PROGRAM EDUCATIONAL OBJECTIVES (PEOs)

1. To enable graduates to pursue research, or have a successful career in academia or industries associated with M.E. Biometrics and Cyber Security, or as entrepreneurs.

2. To provide students with strong foundational concepts and also advanced techniques and tools in order to enable them to build solutions or systems of varying complexity.

3. To prepare students to critically analyze existing literature in an area of specialization and ethically develop innovative and research oriented methodologies to solve the problems identified.

4. To enable students to pursue lifelong multidisciplinary learning as professional engineers and scientists to effectively communicate technical information, function effectively on teams, and apply bio metrics and cyber security related solutions within a global, societal, and environmental context.

5. Prepare students to critically analyze existing literature, identify the gaps in the existing literature, map the existing problems in human identification in Cyber Security and propose innovative and research oriented solutions.

PROGRAM OUTCOMES (POs)
Engineering Graduates will be able to:

1. **Engineering knowledge**: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

2. **Problem analysis**: Identify, formulate, review research literature, and analyze complex Engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

3. **Design/development of solutions**: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

4. **Conduct investigations of complex problems**: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5. **Modern tool usage**: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

6. **The engineer and society**: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

7. **Environment and sustainability**: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

8. **Ethics**: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

9. **Individual and team work**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

10. **Communication**: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

11. **Project management and finance**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

12. **Life-long learning**: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.
MAPPING OF PROGRAM SPECIFIC OBJECTIVES WITH PROGRAMME OUTCOMES

A broad relation between the Program Specific Objectives and the outcomes is given in the following table

<table>
<thead>
<tr>
<th>PROGRAMME EDUCATIONAL OBJECTIVES</th>
<th>PROGRAMME OUTCOMES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>

PROGRAM SPECIFIC OBJECTIVES (PSOS)

1. To analyze, design and develop computing solutions by applying foundational concepts of computer science and engineering.
2. To apply biometric principles and practices for the secure real time systems, scientific and business applications.
3. To diagnose the biometric and cyber problems and to build the system with advance solution to solve problem with cyber ethics.

Provide mapping of 1) POs to PEOs and 2) PSOs to PEOs.
Use the following marking:

Contribution 1: Reasonable 2: Significant 3: Strong

<table>
<thead>
<tr>
<th>PROGRAM SPECIFIC OBJECTIVES</th>
<th>PROGRAMME OUTCOMES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
MAPPING OF PROGRAMME EDUCATIONAL OBJECTIVES WITH PROGRAMME OUTCOMES:
A broad relation between the programme objective and the outcomes is given in the following table.

<table>
<thead>
<tr>
<th>YEAR I</th>
<th>SEMESTER I</th>
<th>COURSE TITLE</th>
<th>PROGRAMME OUTCOMES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>A  B  C  D  E  F  G  H  I  J  K  L</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Applied Probability and Statistics</td>
<td>√  √</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network Design and Programming</td>
<td>√  √  √  √  √</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advanced Data Structures and Algorithms</td>
<td>√  √</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Biometric Systems</td>
<td>√  √  √  √  √  √  √  √  √</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber Security</td>
<td>√  √  √  √  √  √  √  √  √</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mobile and Pervasive Computing</td>
<td>√  √  √  √  √  √  √  √  √</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Structures Laboratory</td>
<td>√  √  √  √</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network Design and Programming</td>
<td>√  √  √  √  √</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>YEAR I</th>
<th>SEMESTER II</th>
<th>COURSE TITLE</th>
<th>PROGRAMME OUTCOMES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>A  B  C  D  E  F  G  H  I  J  K  L</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internet of Things</td>
<td>√  √  √  √  √  √  √  √  √</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Biometric Image Processing</td>
<td>√  √  √  √  √</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cybercrime Investigations and Digital Forensics</td>
<td>√  √  √  √  √  √  √  √  √</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Access Control and Identity Management Systems</td>
<td>√  √</td>
</tr>
<tr>
<td></td>
<td>PROFESSIONAL ELECTIVE I</td>
<td>Applied Cryptography</td>
<td>√  √  √  √</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Machine Learning Techniques</td>
<td>√  √  √  √  √</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Mining Techniques</td>
<td>√  √  √  √  √</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Context Aware Computing</td>
<td>√  √  √  √</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Digital Forensics Laboratory</td>
<td>√  √  √  √  √  √  √  √  √</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Biometric Image Processing Laboratory</td>
<td>√  √  √  √  √  √  √  √  √</td>
</tr>
<tr>
<td>COURSE TITLE</td>
<td>PROGRAMME OUTCOMES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A</td>
<td>B</td>
<td>C</td>
</tr>
<tr>
<td>Social Network Analysis</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Operating Systems Security</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Trust Management in E - Commerce</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Biometric Security</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cyber Security Management and Cyber Laws</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Steganography and Digital Watermarking</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cloud Computing Technologies</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Energy Aware Computing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Advances in Biometrics</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Intrusion Detection and Prevention Systems</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Big data Analytics</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Wireless Security</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Ethical Hacking and Network Defense</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Project Work Phase - I</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Project Work Phase - II</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
### Semester I

<table>
<thead>
<tr>
<th>SL.NO</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>CATEGORY</th>
<th>CONTACT PERIODS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>THEORY</strong></td>
<td></td>
<td>L   T   P   C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4 0 0 4</td>
</tr>
<tr>
<td>1.</td>
<td>MA5160</td>
<td>Applied Probability and Statistics</td>
<td>FC</td>
<td>4 4 0 0 4</td>
</tr>
<tr>
<td>2.</td>
<td>NE5291</td>
<td>Network Design and Programming</td>
<td>PC</td>
<td>3 3 0 0 3</td>
</tr>
<tr>
<td>3.</td>
<td>CP5151</td>
<td>Advanced Data Structures and Algorithms</td>
<td>PC</td>
<td>4 4 0 0 4</td>
</tr>
<tr>
<td>4.</td>
<td>BC5101</td>
<td>Biometric Systems</td>
<td>PC</td>
<td>3 3 0 0 3</td>
</tr>
<tr>
<td>5.</td>
<td>BC5102</td>
<td>Cyber Security</td>
<td>PC</td>
<td>3 3 0 0 3</td>
</tr>
<tr>
<td>6.</td>
<td>CP5093</td>
<td>Mobile and Pervasive Computing</td>
<td>PC</td>
<td>3 3 0 0 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>PRACTICALS</strong></td>
<td></td>
<td>4 0 4 2</td>
</tr>
<tr>
<td>7.</td>
<td>CP5161</td>
<td>Data Structures Laboratory</td>
<td>PC</td>
<td>4 0 4 2</td>
</tr>
<tr>
<td>8.</td>
<td>NE5281</td>
<td>Network Design and Programming Laboratory</td>
<td>PC</td>
<td>4 0 4 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>TOTAL</strong></td>
<td></td>
<td>28 20 8 24</td>
</tr>
</tbody>
</table>

### Semester II

<table>
<thead>
<tr>
<th>SL.NO</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>CATEGORY</th>
<th>CONTACT PERIODS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>THEORY</strong></td>
<td></td>
<td>L   T   P   C</td>
</tr>
<tr>
<td>1.</td>
<td>CP5292</td>
<td>Internet of Things</td>
<td>PC</td>
<td>3 3 0 0 3</td>
</tr>
<tr>
<td>2.</td>
<td>BC5251</td>
<td>Biometric Image Processing</td>
<td>PC</td>
<td>3 3 0 0 3</td>
</tr>
<tr>
<td>3.</td>
<td>BC5201</td>
<td>Cybercrime Investigations and Digital Forensics</td>
<td>PC</td>
<td>3 3 0 0 3</td>
</tr>
<tr>
<td>4.</td>
<td>BC5202</td>
<td>Access Control and Identity Management Systems</td>
<td>PC</td>
<td>3 3 0 0 3</td>
</tr>
<tr>
<td>5.</td>
<td></td>
<td>Professional Elective I</td>
<td>PE</td>
<td>3 3 0 0 3</td>
</tr>
<tr>
<td>6.</td>
<td></td>
<td>Professional Elective II</td>
<td>PE</td>
<td>3 3 0 0 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>PRACTICALS</strong></td>
<td></td>
<td>4 0 4 2</td>
</tr>
<tr>
<td>7.</td>
<td>BC5211</td>
<td>Digital Forensics Laboratory</td>
<td>PC</td>
<td>4 0 4 2</td>
</tr>
<tr>
<td>8.</td>
<td>BC5212</td>
<td>Biometric Image Processing Laboratory</td>
<td>PC</td>
<td>4 0 4 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>TOTAL</strong></td>
<td></td>
<td>26 18 8 22</td>
</tr>
</tbody>
</table>
### SEMESTER III

<table>
<thead>
<tr>
<th>SL. NO</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>CATEGORY</th>
<th>CONTACT PERIODS</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>THEORY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>CP5074</td>
<td>Social Network Analysis</td>
<td>PC</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td>Professional Elective III</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td>Professional Elective IV</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PRACTICALS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>BC5311</td>
<td>Project Work Phase - I</td>
<td>EEC</td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TOTAL</td>
<td></td>
<td></td>
<td>21</td>
<td>9</td>
<td>0</td>
<td>12</td>
</tr>
</tbody>
</table>

### IV SEMESTER

<table>
<thead>
<tr>
<th>SL. NO</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>CATEGORY</th>
<th>CONTACT PERIODS</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>PRACTICALS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>BC5411</td>
<td>Project Work Phase - II</td>
<td>EEC</td>
<td>24</td>
<td>0</td>
<td>0</td>
<td>24</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TOTAL</td>
<td></td>
<td></td>
<td>24</td>
<td>0</td>
<td>0</td>
<td>24</td>
</tr>
</tbody>
</table>

**TOTAL NO. OF CREDITS: 73**
### FOUNDATION COURSES (FC)

<table>
<thead>
<tr>
<th>SL. NO</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>CATEGORY</th>
<th>CONTACT PERIODS</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>MA5160</td>
<td>Applied Probability and Statistics</td>
<td>FC</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>

### PROFESSIONAL CORE (PC)

<table>
<thead>
<tr>
<th>SL. NO</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>CATEGORY</th>
<th>CONTACT PERIODS</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>NE5291</td>
<td>Network Design and Programming</td>
<td>PC</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2.</td>
<td>CP5151</td>
<td>Advanced Data Structures and Algorithms</td>
<td>PC</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>3.</td>
<td>BC5101</td>
<td>Biometric Systems</td>
<td>PC</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4.</td>
<td>BC5102</td>
<td>Cyber Security</td>
<td>PC</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>5.</td>
<td>CP5093</td>
<td>Mobile and Pervasive Computing</td>
<td>PC</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>6.</td>
<td>CP5161</td>
<td>Data Structures Laboratory</td>
<td>PC</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>7.</td>
<td>NE5281</td>
<td>Network Design and Programming Lab</td>
<td>PC</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>8.</td>
<td>CP5292</td>
<td>Internet of Things</td>
<td>PC</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>9.</td>
<td>BC5251</td>
<td>Biometric Image Processing</td>
<td>PC</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>10.</td>
<td>BC5201</td>
<td>Cybercrime Investigations and Digital Forensics</td>
<td>PC</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>11.</td>
<td>BC5202</td>
<td>Access Control and Identity Management Systems</td>
<td>PC</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>12.</td>
<td>BC5211</td>
<td>Digital Forensics Laboratory</td>
<td>PC</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>13.</td>
<td>BC5212</td>
<td>Biometric Image Processing Lab</td>
<td>PC</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>14.</td>
<td>CP5074</td>
<td>Social Network Analysis</td>
<td>PC</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

### EMPLOYABILITY ENHANCEMENT COURSE (EEC)

<table>
<thead>
<tr>
<th>SL. NO</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>CATEGORY</th>
<th>CONTACT PERIODS</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>BC5311</td>
<td>Project Work Phase – I</td>
<td>EEC</td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td>6</td>
</tr>
<tr>
<td>2.</td>
<td>BC5411</td>
<td>Project Work Phase – II</td>
<td>EEC</td>
<td>24</td>
<td>0</td>
<td>0</td>
<td>24</td>
<td>12</td>
</tr>
</tbody>
</table>
### Semester II
#### Elective I

<table>
<thead>
<tr>
<th>SL.No</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>CATEGORY</th>
<th>CONTACT PERIODS</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>BC5001</td>
<td>Applied Cryptography</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2.</td>
<td>CP5191</td>
<td>Machine Learning Techniques</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3.</td>
<td>BC5002</td>
<td>Data Mining Techniques</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4.</td>
<td>MP5391</td>
<td>Context Aware Computing</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

#### Elective II

<table>
<thead>
<tr>
<th>SL.No</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>CATEGORY</th>
<th>CONTACT PERIODS</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>BC5003</td>
<td>Operating Systems Security</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2.</td>
<td>BC5004</td>
<td>Trust Management in E-Commerce</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3.</td>
<td>BC5005</td>
<td>Biometric Security</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4.</td>
<td>BC5006</td>
<td>Cyber Security Management and Cyber Laws</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

#### Elective III

<table>
<thead>
<tr>
<th>SL.No</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>CATEGORY</th>
<th>CONTACT PERIODS</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>BC5007</td>
<td>Steganography and Digital Watermarking</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2.</td>
<td>CP5092</td>
<td>Cloud Computing Technologies</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3.</td>
<td>IF5091</td>
<td>Energy Aware Computing</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4.</td>
<td>BC5008</td>
<td>Advances in Biometrics</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

#### Elective IV

<table>
<thead>
<tr>
<th>SL.No</th>
<th>COURSE CODE</th>
<th>COURSE TITLE</th>
<th>CATEGORY</th>
<th>CONTACT PERIODS</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>BC5009</td>
<td>Intrusion Detection and Prevention Systems</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2.</td>
<td>CP5293</td>
<td>Big Data Analytics</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3.</td>
<td>BC5010</td>
<td>Wireless Security</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4.</td>
<td>BC5011</td>
<td>Ethical Hacking and Network Defence</td>
<td>PE</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>
MA5160  APPLIED PROBABILITY AND STATISTICS  L  T  P  C
4 0 0 4

OBJECTIVES:
This course is designed to provide the solid foundation on topics in applied probability and various statistical methods which form the basis for many other areas in the mathematical sciences including statistics, modern optimization methods and risk modeling. It is framed to address the issues and the principles of estimation theory, testing of hypothesis and multivariate analysis.

UNIT I  PROBABILITY AND RANDOM VARIABLES  12

UNIT II  TWO DIMENSIONAL RANDOM VARIABLES  12
Joint distributions – Marginal and conditional distributions – Functions of two dimensional random variables – Regression curve – Correlation.

UNIT III  ESTIMATION THEORY  12

UNIT IV  TESTING OF HYPOTHESIS  12
Sampling distributions – Type I and Type II errors – Small and large samples – Tests based on Normal, t, Chi square and F distributions for testing of mean, variance and proportions – Tests for independence of attributes and goodness of fit.

UNIT V  MULTIVARIATE ANALYSIS  12
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

TOTAL : 60 PERIODS

OUTCOMES :
After completing this course, students should demonstrate competency in the following topics:

- Basic probability axioms and rules and the moments of discrete and continuous random variables.
- Consistency, efficiency and unbiasedness of estimators, method of maximum likelihood estimation and Central Limit Theorem.
- Use statistical tests in testing hypotheses on data.
- Perform exploratory analysis of multivariate data, such as multivariate normal density, calculating descriptive statistics, testing for multivariate normality.

The students should have the ability to use the appropriate and relevant, fundamental and applied mathematical and statistical knowledge, methodologies and modern computational tools.
REFERENCES:

NE5291 NETWORK DESIGN AND PROGRAMMING L T P C
3 0 0 3

OBJECTIVES:
• To understand the basic networking principles
• To explore various networking devices and protocols required for network design and management
• To study two novel networking technologies: SDN and DTN
• To learn network programming in UNIX C

UNIT I NETWORKING PRINCIPLES

UNIT II PHYSICAL NETWORK DESIGN

UNIT III LOGICAL DESIGN AND MANAGEMENT

UNIT IV INNOVATIVE NETWORKS
UNIT V  NETWORK PROGRAMMING IN UNIX C


TOTAL: 45 PERIODS

OUTCOMES:
After studying this course, the student should be able to
- Apply the networking principles to design a network
- Apply SDN in computing paradigms like Cloud Computing and Internet of Things
- Configure the networking devices and protocols
- Develop network applications in various platforms

REFERENCES:

CP5151 ADVANCED DATA STRUCTURES AND ALGORITHMS  L T P C
4 0 0 4

OBJECTIVES:
- To understand the usage of algorithms in computing.
- To learn and use hierarchical data structures and its operations
- To learn the usage of graphs and its applications.
- To select and design data structures and algorithms that is appropriate for problems.
- To study about NP Completeness of problems.

UNIT I ROLE OF ALGORITHMS IN COMPUTING 12

UNIT II HIERARCHICAL DATA STRUCTURES 12
UNIT III  
GRAPHS  

UNIT IV  
ALGORITHM DESIGN TECHNIQUES  

UNIT V  
NP COMPLETE AND NP HARD  

OUTCOMES:  
Upon the completion of the course the student should be able to
• Design data structures and algorithms to solve computing problems.
• Design algorithms using graph structure and various string matching algorithms to solve real-life problems.
• Apply suitable design strategy for problem solving

REFERENCES:  

BC5101  
BIOMETRIC SYSTEMS  
OBJECTIVES:  
• To understand the basics of Biometrics and its functionalities
• To learn the role of biometric in the organization
• To expose the concept of IRIS and sensors
• To expose the context of Biometric Applications
• To learn to develop applications with biometric security

UNIT I  
INTRODUCTION  
Person Recognition – Biometric systems –Biometric functionalities: verification, identification – Biometric systems errors - The design cycle of biometric systems – Applications of Biometric systems – Security and privacy issues.
UNIT II  FINGER PRINT AND FACIAL RECOGNITION  

UNIT III  IRIS AND OTHER TRAITS  

UNIT IV  BEHAVIORAL BIOMETRICS  

UNIT V  APPLICATIONS AND TRENDS  
Application areas: surveillance applications- personal applications –design and deployment -user system interaction-operational processes – architecture –application development –design validation-disaster recovery plan-maintenance-privacy concerns.

TOTAL :  45  PERIODS

OUTCOMES:
At the end of the course the student should be able to
- Identify the various Biometric technologies.
- Design of biometric recognition for the organization.
- Develop simple applications for privacy.
- Understand the need of biometric in the society

REFERENCES:
5. Paul Reid "Biometrics For Network Security "Person Education 2004
OBJECTIVES:
- Students should be able to understand.
- The difference between threat, risk, attack and vulnerability.
- How threats materialize into attacks.
- Where to find information about threats, vulnerabilities and attacks.
- Typical threats, attacks and exploits and the motivations behind them.

UNIT I INTRODUCTION TO CYBER SECURITY

UNIT II SECURITY IN OPERATING SYSTEM & NETWORKS

UNIT III DEFENCES: SECURITY COUNTERMEASURES

UNIT IV PRIVACY IN CYBERSPACE

UNIT V MANAGEMENT AND INCIDENTS

OUTCOMES:
- Analytical skills
- Group/team working
- Innovation/creativity
- Problem solving skills
- Research

REFERENCES:
OBJECTIVES:
- To learn the basic architecture and concepts till Third Generation Communication systems
- To understand the latest 4G Telecommunication System Principles.
- To introduce the broad perspective of pervasive concepts and management
- To Explore the HCI in Pervasive environment
- Apply the pervasive concepts in mobile environment

UNIT I INTRODUCTION

UNIT II OVERVIEW OF A MODERN 4G TELECOMMUNICATIONS SYSTEM

UNIT III PERVERSIVE CONCEPTS AND ELEMENTS

UNIT IV HCI IN PERVERSIVE COMPUTING
Prototype for Application Migration - Prototype for Multimodalities - Human–Computer Interface in Pervasive Environments - HCI Service and Interaction Migration - Context-Driven HCI Service Selection - Interaction Service Selection Overview - User Devices - Service-Oriented Middleware Support - User History and Preference - Context Manager - Local Service Matching - Global Combination - Effective Region - User Active Scope - Service Combination Selection Algorithm

UNIT V PERVERSIVE MOBILE TRANSACTIONS

TOTAL : 45 PERIODS
OUTCOMES:
Upon completion of this course the students should be able to:
- Obtain a thorough understanding of Basic architecture and concepts of till Third Generation Communication systems.
- Explain the latest 4G Telecommunication System Principles.
- Incorporate the pervasive concepts.
- Implement the HCI in Pervasive environment.
- Work on the pervasive concepts in mobile environment.

REFERENCES:

CP5161 DATA STRUCTURES LABORATORY

OBJECTIVES:
- To acquire the knowledge of using advanced tree structures.
- To learn the usage of heap structures.
- To understand the usage of graph structures and spanning trees.

LIST OF EXPERIMENTS
Each student has to work individually on assigned lab exercises. Lab sessions could be scheduled as one contiguous 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:

EXPERIMENTS:
1. Implementation of Merge Sort and Quick Sort-Analysis
2. Implementation of a Binary Search Tree
3. Red-Black Tree Implementation
4. Heap Implementation
5. Fibonacci Heap Implementation
6. Graph Traversals
7. Spanning Tree Implementation
8. Shortest Path Algorithms (Dijkstra's algorithm, Bellmann Ford Algorithm)
9. Implementation of Matrix Chain Multiplication
10. Activity Selection and Huffman Coding Implementation.

TOTAL: 60 PERIODS
OUTCOMES:
Upon Completion of the course, the students will be able to:
- Design and implement basic and advanced data structures extensively.
- Design algorithms using graph structures
- Design and develop efficient algorithms with minimum complexity using design techniques.

NE5281  NETWORK DESIGN AND PROGRAMMING LABORATORY   L T P C
0 0 4 2

OBJECTIVES:
- To practice LAN and WAN design
- To learn network programming in UNIX C and Python

NETWORK DESIGN
- Establish a LAN with a switch/hub with 3 PCs and check the connectivity and configuration
- Establish a internetwork with 2 routers and two or more LANs using static routes and check the connectivity and configuration
- Establish a dynamic routing based internetwork with 2 routers and two or more LANs using RIP/OSPF and check the connectivity and configuration
- In the internetwork created in experiment number 4, analyze the performance of various TCP variants using an FTP application

NETWORK PROGRAMMING
- Develop a C program that demonstrates inter process communication
- Develop a TCP client/server application
- Develop a UDP client/server application
- Develop an Iterative UDP server with 2 or 3 clients
- Develop a concurrent TCP server with 2 or 3 clients
- Develop a multiprotocol server with TCP and UDP and 2 clients
- Develop simple Python programs that use frequently used syntactic constructs
- Develop a Socket based application in Python
- Build client applications for major APIs (Amazon S3, Twitter etc) in Python
- Develop an application that interacts with e-mail servers in python
- Develop applications that work with remote servers using SSH, FTP etc in Python

TOTAL: 60 PERIODS

OUTCOMES:
- After completing this course the student should be able to
- Design and implement LANs and internetworks
- Develop network based applications in UNIX C and Python
OBJECTIVES:
- To understand the fundamentals of Internet of Things
- To learn about the basics of IOT protocols
- To build a small low cost embedded system using Raspberry Pi.
- To apply the concept of Internet of Things in the real world scenario.

UNIT I  INTRODUCTION TO IoT
Internet of Things - Physical Design - Logical Design - IoT Enabling Technologies - IoT Levels & Deployment Templates - Domain Specific IoTs - IoT and M2M - IoT System Management with NETCONF-YANG - IoT Platforms Design Methodology

UNIT II  IoT ARCHITECTURE
M2M high-level ETSI architecture - IETF architecture for IoT - OGC architecture - IoT reference model - Domain model - information model - functional model - communication model - IoT reference architecture

UNIT III  IoT PROTOCOLS

UNIT IV  BUILDING IoT WITH RASPBERRY PI & ARDUINO

UNIT V  CASE STUDIES AND REAL-WORLD APPLICATIONS
Real world design constraints - Applications - Asset management, Industrial automation, smart grid, Commercial building automation, Smart cities - participatory sensing - Data Analytics for IoT – Software & Management Tools for IoT Cloud Storage Models & Communication APIs - Cloud for IoT - Amazon Web Services for IoT.

OUTCOMES:
Upon completion of this course, the students should be able to:
- Analyze various protocols for IoT
- Develop web services to access/control IoT devices.
- Design a portable IoT using Raspberry Pi
- Deploy an IoT application and connect to the cloud.
- Analyze applications of IoT in real time scenario
REFERENCES:

BC5251 BIOMETRIC IMAGE PROCESSING L T P C
3 0 0 3

OBJECTIVES:
• To understand the basics of Image processing
• To model and visualize the transformation of image
• To understand the evolution of object detection
• To mine the interest of the user

UNIT I IMAGE PROCESSING FUNDAMENTALS
Introduction- images-sampling and frequency –Domain processing-basic image processing operations-point operators –group operations –other statistical operators –mathematical morphology

UNIT II FEATURE EXTRACTION
Low level Feature Extraction: Edge Detection- phase congruency- localized feature extraction-describing image motion. High Level Extraction: Thresholding and subtraction – Template matching-feature extraction by low level features- Hough transformation.

UNIT III OBJECT DETECTION

UNIT IV 3D BIOMETRIC
Classification of 3D biometric imaging methods -3D biometric Technologies- 3D palm print capturing systems-3D information in palm print- Feature Extraction from 3D palm print –matching and fusion – security applications.

UNIT V APPLICATIONS
Mobile Biometrics- Biometric Application Design –Biometric Technologies issues- Biometrics in society –privacy and Biometrics –Ethics and Technology usage – human factors

TOTAL : 45 PERIODS
OUTCOMES:
At the end of the course the student should be able to
- Understand the need of biometric in image processing
- Work on the internals Technologies of biometric
- Mine the behavior of the users in the biometric field
- Predict the possible next outcome of the image processing
- Mine the opinion of the user

REFERENCES:
6. Tinku Acharya and Ajoy K Ray "Image Processing Principles and Applications" John wiley and sons 2005

BC5201 CYBER CRIME INVESTIGATIONS AND DIGITAL FORENSICS

OBJECTIVES:
- To study about cyber crime categories
- Awareness about various hacking, cracking and attacks.
- To study about various investigation strategies
- To study about various Techniques in Digital Forensics
- Basic Laws and Acts for Cyber crime

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.

OUTCOMES:
- Knowledge about Cyber crime issues and conquer techniques
- Analysis about investigation, Encryption and Decryption Methods.
- Familiarity in Open source Digital Forensics Platform and tools

REFERENCES:
2. Cory Altheide and Harlan Carvey, “Digital Forensics with Open Source Tools” Elsevier publication, April 2011

BC5202  
ACCESS CONTROL AND IDENTITY MANAGEMENT  
SYSTEMS  
L  T  P  C  3  0  0  3

OBJECTIVES:
- To understand the importance of IAM with emerging mobile information society, Compliance and regulations and industry standards for Identity management
- To build the capability to assess the risks, techniques of Identity and authentication with context
- To learn and devise various access control techniques
- To study and gain knowledge on access control systems
- To do typical case studies of online applications

UNIT I  
INTRODUCTION  

COMPLYING WITH REGULATIONS
INDUSTRY STANDARDS FOR IDENTITY MANAGEMENT


UNIT II     IDENTITY MANAGEMENT  8


UNIT III    ACCESS MANAGEMENT  9

Types of access control, Layered access controls and “defense in depth”, The Process of Accountability. Access Control Techniques - Discretionary Access Controls (DAC), Nondiscretionary Access Controls (NAC), Mandatory Access Controls (MAC), Role-Based Access Controls (RBAC), Task Based Access Controls (TBAC), Lattice-Based Access Controls. Access Control Methodologies and Implementations - Access Control Administration - Account Administration - Account, Log, and Journal Monitoring/Audits - Access Rights and Permissions.

UNIT IV    ACCESS CONTROL SYSTEMS  9


UNIT V  CASE STUDIES  9

Technology, Architecture and Controlling Access to Online/Mobile Applications - Library, Banking and Shopping

TOTAL : 45 PERIODS

OUTCOMES:
- Able to understand the role of IAM with emerging mobile information society, compliance and regulations and industry standards for Identity management.
- Able to learn techniques of Identity and authentication with risks assessment.
- Build capability to compare various access control techniques.
- Gain knowledge on access control systems.
- Ability to carry out analysis and report strength and weakness if IAM in a given typical online applications.

REFERENCES:
OBJECTIVES:

- Describe digital forensics and relate it to an investigative process.
- Explain the legal issues of preparing for and performing digital forensic analysis based on the investigator's position and duty.
- Perform basic digital forensics.
- Demonstrate use of digital forensics tools.
- Guide a digital forensics exercise.
- Recognize the state of the practice and the gaps in technology, policy, and legal issues.

LIST OF EXPERIMENTS

1. Introduction to legal issues, context, and digital forensics
   Disk Imaging and Cloning
   - Use VMWare and modify device configuration in a VMWare system
   - Image a drive to a file
   - Extract individual partitions from an image file
   - Mount the image as a loopback device and read only for analysis
   - Properly sanitize a disk for cloning
   - Clone a drive versus imaging the drive
   - Verify disk and file integrity with hashing

2. Analysis: disk structure, file systems (NTFS, EXT 2/3, HFS), and physical
   The Sleuth Kit Tools (learn through hands-on labs)
   - Download links for listed tools
     dd.exe .
     http://users.erols.com/gmgarner/forensics/udump.exe
     fport.exe .
     http://www.sysinternals.com/Utilities/PsLoggedOn.html/slist.exe
     http://www.sysinternals.com/Utilities/PsList.html
     kill.exe, auditpol.exe, dumpel.exe .
     http://www.petri.co.il/download_free_reskit_tools.htm/ntlast.exe
     http://www.foundstone.com/resources/proddesc/ntlast.htm

REFERENCES


http://www.foolmoon.net/downloads/Live_Forensics_Using_WFT.pdf

Burdach, Mariusz. Digital forensics of the physical memory, March 2005

http://www.forensicfocus.com/index.php?name=Content&pid=57

Rose, Curtis W. Windows Live Incident Response Volatile Data Collection: Non-Disruptive User & System Memory Forensic Acquisition

3. **Search Word Filtering from Unallocated, Slack and Swap Space**
   Understand the interview process to develop an initial search list for an investigation
   - Extract unallocated space from an image
   - Extract slack space from an image
   - Copy the swap file
   - Filter out and analyze evidence from unallocated, slack and swap space using search list.
   - Modify your list of search words based on the evidence you find and repeat searching as needed.

4. **Unix File Recovery – Data Unit Level**
   Review of unallocated space and extracting with dls
   - Interpret the file system information from the superblock
   - Locate files by block number
   - Recover files from unallocated blocks
   - Understand contiguous and noncontiguous files
   - Using the Autopsy Forensic Browser

5. **FILE RECOVERY: META DATA LAYER**
   Find meta data information for evidence found in a search list
   - Recover a file based on meta data
   - Use the Autopsy Forensic Browser at the meta data layer
   - Observe file deletion behavior at the meta data layer with different file systems

6. **FILE RECOVERY: DATA LAYER REVISITED**
   - Perform searches based on file headers
   - Data Carving with Foremost
   - Zip password recovery

7. **ANALYSIS TECHNIQUES: KEYWORD SEARCHES, TIMELINES, HIDDEN DATA**
   File Encoding and Detection
   Timeline Analysis
   - Use MAC time information to generate a timeline of file activity
   - Interpret timeline for finding evidence.

8. **DATA MINING FOR DIGITAL FORENSICS**
   Encryption and Password Recovery
   Steganography Detection
   File Extension Renaming and Signaturing
   Application Analysis.
   Client and Web
   Web Analysis
   IRC Analysis
   Network Analysis.
   Collection and Analysis of Network Traffic
   Wireless Network Traffic

9. **NETWORK DEVICES: ROUTERS, SWITCHES**
   Analysis of Cell phones, Tablet, iPad, PDAs, etc.
   Cell Phones
   Tablet, iPad
   PDAs
10. **INVESTIGATION OF NON-TRADITIONAL EQUIPMENT: AUTOS, WASHERS**
   MP3 Players
   Flash Media (extra credit)
   Digital Cameras

11. **BINARY CODE ANALYSIS (GUEST LECTURER: ALEX BERRY).**
   Tools for Binary Analysis
   Detection of Malicious Code
   Reverse Engineering
   Encrypted Binaries

12. **EVIDENCE: COLLECTION, PRESERVATION, TESTIMONY**
   Forensic Certifications
   Risk Analysis for Evidence Collection
   Non-IT Parents Ability to Investigate their Child’s Behavior
   EnCase Forensic Toolkit
   Paraben Forensic Toolkit

13. **RESEARCH CHALLENGES.**
   Digital Life Analysis: Undergrad - Single
   Digital Life Analysis: Grad – Children
   Peer to Peer Networks
   Grid Analysis
   Public Computer Analysis
   Large Data Analysis

**REFERENCES**
   [http://isis.poly.edu/kulesh/forensics/list.htm](http://isis.poly.edu/kulesh/forensics/list.htm)

**OUTCOMES:**
Upon Completion of the course, the students will be able to
- Practices and basic knowledge about VMware and various file system.
- Explain in Open source forensics tools
- Hands on Express in sleuth Kit Tools
- Knowledge of filter & analyse

**TOTAL: 60 PERIODS**

**LIST OF EQUIPMENT FOR A BATCH OF 30 STUDENTS:**
(Please include only Open Source Software wherever possible.)
OBJECTIVES:
- To learn to implement Image Enhancement and Segmentation.
- To learn to implement Image Acquisition and Feature Extraction - Fingerprint
- To learn to implement Image Acquisition and Feature Extraction - Face and Iris.
- To learn to implement 3D Biometric and Mobile Biometrics.

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. 3D Biometric – Palmprint
10. Mobile biometrics

TOTAL: 60 PERIODS

OUTCOMES:
Upon Completion of the course, the students will be able to:
- Design and Apply Image Enhancement and Segmentation.
- Design and Apply Image Acquisition and Feature Extraction - Fingerprint
- Design and Apply Image Acquisition and Feature Extraction - Face and Iris.
- Design and Apply 3D Biometric and Mobile Biometrics.

LIST OF EQUIPMENT FOR A BATCH OF 30 STUDENTS:
(Please include only Open Source Software wherever possible.)

CP5074 SOCIAL NETWORK ANALYSIS

OBJECTIVES:
- To understand the components of the social network
- To model and visualize the social network
- To mine the users in the social network
- To understand the evolution of the social network
- To know the applications in real time systems

UNIT I INTRODUCTION
UNIT II  MODELING AND VISUALIZATION

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  APPLICATIONS
A Learning Based Approach for Real Time Emotion Classification of Tweets, A New Linguistic Approach to Assess the Opinion of Users in Social Network Environments, Explaining Scientific and Technical Emergence Forecasting, Social Network Analysis for Biometric Template Protection

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
  • Apply social network in real time applications

REFERENCES:
OBJECTIVES:
The student should be made to:
- Understand OSI security architecture and classical encryption techniques.
- Acquire fundamental knowledge on the concepts of finite fields and number theory.
- Understand various block cipher and stream cipher models.
- Describe the principles of public key cryptosystems, hash functions and digital signature
- Acquire fundamental knowledge on applications of Digital Signature in payments etc.,

UNIT I INTRODUCTION & MATHEMATICAL FOUNDATION
Definitions – Cryptography, cryptanalysis, cryptology, classical cryptosystem- shift cipher, affine cipher, vignere cipher, substitution, transposition techniques, Types of attacks in OSI security architecture-Number Theory concepts – Modular Arithmetic, Properties, Euclidean algorithm, Fermat's and Euler's theorem, Chinese Remainder Theorem, Primitive roots, Discrete Logarithms

UNIT II BLOCK CIPHERS AND MODES OF OPERATIONS
Simplified DES - Data Encryption Standard-Block cipher principles-block cipher modes of operation-AES-TripleDES-Blowfish-RC5

UNIT III PUBLIC KEY CRYPTOGRAPHY

UNIT IV HASH FUNCTIONS AND DIGITAL SIGNATURES

UNIT V APPLICATIONS

OUTCOMES:
Upon Completion of the course, the students should be able to:
- Compare various Cryptographic Techniques.
- Understand security issues, practices and principles in various applications.

REFERENCES:
OBJECTIVES:
- To introduce students to the basic concepts and techniques of Machine Learning.
- To have a thorough understanding of the Supervised and Unsupervised learning techniques.
- To study the various probability based learning techniques.
- To understand graphical models of machine learning algorithms.

UNIT I  INTRODUCTION

UNIT II  LINEAR MODELS

UNIT III  TREE AND PROBABILISTIC MODELS

UNIT IV  DIMENSIONALITY REDUCTION AND EVOLUTIONARY MODELS

UNIT V  GRAPHICAL MODELS

TOTAL: 45 PERIODS
OUTCOMES:
Upon completion of the course, the students will be able to:

- Distinguish between, supervised, unsupervised and semi-supervised learning
- Apply the apt machine learning strategy for any given problem
- Suggest supervised, unsupervised or semi-supervised learning algorithms for any given problem
- Design systems that uses the appropriate graph models of machine learning
- Modify existing machine learning algorithms to improve classification efficiency

REFERENCES:

BC5002 DATA MINING TECHNIQUES

OBJECTIVES:
- Understanding of the value of data mining in solving real-world problems.
- Understanding of foundational concepts underlying data mining.
- Understanding of algorithms commonly used in data mining tools.
- Ability to apply data mining tools to real-world problems

UNIT I INTRODUCTION TO DATA MINING
Introduction to Data Mining – Data Mining and Machine Learning, Examples, Applications, Machine Learning and Statistics, Generalization as search, Data mining and ethics, Input-Concepts, instances and attributes, Output-Knowledge Representation.

UNIT II DATA MINING ALGORITHMS: Basic Methods

UNIT III IMPLEMENTATION
Decision trees, Classification rules, Extending linear models, Instance-based learning, Numeric prediction, Clustering, Bayesian networks.

UNIT IV ADVANCED DATA MINING
Attribute selection, Discretizing numeric attributes, transformations, Automatic data cleansing, Combining multiple models, using unlabeled data, Ensemble learning, Extensions and Applications.
UNIT V  DATA MINING WORKBENCH - WEKA
Introduction, The Explorer, The Experimenter, Command Line Interface, Embedded machine learning, Writing New learning schemes

TOTAL: 45 PERIODS

OUTCOMES:
Upon Completion of the course, the students will be able to
- Display a comprehensive understanding of different data mining tasks and the algorithms most appropriate for addressing them.
- Evaluate models/algorithms with respect to their accuracy.
- Demonstrate capacity to perform a self-directed piece of practical work that requires the application of data mining techniques.
- Develop hypotheses based on the analysis of the results obtained and test them.
- Conceptualise a data mining solution to a practical problem.

REFERENCES:

MP5391 CONTEXT AWARE COMPUTING

OBJECTIVES:
- To understand the concept of context, representation and modeling of context, context ontology and architecture.
- To know the technologies for sensing context, location tracking services.
- To understand the need for and categories of context aware middleware systems.
- To know the UI techniques for contextual information, reconfiguration based on context, context triggered actions.
- Case study based learning on how to apply context aware computing to ubiquitous applications and context data change management.

UNIT I

UNIT II

UNIT III
UNIT IV

UNIT V
Case study - How does context-aware computing fit in with ubicomp. What sensors, infrastructure, are necessary. Fallback condition. How to describe the context that you are in - location, physiological state, emotional state, etc. Challenges in Implementing a Context-Aware System - How to represent context internally - Storage, Data structures and algorithms. How frequently does the system need to be updated on context changes - How often to poll? How often to change behavior.

TOTAL: 45 PERIODS

OUTCOMES:
- Understand the concept of context, representation and modeling of context, context ontology and architecture.
- Gain knowledge on communication the technologies for sensing and transporting context data and location tracking services.
- Understand the categories of context aware middleware systems to realize mobile services
- Gain knowledge on UI techniques for contextual information, reconfiguration and context triggered actions
- Able to apply context aware computing to ubiquitous applications and implement context data change management.

REFERENCES:

BC5003 OPERATING SYSTEMS SECURITY

OBJECTIVES:
- Study the basic concepts and functions of operating systems.
- Understand the structure and functions of OS.
- Learn about Processes and memory management schemes.
- Study I/O management and File systems.
- To gain insight on to the Protection, Security issues

UNIT I FUNDAMENTALS OF OPERATING SYSTEMS
Overview – Operating system concepts – Functions – Structure of Operating system – Types of operating system– Dead lock Prevention, Recovery, Detection and Avoidance
UNIT II  PROCESS MANAGEMENT  9
Introduction to processes – Process Scheduling - Threads-CPU Scheduling objectives, criteria – Types of scheduling algorithms – Performance comparison – Inter process communications- Synchronization – Semaphores.

UNIT III  MEMORY MANAGEMENT  9

UNIT IV  DEVICE AND FILE MANAGEMENT  9

UNIT V  SECURITY ISSUES  9

TOTAL : 45 PERIODS

OUTCOMES:

- Compare and contrast various memory management schemes.
- Design and Implement a prototype file systems.
- Discuss the various synchronization, and memory management issues.
- Demonstrate the Mutual exclusion, Deadlock detection and agreement protocols of Distributed operating system.
- Discuss the various Security issues.

REFERENCES:
   http://nptel.ac.in/.

BC5004  TRUST MANAGEMENT IN E-COMMERCE  L T P C 3 0 0 3

OBJECTIVES:
Study and Basic Knowledge about
- Ecommerce business models and Digital Payments systems
- Knowledge about Ecommerce security Environment
- To study about Ecommerce mechanisms and trusted computing Platform.
UNIT I  INTRODUCTION TO E-COMMERCE  9

UNIT II  E-COMMERCE SECURITY  9

UNIT III  TRUST IN E-COMMERCE  9

UNIT IV  TRUSTED COMPUTING PLATFORM  9
Introduction to trusted computing platform: Overview – Usage Scenarios – Key components of trusted platform – Trust mechanisms in a trusted platform.

UNIT V  TRUST MODELS  9
Trusted platforms for organizations and individuals – Trust models and the E-Commerce domain.

OUTCOMES:
- Awareness about threats in Ecommerce.
- Deep Knowledge about Types of Payment

REFERENCES:

BC5005  BIOMETRIC SECURITY  L T P C
3 0 0 3

OBJECTIVES:
- To understand the fundamentals of biometric security
- To acquire knowledge on standard algorithms and protocols used to provide confidentiality, integrity and authenticity.
- To understand the various key distribution and management strategies.
- To understand how to deploy encryption techniques to secure data using biometric
- To design security applications in the field of Information technology
UNIT I  ATTACKS IN BIOMETRIC
Adversary attacks-attacks at the user Interface-Attacks on the biometric processing, Attacks on template database –system security analysis – spoofing and mimicry attacks

UNIT II  BIOMETRIC AUTHENTICATION PROTOCOLS
Introduction-biometric based secure cryptographic protocols – biometrics based cryptographic key Regeneration and sharing – Biometrics based session key generation and sharing protocol – performance evaluation strategies.

UNIT III  BIOMETRIC CRYPTOGRAPHY

UNIT IV  BIOMETRIC DATA PROTECTION
Biometric data – Concept of personal data – Data protection and privacy – Security criteria for Biometric system – Adoption of security – Revocation procedures – Security and organizational aspects of biometric system.

UNIT V  BIOMETRIC MULTI MODAL AND APPLICATIONS

TOTAL : 45 PERIODS

OUTCOMES:
Upon Completion of the course, the students will be able to
• Implement basic security algorithms required by the biometric system.
• Analyze the vulnerabilities in biometric 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.
• Formulate research problems in the biometric security field

REFERENCES:
5. Liangwang,Xin Geng "Behavioral Biometrics for Human Identifications Intelligent Applications" Medical Information Science Reference, IGI Global 2010
OBJECTIVES:
- To understand the nature of threats and cyber security management goals.
- To understand the landscape of hacking and perimeter defense mechanisms.
- To develop strategies for cyber security and protecting critical infrastructure.
- To understand policies to mitigate cyber risks and digital signature.
- To understand the IT Act, scheme, amendments, IPR and emerging cyber law.

UNIT I

UNIT II

UNIT III

UNIT IV
POLICIES TO MITIGATE CYBER RISK - Promotion of R&D in Cyber security, Reducing Supply Chain Risks, Mitigate Risks through Human Resource Development, Creating Cyber security Awareness, Information sharing Implementing a Cyber security Framework. SIGNATURES - Digital Signature, Electronic Signature, Digital Signature to Electronic.

UNIT V

OUTCOMES:
- Gain knowledge on the nature of threats and cyber security management goals and framework.
- Knowledge on the landscape of hacking and perimeter defense mechanisms.
- Ability to differentiate and integrate strategies for cyber security and protecting critical infrastructure.
- Able to understand policies to mitigate cyber risks.
- Knowledge on IT Act, and amendments, copy rights, IPR and cyber law to deal with offenses.
REFERENCES:
2. NIST Cyber security Framework, Version 1.0, 2014
3. CGI, “Cyber security in Modern Critical Infrastructure Environments,” 2014

BC5007 STEGANOGRAPHY AND DIGITAL WATERMARKING L T P C
3 0 0 3

OBJECTIVES:
- To provide the importance of digital watermarking and Steganography
- To discuss the properties of watermarking and steganography systems
- To discuss the different models of watermarking and steganography
- To understand the various evaluation metrics
- To examine various applications of watermarking and steganography

UNIT I INTRODUCTION 5

UNIT II STEGANOGRAPHY 12

UNIT III WATERMARKING 7

UNIT IV MODELS OF WATERMARKING 12
Notation, Communications, Components of Communications Systems, Classes of Transmission Channels, Secure Transmission, Communication-Based Models of Watermarking, Basic Model, Watermarking as Communications with Side Information at the Transmitter, Watermarking as Multiplexed Communications, Geometric Models of Watermarking, Distributions and Regions in Media Space, Marking Spaces, Modeling Watermark Detection by Correlation, Linear Correlation, Normalized Correlation, Correlation Coefficient, Summary
UNIT V  APPLICATIONS
Applications of Watermarking, Broadcast Monitoring, Copyrights, Proof of Ownership, Transaction Tracking, Content Authentication, Copy Control, Device Control, Legacy Enhancement. Applications of Steganography, Steganography for Dissidents, Steganography for Criminals

TOTAL: 45 PERIODS

OUTCOMES:
Upon Completion of the course, the students will be able to
- Discuss the need for watermarking and steganography
- Distinguish between watermarking and steganography
- Elaborate on the various models of watermarking and steganography.
- Point out various steganalysis algorithms.
- Show how watermarking and steganography can be applied to various applications and evaluate them.

REFERENCES:

CP5092  CLOUD COMPUTING TECHNOLOGIES

OBJECTIVES:
- To understand the concepts of virtualization and virtual machines
- To gain expertise in server, network and storage virtualization.
- To understand and deploy practical virtualization solutions and enterprise solutions
- To gain knowledge on the concept of virtualization that is fundamental to cloud computing
- To understand the various issues in cloud computing
- To be able to set up a private cloud
- To understand the security issues in the grid and the cloud environment

UNIT I  VIRTUALIZATION

39
UNIT II  VIRTUALIZATION INFRASTRUCTURE

UNIT III  CLOUD PLATFORM ARCHITECTURE

UNIT IV  PROGRAMMING MODEL
Introduction to Hadoop Framework - Mapreduce, Input splitting, map and reduce functions, specifying input and output parameters, configuring and running a job –Developing Map Reduce Applications - Design of Hadoop file system –Setting up Hadoop Cluster - Cloud Software Environments - Eucalyptus, Open Nebula, Open Stack, Nimbus

UNIT V  CLOUD SECURITY
Cloud Infrastructure security: network, host and application level – aspects of data security, provider data and its security, Identity and access management architecture, IAM practices in the cloud, SaaS, PaaS, IaaS availability in the cloud - Key privacy issues in the cloud –Cloud Security and Trust Management

OUTCOMES:
Upon completion of this course, the students should be able to:
- Employ the concepts of storage virtualization, network virtualization and its management
- Apply the concept of virtualization in the cloud computing
- Identify the architecture, infrastructure and delivery models of cloud computing
- Develop services using Cloud computing
- Apply the security models in the cloud environment

REFERENCES:
OBJECTIVES:
- To understand the fundamentals of Energy Efficient Computing
- To understand the concept of Energy Efficient Storage Systems
- To introduce the various types of scheduling algorithms in energy efficient computing
- To introduce the concept of Green Networking
- To study Energy Aware Computing Applications

UNIT I INTRODUCTION

UNIT II ENERGY EFFICIENT STORAGE

UNIT III ENERGY EFFICIENT SCHEDULING ALGORITHMS

UNIT IV INTRODUCTION TO GREEN NETWORKING

UNIT V ENERGY AWARE COMPUTING APPLICATIONS

OUTCOMES:
Upon Completion of the course, the students will be able to
- Design Power efficient architecture Hardware and Software
- Analyze the different types of Energy Efficient Storage systems.
- Design the algorithms for Energy Efficient Systems
- Identify the different types of Green Networking schemes in the energy efficient computing
- Explore the applications of Energy Aware Computing

REFERENCES:
OBJECTIVES

- Understand system requirements for biometric design
- To introduce the broad perceptive of advanced biometric technologies
- To understand the concept of Touch less Fingerprint
- To apply different methods and model as per need.
- To be able to set up a implementation of biometric system
- To understand the ethical usage of biometric system

UNIT I INTRODUCTION


UNIT II TOUCHLESS FINGERPRINT

- Touch less Fingerprint Recognition Techniques – Quality Assessment of Touch less Fingerprint Images-Computation of Touch Equivalent images – Quality Assessment of Touch Equivalent Fingerprint- Analysis of Level 1 Features and Level 2 Features in Touch less Fingerprint –Reduction of perspective and rotation Effects –Computation of synthetic Touch less Fingerprint

UNIT III IMPLEMENTATION ASPECTS


UNIT IV AUTHENTICATION


UNIT V BIOMETRIC IN SOCIETY AND ETHICAL USAGE


TOTAL: 45 PERIODS

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

- Compare the strengths and limitations of Touch less Fingerprint
- Describe the requirements for design and implementation
- Explain the challenges in Biometric field
- To explore the characteristics of different types of Biometrics
- To analyze the strengths and limitations for development of Biometric systems
REFERENCES:

BC5009 INTRUSION DETECTION AND PREVENTION SYSTEMS  L  T  P  C
3  0  0  3

OBJECTIVES:
• To understand the vulnerabilities and detection techniques of various attacks
• To understand the network intrusion detection & prevention mechanisms
• To understand the countermeasures of various information security attacks
• To design / make use of a typical intrusion detection system

UNIT I INTRUSION DETECTION SYSTEMS PRINCIPLES
History of Intrusion detection, Audit, Concept and definition, Internal and external threats to data, attacks, Key functions of IDPS technologies - Signature & Anomaly based Detection, Stateful protocol analysis Types of IDS, Information sources Host based information sources, Network based information sources.

UNIT II IDS TECHNOLOGIES
Components & Architecture-Typical components, Network Architectures Security capabilities - Information gathering capabilities, logging capabilities, detection & prevention capabilities. Intrusion Prevention Systems, Network protocol based IDS ,Hybrid IDS, Analysis schemes, thinking about intrusion. A model for intrusion analysis, techniques Responses requirement of responses, types of responses mapping responses to policy Vulnerability analysis, credential analysis non credential analysis

UNIT III NETWORK BASED IDS

UNIT IV HOST BASED IDS
Components and Architecture-Typical components, Network architectures, Agent locations, host architectures. Security capabilities-Logging, detection, prevention and other capabilities.Using & Integrating multiple IDPS technologies-Need for multiple IDPS technologies, Integrating different IDPS technologies-Direct & Indirect IDPS integration. Other technologies with IDPS capabilities-Network Forensic Analysis Tool, Anti-malware technologies, Firewalls and Routers, Honeypots
UNIT V  IDS TOOL : SNORT IDS
Introduction to Snort, Working with Snort Rules, Snort configuration, Snort with MySQL, Running Snort on Multiple Network Interfaces, Snort Modes Snort Alert Modes, Snarf with Snort, Agent development for intrusion detection, Architecture models of IDS and IPS.

TOTAL : 45 PERIODS

OUTCOMES:
Upon successful completion of this course, a student will be able to:
- Design and implement Intrusion Detection System
- Understand t classes of attacks on computer systems
- Identify various types of IDS of signature based and anomaly based techniques to solve problems related to intrusion detection and prevention.
- Employ ID&PS specific feature extraction techniques

REFERENCES:

CP5293  BIG DATA ANALYTICS  L T P C
3 0 0 3

OBJECTIVES:
- To understand the competitive advantages of big data analytics
- To understand the big data frameworks
- To learn data analysis methods
- To learn stream computing
- To gain knowledge on Hadoop related tools such as HBase, Cassandra, Pig, and Hive for big data analytics

UNIT I  INTRODUCTION TO BIG DATA

UNIT II  HADOOP FRAMEWORK
Distributed File Systems - Large-Scale FileSystem Organization – HDFS concepts - MapReduce Execution, Algorithms using MapReduce, Matrix-Vector Multiplication – Hadoop YARN
UNIT III           DATA ANALYSIS
Statistical Methods: Regression modelling, Multivariate Analysis - Classification: SVM & Kernel Methods - Rule Mining - Cluster Analysis, Types of Data in Cluster Analysis, Partitioning Methods, Hierarchical Methods, Density Based Methods, Grid Based Methods, Model Based Clustering Methods, Clustering High Dimensional Data - Predictive Analytics – Data analysis using R.

UNIT IV          MINING DATA STREAMS

UNIT V             BIG DATA FRAMEWORKS

OUTCOMES:
At the end of this course, the students will be able to:
- Understand how to leverage the insights from big data analytics
- Analyze data by utilizing various statistical and data mining approaches
- Perform analytics on real-time streaming data
- Understand the various NoSql alternative database models

REFERENCES:
2. David Loshin, "Big Data Analytics: From Strategic Planning to Enterprise Integration with Tools, Techniques, NoSQL, and Graph", 2013.

BC5010          WIRELESS SECURITY
OBJECTIVES:
- To understand the fundamentals of wireless security.
- To understand the security issues in bluetooth and Wi-Fi.
- To explore the security issues in WiMAX and mobile telecommunication networks.
- To understand the security issues in ad-hoc and wireless sensor networks.
- To study the hacking techniques in IEEE 802.11.
UNIT I  WIRELESS SECURITY FUNDAMENTALS

UNIT II  SECURITY IN BLUETOOTH AND WI-FI

UNIT III  SECURITY IN WIMAX AND MOBILE TELECOMMUNICATION NETWORKS

UNIT IV  SECURITY IN AD HOC AND WIRELESS SENSOR NETWORKS
Attacks to routing protocols- Security mechanisms- Auto-configuration-Authentication issue within ad hoc networks- Group key management within ad hoc networks-Attacks on wireless sensor networks and counter measures- Prevention mechanisms: authentication and traffic protection.

UNIT V  HACKING 802.11 WIRELESS TECHNOLOGY
Introduction to 802.11 Hacking- Scanning and Enumerating 802.11 Networks- Attacking 802.11 Wireless Networks- Attacking WPA-Protected 802.11 Networks- Attack 802.11 Wireless Clients.

TOTAL : 45 PERIODS

OUTCOMES:
On completing this course, the student will be able to:
- Identify various possibilities for security threats in wireless networks.
- Handle the security threats in Bluetooth and Wi-Fi networks.
- Solve the security attacks in WiMAX and mobile telecommunication networks.
- Prevent the attacks in ad-hoc and wireless sensor networks.
- Protect the 802.11 Networks from attacks.

REFERENCES:
OBJECTIVES:
To understand and analyse Information security threats & countermeasures
To perform security auditing & testing
To understand issues relating to ethical hacking
To study & employ network defense measures
To understand penetration and security testing issues

UNIT I ETHICAL HACKING OVERVIEW & VULNERABILITIES 9
Understanding the importance of security, Concept of ethical hacking and essential Terminologies- Threat, Attack, Vulnerabilities, Target of Evaluation, Exploit. Phases involved in hacking

UNIT II FOOTPRINTING & PORT SCANNING 9
Footprinting - Introduction to foot printing, Understanding the information gathering methodology of the hackers, Tools used for the reconnaissance phase. Port Scanning - Introduction, using port scanning tools, ping sweeps, Scripting Enumeration-Introduction, Enumerating windows OS & Linux OS

UNIT III SYSTEM HACKING 9
Aspect of remote password guessing, Role of eavesdropping, Various methods of password cracking, Keystroke Loggers, Understanding Sniffers, Comprehending Active and Passive Sniffing, ARP Spoofing and Redirection, DNS and IP Sniffing, HTTPS Sniffing

UNIT IV HACKING WEB SERVICES & SESSION HIJACKING 9
Web application vulnerabilities, application coding errors, SQL injection into Back-end Databases, cross-site scripting, cross-site request forging, authentication bypass, web services and related flaws, protective http headers Understanding Session Hijacking, Phases involved in Session Hijacking, Types of Session Hijacking, Session Hijacking Tools

UNIT V HACKING WIRELESS NETWORKS 9
Introduction to 802.11, Role of WEP, Cracking WEP Keys, Sniffing Traffic, Wireless DOS attacks, WLANScanners, WLANSniffers, Hacking Tools, Securing Wireless Networks.

TOTAL : 45 PERIODS

OUTCOMES:
Upon successful completion of this course, a student will be able to:
• understand vulnerabilities, mechanisms to identify vulnerabilities/threats/attacks
• perform penetration & security testing
• become a professional ethical hacker

REFERENCES:
1. Kimberly Graves, "Certified Ethical Hacker", Wiley India Pvt Ltd, 2010
5. Thomas Mathew, "Ethical Hacking", OSB publishers, 2003