture, its Security Requirements and Virtualization
- To understand Grid Computing Life Cycle Management and Provisioning
- To identify current Security Challenges in Enterprise Grid Computing.

Prerequisite: Basic understanding of Operating System, Network Security, Parallel and Distributed Computing, Cluster Computing, Computer Organization and Architecture

Course Outcomes: Upon Successful completion the students will be able to:
CO1: Conceptual clarity in Grid and Cloud Computing architecture.

CO2: Conceptual understanding of Virtualization at different levels

CO3: Logical insight for comprehending the Security Primitives in Grid Computing.

CO4: A Research Case Study identifying Security Objectives and proposing a relevant solution

Pedagogy:
The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations, and quizzes. Students would be encouraged to develop an understanding of the subject. The use of ICT and web-based sources will be adopted

UNIT 1
Evolution of Grid computing, Characteristics of Secure System, Security Threats, Different Authentication Schemes Shared Secret Based Authentication, Public Key Based Authentication, Third Party Authentication Schemes, Different Integrity Schemes: Message Authentication Code (MAC), Keyed MAC, Standard Protocols : Public Key Infrastructure, Secure Socket Layer (SSL), Kerberos, IP Security (IPSec) Grid Security Issues, Architecture Related Issues, Infrastructure Related Issues, Management Related Issues,
(10 Hrs)

UNIT 2
Security Architecture in Grid Computing, Grid Information Security Architecture, Grid Security Infrastructure (GSI), Grid Authorization Systems, Different Access Control Models, Push vs. Pull Authorizations, Characteristics of Grid Authorization Systems, VO Level Authorization Systems, Resource Level Authorization Systems.
(10 Hrs)

UNIT 3
Service Level Security in Grid Systems, DoS Attacks and Countermeasures, QoS Violation Attacks and Countermeasures, Host Level Security, Data Protection Issue, Job Starvation Issue, Grid Network Security, Grid Credential Management Systems.
(10 Hrs)

UNIT 4

Managing Trust in the Grid, Definition of Trust, Reputation and Trust, Reputation-BasedTrust Management Systems, Policy-based Trust Management Systems, Grid Monitoring Systems, Case studies
(10 Hrs)

References:

1. Anirban Chakrabarti, Grid Computing Security, 1st edition, 2007, Springer
2. Yang Xiao, Security in Distributed, Grid, Mobile, and Pervasive Computing, 1stedition, 2007, Auerbach Publications.
3. Ian Foster, Carl Kesselman, The Grid: Blueprint for a new computing infrastructure,2nd edition, 2003, Morgan Kaufmann.
4. Barry Wilkinson, Grid Computing: Techniques and Applications, Chapman and Hall,2nd edition, 2011, CRC Press

Paper Code: MIS-607	L	P	C
Paper Title: Ethical Hacking	4	0	4

Introduction:

In lieu of the fact that most of the official work (private and public) is done through computer and computer systems, it is important to ensure security in such cases. All the necessary documents, information, and data are stored in a computer these days which should be protected with utmost care. Following this, there is a lot of demand for ethical hacking professionals to keep all the sensitive information protected from the hackers and develop new computer protecting the system. In this course, students will be taught how to find loopholes in the security system and how to report these threats to their owners and provide necessary solutions to protect the data and networks.

Course Objective:

- To acquire knowledge on about various security threats that exist and can be exploited
- To learn how bots, botnets, viruses, worms, Trojans, DOS attacks, DDOS attacks etc. work and are utilized for hacking
- To learn various ethical laws that exist in India and abroad and their significance
- To understand how loopholes and potential risks can be detected and learn wide variety of solutions that can be applied to protect data and networks.

Pre-requisite: Fundamentals of Information Security (MIS-105)

Course Outcome: On successful completion of this course, students will be able to:

CO1: Understand aspects of security, importance of data gathering, foot printing and system hacking.

CO2: Compare and analyze advanced concepts such as DDoS Attacks, Buffer Overflows, SQL Injection, Cross Site Scripting, Virus Creation

CO 3: Analyze and test ethical hacking tools and techniques

CO 4: Develop technical skills with in-depth knowledge of ethical hacking concepts that will assist them to take certification exam in future

UNIT 1

Introduction to Ethical Hacking, Hacking Laws, Foot-printing, Reconnaissance, Google hacking, Vulnerable sites, Using Google as a Proxy Server , Directory Listings , Locating Directory Listings, Finding Specific Directories, Finding Specific Files , Server Versioning, Scanning, System hacking Cycle, Enumeration, Cracking Password, Types of password attacks.

(10 Hrs)

UNIT 2

Trojans and Backdoors, Types of Trojans, Viruses, Worms, Sniffers, Types of Sniffing, Phishing, Methods of Phishing, Types of Phishing Attacks, Process of Phishing, Denial of Service, Classification of DoS attacks, System and Network Vulnerability.

(10 Hrs)

UNIT 3

Session Hijacking, Spoofing vs Hijacking, Session Hijacking Levels, Network Level Hijacking3 way handshake, IP Spoofing, RST Hijacking, TCP/IP Hijacking, Hacking web servers, Web Server Defacement, Proxy and Packet filtering, SQL Injection.

(10 Hrs)

UNIT 4

Authentication: HTTP, Basic, Digest, NTLM, Negotiate, Certificate based, Forms-bases,RSA SecurID Token, Biometrics, Hacking Wireless Networks, Bluetooth hacking, Mobile Phone Hacking, Tools for ethical hacking.

(10 Hrs)

References:

1. Ankit Fadia , " An unofficial guide to Ethical hacking", 2nd edition, 2006, Mc-Millan Publishing.
2. Ankit Kaufman, Nick Valenteen, " Official Certified Ethical HackerReview Guide", 1st edition, 2008, Sybex Publisher Fadia , "An Ethical guide to Hacking Mobile Phones", 1st edition, 2005, Mc-Millan Publishing

3. Michael T. Simpson, Kent Backman and James Corley, "Hands-On Ethical Hacking andNetwork Defense", 2nd edition, 2010, Cengage Learning
4. By Steven DeFino, Barry

Paper Code: MIS-609	L	P	C
Paper Title: Biometric Systems	4	0	4

Introduction:

This course will introduce students to fundamentals of biometric system security, cryptography, access control mechanisms, system attacks and defenses against them.

Course Objectives:

- Identify the basic security issues in the biometric system.
- Understand the concept of biometric security and issues and challenges associated with it.
- Analyze the vulnerabilities in any computing system and hence be able to design a security solution
- Evaluate various biometric security mechanisms used in real world

Course Outcomes: After studying this course students will be able to:

CO1: To understand the basic concept of Biometric Security and their mathematical models, encrypt and decrypt signatures using block ciphers and public key cryptosystems.

CO2: To identify well-known biometric signature generation and verification algorithms

CO3: To identify and classify biometric security threats and develop a robust security model to prevent, detect and recover from attacks.

CO4: To use and apply various security mechanisms to solve real world problems

Pedagogy:

The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations, and quizzes. Students would be encouraged to develop an understanding of the subject. The use of ICT and web-based sources will be adopted

UNIT 1

Introduction to biometric security, Verification, Identification, Methodology, Accuracy, False match rate, False non match rate, Failure to enroll rate, Derived metrics, Layered biometric solutions, Fingerprint identification, Scan, Features, Components, Operation, Finger Scan technologies, Algorithms used for interpretation.

(10 Hrs)

UNIT 2

Facial Scan, Features, Components, Operation, Facial Scan technologies, Iris Scan, Features, Components, Operation, Iris Scan technologies, Voice Scan, Features, Components, Operation, Voice Scan technologies, Strengths and weakness comparison.

(10 Hrs)

UNIT 3

Other physiological biometrics, Hand scan, Retina scan, AFIS (Automatic Finger Print Identification Systems), Behavioral Biometrics, Signature scan, Keystroke scan, Biometrics Application, Biometric Solution Matrix,. Biometric standards, BioAPI, BAPI

(10 Hrs)

UNIT 4

Bio privacy, Comparison of privacy factor in different biometrics technologies, Designing privacy sympathetic biometric systems, Biometric middleware, Biometrics for Network Security, Statistical measures of Biometrics, Biometric Transactions

(10 Hrs)

References:

1. Samir Nanavati, Michael Thieme, Raj Nanavati, " Biometrics, Identity Verification in a Networked World", 1st edition, 2002, WILEY, Dream Tech.

2. Paul Reid, " Biometrics for Network Security", 1st edition, 2003, Pearson Education.

3. John D. Woodward, " Wiley Dreamtech Biometrics, The Ultimate Reference", 1stedition, 2003, WILEY, Dream Tech

Paper Code: MIS-611	L	P	C
Paper Title: Enterprise Information Security Management	4	0	4

Introduction:

This course will introduce students to fundamentals of enterprise information security management, cryptography, access control mechanisms, system attacks and defenses against them.

Course Objectives:

- Identify the basic security issues in a hyperconnected enterprise world.
- Understand the concept of information security and challenges associated with enterprise security management.
- Analyze the vulnerabilities in any information system and hence be able to design a security solution for the enterprise under consideration
- Evaluate various security mechanisms used in real world enterprises.

Course Outcomes: After studying this course students will be able to:

CO1: To understand the basic concept of Information Security and their mathematical models, encrypt and decrypt messages using block ciphers and public key cryptosystems.

CO2: To identify well-known identity verification algorithms and apply them to sign and authenticate messages for an enterprise.

CO3: To identify and classify information security threats and develop a security model for the enterprise to prevent, detect and recover from security attacks.

CO4: To use and apply various security mechanisms to solve real world problems in an enterprise.

Pedagogy:

The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations, and quizzes. Students would be encouraged to develop an understanding of the subject. The use of ICT and web-based sources will be adopted

UNIT 1

Overview of 27000 family, Evolution of ISO/IEC 27000 family, BS 77pp Part 1 and Part 2, Internationalization, Standardization process, Committees and Working Groups ISO/IEC JTC 1/SC27. Standards supporting ISO /IEC 27000 ISMS family, BSI ISMS Guides

(10 Hrs)

UNIT 2

ISO/IEC 27000 Vocabulary, ISO/IEC 27003 Guidelines, ISO/IEC 27004 Security management Measurements, ISO/IEC 27005 Risk Management, ISO/IEC 27006Accreditation, Mangement of ISMS Risks, Importance of Risk Mangement, Steps of Risk management, Risk management is an ongoing Process, assets, threats and vulnerabilities, Implementation of ISMS, Deployment plan, Information Security Policy.

(10Hrs)

UNIT 3

Contingency Planning: Corporate Issues, Management responsibility, Disaster Life cycle, Definition of the Problem, Business Continuity Concerns, Planning, Characteristics of a sound plan, Cost Reduction Opportunity, Need for Cost effective solutions, back up, BusinessImpact analysis, Objective, critical issues, Awareness and Education, Mind Set, Education, Cost, Regilatory Agency reporting, Requirements, Implementation Strategy

(10Hrs)

UNIT-4

BIA Plan Development, Methodology, Plan requirement, Prevention, Recivery, Accounability, Audit, Plan Development steps, Key Tasks, Continuity Strategies, identifying vital records, Evaluating alternate operating strategies, Computer processing alternatives, account payable, accounts receivables, Documentation, Cost benefits, Corporate benefits, Guidelines for internal consultants and consulting firms.

(10Hrs)

References :

1. Edward Humphreys, "Implementing the ISO/IEC 27001 Information Security Management System Standard", 1st edition, 2007, Artech House publication.
2. Janet G. Butler , Poul Badura, "Contingency Planning and Disaster Recovery: Protecting Your Organization's Resources", 1st edition, 2007, Computer Technology Research Corpoaration Publication.
3. Kenneth N. Myers, "Manager's Guide to Contingency planning for Disasters: Protecting Vital Facilities and Critical Operations", 2nd edition , 2006, John wiley & Sons Publication.

Paper Code: MIS-613	L	P	C
Paper Title: E-Commerce and M-Commerce	4	0	4

Introduction:

The objective of this course is to enable students to understand, explore, and acquire a critical understanding of cyber frauds in e-commerce and m-commerce domains. Develop competencies for dealing with frauds and deceptions (confidence tricks, scams) and other cybercrimes. It also covers overview of Intellectual Property Right and Cyber Laws regarding e-commerce and m-commerce in Indian and global perspectives.

Course Objectives:

- To introduce the financial frauds in cyber world of e-commerce and m-commerce.
- To explain about the various facets of cyber-crimes on e-commerce platforms.
- To enhance the understanding of problems arising out of online transactions and provoke them to find solutions.
- To clarify the Intellectual Property issues in the cyber space and the growth and development of the law in this regard especially in Indian context.
- To educate about the regulation of cyber laws for e-commerce frauds.

Pre-requisites: Cyber Security Fundamentals, IT Act, Web 2.0 and Web 3.0

Course Outcomes: On successful completion of this course, students will be able to:

CO1: Describe the fundamentals of cyber security related laws in the context of e-commerce.

CO2: Regulate issues relating to various facets of cyber-crimes on e-commerce platform.

CO3: Comprehend the Intellectual Property issues regarding e-commerce in the cyber space.

CO4: Distinguish between different laws and regulations for e-commerce and m-commerce platforms at national and international level.

Pedagogy:

The teaching-learning of the course would be organized through lectures, tutorials, assignments, projects/ presentations, and quizzes. Students would be encouraged to develop an understanding of the subject. The use of ICT and web-based sources will be adopted

UNIT 1

Electronic Commerce Introduction:- Definition of E- Commerce ,Electronic commerce and Physical Commerce, Architectural framework, Impact of E-commerce on business, different type of ecommerce, some e-commerce scenario, Economic potential of electronic commerce, Advantages and Disadvantages , Incentives for engaging in electronic commerce, forces behind E-Commerce, Management responses to e-commerce and e-business and Online Commercial Solutions.

(10Hrs)

UNIT 2

E-business strategy: Introduction, Characteristics of e-Business, Business models, E- Business vs E-commerce, e-Business role and their challenges, e-business Requirements, impacts of e-business, Strategic positioning, Levels of e-business strategies, Strategic planning process, consequences of e-Business, Success factors for implementation of e- business strategies, CRM, MRP. **ERP:-** Introduction, need of ERP, Enterprise perspective Production Finance, Personnel disciplines and their relationship, Transiting environment, MIS Integration for disciplines, Information Workflow, Virtual Enterprise, Modules of ERP (HRD, Personnel Management, Training and Development, Skill Inventory Material Planning and Control, Inventory, Forecasting, Sales and Distribution, Finance, Resource Management in global scenario.

(10Hrs)

UNIT 3

Electronic Payment Methods: Overview, SET Protocol for credit card payment, E-cash, E-check, Micropayment system, Credit card, magnetic strip card,Smart cards, Electronics Data Interchange(basics, EDI versus Internet and EDI over Internet), E- Commerce Law.
Security Architecture:- Network structure , Internet and, Client Server Integrator System , Secure online and Offline transaction processing, Encryption techniques, Symmetric Encryption- Keys and data encryption standard, Triple encryption, Asymmetric encryption- Secret key encryption, public and private pair key encryption, Digital Signatures, Virtual Private Network, IPsec, Threats, Firewalls.

(10Hrs)

UNIT-4

M-Commerce: Introduction, Attributes, customer and provider views, Architecture, Infrastructure of m-commerce, Requirement of the m-commerce, characteristics, MobileInformation device, Mobile Computing Applications, Mobile wallet,Mobile payments, G- Cash, P2P, Mobile portals, Research issues in Mobile Commerce, Pros and Cons of m- commerce
Secure Transaction Processes: Wireless Application Protocol, Bluetooth, The role of emerging wireless LANs and 3G/4G wireless networks, personalized content management, Secure Socket Layer and Transport Layer Secure.

(10Hrs)

Text Books:

1. Ravi Kalakota, Andrew Winston, "Frontiers of Electronic Commerce", AddisonWesley.
2. E-Business Organizational and technical foundation (Michael P) Wiley Publication
3. "Enterprise resource Planning- Concepts and Practice",V.K. Garg and N. K. VenkitaKrishna, 1998, PHI.
4. Brian Mennecke and Troy Strader, "Mobile Commerce: Technology, Theory and Applications", Idea Group, 2003.
5. Nansi Shi, "Mobile Commerce Applications", IGI Global, 2004.
6. Dave Chaffey, "E-Business and E-Commerce Management", Third Edition, 2009,Pearson Education.

References:

1. E-Commerce Fundamentals and application (Henry Chan), 1st edition, 2001, Wiley publication
2. Bajaj and Nag, "E-Commerce the cutting edge of Business", 2nd edition, 2005, TMH
3. P. Loshin, John Vacca, "Electronic commerce", Firewall Media, 1st edition, 2005,New Delhi
4. E-Commerce Concepts, Models, Strategies- :- G.S.V.Murthy, 1st edition, 2002,Himalaya Publishing House

Paper Code: MIS-615	L	P	C
Paper Title: Information Security Audit and Security Management Lab	-	2	1

Experiments will be based on the subject Information Security Audit and Security Management

Paper Code: MIS-617	L	P	C
Paper Title: Advance Database Management and information retrieval Lab	-	2	1

Experiments will be based on the subject Advance Database Management and information retrieval

Paper Code: MIS-619	L	P	C
Paper Title: Minor Project	-	8	12

Paper Code: MIS-602	L	P	C
Paper Title: Dissertation	-	30	24

Paper Code: MIS-604	L	P	C
Paper Title: Seminar and Progress Report	-	4	4