AC 6.6.2012
Item No. 4.69

UNIVERSITY OF MUMBAI

Syllabus for the

M. E. (Information Technology)
Information Security subjects

(As per Credit Based Semester and Grading System with effect from the academic year 2012–2013)

Program Structure for
ME (Information Technology - in Information Security subjects)
Mumbai University

(With Effect from 2012-2013)

Semester I

Subject Code	Subject Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
ISC101	Advanced Web Technologies	04	--	--	04	--	--	04
ISC102	Computer Networking & Network Design	04	--	--	04	--	--	04
ISC103	Cryptography and PKI	04	--	--	04	--	--	04
ISE101X	Elective I	04	--	--	04	--	--	04
ISE102X	Elective II	04	--	--	04	--	--	04
ISL101	Laboratory I –Course Lab	--	02	--	--	01	--	01
ISL102	Laboratory II –Elective Lab	--	02	--	--	01	--	01
Total		**20**	**04**	**--**	**20**	**02**	**--**	**22**

Subject Code	Subject Name	Examination Scheme							
		Theory					Term Work	Pract. /oral	Total
		Internal Assessment			End Sem. Exam.	Exam Duration(thr)			
		Test1	Test 2	Avg.					
ISC101	Advanced Web Technologies	20	20	20	80	3	--	--	100
ISC102	Computer Networking & Network Design	20	20	20	80	3	--	--	100
ISC103	Cryptography and PKI	20	20	20	80	3	--	--	100
ISE101X	Elective I	20	20	20	80	3	--	--	100
ISE102X	Elective II	20	20	20	80	3	--	--	100
ISL101	Laboratory I –Course Lab	--	--	--	--		25	25	50
ISL102	Laboratory II –Elective Lab	--	--	--	--		25	25	50
Total		**100**	**100**	**100**	**400**		**50**	**50**	**600**

Semester II

Subject Code	Subject Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
ISC201	Network Security	04	--	--	04	--	--	04
ISC202	Application and Web Security	04	--	--	04	--	--	04
ISC203	Information Security & Risk Management	04	--	--	04	--	--	04
ISE201X	Elective III	04	--	--	04	--	--	04
ISE202X	Elective IV	04	--	--	04	--	--	04
ISL203	Laboratory III - Course Lab	--	02	--	--	01	--	01
ISL204	Laboratory IV - Elective Lab	--	02	--	--	01	--	01
Total		**20**	**04**	**--**	**20**	**02**	**--**	**22**

Subject Code	Subject Name	Examination Scheme							
		Theory							
		Internal Assessment			End Sem. Exam.	Exam Duration(hr)	Term Work	Pract. /oral	Total
		Test1	Test 2	Avg.					
ISC201	Network Security	20	20	20	80	3	--	--	100
ISC202	Application and Web Security	20	20	20	80	3	--	--	100
ISC203	Information Security & Risk Management	20	20	20	80	3	--	--	100
ISE201X	Elective III	20	20	20	80	3	--	--	100
ISE202X	Elective IV	20	20	20	80	3	--	--	100
ISL203	Laboratory III - Course Lab	--	--	--	--		25	25	50
ISL204	Laboratory IV - Elective Lab	--	--	--	--		25	25	50
Total		**100**	**100**	**100**	**400**		**50**	**50**	**600**

Semester III

Subject Code	Subject Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
ISS301	Seminar	--	06	--	--	03	--	03
ISD301	Dissertation I	--	24	--	--	12	--	12
Total		--	30	--	--	15	--	15

Subject Code	Subject Name	Examination Scheme						
		Theory				Term Work	Oral.	Total
		Internal Assessment			End Sem.Exam.			
		Test1	Test 2	Avg.				
ISS301	Seminar $	--	--	--	--	50	50	100
ISD301	Dissertation I *	--	--	--	--	100	--	100
Total		--	--	--	--	**150**	**50**	**200**

***Industrial Training of at least 75 days in Information security firm.**

$ **Seminar on Special topics on Information Security.**

Semester IV

Subject Code	Subject Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
ISD401	Dissertation II	--	30	--	--	15	--	15
Total		--	30	--	--	15	--	15

Subject Code	Subject Name	Examination Scheme						
		Theory				Term Work	Oral.	Total
		Internal Assessment			End Sem.Exam.			
		Test1	Test 2	Avg.				
ISD401	Dissertation II* $	--	--	--	--	100	100	200
Total		--	--	--	--	**100**	**100**	**200**

$ Industrial Training –II of 50 days in Information Security firm. Pre-Synopsis Dissertation Seminar on research project work.

* The Term Work and Oral of Dissertation II of Semester IV should be assessed jointly by the pair of
Internal and External Examiners

Note- The Contact Hours for the calculation of load of teacher are as follows
Seminar - 01 Hour / week / student
Desertation I and II - 02 Hour / week / student

Subject Code	Elective I	Subject Code	Elective II
ISE1011	Mobile and Pervasive Computing	ISE1021	Virtualization and Cloud Computing
ISE1012	Embedded Systems	ISE1022	Distributed Systems
ISE1013	Unix OS	ISE1023	Wireless Sensor Networks

Subject Code	Elective III	Subject Code	Elective IV
ISE2011	Law of Data Security and Investigations	ISE2021	Hacker Technique, Exploits and Incident handling
ISE2012	Mobile Commerce and Security	ISE2022	OS Security
ISE2013	IT Security Strategic Planning, Policy and Leadership	ISE2023	Advanced Computer Forensic Analysis

End Semester Examination: In all six questions to be set, each of 20 marks, out of these any four questions to be attempted by students. Each question will comprise of mixed questions from different units of the subjects.

Subject Code	Subject Name	Credits
ISC101	**Advanced Web Technologies**	**04**

Module	**Detailed content**	**Hours**
1	**HTML 5**: Fundamental Syntax and Semantics, Progressive Markup and Techniques, Forms, Native Audio and Video, Micro data and Custom data, Accessibility, Geolocation, Canvas, Advanced HTML 4 and Javascript	06
2	**XML:** What is XML, XML verses HTML, XML terminology, XML standards, XML syntax checking, The idea of markup, XML Structure, Organizing information in XML, Creating Well-formed XML, XML Namespaces. DTD- Introduction to DTD, Document Type Declaration, Element Type Declaration, Attribute Declaration, Conditional Section, Limitations of DTD, Introduction to Parser, Parsing approaches, JAXP, JAXP and SAX, JAXP and DOM. XML Schema, XML and CSS, XHTML Technological issues: XML processing, RDF processing, middleware technologies (CORBA, IIOP), RMI, and SOA	06
3	**Web Services:** Web services, Evolution and differences with Distributed computing, XML, WSDL, SOAP, UDDI, Transactions, Business Process Execution Language for Web Services, WS-Security and the Web services security specifications, WS-Reliable Messaging, WS-Policy, WS-Attachments. Web 2.0 technologies: search, content networks, user-generated content, blogging, social networking, social media, tagging, social bookmarking, rich Internet applications, RESTfulweb services,Resource Oriented Architecture, location-based services, Web 2.0 monetization and business models, Web mashups, future of the Web.	12
4	**Dynamic Web Programming :** Java Applets, Java script, JSP, JSTL, ASP, PHP, Servlets, Servlet Life cycle, C#, Component Technologies, Java beans, CORBA, Introduction to EJBs, JDBC, Secure Electronics Transactions over Web.	12
5	**AJAX Programming:** Introduction to Ajax: Ajax Design Basics, JavaScript, Blogs, Wikis, RSS feeds **Working with PHP and AJAX:** Process Client Requests, Accessing Files Using PHP **Working with JavaScript Object Notation (JSON):** Create Data in JSON Format, JSON parser, Implement JSON on the Server Side, **Implementing Security and Accessibility in AJAX Applications:** Secure AJAX Applications, Accessible Rich Internet Applications, **Developing Rich Internet Applications using AJAX techniques:** CSS, HTML, DOM, XMLHTTPRequest, JavaScript, PHP, AJAX as REST Client **Framework**: Django	12
6	**E-Commerce:** **An overview of E- Commerce-** Operating System Services, Developer Services, Data Services, Application Services, Store Services, Client Services. Types of E Commerce Solutions- Direct Marketing and Selling, Supply Chain Integration, Corporate Procurement, EDI. **Electronic Payment Systems-**Overview of Electronic Payment Systems, Cybercash (Customer to Merchant Payments, Peer to Peer Payments, Security). Smart Card (Card Types, Closed or Open Security, Privacy, Card Costs, Non Card Costs), Electronic Banking, Electronic Fund	08

	Transfers, Session Management	
7	**Introduction to Web Mining:** Web Content Mining, Web Structure Mining: primary web browsing (crawling, spidering), link topology analysis, PageRank, HITS methods Web Usage Mining: mining for user behavior on the web, internet marketing Search engines optimization and limitations, Introduction to the semantic web,Taxonomies and ontologies for advanced web applications: Ontology modeling, Languages for representing ontologies on the web, Rules and inferences	04

References:

1.HTML 5 Black Book: Kogent Learning solutions
2. AJAX Black book: Kogent Learning Solutions
3. E-commerce: Fundamental and Applications, Wiley, Henry Chan

4. John Davies, Rudi Studer, and Paul Warren John , "Semantic Web Technologies: Trends and Research in Ontology-based Systems", Wiley & Son's
5. Jeffrey C. Jackson , "Web Technologies: A Computer Science Perspective", Prentice Hall , 2006
6. Beginning XML 5th Edition Wiley – Joe Fawcett.
7. Beginning Java Server Pages – Wrox Press - Vivek Chopra.
8. Deitel H.M. and P. J. Deitel, "Internet & World Wide Web. How to Program", 4/e, Prentice Hall
9. Paul J.Deitel & Associates, Inc. Deitel; Harvey M.Deitel & Associates, Inc. Deitel, "Developer Series AJAX, Rich Internet Applications, and Web Development for Programmers", Prentice Hall
10. Kenneth C. Laudon, Carol Guerico Traver , "E-Commerce Business.Technology. Society", Pearson Education.
11. Beginning AJAX with PHP From Novice to Professional Apress, Lee Babin
12. P.T.Joseph, S.J., "E-Commerce An Indian Perspective", PHI.
13. Bing Liu, "Web Data Mining: Exploring Hyperlinks, Contents, and Usage Data", Second Edition, July 2011, Springer

Assessment:

Internal: Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students.Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ISC102	**Computer Network and Design**	**04**

Module	**Detailed content**	**Hours**
1	Internet Protocol (Configuration of DMZ Servers):Detail working of DNS, HTTP, FTP and SMTP/POP - Configuration of DNS, Web , FTP, Mail Server. Internet Protocol – Understanding working of TCP, UDP, IP , ARP, ICMP	8
2.	Introduction to Network analysis, Architecture and Design Process Model for Network analysis, Architecture, and Design	4
3	Requirement Analysis: User Requirement, Device Requirement, Network Requirement, Performance Requirement, Financial Requirement, Enterprise Requirement	4
4.	Network Architecture: Component Architecture –Routing, Network Management, Performance, Security. Architectural models: topological, flow model, Functional model Addressing And Routing Architecture, Network Management Architecture, Performance Architecture Borderless Network Architecture, Dara centre/ Virtualization Architecture	8
5.	Network Design: Designing the network topology and solutions-Top down Approach Network Structure Model: Hierarchical Network Model, Enterprise wide network Architecture model- Enterprise Edge Area, E-commerce, Internet Connectivity, remote, enterprise branch and enterprise Data center module. High Availability Network Services- Workstation to Router redundancy and LAN High Availability protocols, Route, Server Redundancy, Load Balancing., link Media Redundancy.	10
6.	Enterprise LAN Design: Ethernet Design Rule. 100 Mbps Fast Ethernet Design rules, gigabit Ethernet Design Rules, 10 Gigabit Ethernet Design rules, 10GE Media types Understanding Working of Repeater, hub, Bridge, routers, Layer2/3 Switch Campus LAN Design Best Practice Server Farm Design, data centre Design Campus LAN QoS consideration Multicast Trafic Consideration	10
7.	Data Centre Design Architecture, enterprise DC Infrastructure, Virtualization Technologies. Type of Virtualization	4
8	Wireless LAN Design	2
9	WAN Technologies: WAN Transport Technologies, WAN Design Methodology, Traditional WAN Technologies, Remote Access Network Design, VPN Network Design, WAN Backup Design	2
10	Internet routing Protocol: IP Address Classful and CIDR, Private and Public IP address and NAT guidelines, IP Subnet Design, Routing Protocol, RIP, OSPF, Interior and Exterior Routing Protocol.BGP, IPV6 and IPV6 Routing Protocol	4
11	Netowrk Management Prtocols: SNMP v1,v2,v3, RMON2,Netflow,	2

	Syslog	
12	**Network Analysis** Queue Models: Arrival Processes, Service time Queuing System, Clarification M/M/1 Queue and basic multiplexer model M/M/I state probabilities and notion of stability, effect of scale on performance, average packet delay via network, The M/G.I model, service time variability and delay M/M/I system. Erlang Formulas and M/M/c/e system priority queue system	2

References:

1. Netowrk Analysis, Architecture, and Design 3rd Edition, Morgan Kaufman, James D.
2. CCDA Cisco official Guide
3. Behrouz A. Forouzan: Data Communications and Networking, 4th Edition, Tata McGraw-Hill, 2006.
4. Advanced Computer network; Ambavade, dreamtech
5. William Stallings: Data and Computer Communication, 8th Edition, Pearson Education, 2007.
6. Larry L. Peterson and Bruce S. David: Computer Networks – A Systems Approach, 4th Edition, Elsevier, 2007.
7. Wayne Tomasi: Introduction to Data Communications and Networking, Pearson Education, 2005.
8. Tamara's Network+ - Guide Networks, Second edition, published by Thomson Learning, 2002.
9. James F. Kuross, Keith W. Ross, "Computer Networking, A Top-Down Approach Featuring the Internet", Third Edition, Addison Wesley, 2004.
10. Nader F. Mir, "Computer and Communication Networks", Pearson Education, 2007 3. Comer, "Computer Networks and Internets with Internet Applications", Fourth Edition,Pearson Education, 2005.
11. Andrew S. Tanenbaum, "Computer Networks", Sixth Edition, 2003, PHI Learning.
12. William Stallings, "Data and Computer Communication", Sixth Edition, Pearson Education, 2000

Assessment:

Internal: Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students.Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ISC103	**Cryptography and PKI**	**04**

Module	Detailed content	Hours
1	**Cryptography: Concepts and Techniques:** Introduction, Security Trends, Model for Network Security, Plain Text and Cipher Text, Substitution Techniques, Transposition Techniques, Encryption and Decryption, Symmetric and Asymmetric Key Cryptography, Stegnography, Key Range and Key Size, Possible Types of Attacks	10
2	**Symmetric Key Algorithms:** DES,3DES,AES, IDEA, RC4, RC5, Confidentiality using symmetric encryption.	10
3	**Introduction to Number Theory:** Prime Numbers, Fermat's and Euler's Theorems, Testing for Primality, The Chinese Remainder Theorem, Discrete Logarithms **Public- Key Cryptography and RSA:** Principles of Public-Key Cryptosystems, RSA, Key Management, Diffie-Helman Key Exchange, Elliptic Curve Arithmetic, Elliptic Curve Cryptography.	10
4	**Message Authentication and Hash Functions:** Authentication Requirements, Authentication Functions, MAC, Hash Functions, Security of Hash Functions and MACs, SHA, HMAC	10
5	**Digital Signatures and Public Key Infrastructure (PKI):** Digital Signatures, Authentication Protocols, DSS, Authentication Applications: Kerberos, X.509 Authentication Service Digital Certificates, Private Key Management, PKI Trust Models, Public Key Cryptography Standards, Revocation, Directories and PKI, PKIX and Security.	10
6	**Elliptic Curves:** The Addition Law, Elliptic curve Mod p, Factoring with Elliptic Curves, Elliptic Curve Cryptosystems	
6	**Cryptography in Java, .NET and Operating Systems:** Cryptographic Solutions using Java, Cryptographic Solutions using Microsoft .NET Framework, Cryptographic Toolkits, Security and Operating Systems, Database Security.	10

References:

1. Information Security Principal and Practice: Mark stamp, Wiley
2. Cryptography and security, wiley, Shyamala, harini
3. Stallings, W., "Cryptography and Network Security", Fourth Edition, Pearson
4. Introduction to Cryptography with coding Theory, Pearson,WadenTrappe
5. Forouzan B., "Cryptography and Network Security", Second Edition, Tata McGraw Hill
6. Bernard Menezes, "Network Security and Cryptography", Cengage Learning.
7. Charlie Kaufman, Radia Perlman and mike speciner "Network security, private communication in a public world" , Second Edition, Pearson

Assessment: Internal: Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ISL 101	**Open Source Laboratory1**	**01**

Module	**Detailed content**	**Lab. Sessions**
1	Installation of Linux OS in Dual boot Environment Basic Linux Command Practice	01
2	Basic Linux Networking commands Multiple IP address to Single LAN Adding Static Route in Routing table Configure Linux Server as a Router and configure IP Forwarding	01
3	Configuration of Linux as FTP and Web server	01
4	Configuration of Linux as DNS Server	01
5	Configuration of Linux as a Firewall, SNAT and DNAT	01
6	IT Infrastructure monitoring using NEGIOS	01
7.	Virtualization on Linux	01
8.	Working With LaTeX	01
9.	Mini Project –Configuration of Private cloud using Open Source technology	04

Assessment:

Reference book:

1) Linux Lab - Dreamtech Publication
2) Fedora Linux SPD, O'reily publication
3) Learning Negios3.0, Packt publication
4) Xen Virtualization, Packt publication
5) Eucaliptus /beginer's guide

End Semester Examination: Practical/Oral examination is to be conducted by pair of internal and external examiners

Subject Code	Subject Name	Credits
ISL102	**Laboratory II –Elective Lab**	**01**

Module	**Detailed content**	**Lab. Sessions**
1	**1 Mini Project based on any one of the selected elective subject.**	24

Modality and Assessment:

1. Each mini project assignment will be done by individual student. The Faculty teaching elective subject will be required to propose and evaluate the respective mini projects. These will be essentially hands-on practical and not theory / research review types of projects
2. **End Semester Examination:** Practical/Oral examination is to be conducted by pair of internal and external examiners

Subject Code	Subject Name	Credits
ISE1011	**Mobile and Pervasive Computing**	**04**

Module	**Detailed content**	**Hours**
1	**Mobile Networks:** Cellular Wireless Networks, GSM: Architecture, Protocols, Connection Establishment, Frequency Allocation, Routing, Mobility Management, Security, GPRS.	10
2	**Wireless Networks:** Issues and challenges of Wireless networks – Location management, Resource management, Routing, Power management, Security.Wireless Media Access Techniques – ALOHA , CSMA , Wireless LAN , MAN , IEEE 802.11 (a,b,e,f,g,h,i),,Bluetooth, Wi-Fi, WiMAX Wireless routing protocols – Mobile IP, IPv4, IPv6, Wireless TCP. Protocols for 3G & 4G cellular networks – IMT – 2000, UMTS, CDMA2000, Mobility management and handover Technologies, All-IP based cellular network	10
3	**Routing:** Mobile IP, DHCP, AdHoc, Proactive and Reactive Routing Protocols, Multicast Routing. Mobile networks – Ad-hoc networks, Ad-hoc routing, Sensor networks, Peer-Peer networks. Mobile routing protocols – DSR, AODV, Reactive routing, Location aided routing. Mobility models – Entity based, Group mobility, Random Way-Point mobility model.	08
4	**Transport And Application Layers:** Mobile TCP, WAP, Architecture, WWW Programming Model, WDP, WTLS, WTP, WSP, WAE, WTA Architecture, WML, WMLScripts.	10
5	**Pervasive Computing:** Pervasive computing infrastructure, applications, Device Technology, Hardware, Human-machine Interfaces, Biometrics, and Operating systems, Device Connectivity, Protocols, Security, and Device Management, Pervasive Web Application architecture, Access from PCs and PDAs - Access via WAP	10
6	**Mobile Software:** Software adaptation and OS support. Resource sharing. OS for embedded devices: PalmOS, WindowsCE, embedded Linux, WAP/WML, J2ME, Windows Mobile and .Net Framework, BREW. Mobile agents, Resource and service discovery, Mobile Java, Mobile Grid and collaborative processing with Jini. Android Development	08
7.	Security Challenges in Pervasive computing.	04

References:

1. Jochen Schiller, “Mobile Communications”, PHI.
2. Jochen Burkhardt, Pervasive Computing: Technology and Architecture of Mobile Internet Applications, Addison-Wesley Professional; 3rd edition, 2007
3. Frank Adelstein, Sandeep KS Gupta, Golden Richard, Fundamentals of Mobile and Pervasive Computing,McGraw-Hill
4. Debashis Saha, Networking Infrastructure for Pervasive Computing: Enabling Technologies, Kluwer Academic Publisher, Springer; First edition, 2002
5. Introduction to Wireless and Mobile Systems by Agrawal and Zeng, Brooks/ Cole (Thomson Learning.
6. Uwe Hansmann, Lothar Merk, Martin S. Nicklons and Thomas Stober, Principles of Mobile Computing, Springer, New York, 2003

7. R. Riggs, A. Taivalsaari, M. VandenBrink, Programming Wireless Devices with Java2 Platform, Micro Edition, Addison-Wesley, 2001.

Assessment:

Internal:	Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.
End Semester Examination:	Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students.Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ISE1012	**Embedded Systems**	**04**

Module	**Detailed content**	**Hours**
1	**Embedded Architecture :** Embedded Computers, Characteristics of Embedded Computing Applications, Challenges in Embedded Computing system design, Embedded system design process- Requirements, Specification, Architectural Design, Designing Hardware and Software Components, System Integration, Formalism for System Design- Structural Description, Behavioral Description, Design Example: Model Train Controller	10
2	**Embedded Processor And Computing Platform :** ARM processor- processor and memory organization, Data operations, Flow of Control, SHARC processor- Memory organization, Data operations, Flow of Control, parallelism with instructions, CPU Bus configuration, ARM Bus, SHARC Bus, Memory devices, Input/output devices, Component interfacing, designing with microprocessor development and debugging, Design Example : Alarm Clock.	10
3	**Networks :** Distributed Embedded Architecture- Hardware and Software Architectures, Networks for embedded systems- I2C, CAN Bus, SHARC link ports, ethernet, Myrinet, Internet, Network-Based design- Communication Analysis, system performance Analysis, Hardware platform design, Allocation and scheduling, Design Example: Elevator Controller. **Resource Management/scheduling paradigms:** static priorities, static schedules, dynamic scheduling, best effort current best practice in scheduling	10
4	**Interfacing of Microprocessor to Peripherals** Buses & protocols, ISA, EISA, PCI, ARM, I 2C, CAN, FIREWIRE, USB. Wireless protocol: Bluetooth and IEEE 802.11, 802.15, 802.16.: Introduction, features, area of applications. Interface for IRDA, SMART card and WEB enabling. Case study of emerging Serial and Parallel Bus standards (USB 2.0, IEEE1394,PCI, Compact PCI, PCI-X). **Target Devices** Different types of ASICS: FPGA, CPLD architectures.	10
5	**Real Time Operating Systems (RTOS):** OS Services, goals and structures, features, characteristics, process management, memory management, File system organization and implementation, I/O subsystem, Real time task models and performance metrics, Real time features of Vx works, WIN CE, QNX , Nucleus, RT Linux. Network OS, Inter Process communication of Processes, Tasks and Threads , OS Security Issues	08
6	**Programming Concept and Embedded Programming** Programming in assembly Language and High level language C /C++ and/OR Java. Compilers and Cross Compilers, Source Code Engineering Tools, Program modeling concept in single and multiprocessor system software, Software Engineering Practices in the Embedded Software Development Process. Real world issues: blocking, unpredictability, interrupts, caching,	08
7	**Security:** Network Embedded Systems and Resource constraints, Embedded Security Design, KISS Principle, Chossing and optimizing Cryptographic Algorithm for resource-constrained systems, Embedded Application Security	4

References:

1. Wayne Wolf, Computers as Components: Principles of Embedded Computing System Design, Morgan Kaufman Publishers, 2001.
2. Vahid F., Givargies T., “Embedded Systems Design”, John WILEY X SONS 2002
3. Raj Kamal, “Embedded Systems- Architecture, Programming and Design”, TMH 2003
4. Barr M., “RTOS”.
5. Smith M., “Application specific Integrated circuits”.
6 Liu, “Real-Time systems”, Pearson Ed. Asia
7. D. Gajski, F. Vahid, S. Narayan, and J. Gong. Specification and Design of Embedded Systems, PEARSON Education. Jorgan
8. Practical embedded System security, timothy, newness publication

Assessment:

Internal: Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students.Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ISE1013	**Unix OS**	**04**

Module	**Detailed content**	**Hours**
1	**Unix System Overview:** Unix Architecture, Logging in, Files and Directories, Input and Output, Programs and Processes, Error Handling, User Identification, Signals, Time Values, System Calls and Library Functions	04
2	**System Data Files and Information:** Password file, Shadow passwords, Group file, Supplementary Group IDs, Implementation Differences, Login Accounting, System Identification, Time and Date routines	08
3	**Thread Control:** Thread Limits, Thread attributes, synchronization attributes, Reentrancy, Thread-specific data, Cancel options, signals, threads and I/O, threads and fork **Daemon Processes:** Daemon characteristics, coding rules, Error logging, Single-instance daemons, Daemon conventions	10
4	**Advanced I/O:** Nonblocking I/O, Record Locking, Streams, I/O Multiplexing, Asynchronous I/O, Related functions, Memory mapped I/O	10
5	**Interprocess Communication:** Pipes, FIFO, Semaphores, Message Queues, Shared Memory **Network IPC: Sockets** Socket Descriptors, Addressing, Connection Establishment, Data Transfer, Socket Options, Out-of-band data, Nonblocking and Asynchronous I/O **Advanced IPC:** streams-based pipes, Unix Domain Sockets, Passing File Descriptors	10
6	**Terminal I/O:** Special Input characters, Getting and setting terminal attributes, Terminal option flags, sty command, Baud rate functions, Line Control functions, Terminal Identification, canonical, noncanonical mode, Terminal window size, termcap, terminfo, curses	08
7	**Security in Unix OS:** Monitoring The System, Account Security, File system security, network Security, Major service Security	10

References:

1. W. Richard Stevens, UNIX Network Programming, Volume 1: Networking API's, Sockets, and XTI, 2nd edition
2. Maurice Bach, “The Design of the UNIX Operating System
3. Uresh Vahalia, “UNIX Internals: The New Frontiers
4. Arnold Robbins, “Unix in a Nutshell”, O’Reilly
5. Eleen Frisch, “Essential System Administration: Tools and Techniques for Linux and Unix Administration”, O’Reilly

Assessment:

Internal: Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other

is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students.Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ISE1021	**Virtualization and Cloud Computing**	**04**

Module	**Detailed content**	**Hours**
1	Virtualization: What is Virtualization, Virtualization theory, VMDK File Structure, Advantages and Disadvantages of machine being a file, CPU Virtualization, Memory Virtualization, Interrupt Management VMFS file system, Storage Virtualization, Network Virtualization, Virtual machine and Security issues	10
2	VMware Virtualization Technologies : ESX internals Microsoft –Windows Virtualization Technologies :Hyper-V Xen and KVM Hypervisor. QEMU , SUN's VirtualBox	08
3	Introduction to cloud computing, cloud architecture and service models, the economics and benefits of cloud computing, horizontal/vertical scaling, thin client, multimedia content distribution, multiprocessor and virtualization, distributed storage, security and federation/presence/identity/privacy in cloud computing, disaster recovery,	10
4	free cloud services and open source software, and example commercial cloud services Cloud Computing and Virtualization Host Clusters Storage Virtualization VM clusters Cloud security fundamentals, Vulnerability assessment tool for cloud, Privacy and Security in cloud **Cloud computing security architecture:** Architectural Considerations-General Issues, Trusted Cloud computing, Secure Execution Environments and Communications, Micro-architectures; Identity Management and Access control-Identity management, Access control, Autonomic Security **Cloud computing security challenges**: Virtualization security management- virtual threats, VM Security Recommendations, VM-Specific Security techniques, Secure Execution Environments and Communications in cloud.	12
5	Cloud Platform Architectures o Amazon AWS o Microsoft Azure o Google App Engine o Google MapReduce / Yahoo Hadoop o Eucalyptus, Nimbus, OpenStack	12
6	Issues in cloud computing, Implementing real time application over cloud platform Issues in Intercloud environments, QOS Issues in Cloud, Dependability, data migration, streaming in Cloud. Quality of Service (QoS) monitoring in a Cloud computing environment. Cloud Middleware. Mobile Cloud Computing. Inter Cloud issues. A grid of clouds, Sky computing, load balancing, resource optimization, resource dynamic reconfiguration, Monitoring in Cloud	08

Reference Book:

1. Cloud Computing for Dummies by Judith Hurwitz, R.Bloor, M.Kanfman, F.Halper (Wiley India Edition)
2. Enterprise Cloud Computing by Gautam Shroff,Cambridge
3. Cloud Security by Ronald Krutz and Russell Dean Vines, Wiley-India
4. Google Apps by Scott Granneman,Pearson
5. Cloud Security & Privacy by Tim Malhar, S.Kumaraswammy, S.Latif (SPD,O'REILLY)
6. Cloud Computing : A Practical Approach, Antohy T Velte, et.al McGraw Hill,
7. Cloud Computing Bible by Barrie Sosinsky, Wiley India
8. Stefano Ferretti et.al.QoS–aware Clouds", 2010 IEEE 3rd International Conference on Cloud Computing
9. Virtualization for Dummies : , Wiley India.

Assessment:

Internal: Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students.Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ISE1022	**Distributed Systems**	**04**

Module	**Detailed content**	**Hours**
1	Introduction to Distributed systems-examples of distributed systems, challenges-architectural models- fundamental models - Introduction to interprocess communications-external data representation and marshalling-client server communication-group communication – Case study: IPC in UNIX , Case Study: RMI, CORBA**.** Advances in Distributed Systems	08
2	DISTRIBUTED OBJECTS AND FILE SYSTEM Introduction - Communication between distributed objects - Remote procedure call - Events and notifications - Java RMI case Study - Introduction to DFS - File service architecture - Sun network file system - Introduction to Name Services- Name services and DNS - Directory and directory services	08
3	DISTRIBUTED OPERATING SYSTEM SUPPORT The operating system layer – Protection - Process and threads - Communication and invocation - Operating system architecture - Introduction to time and global states - Clocks, Events and Process states - Synchronizing physical clocks - Logical time and logical clocks - Global states - Distributed debugging – Distributed mutual exclusion.	10
4	TRANSACTION AND CONCURRENCY CONTROL – DISTRIBUTED TRANSACTIONS Transactions – Nested transaction – Locks - Optimistic concurrency control - Timestamp ordering - Comparison of methods for concurrency control - Introduction to distributed transactions - Flat and nested distributed transactions - Atomic commit protocols - Concurrency control in distributed transactions - Distributed deadlocks - Transaction recovery	10
5	SECURITY AND REPLICATION Overview of security techniques - Cryptographic algorithms – Digital signatures - Cryptography pragmatics – Replication - System model and group communications – Fault tolerant services – Highly available services – Transactions with replicated data Issues in Designing Distributed System and role of middleware in Distributed System	08
6	**SOA:** Basic SOA Definition, Overview of SOA, SOA and Web Services, Service Oriented Grid, SOA Design and Development, Advantages and Future of SOA SOA support in J2EE – Java API for XML-based web services (JAX-WS) - Java architecture for XML binding (JAXB) – Java API for XML Registries (JAXR) - Java API for XML based RPC (JAX-RPC)- Web Services Interoperability Technologies (WSIT) - SOA support in .NET – Common Language Runtime - ASP.NET web forms – ASP.NET web services – Web Services Enhancements	08

	(WSE)	
7.	SOA Security: New approach to security for SOA, Extending SOAP for Security, Claiming and verifying identity with passwords, WS-security standards, Kerberos with WS-security, Encrypting SOAP messages, XML signatures, Implementing security as a service.	8

Reference Books:

1. Distributed O.S Concepts and Design , P.K.Sinha, PHI
2.Advanced concepts in Operating Systems , Mukesh Singhal & N.G.Shivaratri, TMH
3. Distributed Computing , Sunita Mahajan, Seema Shah, OXFORD University Press
41. Distributed System Principles and Paradigms , Andrew S. Tanenbaum, 2nd edition , PHI
5. Distributed Systems , Colouris , 3rd Edition
6. Thomas Erl, "SOA Principles of Service Design "(The Prentice Hall Service-Oriented Computing Series from Thomas Erl), 2005.
7. Newcomer, Lomow, "Understanding SOA with Web Services", Pearson Education, 2005.
8.SOA Security, Ramarao, Manning

Assessment:

Internal: Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students.Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ISE1023	**Wireless Sensor Network**	**04**

Module	**Detailed content**	**Hours**
1	OVERVIEW OF WIRELESS SENSOR NETWORKS Challenges for Wireless Sensor Networks, Enabling Technologies For Wireless Sensor Networks	08
2	ARCHITECTURES Single-Node Architecture - Hardware Components, Energy Consumption of Sensor Nodes , Operating Systems and Execution Environments, Network Architecture - Sensor Network Scenarios, Optimization Goals and Figures of Merit, Gateway Concepts.	08
3	NETWORKING SENSORS Physical Layer and Transceiver Design Considerations, MAC Protocols for Wireless Sensor Networks, Low Duty Cycle Protocols And Wakeup Concepts - S-MAC , The Mediation Device Protocol, Wakeup Radio Concepts, Address and Name Management, Assignment of MAC Addresses, Routing Protocols- Energy-Efficient Routing, Geographic Routing.	10
4	INFRASTRUCTURE ESTABLISHMENT Topology Control , Clustering, Time Synchronization, Localization and Positioning, Sensor Tasking and Control.	10
5	SENSOR NETWORK PLATFORMS AND TOOLS Sensor Node Hardware – Berkeley Motes, Programming Challenges, Node-level software platforms, Node-level Simulators, State-centric programming.	08
6	Querying, data collection and processing, Collaborative information processing and group connectivity. Target tracking, localization, and identity management. Future research Challenges	04
9	Security in Wireless Sensor network: Vulnerability and attack in WSN, Key management in WSN, WSN Link Layer Security Framework, Secure Routing in WSN, Secure Data aggregation, Privacy protection, Intrusion detection techniques and Remote attestation identification in WSN	12

REFERENCE BOOKS:

1. Holger Karl & Andreas Willig, " Protocols And Architectures for Wireless Sensor Networks" , John Wiley, 2005.
2. Feng Zhao & Leonidas J. Guibas, “Wireless Sensor Networks- An Information Processing Approach", Elsevier, 2007.
3. Kazem Sohraby, Daniel Minoli, & Taieb Znati, “Wireless Sensor Networks- Technology, Protocols, And Applications”, John Wiley, 2007.
4. Wireless Sensor network Security, Javier Lopez IOS press
5. Anna Hac, “Wireless Sensor Network Designs”, John Wiley, 2003.

6. Azzedine Boukerche, Handbook of Algorithms for Wireless Networking and Mobile Computing, Chapman & Hall/CRC, 2006

7. Mohammad Ilyas and Imad Mahgoub, Handbook of Sensor Networks: Compact Wireless and Wired sensing systems, CRC Press, 2005.

8. Nirupama Bulusu and Sanjay Jha, Wireless Sensor Networks : A systems perspective, Artech House, August 2005.

9. Jr., Edgar H. Callaway, Wireless Sensor Networks : Architecture and Protocols, Auerbach, 2003.

10. C.S. Raghavendra, Krishna M. Sivalingam and Taieb Znati, Wireless Sensor Networks, Springer, 2005.

Assessment:

Internal: Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students.Minimum 80% syllabus should be covered in question papers of end semester examination.

SEMESTER II

Subject Code	Subject Name	Credits
ISC201	**Network Security**	**04**

Module	**Detailed content**	**Hours**
1	**Security Problem in TCP/IP Protocol Suite:** Identification of Security issues in Ethernet, ARP, IP, TCP, Application and Routing protocols.	06
2	**Security Models:** Military and civil security, vulnerability and threat models, End-end security (COMSEC), link encryption (TRANSEC), compartments. Privacy. Authentication. Denial of service. Nonrepudiation. Issues in multi-level secure systems. Internet security models: IPv4/IPv6 encapsulation header	04
3	**Security at Network Layer** Routing algorithm vulnerabilities: route and sequence number spoofing, instability and resonance effects. Information hiding: DMZ networks, route aggregation and segregation ICMP redirect hazard: denial of service. ARP hazard: phantom sources, ARP explosions and slow links. Defending against Chernobyl packets and meltdown. Fragmentation vulnerabilities and remedies: (ICMP Echo overrun) **IPSec:** IP Security Overview, IP Security Architecture, Security Associations, Security Association Database, Security Policy Database, Tunnel and Transport mode, AH and ESP, IP and IPv6, Encapsulating Security Payload, Internet Key Exchange	10
4	**Security at Transport Layer: SSL and TLS** Secure network infrastructure services: DNS, NTP, SNMP, SSL Architecture, SSL/TLS Basic Protocol, SSL Message Formats, Session Resumption, Computing the keys, Client Authentication, PKI as deployed by SSL, Version Numbers, Negotiating Cipher Suites, Negotiating Compression Methods, Exportability, Encoding, Mobile systems: Address Export and re-use. Session key management: Blind-key cryptosystems (NTP).	12
5	**Security at Application Layer: PGP, S/MIMIE** E-mail security, PGP, PEM, S/MIME, Secure binding of multimedia streams, Secure RTP. Secure RSVP.	10
6	**Firewalls and IDS** Firewalls: Network partitioning, firewall platforms, partitioning models and methods, Secure SNMP, Secure routing interoperability: virtual networks (DARTnet/CAIRN). Transparent and opaque network services. Source masking and hidden channels. IDS, Honeypots, Honey nets,	06
7	**Wireless Network Security:** Introduction, How wifi works, WEP, Technique of hacking wireless network, countermeasure	04
8	**Network Packet analysis**: Packet analysis and Packet sniffing in Hub and Switched environment, Analysis of packet for security i.e Sync Scan, OS Fingerprinting	04
9	NOS Security issues: Windows and Linux environment	04

References:

1. Stallings, W., “Cryptography and Network Security: Theory and Practice”, Second Edition, John Wiley
2. “Charles P. Pfleeger “Security in computing”, Pearson Education
3. Stalling W., “ Network Security Essentials”, Pearson
4. Garfinkel S., Spafford G., “Practical Unix and Internet Security”, O'Reilly
5. Blacharski D., “Network Security in a Mixed Environment”
6. Practical Packet Analysis: Using Wireshark to Solve Real-Word Network problems by Chris Sanders

Assessment:

Internal:	Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.
End Semester Examination:	Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students.Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ISC202	**Application and Web Security**	**04**

Module	**Detailed content**	**Hours**
1	Introduction to Web applications Cookies , Session , Headers , Same-origin , Terminology Tools	02
2	Gathering Information On Target Finding Owner, IP Addresses And Email Addresses WHOIS tools DNS queries and zone transfers Using Nslookup Infrastructure Fingerprinting The Webserver Fingerprinting Webserver Modules Typical HTTP Services Ports Fingerprinting Frameworks And Applications Fingerprinting Third-Party Add-Ons Fingerprinting Custom Applications Mapping The Attack Surface Enumerating Resources Crawling The Website Finding Hidden Files Finding Back Up And Source Code Files Enumerating users accounts with Burp Proxy Relevant Information Through Misconfigurations Directory Listing Log And Configuration Files Google Hacking	08
3	Vulnerability Assessment Vulnerability Assessment vs Penetration testing Assessing vulnerabilities with using open source tools Browsing anonymously HTTP Proxies, Verifying proxy anonymity ,HTTP_VIA /HTTP_X_FORWARDED_FOR , Tor Network Tunneling for anonymity , SSH Tunneling Cleaning traces ,Cleaning the event log	10
4	Understanding OWASP top 10	2
4	Cross site scripting What it is—Basics Anatomy of a XSS exploitation The three types of XSS Reflected XSS Persistent XSS DOM-based XSS Finding XSS Finding XSS in PHP code XSS Exploitation XSS, Browsers and same origin policy Real world attacks Cookie stealing through XSS Defacement Advanced phishing attacks	6

5	Introduction to SQL Injection How dangerous is a SQL Injection , How SQL Injection works How to find SQL Injections , How to find SQL Injections Finding Blind Sql Injections , SQL Injection Exploitation Exploiting INBAND (Union) SQL Injections Exploiting Error Based SQL Injection, Dumping database data Reading remote file system, Accessing the remote network Exploiting Blind SQL injection, Optimized Blind SQL injection Time Based Blind SQL Injection Tools Sqlmap, BSQL Hacker, Pangolin Tools taxonomy	08
6	Introduction Session attacks , HTTP Session Fixation Finding HTTP Session Fixation, Preventing HTTP Session Fixation CSRF Finding CSRF , Exploiting CSRF , Preventing CSRF File inclusion vulnerabilities , Local File Inclusion , Remote File Inclusion Web 2.0 Attacks How Ajax works , Defeating httpOnly—XST & Ajax Dissecting Ajax API's, Reverse engineering Ajax applications logic Exposed administrative functions	08
7	Application Security: Understanding SOA for EAI, WS-Security Standards	04
8	Application Security basics: Reverse Engineering, Attack vectors, input Validation, Secure SDLC- Data classification, Secure requirement-Secure Architecture. Factors in Developing An Application Security Program-Policies, procedures, baselines and guidelines, ROI on application security	04
9	Software Engineering and Security: Security Challenge in software engineering, Secure Software development methodologies, Waterfall model with security, Comprehensive Lightweight Application Security Process, Extreme Programming and Security, Aspect-Oriented Programming and Security	04
10	Database Security and Auditing: Database Application Security Model, Administration of Users, Profiles, Password policy, Privileges and roles, Virtual Private Database, Database Auditing model	04

References:

1. The Web Application Hacker's handbook, Defydd Stuttard, Wiley Publishing
2. Professional Pen Testing for Web application, Andres andreu, wrox press
3. Carlos Serrao, Vicente Aguilera, Fabio Cerullo, "Web Application Security" Springer; 1st Edition
4. Joel Scambray, Vincent Liu , Caleb Sima ,"Hacking exposed", McGraw-Hill; 3rd Edition (October, 2010)
5. OReilly Web Security Privacy and Commerce 2nd Edition 2011
6. Software Security Theory Programming and Practice, Richard sinn, cengage Learning
7. Database Security and Auditing, Hassan, Cengage Learning

Assessment:

Internal: Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students.Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ISC203	**Information security and risk management**	**04**

Module	**Detailed content**	**Hours**
1	Introduction to assessing Network Vulnerabilities: type and procedure of network vulnerability assessment	08
2	Principles of Security: Information Classification, Policy framework, role based security in an organization	04
3	Risk Assessment: Laws, Mandates and Regulations, Risk assessment best practices, Risk assessment best practice.	10
4	Risk Assessment Methodologies: Defense –in depth approach, risk analysis, Asset valuation approach, Quantitative and Qualitative risk-assessment approaches. Scoping the project, Understanding the attacker.	10
5	Performing the Assessment: Vulnerability scan and Exploitation: Internet Host and network enumeration, IP network Scanning, Assessing Remote Information Services, Assessing Web servers, Assessing Web Applications, Assessing Remote Maintenance Services, Assessing Database services, Assessing Windows Networking Services, Assessing Email services.	12
6	Open source tools used for Assessment and Evaluation, and exploitation framework	10
7	Final Report Preparation and Post Assessment Activists	06

Reference books:

1. Network Security assessment, Chris McNab, O'reilly
2. Inside Network Security Assessment, Michael Gregg, Pearson
3. Security in Computing, fourth Edition, Charles Pfleeger, Pearson
4. The Security Risk Assessment Handbook: Douglas LanDoll, Auerbach Publication.
5. Nina Godbole, "Information Systems Security", Wiley
6. Cyber Security: Sunit Belapur, Wiley
7. Whitman & Mattord. Management of Information Security. Thomson Course Technology (2004). ISBN: 0-619-21515-1

Assessment:

Internal: Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students.Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ISL203	**Open Source Laboratory III**	**01**

Module	**Detailed content**	**Lab. Sessions**
1	- Working With Wireshark in Hub Environment for Packet Sniffing - Packet sniffing in Switch Environment	02
2	- Vulnerability Scanning technique using NESSUS	01
3	- REST Architecture :Web Mash up using PHP	02
4	- Vesrion Control – Software Configuration Management in Linux	01
5	- Customization of Linux Live CD	01
6	- Working with LVM in Linux	01
7.	- Exploring atleast two linux based web designing tools (Bluefish, Komodo etc.)	02
8.	- Exploring Content Management system on Linux	02

Reference Book:

1. linux Network Security. SPD
2. CMS design using PHP and Jquery , PACT
3. Wordpress MU beginners guide , PACT

Assessment:

End Semester Examination: Practical/Oral examination is to be conducted by pair of internal and external examiners

Subject Code	Subject Name	Credits
ISL204	**Laboratory IV –Elective Lab**	**01**

Module	**Detailed content**	**Lab. Sessions**
1	**1 Mini Project based on any one of the selected elective subject.**	24

Modality and Assessment:

1. Each mini project assignment will be done by individual student. The Faculty teaching elective subject will be required to propose and evaluate the respective mini projects. These will be essentially hands-on practical and not theory / research review types of projects
2. **End Semester Examination:** Practical/Oral examination is to be conducted by pair of internal and external examiners

Subject Code	Subject Name	Credits
NSE2011	**Law of Data Security and Investigations**	**04**

Module	Detailed content	Hours
1	**Introduction:** Laws, Investigation and Ethics: Cyber Crime, Information Security and Law, Types & overview of Cyber Crimes, Cyber Law Issues in E-Business Management Overview of Indian IT Act, Ethical Issues in Intellectual property rights, Copy Right, Patents, Data privacy and protection, Domain Name, Software piracy, Plagiarism, Issues in ethical hacking.	08
2	**Fundamentals of IT Security Law and Policy:** Security Policy, Privacy Notice & Privacy Laws, Computer Crime Laws, Intellectual Property, Non-Disclosure Agreements and Terms of Use, Honeypots & Entrapment, Active Defenses, Hacking Back	04
3	**E-Records, E-Discovery and Business Law:** Vicarious Liability, E-Discovery, Records Retention, Destruction, Email Retention, Forensics, Privacy Policies, Evidence Law, Signatures	08
4	**Contracting for Data Security and Other Technology:** Click Through Agreements, Contract Formation, Battle of the Forms, Liability, Breach, Bonds, Assent, Warranty, Remedies, Liens, Ownership Issues, Subpoenas, Documentation, Audits, Exceptions, Maintenance, Termination, Escrow, Investigations, Competition, Disputes, Non-Disclosure	10
5	**The Law of IT Compliance: How to conduct investigations:** Cooperation with investigations, Numerous Examples of Fraud (Post-Mordems), SOX, Securities Fraud, Federal Sentencing Guidelines, Codes of Ethics, Hotlines, Reporting, Whistleblowing, Employee Monitoring, Entrapment, Raids & Seizures	10
6	**Applying Law to Emerging Dangers: Cyber Defense** Sony Root Kit Case Study, Crisis Communications, Choicepoint Case Study, Relationship with Law Enforcement, TJX Case Study, Publicity, Safely Monitoring Threats w/o Incurring Liability, Factors Mitigating Legal Risk, Public Accountability, Political Diplomacy, Strategic Legal Procedures, Competitive Boundaries	10

References:

1. Sood,"Cyber Laws Simplified", Mc Graw Hill
2. Anthony Reyes, "Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors"
3. Marcia P. Miceli, "Whistle-Blowing in Organizations",

Assessment:

Internal: Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students.Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ISE2012	**Mobile Commerce and Security**	**04**

Module	**Detailed content**	**Hours**
1	**Introduction to m-commerce :** Infrastructure Of M–Commerce, Types Of Mobile Commerce Services, Technologies Of Wireless Business, Benefits And Limitations, Support, Mobile Marketing & Advertisement, Non–Internet Applications In M–Commerce, Wireless/Wired Commerce Comparisons. Emerging applications, different players in m-commerce, m-commerce life cycle, M-commerce business models, The m-commerce value chain, M-commerce information system functional model. Case study	08
2	**M-commerce technology:** Mobile clients: Types: mobile phones, PDAs, laptop computers, vehicle-mounted devices, hybrid devices Device limitations: considerations for user interface and application design Device location technology: GPS, triangulation Mobile client software, Mobile device operating systems, Micro browsers Mobile device communications protocols: WAP, i-Mode, Mobile device page description languages, Mobile device application software	08
3	**Mobile Commerce: Theory And Applications:** The Ecology Of Mobile Commerce, The Wireless Application Protocol, Mobile Business Services, Mobile Portal, Factors Influencing The Adoption Of Mobile Gaming Services, Mobile Data Technologies And Small Business Adoption And Diffusion, E–Commerce In The Automotive Industry, Location–Based Services: Criteria For Adoption And Solution Deployment, The Role Of Mobile Advertising In Building A Brand, Mobile financial services, Mobile proactive service management, Mobile auction, Mobile entertainment, Mobile distance education, Mobile information access, Vehicular mobile commerce, Telematics	10
4	**Management of mobile commerce services :** Content development and distribution to hand-held devices, content caching, pricing of mobile commerce services The emerging issues in mobile commerce : The role of emerging wireless LANs and 3G/4G wireless networks, personalized content management, implementation challenges in m-commerce, futuristic m-commerce services	08
5	**M-commerce trust, security, and payment:** Trust in m-commerce, Encryption, Authentication, confidentiality, integrity, and non-repudiation, Mobile payment **M-commerce issues:** Technology issues, Mobile client issues, Communications infrastructure issues, Other technology issues, Application issues, Global m-commerce issues Security Issues: Introduction, Information security, Security techniques and Algorithms, security Protocols, Public Key Infrastructure, Trust, Security Models, Security Frameworks for Mobile Environment	10
6	**Business–To–Business Mobile E– Commerce:** Enterprise Enablement , Email And Messaging, Field Force Automation (Insurance, Real Estate, Maintenance, Healthcare), Field Sales Support (Content Access, Inventory), Asset Tracking And Maintenance/Management, Remote IT Support, Customer Retention (B2c Services, Financial, Special Deals), Warehouse Automation, Security.	08

References:

1. Mobile Commerce: Technology, Theory and Applications by Brian Mennecke and Troy J. Strader, Idea Group Publishing

2. Mobile Commerce and Applications, Upkar Varshney, A tutorial at IEEE International Conference on Wireless Communications (WCNC)

3. Mobile Commerce: Frameworks, Applications and Networking Support, ACM/Kluwer Journal on Mobile Networks and Applications (MONET), June 2002 (Upkar Varshney and Ron Vetter)

4. Location-based Mobile Commerce Services, ACM Transactions on Internet Technology, August 2003, (Upkar Varshney)

5. Mobile Commerce: An Emerging Frontier, IEEE Computer, Oct 2000 (Varshney and others)

6. Ravi Kalakota, B.Andrew Whinston, "Frontiers of Electronic Commerce", Pearson Education, 2003.

7. P. J. Louis, "M-Commerce Crash Course", McGraw- Hill Companies February 2001.

8. Paul May, "Mobile Commerce: Opportunities, Applications, and Technologies Of Wireless Business" Cambridge University Press March 2001.

Assessment:

Internal: Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students.Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ISE2013	**IT Security Strategic Planning, Policy and Leadership**	**04**

Module	**Detailed content**	**Hours**
1	Strategic Planning Process: Value of strategic planning, implementation of strategic planning, overall planning process and strategic matrix model, horizon analysis, visioning, environmental scans (SWOT, PEST, Porter's 5 forces), historical analysis, mission, vision, and value statements, planning process core, candidate initiatives, the prioritization process, resource and IT change management in planning, how to build the roadmap, setting up assessments, Institutional assessment, revising the plan.	08
2	Information Security Management: Risks and attacks in an information system environment, Requirements on confidentiality, integrity, availability, authentication, non-repudiation, Information Security Technologies, Types of Information Security policies and their hierarchy, relationship to business process, Security organizations, Risk assessment, different approaches, Information Security Management Standards, Audit policy, Protecting Computer-Held Information Systems.	08
3	**Legal Issues:** **Computer crimes, Disk Protection, Intellectual property, E-commerce law, Data Protection issues, Information Security Audits.**	08
4	**Security Policy Development:** positive and negative tone, consistency of policy bullets, the role of policy, awareness and training, the SMART approach to policy development and assessment, ISMS as governing policy, Policy versus procedure, Organizational Assumptions, Beliefs and Values (ABVs), Relationship of mission statement to policy, Organizational culture	08
5	Security Policy Assessment: Using the principles of psychology to implement policy, How policy protects people, organizations and information, Case study, the process to handle a new risk (Sexting), Policy header components and how to use them, Issue-specific policies, Behavior related polices, acceptable use, ethics, Warning banners, Policy development process, Policy review	10
6	Management and Leadership Skills: Leadership building blocks, Coaching & training, Change management, Team development, Motivating, Developing the vision, Leadership development, Building competencies, Importance of communication, Self-direction, Brainstorming, Relationship building, Teamwork concepts, Leader qualities, Leadership benefits	08

References:

1. http://iscanotes.com/MAY%202011/ISCA_Chap9_May-11.pdf
2. http://www.sans.org
3. Robert M. Grant, "Contemporary Strategy Analysis: Concepts, Techniques, Applications", 5th Edition
4. Mickie Krause Nozaki, "Information Security Management Handbook", 4th Edition
5. Michael E. Whitman, **"**Management Of Information Security",
6. http://www.sans.org/reading_room/whitepapers/policyissues/security-policy-roadmap-process-creating-security-policies_494
7. Information Security Policies Made Easy, 10th Edition
8. http://net.educause.edu/ir/library/pdf/pub7008i.pdf

9. Marlene Caroselli, “Leadership Skills for Managers”
10. http://managementhelp.org/freebusinesstraining/leadership.htm

Assessment:

Internal:	Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.
End Semester Examination:	Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students.Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ISE2021	**Hacker Technique, Exploits and Incident handling**	**04**

Module	**Detailed content**	**Hours**
1	Incident Handling Overview and preparation – Incident Handling Phase 2 identification, Incident Handling phase 3 containment Incident Handling: Recovering and improving capabilities, Type of incidents	06
2	Hacking Methodology : Enumeration, Scanning, Gaining Access , Maintaining access, Clearing Tracks	06
3	Reconnaissance , Scanning Host discovery, Network devices discovery, service discovery	08
4	Backdoors and Trojan horses , Buffer Overflows	04
5	Covering Tracks : Networks and Systems	06
6	Denial of Service Attacks, Exploiting System using Netcat	08
7	Format String Attacks	04
8	IP address Spoofing, Network sniffing	06
9	Password Attacks, rootkits	04
10	Session Hijacking and Defenses	04
11	Virtual Machine Attacks, Web application attacks, Worms, Bots & Bot-nets	04

Reference Books:

1. Jon Erickson, Hacking: The Art of Exploitation, Second Edition
2. Hacker Techniques, Exploits & Incident Handling (Security 504) http://www.sans.org/training/description.php?mid=40
3. Brain Hatch, Hacking Linux Exposed, 3rd edition Hacking Linux Exposed, 3rd edition

Assessment:

Internal: Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
NSE2022	**OS Security**	**04**

Module	Detailed content	Hours
1	**Introduction:** Secure Os, Security Goals, Trust Model, Threat Model, Access Control Fundamentals: Protection system, Lampson's Access Matrix, Mandatory protection system	06
2	**Multics:** Fundamentals, multics protection system models, multics reference model, multics security, multics vulnerability analysis	08
3	**Security in ordinary operating system:** Unix security, windows security Verifiable security goals: Information flow, information flow secrecy models, information flow integrity model, the challenges of trusted process, covert channels	10
4	**Security Kernels:** The Security Kernels, secure communications processor - Scomp, Gemini secure OS. Securing commercial OS: Retrofitting security into a commercial OS, History Retrofitting commercial OS, Commercial era, microkernel era, unix era- IX, domain and type enforcement.	10
5	**Case study:** Solaris Extensions Trusted extensions, access control, Solaris compatibility, trusted extensions, mediations process rights management, role based access control, trusted extensions, networking trusted extensions, multilevel services, trusted extensions administration. **Case study: Building secure OS for Linux:** Linux security modules, security enhanced Linux.	08
6	**Secure capability system:** Capability security, challenges in capability systems, building secure capability systems. Secure Virtual Systems: Separation kernels, VAX VMM security machine systems. Orange Book.	08

References:

1. Trent Jaeger, Operating system security, Morgan & Claypool Publishers, 2008
2. Guide to Operating system security , Thomson
3. Andrew S Tanenbaum , Modern Operating systems
4. Secure Operating Systems. John Mitchell. Multics-Orange Book-Claremont

Assessment:

Internal: Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students.Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ISE2023	**Advanced Computer Forensic Analysis**	**04**

Module	Detailed content	Hours
1	**Overview of computer Forensics Technology**- Introduction to computer forensics, use of forensics in law enforcement, employment proceedings, computer Forensics services. Types of computer Forensics Technology- Military, law, spyware and Adware, Biometrics security systems.	06
2	**Types of Computer Forensics systems** Internet security, IDS, Firewall, Public key, net privacy systems, vendor and computer Forensics services.	08
3	**Computer Forensics evidence and capture** Data recovery, evidence collection and data seizure, duplication and preservation of digital evidence, computer image verification and authentication	10
4	**Computer Forensics Analysis** Discovery of electronic evidence- electronic document discovery, identification of data- Time keeping, forensic identification and analysis of technical surveillance devices. Reconstructing fast events	10
5	**The information warfare Arsenal and Tactics of terrorists and Rogues** The Terrorist profile, the dark world of the cyber underground, new tools of terrorism, information warfare, Arsenal and Tactics of private companies.	08
6	**Civilian casualties** The violation of privacy during information words. The individual exposed. Advanced computer Forensics systems and future directions- advanced encryption, hacking, advanced trackers, case studies.	08

Reference BOOKS:

1. Cyber Security : Belapure: wiley
2. By John R. Vacca Computer forensics: computer crime scene investigation, Volume 1
3. EnCase Computer Forensics . Sybex
4. Computer Forensics: Incident Response Essentials, Warren G. Kruse II & Jay G. Heiser
5. Computer Forensics & Privacy, Michael Caloyannides
6. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, edited by Albert J. Marcella Jr. & Robert S. Greenfield
7. Handbook of Computer Crime Investigation, edited by Eoghan Casey

Assessment:

Internal: Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students.Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
ISD301	**Seminar**	**03**

Guidelines for Seminar

- Seminar should be based on thrust areas in Information Security.
- Students should do literature survey and identify the topic of seminar and finalize in consultation with Guide/Supervisor. Students should use multiple literatures (at least 10 papers from Refereed Journals) and understand the topic and compile the report in standard format and present in front of Panel of Examiners. (pair of Internal and External examiners appointed by the University of Mumbai)
- **Seminar should be assessed based on following points**
  - Quality of Literature survey and Novelty in the topic
  - Relevance to the specialization
  - Understanding of the topic
  - Quality of Written and Oral Presentation

IMPORTANT NOTE :

1. Assessment of Seminar will be carried out by a pair of Internal and External examiner. The external examiner should be selected from approved panel of examiners for Seminar by University of Mumbai, OR faculty from Premier Educational Institutions /Research Organizations such as IIT, NIT, BARC, TIFR, DRDO, etc. OR a person having minimum Post-Graduate qualification with at least five years' experience in Industries.

2. Literature survey in case of seminar is based on the broader area of interest in recent developments and for dissertation it should be focused mainly on identified problem.

3. At least 4-5 hours of course on Research Methodology should be conducted which includes Literature Survey, Problems Identification, Analysis and Interpretation of Results and Technical Paper Writing in the beginning of 3rd Semester.

Subject Code	Subject Name	Credits
ISD301 / ISD401	**Dissertation (I and II)**	**12 + 15**

Guidelines for Dissertation

- Students should do literature survey and identify the problem for Dissertation and finalize in consultation with Guide/Supervisor. Students should use multiple literatures and understand the problem. Students should attempt solution to the problem by analytical/simulation/experimental methods. The solution to be validated with proper justification and compile the report in standard format.

Guidelines for Assessment of Dissertation I

- Dissertation I should be assessed based on following points
-
  - Quality of Literature survey and Novelty in the problem
  - Clarity of Problem definition and Feasibility of problem solution
  - Relevance to the specialization
  - Clarity of objective and scope
- Dissertation I should be assessed through a presentation by a panel of Internal examiners appointed by the Head of the Department/Institute of respective Programme.

Guidelines for Assessment of Dissertation II

- Dissertation II should be assessed based on following points
  - Quality of Literature survey and Novelty in the problem
  - Clarity of Problem definition and Feasibility of problem solution
  - Relevance to the specialization or current Research / Industrial trends
  - Clarity of objective and scope
  - Quality of work attempted
  - Validation of results
  - Quality of Written and Oral Presentation
- Dissertation II should be assessed through a presentation jointly by Internal and External Examiners appointed by the University of Mumbai
- Students should publish at least one paper based on the work in reputed International / National Conference (desirably in Refereed Journal)