

CENTRAL UNIVERSITY OF PUNJAB

Master's Programme Course Structure

School: Engineering & Technology								
Department: Computer Science & Technology								
Programme: M-Tech. Computer Science & Technology (Cyber Security)								
Batch: 2018-19								
Semester : I								
S.No.	Course Code	Course Title	Course Type	Name of Course Coordinator	Credit Hours			
					L	T	P	Total credit
1.	CBS.501	Research Methodology and Statistics for Engineering	FC		3	1	-	4
2.	CBS.506	Secure Coding	CC		3	1	-	4
3.	CBS.507	Network Technologies and Protocols	CC		3	1	-	4
4.	CBS.508	Data Structure with Python	CC		3	1	-	4
5.	CBS.509	Programming Methodologies - Lab (Practical)	CC		-	-	4	2
6.	CBS.510	Data Structure with Python – Lab (Practical)	CC		-	-	4	2
7.	XXX.YYY	Inter-Disciplinary Elective -1 (From Other Departments)	IDC		2	-	-	2
Total					14	4	8	22

Semester : II								
S.No.	Course Code	Course Title	Course Type	Name of Course Coordinator	Credit Hours			
					L	T	P	Total credit
1.	CBS.521	Information & Network Security	CC		3	1	-	4
2.	CBS.522	Ethical Hacking and Forensics	CC		3	1	-	4
3.	CBS.523	IT Act & Cyber Laws	CC		3	1	-	4
4.	CBS.524	Web Application Penetration Testing	CC		3	1	-	4
5.	CBS.525	Embedded System Design	EC		3	1	-	4
6.	CBS.526	Software Testing and Maintenance	EC					
7.	CBS.527	Data Warehouse and Mining	EC					
8.	CBS.528	Web Services	EC					
9.	CBS.529	Wireless Ad-hoc Sensor Networks and IoTs	EC					
10.	CBS.530	Information & Network Security – Lab	CC		-	-	4	2
11.	CBS.531	Ethical Hacking and Forensics - Lab	CC		-	-	4	2
12.	XXX.YYY	Inter-Disciplinary Elective-2 (From Other Departments) (Practical)	IDC		2	-	-	2
Total					18	4	8	26

Semester : III								
S.No.	Course Code	Course Title	Course Type	Name of Course Coordinator	Credit Hours			
					L	T	P	Total credit
1.	CBS.551	Capstone Lab-I	EC		-	-	8	4
2.	CBS.552	Big Data Analytics	EC					
3.	CBS.553	Image Processing & Biometric Security						
4.	CBS.554	E-Privacy: Privacy & Trust In The Electronic Society						
5.	CBS.555	Information Retrieval			3	1	-	4
6.	CBS.556	Dissertation	EC		-	-	-	16
Total					3	1	8	24

Semester : IV								
S.No.	Course Code	Course Title	Course Type	Name of Course Coordinator	Credit Hours			
					L	T	P	Total credit
1.	CBS.571	Capstone Lab-II	EC		-	-	8	4
2.	CBS.600	Dissertation	EC		-	-	-	20
Total							8	24

The ratio of students in offered elective courses will be maintained evenly and the elective course will be allocated to the students based on their merit & preference.

Semester-I

CBS.501

Research Methodology and Statistics

Credits: 3-1-0

Objective: The objective of this course is to ensure that a student learns basis of scientific research and statistical methods to arrive at and verify the conclusions drawn.

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

- Prepare research proposal and plan.
- Understand how to interpret data using hypothesis testing.
- Describe the concept of multivariate analysis.
- Explain the concept of plagiarism and intellectual property rights.

Unit I

General principles of research: Meaning and importance of research, Critical thinking, Formulating hypothesis and development of research plan, Review of literature, Interpretation of results and discussion.

Bibliographic index and research quality parameters- citation index, impact factor, *h* index, i10 index, etc. Research engines such as google scholar, Scopus, web of science, etc.

Technical & scientific writing: Technical & Scientific writing - theses, technical papers, reviews, electronic communication, and research papers, etc., Poster preparation and Presentation and Dissertation. Reference Management using various softwares such as Endnote, reference manager, Ref works, etc. Communication skills – defining communication; type of communication; techniques of communication, etc.

Library: Classification systems, e-Library, Reference management, Web-based literature search engines.

Unit II

Plagiarism: Plagiarism, definition, Search engines, regulations, policies and documents/thesis/manuscripts checking through softwares, Knowing and Avoiding Plagiarism during documents/thesis/manuscripts/scientific writing.

Intellectual Property Rights: Intellectual Property, intellectual property protection (IPP) and intellectual property rights (IPR), WTO (World Trade Organization), WIPO (World Intellectual Property Organization), GATT (General Agreement on Tariff and Trade), TRIPs (Trade Related Intellectual Property Rights), TRIMS (Trade Related Investment Measures) and GATS (General Agreement on Trades in Services), Nuts and Bolts of Patenting, Technology Development/Transfer Commercialization Related Aspects, Ethics and Values in IP.

Unit III

Descriptive Statistics: Meaning, need and importance of statistics. Attributes and variables. Measurement and measurement scales. Collection and tabulation of data. Diagrammatic representation of frequency distribution: histogram, frequency polygon, frequency curve, ogives, stem and leaf plot, pie chart.

Measures: Measures of central tendency, dispersion (including box and whisker plot), skewness and kurtosis. Linear regression and correlation (Karl Pearson's and Spearman's) and residual plots.

Unit IV

Random variables and Distributions: Discrete and continuous random variables. Discrete Probability distributions like Binomial, Poisson and continuous distributions like Normal, F and student-t distribution.

Differences between parametric and non-parametric statistics. Confidence interval, Errors, Levels of significance, Hypothesis testing.

Parametric tests: Test for parameters of Normal population (one sample and two sample problems) z-test, student's t-test, F and chi-square test and Analysis of Variance (ANOVA).

Non-Parametric tests: One sample: Sign test, signed rank test, Kolmogrov-Smirnov test, run test. Critical difference (CD), Least Significant Difference (LSD), Kruskal–Wallis one-way ANOVA by ranks, Friedman two-way ANOVA by ranks.

Text books:

1. Theil, D.V. (2014). David Research Methods for Engineers, Cambridge University Press.
2. Kothari, C.R. (2013). Research Methodology: Methods and Techniques. New Age International.
3. S.C. Gupta (2014), Fundamentals of Statistics, Himalaya Publishing House

Suggested readings:

1. David J. Sheskin (2011), Handbook of Parametric and Nonparametric Statistical Procedures, Chapman and Hall/CRC.2.
2. Best J. W. (1999). Research in Education, New Delhi: Prentice Hall of India Pvt. Ltd.

Objective: This course aims to provide an understanding of the various security measure required for the source code of software and major coding errors that lead to vulnerabilities.

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

- Identify the elements of secure coding
- Describe various possible security attacks
- Classify various errors that lead to vulnerabilities

Unit I

Software Security: Security Concepts, Security Policy, Security Flaws, Vulnerabilities, Exploitation and Mitigations. Software Security problems, Classification of Vulnerabilities.

Security Analysis: Problem Solving with static analysis: Type Checking, Style Checking, Program understanding, verifications and property checking, Bug finding and Security Review. Analysing Source versus Analyzing Compiled code.

Unit II

Strings: Common String manipulating Errors, String Vulnerabilities and Exploits, Mitigation Strategies for strings, String handling functions, Runtime protecting strategies, Notable Vulnerabilities.

Integer Security: Integer data Type, Integer Conversions, Integer Operations, Integer Vulnerabilities, Mitigation Strategies.

Unit III

Handling Inputs: What to validate, How to validate, Preventing metadata Vulnerabilities,

Buffer Overflow: Introduction, Exploiting buffer overflow vulnerabilities, Buffer allocation strategies, Tracking buffer sizes, buffer overflow in strings, Buffer overflow in Integers Runtime protections

Errors and Exceptions: Handling Error with return code, Managing exceptions, Preventing Resource leaks, Logging and debugging

Unit IV

Web Applications: Input and Output Validation for the Web: Expect That the Browser Has Been Subverted, HTTP Considerations: Use POST, Not GET, Request Ordering, Error Handling, Request Provenance
Maintaining Session State: Use Strong Session Identifiers, Enforce a Session Idle Timeout and a Maximum Session Lifetime, Begin a New Session upon Authentication.

Text Books:

1. Seacord, R. C. (2013). Secure Coding in C and C++. 2nd edition. Addison Wisley for Software Engineering Institute,
2. Chess, B., and West, J. (2007). Secure Programming with static Analysis. Addison Wisley Software Security Series.

Suggested Readings:

1. Seacord, R. C. (2009). The CERT C Secure Coding Standard. Pearson Education.
2. Howard, M., LeBlanc, D. (2002). Writing Secure Code. 2nd Edition. Pearson Education.

Objective: This course aims to provide background on relevant computer networking protocols to have a comprehensive and deep knowledge in computer networks.

Course Outcomes: After successfully completing this course, students will be able to

- Describe functioning of protocol stacks related to different networks.
- Understand functioning of various networking protocols.
- Discover state of communication from values mentioned in header structure of protocols.

Unit I

Introduction: Overview of Computer Networks, ISO-OSI and TCP/IP reference models, Gigabit Ethernet, Wireless LAN, MAC protocols for LANs: Aloha, Pure Aloha, CSMA/CD, CSMA/CA, Layer 2 headers.

Unit II

IPv4: Header, Class-full and Classless addresses, Subnets and supernets, IPv6: Basic protocol, Header, Extensions and options, Tunneling, Addressing, Neighbor Discovery, Auto-configuration, IPv6 in an IPv4 Internet Migration and Coexistence, Mobile IPv6: Overview, Route Optimization, Handover and its impacts on TCP and UDP, Security requirements.

Internet Control Message Protocol, Address Resolution Protocol, Reverse Address Resolution Protocol

Unit III

TCP header, TCP Three way handshake, TCP for Wired networks, TCP extensions for wireless networks, UDP header. Commonly used TCP and UDP ports. Remote Procedure Call, RTP Control Protocol, Secure Shell. Application Protocols: File Transfer Protocol, Domain Name System, Bittorrent: peer-to-peer file sharing protocol, Hypertext Transfer Protocol, Hypertext Transfer Protocol Secure, Internet Relay Chat, Network Time Protocol, Post Office Protocol Version 3, Simple Mail Transfer Protocol, Simple Network Management Protocol, Telnet.

Unit IV

Wireless Networks: WLAN, Bluetooth. Cellular Technologies: Cellular Concept: Introduction, Frequency Reuse, Channel Assignment, Handoff Strategies, Interference, Cell Splitting and Sectoring. GSM: GSM services, features, system architecture, GPRS: Introduction, network architecture, data services, applications and limitations, 3G, 4G and 5G.

Text books:

1. Behrouz A. Forouzan, (2012), Data Communications and Networking, McGraw-Hill.
2. Andrew S. Tanenbaum, David J. Wetherall, 2013, Computer Networks, Pearson.
3. Hesham Soliman, (2014), Mobile IPv6 Mobility in Wireless Internet, Pearson Education.

Suggested Books

1. Ashok K. Talukdar, (2007), Mobile Computing Technology, Applications and Service Creation, 2nd Edition, McGraw-Hill.
2. Theodore S. Rappaport: Wireless Communications Principles and Practice, Prentice Hall.

Objective: The objective of this course is to introduce students to the Python programming language.

Learning Outcomes: On completion of the course the students should be able to

- Define python environment and constructs of Python language.
- Explain the various data structures
- Construct scripts in Python language.

Unit I

Python Introduction, Installing and setting Python environment in Windows and Linux, basics of Python interpreter, Execution of python program, Editor for Python code, syntax, variable, types. Flow control: if, ifelse, for, while, range () function, continue, pass, break. Strings: Sequence operations, String Methods, Pattern Matching.

Unit II

Lists: Basic Operations, Iteration, Indexing, Slicing and Matrixes; Dictionaries: Basic dictionary operations; Tuples and Files, Functions Declaration; Modules: Module Coding Basics, Importing Programs as Modules, Input output and file handling,

Unit III

Object Oriented Programming features in Python: Classes, Objects, Inheritance, Operator Overloading, Errors and Exceptions: try, except and else statements, Exception Objects, Regular expressions. Data Structures and Abstract Data Type in Python: Stack, Queues, Link List, Binary Search Trees

Unit IV

Data Structure in Python: Searching (Linear Search, Binary Search, and Sorting Algorithms (Selection Sort, Insertion Sort, Merge Sort, Quick Sort, Heap Sort), Divide and Conquer Algorithm, Dynamic Programming, Security Trends with Python Programming

Text books:

1. Mark Lutz.,2009, “Learning Python”,4th ed., O’REILLY Media, Inc..
2. Justin Seitz,2009, “Gray Hat Python: Python Programming with Hackers and Reverse Engineers”, No Starch Press, Inc.

Suggested readings:

1. Paul Berry,2011,“Head First Python”. O’REILLY Media, Inc.
2. Jeeva Jose & P. Sojan Lal. 2016. Introduction to Computing & Problem Solving With Python.

CBS.509

Programming Methodologies - Lab

Credits: 0-0-2

Students will implement the lab practical using any programming language.

Understand fundamentals of object-oriented programming, including defining classes, invoking methods, using class libraries, packages and interfaces, util package etc.

CBS.510

Data Structures with Python - Lab

Credits: 0-0-2

Students will implement the lab practical as per the syllabus of the subject.

Semester-II

CBS.521

Information and Network Security

Credits: 3-1-0

Objective: The main objective of this course is to provide students with an overall understanding of the main concepts of information systems, cryptographic techniques and network security tools and to highlight the importance in modern organizations.

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

- explain the principles of information security and its significance
- identify the domain specific security issues
- describe the design and working of different cryptographic methods and filtering rules

Unit I

History of Information Systems: Importance of Information Systems, Basics of Information Systems, Need for Security, Three Pillars of Security.

Encryption and Decryption: Attackers and Types of Threats, Encryption Techniques, Classical Cryptographic Algorithms: Monoalphabetic Substitutions such as the Caesar Cipher, Cryptanalysis of Monoalphabetic ciphers, Polyalphabetic Ciphers such Vigenere, Vernam Cipher, Stream & Block Ciphers.

Unit II

Symmetric Key Systems: Data encryption Standard (DES), DES Structure, DES Analysis, Multiple DES, Advance Encryption Standard (AES).

Key Management Protocols: Solving Key Distribution Problem, Diffie-Hellman Key Exchange Algorithm.

Unit III

Public Key Encryption Systems: Concept and Characteristics of Public Key Encryption System, Rivest-Shamir-Adleman (RSA) Encryption.

Hash Algorithms: Hash concept, Description of Hash Algorithms (MD5 and SHA-1), Digital Signature/Certificate.

Unit IV

Network Perimeter Security Fundamentals: Introduction to Network Perimeter, Multiple layers of Network Security, Security by Router.

Firewalls: Firewall Basics, Types of Firewalls, Network Address Translation Issues, Linux IP Chains.

Access Control Lists: Ingress and Egress Filtering, Types of Access Control Lists, ACL types: standard and extended, ACL commands.

Virtual Private Networks: VPN Basics, Types of VPN, IPsec Tunneling, IPsec Protocols. VLAN: introduction to VLAN, VLAN Links, VLAN Tagging, VLAN Trunk Protocol (VTP).

Text Books:

1. Forouzan, B.A. (2010). Cryptography & Network Security. Tata McGraw-Hill Education.
2. Kahate, A. (2009). Cryptography and Network Security. McGraw-Hill Higher Ed.
3. Godbole, N. (2009). Information Systems Security: Security Management, Metrics, Frameworks and Best Practices. 1st Ed. John Wiley & Sons India.
4. Riggs, C. (2005). Network Perimeter Security: Building Defence In-Depth, AUERBACH, USA.
5. Northcutt S. (2005) Inside Network Perimeter Security, 2nd Ed., Pearson Education.

Suggested Readings:

1. Stallings, W. (2007). Network Security Essentials: applications and standards. 3rd ed. Pearson Education India.
2. Stallings, W. 2014. Cryptography and Network Security: Principles and Practice. 6th ed. Pearson.
3. Kim, D., and Solomon, M. G. (2010). Fundamentals of Information Systems Security. Jones & Bartlett Learning.

Objective: This course will introduce basics of ethical hacking and Forensics.

Course Outcomes: After successfully completing this course, students will be able to

- Describe phases of Ethical Hacking
- Identification and Evaluation of tools and techniques to perform ethical hacking.
- Investigation of cyber-crimes and preservation of cyber evidences.

Unit I

Ethical hacking process, Hackers behaviour & mind set, Maintaining Anonymity, Hacking Methodology, Information Gathering, Active and Passive Sniffing, Physical security vulnerabilities and countermeasures. Preparation of Ethical Hacking Documents. Social Engineering attacks and countermeasures.

Unit II

Network Infrastructure Vulnerabilities, IP spoofing, DNS spoofing, DoS attacks. Web server and application vulnerabilities.

Wireless Hacking: Wireless footprint, Wireless scanning and enumeration, Gaining access (hacking 802.11), WEP, WPA, WPA2.

Introduction to Metasploit: Metasploit framework, Metasploit Console, Payloads, Metpreter, Introduction to Armitage.

Unit III

Cyber Forensics: Incident- Response Methodology, Evidence – Search, Seizure, Identification, Preservation and Analysis, Image Capturing, Hidden Data Extraction: Recovery of deleted files, Cracking Passwords

Unit IV

Network Forensics and Investigating Logs, Document Forensics: Information in Metadata, Web Attack Investigations, Internet Crime Investigations, Email Crime Investigations: Email Structure, Email Addressing, Email Headers Analysis, Mobile forensics

Text books:

1. Baloch, R. (2015). Ethical Hacking and Penetration Testing Guide, CRC Press.
2. Beaver, K. (2013). Hacking for Dummies, 3rded. John Wiley & sons.
3. Council, Ec. (2009). Computer Forensics: Investigating Network Intrusions and Cybercrime, Cengage Learning.

Suggested readings:

1. McClure S., Scambray J., and Kurtz G, (2009), Hacking Exposed. Tata McGraw-Hill Education.
2. International Council of E-Commerce Consultants by Learning, Penetration Testing Network and Perimeter Testing Ec-Council/ Certified Security Analyst Vol. 3 of Penetration Testing .
3. Davidoff, S. and Ham, J. (2012). Network Forensics Tracking Hackers through Cyberspace, Prentice Hall.
4. Michael G. Solomon , K Rudolph, Ed Tittel, Broom N., and Barrett, D. (2011), Computer Forensics Jump Start, Willey Publishing, Inc.

Objective: The objective of this course is to provide knowledge about the basic information on IT Act and Cyber law as well as the legislative and judicial development in the area.

Course Outcomes: By the end of this Course, students should be able to:

- Analyze fundamentals of Cyber Law
- Discuss IT Act & its Amendments
- Relate Cyber laws with security incidents.

Unit I

Concept of Cyberspace, Issues of Jurisdiction in Cyberspace: Jurisdiction Principles under International law, Jurisdiction in different states, Position in India. Conflict of Laws in Cyberspace, International Efforts for harmonization Privacy in Cyberspace

Unit II

Electronic Commerce, Cyber Contract, Intellectual Property Rights and Cyber Laws
UNCITRAL Model Law, Digital Signature and Digital Signature Certificates, E-Governance and Records.

Unit III

Define Crime, *Mens Rea*, Crime in Context of Internet, Types of Cyber Crime, Computing Damage in Internet Crime, Offences under IPC (Indian Penal Code, 1860), Offences & Penalties under IT Act 2000, IT Act Amendments, Investigation & adjudication issues, Digital Evidence

Unit IV

Obscenity and Pornography, Internet and potential of Obscenity, International and National Instruments on Obscenity & Pornography, Child Pornography, Important Case Studies

Text books:

1. Cyber Law in India – Dr. Farooq Ahmad
2. Cyber Laws – J.P. Sharma, Sunaina Kanojia
3. Cyber Laws and IT Protection – Harish Chander

Suggested readings:

1. Cyber Laws – Justice Yatindra Singh
2. An Introduction to cyber crime and cyber law – Prof. R.K. Chaubey
3. Understanding Laws – Garima Tiwari
4. Computers Internet and New Technology Laws – Karnika Seth, Justice Altamas Kabir

Objective: This course will introduce basics of ethical hacking and Forensics.

Course Outcomes: After successfully completing this course, students will be able to

- Describe phases of Penetration Testing
- Identification and Evaluation of tools and techniques to perform Penetration Testing.
- Prepare penetration test reports.

Unit I

Introduction to Web Application Technologies: HTTP Protocol, REST, Cookies, Encoding Schemes.

Web Functionalities: Server Side and Client Side. Phases of Penetration Testing, Mapping the Application: Enumerating content and functionality. Web Spidering, Discovering Hidden Parameters, Analyzing the Application, Mapping the attack Surface.

Unit II

Bypassing Client Side Controls: Client side data transmission, capturing user data from HTML forms and browser extensions, Handling client side data securely.

Attacking authentication: Authentication technologies, Design flaws in Authentication, Implementation Flaws in Authentication, Securing Authentication. Attacking Session Management: Session Management, Weaknesses in token generation, weaknesses in Session token handling, Securing Session Management.

Unit III

Attacking Access Controls: Common vulnerabilities, Testing access control mechanisms, Securing Access Control. Database testing: Injection Attacks: SQL Injection- First order and second order SQL Injection, SQL exploitation tools, Preventing SQL Injection, Escalating the Database attack.

Attacking Backend components: Injecting operating System commands, Manipulating File Paths, Injecting into email services.

Unit IV

Cross Site Scripting (XSS): XSS Types, Finding and exploiting XSS vulnerabilities, XSS Security measures. Request Forgery, Capturing cross domain data, Same origin policy, Open redirection vulnerabilities, Attacking the browser. Exploiting error messages, Preventing Information Leakage, Attacking the application Server: Configuration vulnerabilities, Server Software Flaws, Writing test reports.

Text books:

1. Stuttard, D. and Pinto, M. (2011). The Web Application Hacker's Handbook, 2nd Edition, Wiley.
2. Open Web Application Security Project Testing Guide v4.0.
<https://www.owasp.org/images/1/19/OTGv4.pdf>

Suggested readings:

1. Prasad, P.(2016), Mastering Modern Web Penetration Testing, Packt Publishing.
2. Mahajan, A.(2015), Burp Suite Essentials, Packt Publishing.

Objective: The objective of the course is to teach the concepts embedded system design. The course focuses on how to write program and peripheral interfacing of AVR microcontroller and develop the applications.

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

- Understand the fundamentals of embedded systems.
- Describe the differences of microprocessor and microcontroller and explain the microcontroller architecture.
- Construct the assemble language programs.

Unit I

INTRODUCTION TO EMBEDDED SYSTEM: embedded system architecture, classifications of embedded systems, challenges and design issues in embedded systems, fundamentals of embedded processor and microcontrollers, CISC vs. RISC, fundamentals of Vonneuman/Harvard architectures, types of microcontrollers, and selection of microcontrollers.

Unit II

8051 ARCHITECTURE : Basic organization, 8051 CPU structure, Register file, Interrupts, Timers, Port circuits, Instruction set, Timing diagram, Addressing modes, Simple Program and Applications.

Unit III

PERIPHERALS AND INTERFACING Typical Bus structure – Bus – memory organization – Timing characteristics – Extended Model and Memory Interfacing – Polling – Interfacing Basic I/O devices – Analog and Digital interfacing – PWM mode operation – Serial port application.

Unit IV

INTRODUCTION TO REAL TIME OPERATING (RTO): Embedded System Design (Host and target machines – Linkers / Locators for Embedded Software – Debugging techniques – Instruction set simulators Laboratory tools – Practical example – Source code), Case Study: RTOS.

Text book:

1. Muhammad Ali Mazidi, Janice Gillispie Mazidi Rolin D. McKinlay The 8051 Microcontroller and Embedded Systems, McGraw-Hill
2. Raj Kamal Embedded Systems, Person
3. Manish K Patel, The 8051 Microcontroller based Embedded Systems, McGraw-Hill

Reference Book:

1. Dhananjay V. Gadre, Programming and Customizing the AVR Microcontroller, TAB Electronics
2. T Bezboruah, K C Sharma , A Goswami, Embedded System design based on 8051 and PIC family microcontroller, Lambert

Objective: This course is designed to enable a clear understanding and knowledge of the foundations, techniques, and tools in the area of software testing and its practice in the industry. The course will prepare students to be leaders in software testing.

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

- Able to apply software testing knowledge, verification & validation and engineering methods.
- Design and conduct a software test process for a quality software test.
- Understand and identify various software testing problems, and solve these problems by designing and selecting software test models, criteria, strategies, and methods.

Unit I

Overview of Software Engineering: Phases in development of Software, Software Engineering Ethics, Life cycle Revisited(Incremental Development, Agile Methods, RAD), Model-Driven Architecture, Software Product Line, Process Modelling.

Project Management: Project Planning, Project Control (Work Break Down Structure, GANTT Charts, PERT Charts) Project Team Organization, Risk Management, CMM

Unit II

Testing of OO systems: Objects and Classes, OO Testing, Class Testing, Regression Testing, Non-Functional Testing, Acceptance Testing

Software Testing: Levels of testing, Module, Integration, System, Regression, Testing techniques and their Applicability, Functional testing and Analysis Structural testing and Analysis, Error Oriented testing and Analysis, Hybrid Approaches, Integration Strategies, Transaction Flow Analysis, Stress Analysis, Failure Analysis, Concurrency Analysis

Unit III

Overview of Software Metrics: Measurement in Software Engineering, Scope of Software Metrics, Measurement and Models Meaningfulness in measurement, Measurement quality, Measurement process, Scale, Measurement validation, Object-oriented measurements.

Measuring Internal External Product Attributes: Measuring size, aspects of software size, length, functionality and complexity, measuring structure, types of structural measures, Modeling software quality, measuring aspects of software quality, software reliability, basics of software reliability

Unit IV

Software Maintenance: Maintenance Categories, Major causes of Maintenance Problems, Reverse Engineering, Software Evolutions, Organizational and Managerial Issues of Maintenance activities, Maintenance Measurements

Software Refactoring: Principles of Refactoring, Bad Smells in code, Composing Methods of Refactoring, Moving features between objects.

Text book:

1. Pressman Roger S. (2014). Software Engineering a Practitioners Approach, Latest Edition, McGraw-Hill Singapore
2. Peters, James S. Witold Pedrycz, (2011). Software engineering an engineering approach, Wiley India,.
3. Anirban Basu, (2015). Software Quality Assurance, Testing and Metrics, Latest Edition, PHI India.

Reference Book:

1. Vliet Hans Van, (2015). Software Engineering Principles and Practice, Latest Edition, John Wiley & Sons
2. Carlo Ghezzi, Mehdi Jazayeri, Dino Mandriolo,(2003). Fundamental of Software Engineering. Latest Edition, Printice Hall India

Objective: The objective of this course is to ensure that a student learns to understand and implement basic models and algorithms in data warehousing and data mining. The students will learn how to analyze the data and identify the related issues.

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

- Describe the concepts related to data warehousing and data mining
- Summarize the dominant data warehousing architectures
- Use information from a variety of different sources and extract knowledge from large data repositories

Unit I

Fundamentals of Data Mining, Data Mining Architecture: Data Mining primitives, Task relevant data, interestingness measures, presentation and visualization of patterns, Data Mining Architecture, Basic Statistical Descriptions of Data, Data Generalization and Summarization, Attributed oriented induction, Analytical characterization, Mining class comparisons, Measuring Data Similarity and Dissimilarity

Unit II

Data warehouse: Basic Concepts, Multi-tier Architecture, Data Warehousing Modeling: Multidimensional Data Model, Schemas for multidimensional data models, OLAP, Data Warehouse Implementation. Further Development of Data Cube Technology, From Data Warehousing to Data Mining Data Cube Computation and Data Generalization

Unit III

Association Rules: Association rules mining, Mining Association rules from single level, multilevel transaction databases, multidimensional relational databases and data warehouses, Correlational analysis, Constraint based association mining

Advanced Pattern Mining: Pattern Mining in Multilevel, Multidimensional space, Constraint-Based Frequent Pattern Mining, Mining High-Dimensional Data and Colossal Patterns.

Unit IV

Classification and Clustering: Classification and prediction, Decision tree induction, Bayesian classification, Rule based Classification, Classification by Support Vector Machine Cluster analysis, Types of data in clustering, Major Clustering Methods: Partitioning Methods, Hierarchical Methods, Density-based methods, Grid-based methods, Model based clustering methods, clustering high dimensional data, clustering with constraints.

Case studies based on recent trends in data mining.

Text Book:

1. Han, J., Kamber, M. and Pei, J. (2011). Data Mining: Concepts and Techniques. Elsevier.
2. Berson, A. and Smith S.J. (2008). Data Warehousing, Data Mining, & Olap. Tata McGraw-Hill Education

Suggested Readings:

1. Dunham, M.H. (2008). Data Mining: Introductory and Advanced Topics. India: Pearson Education.
2. Data Warehousing Fundamentals – Paulraj Ponnaiah Wiley student Edition

Objective: The objective of this course is to ensure that a student learns to understand and implement basic small web pages using Java and Scripting language. The students will also learn how to develop Dynamic Web sites.

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

- Describe the concepts related to Web Technologies
- Develop Web pages using Scripting Languages
- Develop Dynamic Web Pages and learn the advancements in the field of World Wide Web

Unit I

Internet and World Wide Web: Introduction, Internet addressing, ISP, types of Internet connections, introduction to WWW, web browsers, web servers, URL, HTTP, DNS, web applications, tools for web site creation.

HTML: Introduction to HTML, lists, adding graphics to HTML page, creating tables, linking documents, frames, DHTML and cascading style sheets.

Unit II

Java Script: Introduction, programming constructs: variables, operators and expressions, conditional checking, functions and dialog boxes, JavaScript DOM, creating forms, objects like Window, Navigator, History, Location, introduction to cookies,

Unit III

XML: Why XML, XML syntax rules, XML elements, XML attributes, XML DTD displaying XML with CSS.

PHP: Introduction, syntax, variables, statements, operators, decision making, loops, arrays, strings, forms, get and post methods, functions, cookies, and sessions.

Unit IV

PHP and MySQL: Introduction to MySQL, connecting to MySQL database, creation, insertion, deletion and retrieval of MySQL data using PHP, PHP and XML, XML parsers, XML DOM.

Text Books:

1. Deitel, Deitel, Nieto, and Sandhu, XML How to Program, Pearson Education.
2. Herbert Schildt, Java 2: The Complete Reference, TMH, Fifth Edition.
3. Ivan Bayross : Commercial, Web Enabled Development Application, BPB

Suggested Readings:

1. Schafer Textbooks, HTML, CSS, JavaScript, Perl, Python and PHP, Wiley India

Objective: The main objective of this course is to provide the students with basic as well as advanced knowledge and concepts of Wireless Ad Hoc and Sensor Networks.

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

- identify the basic problems, limitations, strengths of MANETs and WSN;
- explain the current wireless MANETs and WSN networking mechanisms
- Implement basic IoT applications on embedded platform

Unit I

MANET Introduction: Basics of Ad Hoc Networks and their applications, Overview of different challenges in implementing Ad Hoc Networks, Overview of different solutions proposed for overcoming the challenges in these networks.

Self-organizing behaviour: Properties of self-organizing systems, Differences between the self-organizing systems and the conventional ones, Mechanisms for ensuring self-organization in MANETs, **Co-operation:** Dealing with misbehaviors in MANETs, Incentive mechanisms for countering misbehaviors.

Unit II

MAC: Need for MAC protocols for MANETs, Classification of MAC protocols, Hidden and exposed terminal problems, Four MAC protocols explained -MACA -MACAW -DBTMA -MARCH. Routing challenges in MANETs, Proactive, reactive, and hybrid routing protocols.

Multicast routing: Challenges of multicasting in MANETs, Classification of multicast routing protocols, **Mobility model:** Basics of mobility models, Classification of mobility models.

Unit III

Transport layer: Problems of using TCP in MANETs, Different transport protocols for MANETs

Opportunistic Mobile Networks: Basic understanding of OMNs/DTNs, How OMNs differ from other networks, **UAV networks:** Basics of UAV Physics, Challenges in UAV networks.

Wireless Sensor Networks: Introduction, Coverage, Topology management, Mobile Sensor Networks MAC, Congestion control, Routing Underwater WSN, Structure of sensor nodes.

Unit IV

Introduction to IoT: Defining IoT, Characteristics of IoT, Physical design of IoT, Logical design of IoT, Functional blocks of IoT, Communication models & APIs. **IoT & M2M:** Introduction, Machine to Machine, Difference between IoT and M2M, Software defineNetwork.

Implementing IoT concepts with python, Arduino Programming.

Text Books:

1. Murthy, C.S. R. and Manoj, B.S. (2007). Ad hoc Wireless Networks Architectures and protocols, 2nd edition, Pearson Education.
2. Obaidat M. S. and Misra, S. Principles of Wireless Sensor Networks, Cambridge University Press, U.K.
3. Vijay Madiseti, Arshdeep Bahga, "Internet of Things: A Hands-On Approach"
4. Walteneus Dargie, Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice"

Suggested Readings:

1. Toh, C.K. Ad Hoc Wireless Networks: Protocols and Systems, Prentice Hall PTR Upper Saddle River, NJ, USA.
2. Misra,S., Woungang, I. and Misra S. C. Guide to Wireless Sensor Networks, Computer Communications and Networks Series, Springer-Verlag, London, U.K.
3. Francis daCosta, “Rethinking the Internet of Things: A Scalable Approach to Connecting Everything”, 1 st Edition, Apress Publications, 2013.
4. Getting Started with Raspberry Pi, Matt Richardson & Shawn Wallace, O'Reilly (SPD), 2014.

CBS.531

Information and Network Security - Lab

Credits: 0-0-2

Students will implement the lab practical as per the syllabus of the subject.

CBS.532

Ethical Hacking & Forensics - Lab

Credits: 0-0-2

Students will implement the lab practical as per the syllabus of the subject.

SEMESTER- III

CBS.551

Capstone Lab-I

Credits: 0-0-4

The students should be required to implement an application for the Industrial/Scientific/Research Community.

Objective: To have an advanced level of understanding of most recent advancements in Big Data and using insights, statistical models, visualization techniques for its effective application in Business intelligence.

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

1. Understand the concepts and challenge of Big Data.
2. Collect, Manage, store, query, and analyze various forms of Big Data
3. Understand the impact of Big Data for business decisions and strategy.

Unit I

Introduction to Data Analytics: Data and Relations, Data Visualization, Correlation, Regression, Forecasting

Big Data Technology: Fundamentals of Big Data Types, Big data Technology Components, Big Data Architecture, Big Data Warehouses, Functional vs. Procedural Programming Models for Big Data.

Unit II

Hadoop: Introduction to Hadoop Ecosystem, HDFS, Map-Reduce Programming, Spark, PIG, JAQL. Understanding Text Analytics and Big Data, Predictive analysis on Big Data, Role of Data analyst.

Unit III

Supervised Learning: Regression Bias-Variance Dichotomy, Model Validation Approaches, Logistic Regression, Linear Discriminant Analysis, Quadratic Discriminant Analysis, and Regression.

Supervised Learning for Big Data with Classification technique: Classification Trees Support Vector Machines. Ensemble Methods: Random Forest, Neural Networks, Introduction Deep learning

Unit IV

Unsupervised Learning and Challenges for Big Data Analytics: Clustering, Clustering Analysis, Associative Rule Mining, Challenges for Big data Analytics.

Text Book:

1. Minelli M., Chambers M., Dhiraj A., Big Data, Big Analytics: Emerging Business
2. White T., Hadoop: The Definitive Guide, O' Reilly Media (2012), 3rd ed.

Objective: The main objective is to make the students understand the problems with traditional security systems and introduce the concept of biometric security systems.

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

- Describe the theory of biometric security
- Classify algorithms related to various biometrics
- Evaluate the performance of various biometric systems

Unit I

Introduction: Fundamental steps in Image Processing System, Image Sensing and acquisition, Image sampling & Quantization, Basic Relationship between pixels.

Image Enhancement Techniques: Spatial Domain Methods: Basic grey level transformation, Histogram equalization, Image subtraction, image averaging, Spatial filtering: Smoothing, sharpening filters, Laplacian filters, Frequency domain filters, Smoothing and sharpening filters.

Unit II

Image Restoration & Reconstruction: Model of Image Degradation/restoration process, Noise models, spatial filtering, inverse filtering, Minimum mean square Error filtering, and constrained least square filtering.

Image edge detection: Introduction to edge detection, types of edge detectors.

Biometrics Introduction: Benefits of biometrics over traditional authentication systems, Benefits of biometrics in identification systems, Comparison of various biometric traits, Applications. Key biometric terms and processes: biometric verification and identification, how biometric matching works.

Unit III

Physiological Biometric Technologies: Fingerprints: Working, characteristics, Competing technologies, strengths, weaknesses and deployment.

Facial scan: Working, Strengths, weaknesses and deployment. Advanced Topics: Handling pose, illumination, and expression variations, Heterogeneous face recognition, Face modelling.

Iris Scan: working, strengths, weaknesses and deployment

Unit IV

Signature technology: Technical description, classification, keystroke-scan.

Security of Biometric Systems: Adversary Attacks, Attack on biometric processing, Attacks on the template database, Database security, Template security techniques.

Text books:

1. Jain, A. K., Ross, A. A. (2011). Introduction to Biometrics. Springer Science & Business Media.
2. Gonzalez, R.C. and Woods, R.E. (2009). Digital Image Processing. 2nd ed. India: Person Education.
3. G.R. Sinha, Sandeep B. Patil. (2013). Biometrics: Concepts and Applications. Wiley India.

Suggested readings:

1. Chirillo, J. and Blaul, S. (2003). Implementing Biometric Security. Wiley.
2. Wang, P. S. P. (2012). Pattern Recognition, Machine Intelligence and Biometrics. Springer Science & Business Media.
3. Nanavati, S., Thieme, M. and Nanavati, R. (2002). Biometrics: Identity Verification in a Networked World. John Wiley & Sons.

CBS.554

E-Privacy: Privacy & Trust in the Electronic Society

Credits: 3-1-0

Objective: This subject will provide the knowledge of various concepts involved in efficient E-Privacy that would help in prevent from the crimes.

Course Outcomes:

1. Gain an in-depth look into privacy laws and regulations as well as into technologies for achieving privacy in an electronic world.
2. Differentiate clearly between security and privacy and understand the tradeoffs.
3. Understand various trust metrics, designs and trust models

Unit I

Introduction: Privacy and Security Issues in a Digital World, Privacy Principles and Policies, Authentication and Privacy, Data Mining, Privacy on the Web, E-mail Security, Impacts on Emerging Technologies. Ethical Aspects of Information Security and Privacy

Unit II

Data and System Security

Authorization and Access Control, Role-Based Access Control, Database Security Trust Management, Trusted Platforms, Strong Authentication with Physical Unclonable Functions

Unit III

Privacy Enhancing

Privacy-Preserving Data Mining, Statistical Database Security, Different Search Strategies on Encrypted Data Compared, Client-Server Trade-Offs in Secure Computation, Federated Identity Management, Accountable Anonymous Communication

Unit IV

Digital Asset Protection

An Introduction to Digital Rights Management Systems , Copy Protection Systems Forensic Watermarking in Digital Rights Management , Person-Based and Domain-Based Digital Rights Management , Digital Rights Management Interoperability, DRM for Protecting Personal Content

Enhancing Privacy for Digital Rights Management: Privacy Policies, RFID and Privacy, Malicious Software in Ubiquitous Computing

TEXT BOOK

1. **Security, Privacy and Trust in Modern Data Management** By Milan Petkovic, Willem Jonker, Springer, ISBN: 978-3-540-69860-9

REFERENCE BOOK

1. **Security in Computing**, Prentice Hall, Charles P. Pfleeger , Shari Lawrence Pfleeger

Objective: This subject will provide the knowledge of various concepts involved in efficient information retrieval that leads to the development of efficient Web crawling techniques.

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

- Understand efficient techniques for indexing of document object that are to be retrieved
- Analyze the performance of retrieval systems using test collections
- Apply Information Retrieval principles to locate relevant information in large collection of data

Unit I

Introduction: Introduction to Information Retrieval. Inverted indices and Boolean queries. Query optimization. The nature of unstructured and semi-structured text.

The term vocabulary and postings lists: Text encoding: tokenization, stemming, lemmatization, stop words, phrases. Optimizing indices with skip lists. Proximity and phrase queries. Positional indices.

Unit II

Dictionaries and tolerant retrieval: Dictionary data structures. Wild-card queries, permuterm indices, n-gram indices. Spelling correction and synonyms: edit distance, Soundex, language detection.

Index construction: Postings size estimation, sort-based indexing, dynamic indexing, positional indexes, n-gram indexes, distributed indexing, real-world issues.

Unit III

Scoring: Term weighting and the vector space model. Parametric or fielded search. Document zones. The vector space retrieval model. Weighting. The cosine measure. Scoring documents.

Computing scores in a complete search system: Components of an IR system. Efficient vector space scoring. Nearest neighbor techniques, reduced dimensionality approximations, random projection.

Unit IV

Classification: Naive Bayes models. Spam filtering, K Nearest Neighbors, Decision Trees, Support vector machine classifiers.

Web Crawling: What makes the web different? Web search overview, web structure, the user, paid placement, search engine optimization. Web size measurement, Crawling and web indexes. Near-duplicate detection, Link analysis, learning to rank, focused web crawler and its different architectures.

Text Book

1. C. Manning, P. Raghavan, and H. Schütze: *Introduction to Information Retrieval*, Cambridge University Press, 2008
2. R. Baeza-Yates, B. Ribeiro-Neto: *Modern Information Retrieval*, Addison-Wesley, 1999

Objectives:

1. The student shall have to write his/ her synopsis including an extensive review of literature with simultaneous identification of scientifically sound (and achievable) objectives backed by a comprehensive and detailed methodology. The students shall also present their synopsis to the synopsis approval committee. The Evaluation criteria will be as detailed below:

Evaluation Parameter	Grade
Review of literature	Satisfactory/Un-Satisfactory
Identification of gaps in knowledge and Problem Statement	Satisfactory/Un-Satisfactory
Objective formulation & Methodology	Satisfactory/Un-Satisfactory
Presentation	Satisfactory/Un-Satisfactory
Total	Satisfactory/Un-Satisfactory

2. The second objective of Dissertation would be to ensure that the student learns the nuances of the scientific research. Herein the student shall have to carry out the activities/experiments to be completed during Dissertation (as mentioned in the synopsis).

The students would present their work to the Evaluation Committee (constituted as per the university rules). The evaluation criteria shall be as detailed below:

Evaluation Parameter	Maximum Marks	Evaluated By
Mid Term Review and Presentation	Satisfactory/Un-Satisfactory	Evaluation Committee
Continuous evaluation	Satisfactory/Un-Satisfactory	Supervisor
Total	Satisfactory/Un-Satisfactory	
Total Objective 1 + Objective 2	Satisfactory/Un-Satisfactory	

SEMESTER IV

CBS.571

Capstone Lab-II

Credits: 0-0-4

The students should be required to implement an application for the Industrial/Scientific/Research Community

CBS.600

Dissertation

Credits: 20

In Dissertation the student shall have to carry out the activities/experiments to be completed during Dissertation (as mentioned in the synopsis). The students would present their work to the evaluation Committee (constituted as per the university rules). One research paper (either accepted or published) out of the dissertation research work is compulsory before pre-submission evaluation of dissertation. The Evaluation criteria shall be as detailed below:

Evaluation Parameter	Maximum Marks	Evaluated By
Parameters by External Expert (As per University Criteria)	Satisfactory/Un-Satisfactory	External Expert
Presentation and defence of research work	Satisfactory/Un-Satisfactory	Evaluation Committee
Total	Satisfactory/Un-Satisfactory	