PRESERVING AND RECOVERING DIGITAL EVIDENCE
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – II

Subject Code	**16SFC21**	**IA Marks**	20
Number of Lecture Hours/Week	04	**Exam Marks**	80
Total Number of Lecture Hours	50	**Exam Hours**	3

CREDITS – 04

Course objectives: This course will enable students to

- Different laws related to computer crime
- How to Secure Digital Evidences
- To Understand Investigation Process

Module 1	**Teaching Hours**
Digital evidence and computer crime: history and terminals of computer crime investigation, technology and law, the investigate process, investigate reconstruction, modus operandi, motive and technology, digital evidence in the court room.	**10**
Module 2	
Computer basics for digital investigators: applying forensic science to computers, forensic examination of windows systems, forensic examination of Unix systems, forensic examination of Macintosh systems, and forensic examination of handheld devices.	**10**
Module 3	
Networks basics for digital investigators: applying forensic science to networks, digital evidence on physical and datalink layers, digital evidence on network and transport layers, digital evidence on the internet.	**10**
Module 4	
Investigating computer intrusions, investigating cyber stalking, digital evidence as alibi.	**10**
Module 5	
Handling the digital crime scene, digital evidence examination guidelines.	**10**

Course Outcomes

The students should be able to:

- Explain Digital evidence and computer crime and Laws
- Illustrate the Computer basics for digital investigators w.r.t Unix and Macintosh systems
- Illustrate the Networks basics for digital investigators
- Able to Investigating computer intrusions and cyber stalking
- Explain the basic concepts how to Handling the digital crime scene, digital evidence examination guidelines

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Digital Evidence and Computer Crime Forensic science, Computers and Internet -Eoghan Casey Elsevier Academic Press, Second Edition.

Reference Books:

1. A Electronic Discovery and Digital Evidence in a Nut Shell-Shira A scheindlin, Daniel J Capra The Sedona Conference, Academic Press, Third Edition (No where available).
2. Digital Forensic for Network, Internet, and Cloud Computing A forensic evidence guide for moving Targets and Data' – Terrence V.Lillard, Glint P.Garrison, Craig A..Schiller, James Stee Syngress.

3. The Best Damn Cybercrime and Digital Forensics Book Period' [Paperback] Jack Wiles , Anthony Reyes , Jesse Varsalone, Syngress Edition, 2007.

OPERATING SYSTEM SECURITY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – II

Subject Code	**16SFC22**	**IA Marks**	20
Number of Lecture Hours/Week	04	**Exam Marks**	80
Total Number of Lecture Hours	50	**Exam Hours**	3

CREDITS – 04

Course objectives: This course will enable students to

- Define fundamental concepts and mechanisms for enforcing security in OS.
- Build a secure OS by exploring the early work in OS.
- Illustrate formal security goals and variety of security models proposed for development of secure operating systems.
- Explain architectures of various secure OS and retrofitting security feature on existing commercial OS's.
- Analyze variety of approaches applied to the development & extension services for securing operating systems.

Module 1	**Teaching Hours**
Introduction: Secure Os, Security Goals, Trust Model, Threat Model, Access Control. Fundamentals: Protection system, Lampson's Access Matrix, Mandatory protection system.	**10**
Module 2	
Multics: Fundamentals, multics protection system models, multics reference model, multics security, multics vulnerability analysis.	**10**
Module 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**
Module 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**
Module 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.	**10**
Course Outcomes	
The students should be able to:	

- Gain the knowledge of fundamental concepts and mechanisms for enforcing security in OS.
- Analyze how to build a secure OS by exploring the early work in OS.
- Identify and compare different formal security goals and variety of security models proposed for development of secure operating systems.
- Interpret architectures of various secure OS and retrofitting security feature on existing commercial OS's.
- Shows variety of approaches applied to the development & extension services for securing operating systems.

Question paper pattern:
The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Trent Jaeger, Operating system security, Morgan & Claypool Publishers, 2008

Reference Books:

1. Michael Palmer, Guide to Operating system Security Thomson
2. Andrew S Tanenbaum, Modern Operating systems, 3rd Edition
3. Secure Operating Systems. John Mitchell. Multics-Orange Book-Claremont.

SECURED PROGRAMMING
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – II

Subject Code	**14SFC23**	**IA Marks**	20
Number of Lecture Hours/Week	04	**Exam Marks**	80
Total Number of Lecture Hours	50	**Exam Hours**	3

CREDITS – 04

Course objectives: This course will enable students to

- Explain the basics of secure programming.
- Demonstrate the most frequent programming errors leading to software vulnerabilities.
- Identify and analyze security problems in software
- Illustrate how to protect against security threats and software vulnerabilities

Module 1	**Teaching Hours**
Validating all input & Designing secure programs: Command line and environment variables, File descriptors, names and contents, Web based application inputs, Locale selection and character encoding, Filtering represent able URIs, preventing cross site malicious input content, Forbidding HTTP Input to perform non-queries. Good security design principles: Securing the interface, separation of data and control. Minimize privileges: Granted, time, modules, resources etc, Using chroot, careful use of setuid/setgid, Safe default value and load initializations. Avoid race conditions, Trustworthy channels and trusted path, Avoiding semantics and algorithmic complexity attacks.	**10**
Module 2	
Declarations and Initializations and Expressions: Declare objects with appropriate storage durations, Identifier declaration with conflict linkage classifications, Using	**10**

correct syntax for declaring flexible array member, Avoiding information leakage in structure padding, Incompatible declarations of same function or object. Dependence on evaluation order for side effects: Reading uninitialized memory and dereferencing null pointers, Modifying objects with temporary lifetime, Accessing variable through (pointer) incompatible type, Modifying constant objects and comparing padding data.	
Module 3	
Integers and Floating Points: Wrapping of unsigned integers, Integer conversions and misrepresented data, Integer overflow and divide by zero errors, Shifting of negative numbers, Using correct integer precisions, Pointer conversion to integer and vice versa. Floating point values for counters: Domain and range errors in math functions, Floating point conversions and preserving precision.	**10**
Module 4	
Arrays , Strings and Memory Management: Out of bounds subscripts and valid length arrays, Comparing array pointers, Pointer arithmetic for non-array object, scaled integer, Modifying string literals, Space allocation for strings (Null terminator), Casting large integers as unsigned chars, Narrow and wide character strings and functions. Accessing freed memory: Freeing dynamically allocated memory, Computing memory allocation for an object, Copying structures containing flexible array members, Modifying object alignment by using realloc.	**10**
Module 5	
I/O, Signals and Error Handing: User input and format strings, Opening an pre-opened file, Performing device operations appropriate for files, Dealing with EOF, WEOF, Copying FILE object, Careful use of fgets, fgetws, getc, putc, putwc. Use of fsetops and fgetops, Accessing closed files. Using asynchronous safe functions and signal handlers: Shared objects and signal handlers, Using signal() within interruptible signal handlers, Returning computation exception signal handler. Using errno: check and set, Depending upon indeterminate values of errno, Handling standard library errors.	**10**
Course Outcomes	
The students should be able to: • How to respond to security alerts which identifies software issues • Identify possible security programming errors • Define methodology for security testing and use appropriate tools in its implementation • Apply new security-enhanced programming models and tools	
Question paper pattern: The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.	
Text Books 1. Robert C. Seacord, "The CERT ® C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems, Second Edition", Addison Wesley Professional, April 2014 2. David Wheeler, "Secure Programming for Linux and Unix HowTo", Linux Documentation project, Aug 2004	
Reference Books: 1. JohnViega, Matt Messier, "Secure Programming Cookbook for C and C++", O'Reilly Media, 1st Edition, July 2003.	

CYBER LAWS AND ETHICS
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – II

Subject Code	**14SFC24**	**IA Marks**	20
Number of Lecture Hours/Week	04	**Exam Marks**	80
Total Number of Lecture Hours	50	**Exam Hours**	3

CREDITS – 04

Course objectives: This course will enable students to

- Explain the Indian legal system, ITA 2000/2008, cyber security and related legal issues.
- Explain the Types of contract law, Digital signature and related legal issues, the Intellectual property rights, types of cyber properties, copyright law, patent and related legal issues, the types of cyber crimes and related legal issues
- Explain cyber crime investigation and prosecution in depth.

Module 1	**Teaching Hours**
Introduction to Cyber Law and Cyber Ethics: Introduction to Cyber Crimes and Ethical Issues in IT**,** Basic concepts of Law and Information Security, overview of Information Security obligations under ITA 2008, Privacy and data protection concepts.	**10**
Module 2	
Law of Contracts applicable for Cyber Space transactions: introduction to Contract law, legal recognition of Electronic Documents, Authentication of Electronic Documents, Authentication of Electronic Documents, Cyber space contracts, Resolution of Contractual disputes, stamping of Contractual document.	**10**
Module 3	
Intellectual Property Law for Cyber Space: Concept of Virtual assests, nature of Intellectual property, Trademarks and domain names, copyright law, law of patents.	**10**
Module 4	
Intellectual Property Law for Cyber Space: Concept of Virtual assests, nature of Intellectual property, Trademarks and domain names, copyright law, law of patents.	**10**
Module 5	
Miscellaneous Issues in Cyber Crimes and Cyber Security: Cyber Crime Investigation and Prosecution, Digital evidence and Cyber forensics, Jurisdiction issues, Information Security Management in corporate Sector.	**10**

Course Outcomes

The students should be able to:

- Describe the Indian legal system, ITA 2000/2008, cyber security and related legal issues.
- Classify the Types of contract law, Digital signature , related legal issues, the Intellectual property rights, types of cyber properties, copyright law, patent and related legal issues, the types of cyber crimes and related legal issues, the types of cyber crimes and related legal issues.
- Interpret the cyber crime investigation and prosecution in depth.

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Cyber Laws for Engineers, Naavi, Ujvala Consultants Pvt Ltd, 2010.

Reference Books:

1. Deborah G Johnson, Computer Ethics, Pearson Education Pub., ISBN : 81-7758-593-2.
2. Earnest A. Kallman, J.P Grillo, Ethical Decision making and Information Technology: An Introduction with Cases, McGraw Hill Pub.
3. John W. Rittinghouse, William M. Hancock, Cyber security Operations Handbook, Elsevier Pub.
4. Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, 2nd Edition, Cengage Learning Pub.
5. Randy Weaver, Dawn Weaver, Network Infrastructure Security, Cengage Learning Pub

BIOMETRIC SECURITY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – II

Subject Code	**14SFC251**	**IA Marks**	20
Number of Lecture Hours/Week	03	**Exam Marks**	80
Total Number of Lecture Hours	40	**Exam Hours**	3

CREDITS – 03

Course objectives: This course will enable students to

- Explain the principles used in biometrics algorithms and systems and most important biometric approaches.
- Illustrate the capability to select a suitable algorithm / system for a given application context (e.g. physical access control)
- Demonstrate a good understanding of the complex relationships between biometric systems and environmental conditions (e.g. illumination, pose variations etc.) and their impact on biometric performance.
- Illustrate of data privacy principles and the impact on the design and configuration of biometric systems.

Module 1	**Teaching Hours**

Biometrics: Introduction, benefits of biometrics over traditional authentication systems, benefits of biometrics in identification systems, selecting a biometric for a system, Applications, Key biometric terms and processes, biometric matching methods, Accuracy inbiometric systems.	**8 Hours**
Module 2	
Physiological Biometric Technologies: Fingerprints: Technical description, characteristics, Competing technologies, strengths, weaknesses, deployment. Facial scan: Technical description, characteristics, weaknesses, deployment. Iris scan: Technical description, characteristics, strengths, weaknesses, deployment. Retina vascular pattern: Technical description, characteristics, strengths, weaknesses, deployment. Hand scan: Technical description, characteristics, strengths, weaknesses, deployment , DNA biometrics.	**8 Hours**
Module 3	
Behavioral Biometric Technologies: Handprint Biometrics, DNA Biometrics, signature and handwriting technology, Technical description, classification, keyboard / keystroke Dynamics, Voice, data acquisition, feature extraction, characteristics, strengths, weaknesses deployment.	**8 Hours**
Module 4	
Multi biometrics: Multi biometrics and multi factor biometrics, two-factor authentication with passwords, tickets and tokens, executive decision, implementation plan.	**8 Hours**
Module 5	
Case studies on Physiological, Behavioral and multifactor biometrics in identification systems.	**8 Hours**
Course Outcomes	
The students should be able to: • Visualize traditional and biometric systems. • Analyze different algorithms of biometric systems. • Compare strengths and weaknesses of different biometric systems. • Design different biometric system. • Design multimodal biometric systems.	
Question paper pattern: The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.	
Text Books 1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, Biometrics –Identity verification in a networked World, Wiley Eastern, 2002. 2. John Chirillo and Scott Blaul, Implementing Biometric Security, Wiley Eastern Publications, 2005.	
Reference Books: 1. John Berger, Biometrics for Network Security, Prentice Hall, 2004.	

TRUST MANAGEMENT IN E-COMMERCE
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)

SEMESTER – II			
Subject Code	**14SFC252**	**IA Marks**	20
Number of Lecture Hours/Week	03	**Exam Marks**	80
Total Number of Lecture Hours	40	**Exam Hours**	3

CREDITS – 03

Course objectives: This course will enable students to

- Explain fundamental principles of E-Commerce
- Illustrate technologies & tools for E-Commerce with emphasis on Security
- Identify best techniques & practices for different types of legacy & partner requirements
- Handle & address risk management

Module 1	**Teaching Hours**
Introduction to E-Commerce: Network and E-Commerce, Types of E-Commerce. Ecommerce Business Models: B2C, B2B, C2C, P2P and M-commerce business models. Ecommerce Payment systems: Types of payment system, Credit card E-Commerce transactions, B2C E-Commerce Digital payment systems, B2B payment system.	**8 Hours**
Module 2	
Security and Encryption: E-Commerce Security Environment, Security threats in Ecommerce environment, Policies, Procedures and Laws.	**8 Hours**
Module 3	
Inter-organizational trust in E-Commerce: Need, Trading partner trust, Perceived benefits and risks of E-Commerce, Technology trust mechanism in E-Commerce, Perspectives of organizational, economic and political theories of inter-organizational trust, Conceptual model of inter-organizational trust in E-Commerce participation.	**8 Hours**
Module 4	
Introduction to trusted computing platform: Overview, Usage Scenarios, Key components of trusted platform, Trust mechanisms in a trusted platform.	**8 Hours**
Module 5	
Trusted platforms for organizations and individuals: Trust models and the E-Commerce domain.	**8 Hours**

Course Outcomes

The students should be able to:

- Explain the types of E-Commerce, E-Commerce business models and E-commerce payment systems.
- Illustrate the Policies, Procedures and Laws and Security threats in E-Commerce environment.
- Analysis and explain the issues, risks and challenges in inter-organisational trust in E-Commerce
- Explain the Key components and Trust mechanisms of trusted computing platform.
- Describe the Trusted platforms for organizations and individuals

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Kenneth C. Laudon and Carol Guercio Trave, Study Guide to E-Commerce Business Technology Society, Pearson Education, 2005.
2. Pauline Ratnasingam, Inter-Organizational Trust for Business-to-Business E- Commerce,IRM Press, 2005.

Reference Books:

1. Siani Pearson, et al, Trusted Computing Platforms: TCPA Technology in Context, Prentice Hall PTR, 2002.

INFORMATION SECURITY POLICIES IN INDUSTRY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – II

Subject Code	**14SFC253**	**IA Marks**	20
Number of Lecture Hours/Week	03	**Exam Marks**	80
Total Number of Lecture Hours	40	**Exam Hours**	3

CREDITS – 03

Course objectives: This course will enable students to

The objectives of this course is to make students to learn

- Explain management's responsibilities and role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines.
- Illustrate the differences between the organization's general information security policy and the needs and objectives of the various issue-specific and system-specific policies the organization will create.
- Know what an information security blueprint is and what its major components are.
- How an organization institutionalizes its policies, standards, and practices using education, training and awareness programs.
- Become familiar with what viable information security architecture is, what it includes, and how it is used.

Module 1	**Teaching Hours**
Introduction to Information Security Policies: About Policies, why Policies are Important, When policies should be developed, How Policy should be developed, Policy needs, Identify what and from whom it is being protected, Data security consideration, Backups, Archival storage and disposal of data, Intellectual Property rights and Policies, Incident Response and Forensics, Management Responsibilities, Role of Information Security Department, Security Management and Law Enforcement, Security awareness training and support.	**8 Hours**
Module 2	
Policy Definitions, Standards, Guidelines, Procedures with examples, Policy Key elements, Policy format and Basic Policy Components, Policy content considerations, Program Policy Examples, Business Goal Vs Security Goals, Computer Security Objectives, Mission statement Format, Examples, Key roles in Organization, Business Objectives, Standards: International Standards.	**8 Hours**
Module 3	
Writing The Security Policies: Computer location and Facility construction, Contingency Planning, Periodic System and Network Configuration Audits, Authentication and Network Security, Addressing and Architecture, Access Control, Login Security, Passwords, User Interface, Telecommuting and Remote Access, Internet Security Policies, Administrative and User Responsibilities, WWW Policies, Application Responsibilities, E-mail Security Policies.	**8 Hours**
Module 4	

Establishing Type of Viruses Protection: Rules for handling Third Party Software, User Involvement with Viruses, Legal Issues, Managing Encryption and Encrypted data, Key Generation considerations and Management, Software Development policies, Processes Testing and Documentation, Revision control and Configuration management, Third Party Development, Intellectual Property Issues.	**8 Hours**
Module 5	
Maintaining the Policies: Writing the AUP, User Login Responsibilities, Organization's responsibilities and Disclosures, Compliance and Enforcement, Testing and Effectiveness of Policies, Publishing and Notification Requirements of the Policies, Monitoring, Controls and Remedies, Administrator Responsibility, Login Considerations, Reporting of security Problems, Policy Review Process, The Review Committee, Sample Corporate Policies, Sample Security Policies.	**8 Hours**

Course Outcomes

The students should be able to:

- Explain the content, need, and responsibilities of information security policies.
- Explain the standards, guidelines, Procedures, and key roles of the organization.
- Able to write policy document for securing network connection and interfaces.
- Explain the threats to the stored data or data in transit and able to write policy document.
- Able to write, monitor, and review policy document.

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Scott Barman, Writing Information Security Policies, Sams Publishing, 2002.
2. Thomas.R.Peltier, Information Policies, Procedures and Standards, CRC Press, 2004.

Reference Books:

1. Thomas R Peltier, Justin Peltier, John Backley, " Information Security Fundamentals", Auerbach publications, CRC Press, 2005.
2. Harold F. Tipton and Micki Krause "Information Security Management Handbook", Auerbach publications, 5th Edition, 2005.

DATABASE SECURITY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – II

Subject Code	**14SFC254**	**IA Marks**	20
Number of Lecture Hours/Week	03	**Exam Marks**	80
Total Number of Lecture Hours	40	**Exam Hours**	3

CREDITS – 03

Course objectives: This course will enable students to

- Fundamental security concepts and architectures that serve as building blocks to database security
- Concepts of user account management and administration, including security risks
- To use current database management system to design and configure the user and data permissions
- Operational components necessary to maximize database security using various security models

Module 1	**Teaching Hours**
Introduction: Introduction to Databases, Security Problems in Databases Security Controls Conclusions. Security Models 1: Introduction, Access Matrix Model, Take-Grant Model, Acten Model, PN Model, Hartson and Hsiao's Model, Fernandez's Model, Bussolati and Martella's Model for Distributed databases.	**8 Hours**
Module 2	
Security Models 2: Bell and LaPadula's Model, Biba's Model, Dion's Model, Sea View Model, Jajodia and Sandhu's Model, The Lattice Model for the Flow Control conclusion. Security Mechanisms: Introduction, User Identification/Authentication, Memory Protection, Resource Protection, Control Flow Mechanisms, Isolation, Security Functionalities in Some Operating Systems, Trusted Computer System, Evaluation Criteria.	**8 Hours**
Module 3	
Security Software Design: Introduction, A Methodological Approach to Security, Software Design, Secure Operating System Design, Secure DBMS Design, Security Packages, Database Security Design.	**8 Hours**
Module 4	
Statistical Database Protection & Intrusion Detection Systems: Introduction, Statistics, Concepts and Definitions, Types of Attacks, Inference Controls, evaluation Criteria for Control Comparison, Introduction IDES System, RETISS System, ASES System Discovery.	**8 Hours**
Module 5	
Models For The Protection Of New Generation Database Systems 1: Introduction, A Model for the Protection of Frame Based Systems, A Model for the Protection of Object-Oriented Systems, SORION Model for the Protection of Object-Oriented Databases. Models For The Protection Of New Generation Database Systems 2: A Model for the Protection of New Generation Database Systems, the Orion Model, Jajodia and Kogan's Model, A Model for the Protection of Active Databases Conclusions.	**8 Hours**
Course Outcomes	
The students should be able to: • Carry out a risk analysis for a large database	

- Implement identification and authentication procedures, fine-grained access control and data encryption techniques
- Set up accounts with privileges and roles
- Audit accounts and the database system

Question paper pattern:
The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Database Security and Auditing, Hassan A. Afyoun i, India Edition, CENGAGE Learning, 2009.
2. Database Security, Castano, Second edition, Pearson Education.

Reference Books:

1. Database security by Alfred Basta, Melissa Zgola , CENGAGE learning..

MINIPROJECT
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – II

Laboratory Code	16LNI26/ 16SCE26 / 16SCN26 /16SCS26 /**16SFC26** / 16SIT26 / 16SSE26	IA Marks	20
Number of Lecture Hours/Week	03 hours of lab	Exam Marks	80
Total Number of Lecture Hours	------	Exam Hours	03

CREDITS – 02

C**ourse objectives:** This course will enable students to

- Enable the student to design, develop and analyze an application development

The student will carry out a mini project relevant to the course. The project must be development of an application (Hardware/Software). It is preferable if the project is based on mobile application development.

Course outcomes:

- Design, develop and to analyze an application development.
- Prepare report of the project.

Conduction of Practical Examination:

The student shall prepare the report by including:

1. Define project (Problem Definition)
2. Prepare requirements document
   a. Statement of work
   b. Functional requirements
   c. Software / Hardware requirements
3. Develop use cases
4. Research, analyze and evaluate existing learning materials on the application
5. Develop user interface and implement code
6. Prepare for final demo

Evaluation:

Evaluation shall be taken up at the end of the semester. Project work evaluation and viva-voce examination shall be conducted. Internal evaluation shall be carried by the Guide and Head of the department for 20 marks. Final examination which includes demonstration of the project and viva-voce shall be conducted for 80 Marks viz report + Outputs of the project + presentation = 30+30+20 = 80 marks.

SEMINAR
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – II

Subject Code	16SCE27 / 16SCN27 / 16LNI27 / 16SIT27 / 16SSE27 / 16SCS27 / **16SFC27**	IA Marks	100
Number of Lecture Hours/Week	----	Exam Marks	-
Total Number of Lecture Hours	----	Exam Hours	-

CREDITS – 01

Course objectives: This course will enable students to

- Motivate the students to read technical article
- Discover recent technology developments

Descriptions

The students should read a recent technical article (try to narrow down the topic as much as possible) from any of the leading reputed and refereed journals like:

1. IEEE Transactions, journals, magazines, etc.
2. ACM Transactions, journals, magazines, SIG series, etc.
3. Springer
4. Elsevier publications etc

In the area of (to name few and not limited to)

- Web Technology
- Cloud Computing
- Artificial Intelligent
- Networking
- Security
- Data mining

Course Outcomes

The students should be able to:

- Conduct survey on recent technologies
- Infer and interpret the information from the survey conducted
- Motivated towards research

Conduction:

The students have to present at least ONE technical seminar on the selected topic and submit a report for internal evaluation.

Marks Distribution: Literature Survey + Presentation (PPT) + Report + Question & Answer + Paper: 20 + 30 + 30 + 20 (100).

FILE SYSTEM FORENSIC ANALYSIS

[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – IV

Subject Code	**16SFC41**	**IA Marks**	20
Number of Lecture Hours/Week	04	**Exam Marks**	80
Total Number of Lecture Hours	50	**Exam Hours**	3

CREDITS – 04

Course objectives: This course will enable students to

- Computer file system and storage analysis
- Basics of Computer forensics
- Role of forensics in business world

Module 1	**Teaching Hours**
Volume Analysis: Introduction, Background, Analysis Basics, Summary. PC-based Partitions: DOS Partitions, Analysis Considerations, Apple Partitions, Removable Media. Server-based Partitions: BSD Partitions, Sun Solaris Slices, GPT Partitions, Multiple Disk Volumes: RAID, Disk Spanning.	**10**
Module 2	
File System Analysis: What Is a File System?, File System Category, Content Category, Metadata Category, File Name Category, Application Category, Application-level Search Techniques, Specific File Systems FAT Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, The Big Picture, Other Topics. FAT Data Structures: Boot Sector, FAT32 FSINFO, FAT, Directory Entries, Long File Name Directory Entries	**10**
Module 3	
NTFS Concepts: Introduction, Everything is a File, MFT Concepts, MFT Entry Attribute Concepts, Other Attribute Concepts, Indexes, Analysis Tools. NTFS Analysis: File System Category, Content Category, Metadata Category, File Name Category, Application Category, The Big Picture. NTFS Data Structures: Basic Concepts, Standard File Attributes, Index Attributes and Data Structures, File System Metadata Files.	**10**
Module 4	
Ext2 and Ext3 Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, Application Category. The Big Picture. Ext2 and Ext3 Data Structures: Superblock, Group Descriptor Tables, Block Bitmap, Inodes, Extended Attributes, Directory Entry, Symbolic Link, Hash Trees, Journal Data Structures	**10**
Module 5	
UFS1 and UFS2 Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, The Big Picture. UFS1 and UFS2 Data Structures: UFS1 Superblock, UFS2 Superblock, Cylinder Group Summary, UFS1 Group Descriptor, UFS2 Group Descriptor, Block and Fragment Bitmaps, UFS1 Inodes, UFS2 Inodes, UFS2 Extended Attributes, Directory Entries	**10**

Course Outcomes

The students should be able to:

- Compare the different file systems for storing information
- Illustrate the role of computer forensics in the business and private world
- Identify some of the current techniques and tools for forensic examinations

Question paper pattern:
The question paper will have ten questions.
There will be 2 questions from each module.

Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Brian Carrier, File System Forensic Analysis, Pearson Education, 2005

Reference Books:

1. Machtelt Garrels, "Introduction to Linux A Hands-On Guide", Third Edition, Fultus Corporatio Publisher, 2010.

Laboratory Experiments

1. Design a simple experiment to test whether a bootable CD/DVD examination altered the hard d of the suspect's computer system when the system was booted using the bootable CD/DVD.
2. Design a simple experiments that shows that the correct application of a virtual environment approach results in a less time spent on analysing the evidence, giving more chance of discover important data, and allowing less qualified personnel to be involved in a more productive way.
3. Write a program to find a unique pattern in each sector of disk.
4. Write a program to compare two partitions.
5. Write a program to compare two disks.
6. Write a program to change or corrupt one byte in a file.

The above experiments can be simulated using freely available forensic tool.

SECURITY ARCHITECTURE DESIGN

[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – IV

Subject Code	**16SFC421**	**IA Marks**	20
Number of Lecture Hours/Week	03	**Exam Marks**	80
Total Number of Lecture Hours	40	**Exam Hours**	3

CREDITS – 03

Course objectives: This course will enable students to

- Describe the intent of effective site security
- List different security zones
- Select appropriate elements to apply to specific security zones

Module 1	**Teaching Hours**
Architecture and Security: Architecture Reviews, Software Process, Reviews and the Software Development Cycle, Software Process and Architecture Models, Software Process and Security, Architecture Review of System, Security Assessments, Security Architecture Basics, Architecture Patterns in Security	**8 Hours**
Module 2	
Low-Level Architecture: Code Review, importance of code review, Buffer Overflow	**8 Hours**

Exploits, Countermeasures Against Buffer Overflow Attacks, patterns applicable, Security and Perl, Bytecode Verification in Java-Good Coding Practices Lead to Secure Code, Cryptography, Trusted Code, Secure Communications.	
Module 3	
Mid-Level Architecture: Middleware Security, Middleware and Security, The Assumption of Infallibility, The Common Object Request Broker Architecture, The OMG CORBA Security Standard, Vendor Implementations of CORBA Security, CORBA Security Levels, Secure Interoperability, Application, Unaware Security, Application, Aware Security, Application Implications, Web Security, Application and OS Security, Database Security.	**8 Hours**
Module 4	
High-Level Architecture: Security Components, Secure Single Sign-On- Public-Key Infrastructures, Firewalls, Intrusion Detection Systems, LDAP and X.500 Directories, Kerberos, Distributed Computing Environment,The Secure Shell, or SSH, The Distributed Sandbox, Security and Other Architectural Goals, Metrics for Non-Functional Goals, Force Diagrams around Security, High Availability, Robustness, Reconstruction of Events, Ease of Use, Maintainability, Adaptability, and Evolution, Scalability, Interoperability, Performance, Portability.	**8 Hours**
Module 5	
Enterprise Security Architecture: Security as a Process, Security Data, Enterprise Security as a Data Management Problem, Tools for Data Management, David Isenberg and the "Stupid Network", Extensible Markup Language,The XML Security Services Signaling Layer, XML and Security Standards, The Security Pattern Catalog Revisited, XML-Enabled Security Data-HGP: A Case Study in Data Management, Business Cases and Security, Building Business Cases for Security **Case study:** Building secure OS for Linux: Linux security modules, security enhanced Linux.	**8 Hours**
Course Outcomes	
The students should be able to: • Design the secured sites based on tools & techniques • Map site zones with level of security • Identify the components targeted for each zone	
Question paper pattern: The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.	
Text Books 1. Jay Ramachandran, Designing Security Architecture Solutions, Wiley Computer Publishing, 2010.	
Reference Books: 1. Markus Schumacher, Security Patterns: Integrating Security and Systems Engineering, Wiley Software Pattern Series, 2010.	

STEGANOGRAPHY AND DIGITAL WATERMARKING

[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – IV

Subject Code	**16SFC422**	**IA Marks**	20
Number of Lecture Hours/Week	03	**Exam Marks**	80
Total Number of Lecture Hours	40	**Exam Hours**	3

CREDITS – 03

Course objectives: This course will enable students to

- Basics of Data hiding by using Steganography & Watermarking
- Compare and contrast several different methods of steganography
- Apply digital watermarking as an authentication tool for distribution of content over the Internet

Module 1	**Teaching Hours**
Introduction to Information hiding: Brief history and applications of information hiding, Principles of Steganography, Frameworks for secret communication, Security of Steganography systems, Information hiding in noisy data, Adaptive versus non adaptive algorithms, Laplace filtering, Using cover models, Active and malicious attackers, Information hiding in written text, Examples of invisible communications.	**8 Hours**
Module 2	
Survey of steganographic techniques: Substitution system and bit plane tools, Transform domain techniques, Spread spectrum and information hiding, Statistical Steganography, Distortion and code generation techniques, Automated generation of English text.	**8 Hours**
Module 3	
Steganalysis: Detecting hidden information, Extracting hidden information, Disabling hidden information, Watermarking techniques, History, Basic Principles, applications, Requirements of algorithmic design issues, Evaluation and benchmarking of watermarking system.	**8 Hours**
Module 4	
Survey of current watermarking techniques: Cryptographic and psycho visual aspects, Choice of a workspace, binary image, audio, video. Formatting the watermark beds: Digital watermarking schemes, Spread Spectrum, DCT (Discrete Cosine Transform), Domain and Quantization schemes, Watermarking with side information, Robustness to temporal and geometric distortions.	**8 Hours**
Module 5	
Data Right Management: DRM Products and Laws, Fingerprints, Examples, Protocols and Codes, Boneh-Shaw finger printing Scheme, Steganography and watermarking applications, Military, Digital copyright protection and protection of intellectual property.	**8 Hours**

Course Outcomes

The students should be able to:

- Distinguish Stegnography & Digital watermarking from other related fields.
- Knowledge of how to use steganography techniques in conjunction with encryption systems to protect data.
- Explain different types of watermarking applications and watermarking frameworks.

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Stefan Katzenbelsser and Fabien A. P. Petitcolas, Information hiding techniques for Steganography and Digital Watermarking, ARTECH House Publishers, January 2004.
2. I.J. Cox, M.L. Miller, J.Fridrich and T.Kalker, Digital Water Marking and Steganography, 2nd Edition, Morgan Kauffman Publishers, 2008.
3. Johnson, Neil F. / Duric, Zoran / Jajodia, Sushil G , Information Hiding: Steganography and Watermarking -Attacks and Countermeasures (Advances in Information Security, Volume 1), 2001.

Reference Books:

1. Peter Wayner , "Disappearing Cryptography: Information Hiding, Steganography and Watermarking 2/e", Elsevier.
2. Practical Cryptography, N.Ferguson and B.Schneier, Wiley Publishing Inc., 2003.
3. Bolle, Connell et. al., "Guide to Biometrics", Springer
4. John Vecca, "Computer Forensics: Crime scene Investigation", Firewall Media
5. Christopher L.T. Brown, "Computer Evidence: Collection and Preservation", Firewall Media

MOBILE DEVICE FORENSICS

[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – IV

Subject Code	**16SFC423**	**IA Marks**	20
Number of Lecture Hours/Week	03	**Exam Marks**	80
Total Number of Lecture Hours	40	**Exam Hours**	3

CREDITS – 03

Course objectives: This course will enable students to

- Basic Concepts in Mobile Forensics
- Mobile Device Data Storage
- Identify, preserve, extract, analyze, and report data from mobile devices
- Acquiring Evidence from Mobile devices

Module 1	**Teaching**

	Hours
Android and mobile forensics: Introduction, Android platform, Linux, Open source software and forensics, Android Open Source Project, Internationalization, Android Market, Android forensics	**8 Hours**
Module 2	
Android hardware platforms: Overview of core components, Overview of different device types, Read-only memory and boot loaders, Manufacturers, Specific devices	**8 Hours**
Module 3	
Android software development kit and android debug bridge: Android platforms, Software development kit (SDK), Android security model, Forensics and the SDK.	**8 Hours**
Module 4	
Android file systems and data structures: Data in the shell, Type of memory, File systems, Mounted file systems and directory structures. Android forensic techniques: Procedures for handling an Android device, Imaging Android USB mass storage devices, Logical techniques, Physical techniques	**8 Hours**
Module 5	
Android device data and app security: Data theft targets and attack vectors, Security considerations, Individual security strategies, Corporate security strategies, App development security strategies. Android application and forensic analysis: Analysis techniques, FAT forensic analysis, YAFFS2 forensic analysis, Android app analysis	**8 Hours**

Course Outcomes

The students should be able to:

- Describe security risks and vulnerabilities from mobile devices and network access.
- Explain the methods and procedures used in forensics investigations.
- Have knowledge of the global security threats and vulnerabilities of mobile devices and networks.
- Carry out a forensics investigation of mobile and network devices.

Question paper pattern:

The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Android Forensics Investigation, Analysis, and Mobile security for Google Android, Andrew Hoog, John McCash, Technical Editor, Elsevier, 2011.

Reference Books:

1. Satish Bommisetty, Rohit Tamma, Heather Mahalik “Practical Mobile Forensics”, Kindle Edition, Packt Publishing (21 July 2014).
2. Andrew Martin,” Mobile Device Forensics”, © SANS Institute 2009

SECURITY ASSESSMENT AND VERIFICATION

[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – II

Subject Code	**16SFC424**	**IA Marks**	20
Number of Lecture Hours/Week	03	**Exam Marks**	80
Total Number of Lecture Hours	40	**Exam Hours**	3

CREDITS – 03

Course objectives: This course will enable students to

- Explain the role of assessment & verification for information security
- Demonstration of different existing tools and procedures for assessment planning
- Recall awareness of risk management

Module 1	**Teaching Hours**
Evolution of information security: information assets, security standards, organizational impacts, security certifications, elements of information security program, need for security assessment, security assessment process.	**8 Hours**
Module 2	
Security assessment planning: Business drivers, scope definition, consultant's perspective, Client's perspective, Development of project plan. Initial information gathering, Initial preparation, analysis of gathered information.	**8 Hours**
Module 3	
Business process evaluation, Technology evaluation, Risk analysis, Risk mitigation.	**8 Hours**
Module 4	
Security Risk assessment project management, Security risk assessment approaches and methods.	**8 Hours**
Module 5	
Information security standards, Information security Legislation, Formal security verification, Security verification with SSL.	**8 Hours**

Course Outcomes

The students should be able to:

- Illustrate the roles information security and its management
- Select appropriate techniques to tackle and solve problems in the discipline of information security assessment
- Design an information security and validation system

Question paper pattern:
The question paper will have ten questions.
There will be 2 questions from each module.
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books

1. Sudhanshu Kairab, A practical guide to security assessments, CRC press, 2005.
2. Douglas J. Landoll, A Security risk assessment Handbook, Auerbach publications, 2006.

Reference Books:

1. Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, 2nd Edition, Cengage Learning Pub.
2. Thomas R Peltier, Justin Peltier and John Blackley, ”Information Security Fundamentals”, 2nd Edition, Prentice Hall, 1996