### AFFILIATED INSTITUTIONS
### ANNA UNIVERSITY, CHENNAI
### REGULATIONS – 2013
### M.E. BIOMETRICS AND CYBER SECURITY
### I TO IV SEMESTERS CURRICULA AND SYLLABI (FULL TIME)

#### SEMESTER I

<table>
<thead>
<tr>
<th>SL. NO.</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>THEORY</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>MA7155</td>
<td>Applied Probability and Statistics</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>2.</td>
<td>CP7101</td>
<td>Design and Management of Computer Networks</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3.</td>
<td>CP7102</td>
<td>Advanced Data Structures and Algorithms</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4.</td>
<td>BC7101</td>
<td>Biometric Systems</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>5.</td>
<td>BC7102</td>
<td>Database Design and Security</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>6.</td>
<td>Elective I</td>
<td></td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td><strong>PRACTICAL</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>BC7111</td>
<td>Advanced Data Structures Laboratory</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>8.</td>
<td>BC7112</td>
<td>Technical Seminar</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td></td>
<td></td>
<td>18</td>
<td>1</td>
<td>6</td>
<td>22</td>
</tr>
</tbody>
</table>

#### SEMESTER II

<table>
<thead>
<tr>
<th>SL. NO.</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>THEORY</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>NE7202</td>
<td>Network and Information Security</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2.</td>
<td>BC7201</td>
<td>Biometric Image Processing</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3.</td>
<td>BC7202</td>
<td>Intrusion Detection and Prevention Systems</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4.</td>
<td>BC7203</td>
<td>Cyber Security</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>5.</td>
<td>Elective II</td>
<td></td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>6.</td>
<td>Elective III</td>
<td></td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td><strong>PRACTICAL</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>BC7211</td>
<td>Cyber Security Laboratory</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>8.</td>
<td>BC7212</td>
<td>Biometric Image Processing Laboratory</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td></td>
<td></td>
<td>18</td>
<td>0</td>
<td>6</td>
<td>22</td>
</tr>
</tbody>
</table>

#### SEMESTER III

<table>
<thead>
<tr>
<th>SL. NO.</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>THEORY</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>BC7301</td>
<td>Ethical Hacking and Network Defense</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2.</td>
<td>Elective IV</td>
<td></td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3.</td>
<td>Elective V</td>
<td></td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td><strong>PRACTICAL</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>BC7311</td>
<td>Project Work Phase I</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td>6</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td></td>
<td></td>
<td>9</td>
<td>0</td>
<td>12</td>
<td>15</td>
</tr>
</tbody>
</table>
### SEMESTER IV

<table>
<thead>
<tr>
<th>SL. NO</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>PRACTICAL</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>BC7411</td>
<td>Project Work Phase II</td>
<td>0</td>
<td>0</td>
<td>24</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>TOTAL</strong></td>
<td>0</td>
<td>0</td>
<td>24</td>
<td>12</td>
</tr>
</tbody>
</table>

**TOTAL NO. OF CREDITS: 71**

### LIST OF ELECTIVES

#### SEMESTER I

<table>
<thead>
<tr>
<th>SL. NO</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>BC7001</td>
<td>Multicore Architectures and Security Analysis</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2.</td>
<td>BC7002</td>
<td>Software Engineering</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3.</td>
<td>BC7003</td>
<td>Applied Cryptography</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4.</td>
<td>SE7003</td>
<td>Machine Learning</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>5.</td>
<td>CP7025</td>
<td>Data Mining Techniques</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

#### SEMESTER II

<table>
<thead>
<tr>
<th>SL. NO</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>NE7003</td>
<td>Web Engineering</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2.</td>
<td>BC7004</td>
<td>Access Control and Identity Management System</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3.</td>
<td>EL7001</td>
<td>Artificial Intelligence</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4.</td>
<td>BC7005</td>
<td>Operating Systems Security</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>5.</td>
<td>BC7006</td>
<td>Trust Management in E - Commerce</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>6.</td>
<td>BC7007</td>
<td>Biometric Security</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>7.</td>
<td>BC7008</td>
<td>Distributed System Security</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>8.</td>
<td>NE7002</td>
<td>Mobile and Pervasive Computing</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

#### SEMESTER III

<table>
<thead>
<tr>
<th>SL. NO</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>CU7001</td>
<td>Real Time Embedded Systems</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2.</td>
<td>NE7201</td>
<td>Network Programming</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3.</td>
<td>NE7012</td>
<td>Social Networks Analysis</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4.</td>
<td>CP7022</td>
<td>Software Design</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>5.</td>
<td>BC7009</td>
<td>Steganography and Digital Watermarking</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>6.</td>
<td>BC7010</td>
<td>Security Threats</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>7.</td>
<td>CP7019</td>
<td>Managing Big Data</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>8.</td>
<td>NE7011</td>
<td>Mobile Application Development</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>9.</td>
<td>BC7011</td>
<td>Wireless Security</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>10.</td>
<td>IF7202</td>
<td>Cloud Computing</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>11.</td>
<td>BC7012</td>
<td>Cybercrime Investigations and Digital Forensics</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>
OBJECTIVES:
- To introduce the basic concepts of one dimensional and two dimensional Random Variables.
- To provide information about Estimation theory, Correlation, Regression and Testing of hypothesis.
- To enable the students to use the concepts of multivariate normal distribution and principle components analysis.

UNIT I ONE DIMENSIONAL RANDOM VARIABLES
Random variables - Probability function – Moments – Moment generating functions and their properties – Binomial, Poisson, Geometric, Uniform, Exponential, Gamma and Normal distributions – Functions of a Random Variable.

UNIT II TWO DIMENSIONAL RANDOM VARIABLES
Joint distributions – Marginal and Conditional distributions – Functions of two dimensional random variables – Regression Curve – Correlation.

UNIT III ESTIMATION THEORY

UNIT IV TESTING OF HYPOTHESES
Sampling distributions - Type I and Type II errors - Tests based on Normal, t,2 and F distributions for testing of mean, variance and proportions – Tests for Independence of attributes and Goodness of fit.

UNIT V MULTIVARIATE ANALYSIS
Random Vectors and Matrices - Mean vectors and Covariance matrices - Multivariate Normal density and its properties - Principal components Population principal components - Principal components from standardized variables.

OUTCOME:
- The student will able to acquire the basic concepts of Probability and Statistical techniques for solving mathematical problems which will be useful in solving Engineering problems

REFERENCES:
UNIT I  INTRODUCTION TO NETWORK MANAGEMENT  9

UNIT II  REQUIREMENTS ANALYSIS  9
Requirement Analysis Process – Gathering and Listing Requirements- Developing service metrics – Characterizing behavior – Developing RMA requirements – Developing delay Requirements - Developing capacity Requirements - Developing supplemental performance Requirements – Requirements mapping – Developing the requirements specification

UNIT III  FLOW ANALYSIS  9

UNIT IV  NETWORK ARCHITECTURE  9

UNIT V  NETWORK DESIGN  9

REFERENCES:

TOTAL: 45 PERIODS
OBJECTIVES:
- To understand the principles of iterative and recursive algorithms.
- To learn the graph search algorithms.
- To study network flow and linear programming problems.
- To learn the hill climbing and dynamic programming design techniques.
- To develop recursive backtracking algorithms.
- To get an awareness of NP completeness and randomized algorithms.
- To learn the principles of shared and concurrent objects.
- To learn concurrent data structures.

UNIT I  ITERATIVE AND RECURSIVE ALGORITHMS  9

UNIT II  OPTIMISATION ALGORITHMS  9

UNIT III  DYNAMIC PROGRAMMING ALGORITHMS  9

UNIT IV  SHARED OBJECTS AND CONCURRENT OBJECTS  9

UNIT V  CONCURRENT DATA STRUCTURES  9

TOTAL : 45 PERIODS

OUTCOMES:
Upon completion of the course, the students will be able to
- Design and apply iterative and recursive algorithms.
- Design and implement optimisation algorithms in specific applications.
- Design appropriate shared objects and concurrent objects for applications.
- Implement and apply concurrent linked lists, stacks, and queues.
REFERENCES:

BC7101 BIOMETRIC SYSTEMS  L  T  P  C  3  0  0  3

UNIT I  INTRODUCTION  9
Biometric fundamentals – Biometric technologies – Biometrics Vs traditional techniques – Characteristics of a good biometric system – Benefits of biometrics – Key biometric processes: verification, identification and biometric matching – Performance measures in biometric systems: FAR, FRR, FTE rate, EER and ATV rate.

UNIT II  PHYSIOLOGICAL BIOMETRICS  9

UNIT III  AUTOMATED BIOMETRIC SYSTEM AND BEHAVIOURAL BIOMETRICS  9
Automated fingerprint identification systems - Leading technologies: Signature-scan – Keystroke scan – components, working principles, strengths and weaknesses.

UNIT IV  BIOMETRIC APPLICATIONS  9
Categorizing biometric applications – application areas: criminal and citizen identification, surveillance, PC/network access, e-commerce and retail/ATM – costs to deploy – other issues in deployment

UNIT V  PRIVACY AND STANDARDS IN BIOMETRICS  9

TOTAL : 45 PERIODS

REFERENCES:
UNIT I  INTRODUCTION  9
Data models, structure of relational databases, component of management system – DDL, DML, database languages, SQL standard, database users and administrators.

UNIT II  RELATIONAL DBMS  9
Design issues - basic normal forms and additional normal forms, Transforming E-R diagram to relations, Integrity constraints, Query processing and optimization

UNIT III  TRANSACTION PROCESSING  9
Transaction concept, concurrent execution, isolation, testing for serializability, Concurrency control, lock based - time-stamp based - validation based protocols, multi-version schemes, deadlock handling.

UNIT IV  DATABASE SECURITY  9
Introduction to database security, security models, physical and logical security, security requirements, reliability and integrity, sensitive data, inference, multilevel databases and multilevel security, access control- mandatory and discretionary, security architecture, issues.

UNIT V  SECURITY ISSUES  9
Application access, security and authorization, authorization in SQL, encryption and authentication, secure replication mechanisms, Audit- logon/logoff, sources, usage and errors, changes, external audit system architecture, archive and secure auditing information

REFERENCES:

BC7111  ADVANCED DATA STRUCTURES LABORATORY  L T P C
OBJECTIVES:
• To learn to implement iterative and recursive algorithms.
• To learn to design and implement algorithms using hill climbing and dynamic programming techniques.
• To learn to implement shared and concurrent objects.
• To learn to implement concurrent data structures.

LAB EXERCISES:
Each student has to work individually on assigned lab exercises. Lab sessions could be scheduled as one contiguous us four-hour session per week or two two-hour sessions per week. There will be about 15 exercises in a semester. It is recommended that all implementations are carried out in Java. If C or C++ has to be used, then the threads library will be required for concurrency. Exercises should be designed to cover the following topics:
• Implementation of graph search algorithms.
• Implementation and application of network flow and linear programming problems.
• Implementation of algorithms using the hill climbing and dynamic programming design techniques.
• Implementation of recursive backtracking algorithms.
• Implementation of randomized algorithms.
• Implementation of various locking and synchronization mechanisms for concurrent linked lists, concurrent queues, and concurrent stacks.
• Developing applications involving concurrency.

TOTAL: 60 PERIODS

BC7112   TECHNICAL SEMINAR

The objective of this technical seminar is to enable the students to read technical article, comprehend and to share with others

The students should read a recent technical article from any of the leading reputed journals like:
• IEEE Transactions
• ACM
• Springer
• Elsevier publications

In the area of
• Biometric Systems
• Biometric Image Processing
• Intrusion Detection and Prevention Systems
• Cyber Security
• Ethical Hacking
• Network Defense

and present to the fellow students with a technical report. External assessment should be conducted along with web technology lab.

TOTAL: 30 PERIODS

NE7202   NETWORK AND INFORMATION SECURITY

OBJECTIVES:
• To understand the fundamentals of Cryptography
• To acquire knowledge on standard algorithms used to provide confidentiality, integrity and authenticity.
• To understand the various key distribution and management schemes.
• To understand how to deploy encryption techniques to secure data in transit across data networks
• To design security applications in the field of Information technology
UNIT I INTRODUCTION 9

UNIT II CRYPTO SYSTEMS & AUTHENTICATION 9

UNIT III PUBLIC KEY CRYPTO SYSTEMS 9
Introduction to Public key Cryptography - Number theory - The RSA Cryptosystem and Factoring Integer - Attacks on RSA - The ELGamal Cryptosystem - Digital Signature Algorithm - Finite Fields - Elliptic Curves Cryptography - Key management – Session and Interchange keys, Key exchange and generation - PKI

UNIT IV SYSTEM IMPLEMENTATION 9

UNIT V NETWORK SECURITY 9
Secret Sharing Schemes - Kerberos - Pretty Good Privacy (PGP) - Secure Socket Layer (SSL) - Intruders – HIDS - NIDS - Firewalls - Viruses

TOTAL : 45 PERIODS

OUTCOMES:
Upon Completion of the course, the students will be able to
• Implement basic security algorithms required by any computing system.
• Analyze the vulnerabilities in any computing system and hence be able to design a security solution.
• Analyze the possible security attacks in complex real time systems and their effective countermeasures
• Identify the security issues in the network and resolve it.
• Evaluate security mechanisms using rigorous approaches, including theoretical derivation, modeling, and simulations
• Formulate research problems in the computer security field

REFERENCES:
UNIT I  FUNDAMENTALS OF IMAGE PROCESSING  

UNIT II  FINGERPRINT BIOMETRICS  
Fingerprint Patterns, Fingerprint Features, Fingerprint Image, width between two ridges - Fingerprint Image Processing - Minutiae Determination - Fingerprint Matching: Fingerprint Classification, Matching policies.

UNIT III  FACE RECOGNITION  
Detection and Location of Faces: Statistics-Based method, Knowledge-Based method - Feature Extraction and Face Recognition: Gray value Based method, Geometry Feature Based method, Neural Networks method.

UNIT IV  IRIS BIOMETRICS  

UNIT V  FUSION IN BIOMETRICS  
Introduction to Multibiometrics - Information Fusion in Biometrics - Issues in Designing a Multibiometric System - Sources of Multiple Evidence - Levels of Fusion in Biometrics - Sensor level, Feature level, Rank level, Decision level fusion - Score level Fusion.

TOTAL :45 PERIODS

REFERENCES:
UNIT IV LEGAL ISSUES AND ORGANIZATIONS STANDARDS
Intrusion detection in security – Threat Briefing – Quantifying risk – Return on Investment (ROI)
Law Enforcement / Criminal Prosecutions – Standard of Due Care – Evidentiary Issues, Organizations and Standardizations.

UNIT V APPLICATIONS AND TOOLS:
Tool Selection and Acquisition Process – Bro Intrusion Detection – Prelude Intrusion Detection –
Cisco Security IDS - Snorts Intrusion Detection – NFR security

REFERENCES:

REFERENCES:
1. Jennifer L. Bayuk, J. Healey, P. Rohmeyer, Marcus Sachs, Jeffrey Schmidt, Joseph Weiss
to Do About It” Ecco 2010
BC7211 CYBER SECURITY LABORATORY

1. Implementation of Substitution and Transposition ciphers
2. Implementation of Data Encryption Standard
3. Implementation of International Data Encryption Algorithm
4. Implementation of Advanced Encryption Standard
5. Implementation of RSA Algorithm
6. Implementation of Diffie-Hellman Key Exchange
7. Implementation of Message Authentication Codes
8. Implementation of Hash functions
9. Implementation of Digital Signature Standard
10. Hiding of confidential information within Image

TOTAL: 45 PERIODS

BC7212 BIOMETRIC IMAGE PROCESSING LABORATORY

List of Experiments
1. Image Enhancement
2. Image Segmentation
3. Image Acquisition - Fingerprint
4. Feature Extraction - Fingerprint
5. Image Acquisition - Face
6. Feature Extraction - Face
7. Image Acquisition - Iris
8. Feature Extraction - Iris
9. Multimodal Biometrics - Serial
10. Multimodal Biometrics - Parallel

TOTAL: 45 PERIODS

BC7301 ETHICAL HACKING AND NETWORK DEFENSE

UNIT I ETHICAL HACKING AND SOCIAL ENGINEERING

UNIT II SERVICE SCANNING

UNIT III HACKING NETWORKS
UNIT IV  Hacking Operating Systems  9
Share Permissions – Hardcore Vulnerability Exploitation. Linux: Vulnerabilities – Information
Gathering – Unconnected Services - .rhosts and hosts.equiv Files – NFS – File Permissions –
Buffer Overflow.

UNIT V  Hacking Applications  9
Messaging Systems – Web Applications – Mobile Applications - Databases - Reporting Results.

References:
1. Michael T. Simpson, “Ethical Hacking and Network Defense”, Cengage Learning, New Delhi,
   2010.
5. Bensmith, and Brian Komer, “Microsoft Windows Security Resource Kit”, Prentice Hall of
   India, 2010.

BC7001  Multicore Architectures and Security Analysis  L T P C
                                                3 0 0 3

Objectives:
- To understand the recent trends in the field of Computer Architecture and identify performance
  related parameters
- To appreciate the need for parallel processing
- To expose the students to the problems related to multiprocessing
- To understand the different types of multicore architectures
- To expose the students to warehouse-scale and embedded architectures

Unit I  Fundamentals of Quantitative Design and Analysis  9
Measuring, Reporting and Summarizing Performance – Quantitative Principles of Computer Design
– Classes of Parallelism - ILP, DLP, TLP and RLP - Multithreading - SMT and CMP Architectures –
Limitations of Single Core Processors - The Multicore era – Case Studies of Multicore
Architectures.

Unit II  RLP and DLP in Warehouse-Scale Architectures  9
Programming Models and Workloads for Warehouse-Scale Computers – Architectures for
Warehouse-Scale Computing – Physical Infrastructure and Costs – Cloud Computing – Case
Studies.

Unit III  Architectures for Embedded Systems  9
Features and Requirements of Embedded Systems – Signal Processing and Embedded

Unit IV  Security Analysis  9
Basic components of Security - Confidentiality - Integrity, Availability – Threats Security policies -
types , role of trust - types of access control
UNIT V AUTHENTICATION AND CONFINEMENT
Basics, Passwords: attacking, countering, password ageing Biometrics Confinement Problem - Introduction, isolation virtual machines, sandboxes, covert channels, detection analysis, mitigation

OUTCOMES:
Upon completion of the course, the students will be able to
• Identify the limitations of ILP and the need for multicore architectures
• Discuss the issues related to multiprocessing and suggest solutions
• Point out the salient features of different multicore architectures and how they exploit parallelism
• Critically analyze the different types of interconnection networks
• Discuss the architecture of GPUs, warehouse-scale computers and embedded processors

REFERENCES:

BC7002 SOFTWARE ENGINEERING

OBJECTIVES:
• To provide information about wider engineering issues that form the background to develop complex, evolving (software-intensive) systems.
• To plan a software engineering process to account for quality issues and non-functional requirements.
• To employ a selection of concepts and techniques to complete a small-scale analysis and design in mini projects.
• To impart knowledge to translate requirement specifications into a design, and then realize that design practically, all using an appropriate software engineering methodology.
• To provide basic knowledge about software project management.

UNIT I INTRODUCTION

UNIT II REQUIREMENT ANALYSIS

UNIT III SOFTWARE DESIGN

UNIT IV SOFTWARE TESTING
UNIT V SOFTWARE MAINTENANCE AND SOFTWARE METRICS


TOTAL: 45 PERIODS

OUTCOMES:
Upon completion of the course, the students should be able to:
- Familiarize the basic concepts of Software design and implementation.
- Perform software testing on various applications.
- Apply various software metrics on software quality products.

REFERENCES:

BC7003 APPLIED CRYPTOGRAPHY

UNIT I INTRODUCTION
Cryptography and modern cryptography – The setting of private-key encryption – Historical ciphers and their cryptanalysis – Basic principles of modern cryptography – Services, Mechanisms and Attacks – OSI security architecture.

UNIT II SYMMETRIC TECHNIQUES

UNIT III ASYMMETRIC TECHNIQUES

UNIT IV MESSAGE AUTHENTICATION
Authentication requirements – Authentication functions – Message Authentication Codes (MAC) – Hash functions – Security of hash functions and MACs.

UNIT V HASH AND DIGITAL SIGNATURES

TOTAL : 45 PERIODS

REFERENCES:
UNIT I  INTRODUCTION  9

UNIT II  NEURAL NETWORKS AND GENETIC ALGORITHMS  9

UNIT III  BAYESIAN AND COMPUTATIONAL LEARNING  9

UNIT IV  INSTANT BASED LEARNING  9
K-Nearest Neighbour Learning – Locally weighted Regression – Radial Bases Functions – Case Based Learning.

UNIT V  ADVANCED LEARNING  9

REFERENCES:

TOTAL: 45 PERIODS
UNIT III  CLASSIFICATIONS

UNIT IV  CLUSTER ANALYSIS

UNIT V  ASSOCIATION RULE MINING AND VISUALIZATION

TOTAL: 45 PERIODS

REFERENCE S:

NE7003  WEB ENGINEERING

OBJECTIVES:
- To understand the issues and process of Web design.
- To learn the concepts of Web design patterns and page design.
- To understand and learn the scripting languages with design of web applications.
- To learn the maintenance and evaluation of web design management.

UNIT I  INTRODUCTION TO WEB ENGINEERING

UNIT II  INFORMATION ARCHITECTURE
UNIT III  HTML & DHTML  9
HTML Basic Concept, Static & dynamic HTML, Structure of HTML documents, HTML Elements, Linking in HTML, Anchor Attributes, Image Maps, Meta Information, Image Preliminaries, Layouts, backgrounds, Colors and Text, Fonts, Tables, Frames and layers, Audio and Video Support with HTML Database integration, CSS, Positioning with Style sheets, Forms Control, Form Elements, Introduction to CGI PERL, JAVA SCRIPT, PHP, ASP , Cookies Creating and Reading Cookies.

UNIT IV  XML  9

UNIT V  APPLICATIONS AND SECURITY  9

OUTCOMES:
Upon completion of the course, the students will be able to
1. Identify the various issues of web design process and evaluation.
2. Determine templates for web pages and layout.
3. Develop simple web applications using scripting languages.
4. Determine the various issues of web project development.
5. Address the core issues of web page maintenance and evaluation.

REFERENCES:
4. NEIL GRAY , “Web server Programming” Wiley
5. CHRIS BATES Web Programming :Building Internet applications, Wiley

BC7004  ACCESS CONTROL AND IDENTITY MANAGEMENT SYSTEM  L T P C
3 0 0 3

UNIT I  ACCESS CONTROL  9

UNIT II  TRUST PARADIGMS IN COMPUTING  9
UNIT III   MANDATORY ACESS CONTROL
Mandatory access control - Comparing information flow in BLP and BIBA models – Combining the BLP and BIBA models – Chinese wall problem.

UNIT IV   DISCRETIONARY ACCESS CONTROL

UNIT V   ROLE BASED ACCESS CONTROL
Role based access control – Hierarchical Access Control - Mapping of a mandatory policy to RABC – Mapping discretionary control to RBAC – RBAC flow analysis – Separation of Duty in RBAC – RBAC consistency properties - The privileges perspective of separation of duties – Functional specification for RBAC.

REFERENCES

TOTAL : 45 PERIODS

EL7001   ARTIFICIAL INTELLIGENCE

OBJECTIVES:  
To provide in-depth knowledge about
• Searching Techniques
• Knowledge Representation
• Learning

OUTCOMES:  
Students will be able to
• Explain Uniform search strategies and searching with partial information
• Understand Backtracking, Local and Adversarial Search
• Describe Learning decision trees
• Explain Probabilistic language processing

UNIT I   INTRODUCTION

UNIT II   SEARCHING TECHNIQUES
UNIT III KNOWLEDGE REPRESENTATION 10

UNIT IV LEARNING 9

UNIT V APPLICATIONS 8

REFERENCES:
REFERENCES:

BC7006 TRUST MANAGEMENT IN E-COMMERCE

UNIT I INTRODUCTION TO E-COMMERCE

UNIT II E-COMMERCE SECURITY

UNIT III TRUST IN E-COMMERCE

UNIT IV TRUSTED COMPUTING PLATFORM
Introduction to trusted computing platform: Overview – Usage Scenarios – Key components of trusted platform – Trust mechanisms in a trusted platform

UNIT V TRUST MODELS
Trusted platforms for organizations and individuals – Trust models and the E-Commerce domain.

TOTAL: 45 PERIODS

REFERENCES

BC7007 BIOMETRIC SECURITY

UNIT I BIOMETRICS
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 in biometric systems.
UNIT II PHYSIOLOGICAL BIOMETRIC TECHNOLOGIES

UNIT III BEHAVIORAL BIOMETRIC TECHNOLOGIES

UNIT IV MULTI BIOMETRICS
Multi biometrics: Multi biometrics and multi factor biometrics - two-factor authentication with passwords - tickets and tokens – executive decision - implementation Plan.

UNIT V CASE STUDIES
Case studies on Physiological, Behavioral and multifactor biometrics in identification systems.

REFERENCES

BC7008 DISTRIBUTED SYSTEMS SECURITY

UNIT I INTRODUCTION

UNIT II HOST-LEVEL THREATS AND VULNERABILITIES

UNIT III APPLICATION-LEVEL THREATS AND VULNERABILITIES
UNIT IV HOST-LEVEL SOLUTIONS
Sandboxing – Virtualization - Resource Management - Proof-Carrying Code - Memory

UNIT V SERVICE-LEVEL SOLUTIONS

TOTAL:45 PERIODS

REFERENCES
1. Abhijit Belapurkar, Anirban Chakrabarti and et al., “Distributed Systems Security:

NE7002 MOBILE AND PERVASIVE COMPUTING

OBJECTIVES :
- To understand the basics of Mobile Computing and Personal Computing
- To learn the role of cellular networks in Mobile and Pervasive Computing
- To expose to the concept of sensor and mesh networks
- To expose to the context aware and wearable computing
- To learn to develop applications in mobile and pervasive computing environment

UNIT I INTRODUCTION

UNIT II 3G AND 4G CELLULAR NETWORKS

UNIT III SENSOR AND MESH NETWORKS
UNIT IV  CONTEXT AWARE COMPUTING & WEARABLE COMPUTING  9
Health BAN- Medical and Technological Requirements-Wearable Sensors-Intra-BAN communications

UNIT V  APPLICATION DEVELOPMENT  9
Three tier architecture - Model View Controller Architecture - Memory Management – Information Access Devices – PDAs and Smart Phones – Smart Cards and Embedded Controls – J2ME – Programming for CLDC – GUI in MIDP – Application Development ON Android and iPhone

TOTAL:45 PERIODS

OUTCOMES:
At the end of the course the student should be able to
• Design a basic architecture for a pervasive computing environment
• Design and allocate the resources on the 3G-4G wireless networks
• Analyze the role of sensors in Wireless networks
• Work out the routing in mesh network
• Deploy the location and context information for application development
• Develop mobile computing applications based on the paradigm of context aware computing and wearable computing

REFERENCES:

CU7001  REAL TIME EMBEDDED SYSTEMS  L T P C 3 0 0 3
UNIT I  INTRODUCTION TO EMBEDDED COMPUTING  9
Complex systems and microprocessors – Design example: Model train controller – Embedded system design process – Formalism for system design – Instruction sets Preliminaries – ARM Processor – CPU: Programming input and output – Supervisor mode, exception and traps – Coprocessor – Memory system mechanism – CPU performance – CPU power consumption.
UNIT II  COMPUTING PLATFORM AND DESIGN ANALYSIS  9
CPU buses – Memory devices – I/O devices – Component interfacing – Design with
microprocessors – Development and Debugging – Program design – Model of programs –
Assembly and Linking – Basic compilation techniques – Analysis and optimization of execution
time, power, energy, program size – Program validation and testing.

UNIT III  PROCESS AND OPERATING SYSTEMS  9
Multiple tasks and multi processes – Processes – Context Switching – Operating Systems –
Scheduling policies - Multiprocessor – Inter Process Communication mechanisms – Evaluating
operating system performance – Power optimization strategies for processes.

UNIT IV  HARDWARE ACCELERATES & NETWORKS  9
Accelerators – Accelerated system design – Distributed Embedded Architecture – Networks for
Embedded Systems – Network based design – Internet enabled systems.

UNIT V  CASE STUDY  9
Hardware and software co-design - Data Compressor - Software Modem – Personal Digital
Assistants – Set–Top–Box. – System-on-Silicon – FOSS Tools for embedded system
development.

REFERENCES:
Morgan Kaufmann Publisher, 2006.
Publisher, 2004.

TOTAL: 45 PERIODS

NE7201  NETWORK PROGRAMMING  L T P C  3 0 0 3
OBJECTIVES :
• To understand interprocess and inter-system communication
• To understand socket programming in its entirety
• To understand usage of TCP/UDP / Raw sockets
• To understand how to build network applications

UNIT I  INTRODUCTION  9
Overview of UNIX OS - Environment of a UNIX process - Process control – Process relationships
Signals – Interprocess Communication- overview of TCP/IP protocols

UNIT II  ELEMENTARY TCP SOCKETS  9
Introduction to Socket Programming –Introduction to Sockets – Socket address Structures – Byte
ordering functions – address conversion functions – Elementary TCP Sockets – socket, connect,
bind, listen, accept, read, write , close functions – Iterative Server – Concurrent Server.
UNIT III APPLICATION DEVELOPMENT

UNIT IV SOCKET OPTIONS, ELEMENTARY UDP SOCKETS

UNIT V ADVANCED SOCKETS

TOTAL : 45 PERIODS

OUTCOMES:
- To write socket API based programs
- To design and implement client-server applications using TCP and UDP sockets
- To analyze network programs

REFERENCES:
UNIT III  MINING COMMUNITIES

Aggregating and reasoning with social network data, Advanced Representations - Extracting evolution of Web Community from a Series of Web Archive - Detecting Communities in Social Networks - Evaluating Communities – Core Methods for Community Detection & Mining - Applications of Community Mining Algorithms - Node Classification in Social Networks.

UNIT IV  EVOLUTION


UNIT V  TEXT AND OPINION MINING

Text Mining in Social Networks -Opinion extraction – Sentiment classification and clustering - Temporal sentiment analysis - Irony detection in opinion mining - Wish analysis - Product review mining – Review Classification – Tracking sentiments towards topics over time.

TOTAL: 45 PERIODS

OUTCOMES:

Upon Completion of the course, the students will be able to

- Work on the internals components of the social network
- Model and visualize the social network
- Mine the behaviour of the users in the social network
- Predict the possible next outcome of the social network
- Mine the opinion of the user

REFERENCES:


CP7022 SOFTWARE DESIGN

OBJECTIVES:

- Analyze specifications
- Describe approaches to design
- Develop design documentation
- Evaluate the design
UNIT I SOFTWARE DESIGN PRINCIPLES

UNIT II OO DESIGN
Object model – Classes and objects – Object oriented analysis – Key abstractions and mechanisms – Object oriented design – Identifying design elements – Detailed design – Case studies.

UNIT III DESIGN PATTERNS

UNIT IV FUNCTION AND SERVICE ORIENTED DESIGNS
Structural decomposition – Detailed Design – Function oriented design Case study – Services – Service identification – Service design – Service composition – choreography and orchestration – Service oriented design Case study

UNIT V USER CENTERED DESIGN AND DESIGN REVIEW

TOTAL : 45 PERIODS

OUTCOMES:
Upon completion of the course, the students will be able to
- Describe different approaches to designing a software application
- Analyze specifications and identify appropriate design strategies.
- Develop an appropriate design for a given set of requirements
- Identify applicable design patterns for the solution
- Abstract and document reusable design patterns
- Evaluate a given design against the specifications

REFERENCES:
6. Eric Gamma et al., "Design Patterns: Elements of Reusable Object-Oriented Software", Addison-Wesley Professional, 1994
UNIT I  STEGANOGRAPHY
9
Steganography communication – Notation and terminology – Information-theoretic foundations of steganography – Practical steganographic methods – Minimizing the embedding impact – Steganalysis

UNIT II  WATERMARKING
9

UNIT III  WATERMARKING WITH SIDE INFORMATION & ANALYZING ERRORS
9

UNIT IV  PERCEPTUAL MODELS
9
Evaluating perceptual impact – General form of a perceptual model – Examples of perceptual models – Robust watermarking approaches - Redundant Embedding, Spread Spectrum Coding, Embedding in Perceptually significant coefficients

UNIT V  WATERMARK SECURITY & AUTHENTICATION
9

REFERENCES:

TOTAL: 45 PERIODS
UNIT I  SECURITY THREATS
Security threats - Sources of security threats - Motives - Target Assets and vulnerabilities - Consequences of threats - E-mail threats - Web-threats - Intruders and Hackers, Insider threats, Cyber crimes.

UNIT II  NETWORK THREATS

UNIT III  SECURITY THREAT MANAGEMENT

UNIT IV  SECURITY ELEMENTS

UNIT V  ACCESS CONTROL

REFERENCES

CP7019  MANAGING BIG DATA
OBJECTIVES:
- Understand big data for business intelligence
- Learn business case studies for big data analytics
- Understand nosql big data management
- Perform map-reduce analytics using Hadoop and related tools

UNIT I  UNDERSTANDING BIG DATA
UNIT II  NOSQL DATA MANAGEMENT

UNIT III  BASICS OF HADOOP

UNIT IV  MAPREDUCE APPLICATIONS
MapReduce workflows – unit tests with MRUnit – test data and local tests – anatomy of MapReduce job run – classic Map-reduce – YARN – failures in classic Map-reduce and YARN – job scheduling – shuffle and sort – task execution – MapReduce types – input formats – output formats

UNIT V  HADOOP RELATED TOOLS

OUTCOMES:
Upon Completion of the course, the students will be able to
• Describe big data and use cases from selected business domains
• Explain NoSQL big data management
• Install, configure, and run Hadoop and HDFS
• Perform map-reduce analytics using Hadoop
• Use Hadoop related tools such as HBase, Cassandra, Pig, and Hive for big data analytics

REFERENCES:

NE7011  MOBILE APPLICATION DEVELOPMENT  L T P C
OBJECTIVES:
• Understand system requirements for mobile applications
• Generate suitable design using specific mobile development frameworks
• Generate mobile application design
• Implement the design using specific mobile development frameworks
• Deploy the mobile applications in marketplace for distribution
UNIT I  INTRODUCTION  5
Introduction to mobile applications – Embedded systems - Market and business drivers for mobile applications – Publishing and delivery of mobile applications – Requirements gathering and validation for mobile applications

UNIT II  BASIC DESIGN  8
Introduction – Basics of embedded systems design – Embedded OS - Design constraints for mobile applications, both hardware and software related – Architecting mobile applications – User interfaces for mobile applications – touch events and gestures – Achieving quality constraints – performance, usability, security, availability and modifiability.

UNIT III  ADVANCED DESIGN  8
Designing applications with multimedia and web access capabilities – Integration with GPS and social media networking applications – Accessing applications hosted in a cloud computing environment – Design patterns for mobile applications.

UNIT IV  TECHNOLOGY I - ANDROID  12

UNIT V  TECHNOLOGY II - IOS  12
Introduction to Objective C – iOS features – UI implementation – Touch frameworks – Data persistence using Core Data and SQLite – Location aware applications using Core Location and Map Kit – Integrating calendar and address book with social media application – Using Wifi - iPhone marketplace.

TOTAL: 45 PERIODS

OUTCOMES:
Upon the students will be able to
1. Describe the requirements for mobile applications
2. Explain the challenges in mobile application design and development
3. Develop design for mobile applications for specific requirements
4. Implement the design using Android SDK
5. Implement the design using Objective C and iOS
6. Deploy mobile applications in Android and iPhone marketplace for distribution

REFERENCES:

BC7011  WIRELESS SECURITY  L T P C
3 0 0 3

UNIT I  WIRELESS TECHNOLOGIES  9
UNIT II WIRELESS THREATS

UNIT III SECURITY IN DATA NETWORKS
Wireless Device security issues - CDPD security (Cellular Digital Packet Data)-GPRS security (General Packet Radio Service) - GSM (Global System for Mobile Communication) security – IP security

UNIT IV WIRELESS TRANSPORT LAYER SECURITY

UNIT BLUETOOTH SECURITY

TOTAL : 45 PERIODS

REFERENCES:

IF7202 CLOUD COMPUTING

OBJECTIVES:
- To introduce the broad perceptive of cloud architecture and model
- To understand the concept of Virtualization
- To be familiar with the lead players in cloud.
- To understand the features of cloud simulator
- To apply different cloud programming model as per need.
- To be able to set up a private cloud.
- To understand the design of cloud Services.
- To learn to design the trusted cloud Computing system

UNIT I CLOUD ARCHITECTURE AND MODEL

UNIT II VIRTUALIZATION
UNIT III CLOUD INFRASTRUCTURE

UNIT IV PROGRAMMING MODEL
Parallel and Distributed Programming Paradigms – MapReduce, Twister and Iterative Map Reduce – Hadoop Library from Apache – Mapping Applications - Programming Support - Google App Engine, Amazon AWS - Cloud Software Environments -Eucalyptus, Open Nebula, OpenStack, Aneka, CloudSim

UNIT V SECURITY IN THE CLOUD

TOTAL:45 PERIODS

OUTCOMES:
• Compare the strengths and limitations of cloud computing
• Identify the architecture, infrastructure and delivery models of cloud computing
• Apply suitable virtualization concept.
• Choose the appropriate cloud player
• Choose the appropriate Programming Models and approach.
• Address the core issues of cloud computing such as security, privacy and interoperability
• Design Cloud Services
• Set a private cloud

REFERENCES:
5. George Reese, “Cloud Application Architectures: Building Applications and Infrastructure in the Cloud” O'Reilly
UNIT I  INTRODUCTION  

UNIT II  CYBER CRIME ISSUES  

UNIT III  INVESTIGATION  

UNIT IV  DIGITAL FORENSICS  

UNIT V  LAWS AND ACTS  
Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC, Electronic Communication Privacy ACT, Legal Policies.

TOTAL: 45 PERIODS

REFERENCES: