Faculty of Science and Technology
Savitribai Phule Pune University
Maharashtra, India

Honours* in Cyber Security
Board of Studies
(Computer Engineering)
(with effect from A.Y. 2020-21)
### Honours* in Cyber Security
### With effect from 2020-21

<table>
<thead>
<tr>
<th>Year &amp; Semester</th>
<th>Course Code and Course Title</th>
<th>Teaching Scheme Hours / Week</th>
<th>Examination Scheme and Marks</th>
<th>Credit Scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Theory</td>
<td>Tutorial</td>
<td>Practical</td>
</tr>
<tr>
<td>TE &amp; V</td>
<td>310401 Information and Cyber Security</td>
<td>04</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td></td>
<td>310402 Information and Cyber Security Laboratory</td>
<td>--</td>
<td>--</td>
<td>02</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>04</td>
<td>-</td>
<td>02</td>
</tr>
<tr>
<td>Total Credits</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TE &amp; VI</td>
<td>310403 Enterprise Architecture and Components</td>
<td>04</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>04</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Total Credits</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BE &amp; VII</td>
<td>410401 Internet of Things and Embedded Security</td>
<td>04</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td></td>
<td>410402 Risk Assessment Laboratory</td>
<td>--</td>
<td>--</td>
<td>02</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>04</td>
<td>-</td>
<td>02</td>
</tr>
<tr>
<td>Total Credits</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BE &amp; VIII</td>
<td>410403 Information Systems Management</td>
<td>04</td>
<td>-</td>
<td>--</td>
</tr>
<tr>
<td></td>
<td>410404 Seminar</td>
<td>--</td>
<td>02</td>
<td>--</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>04</td>
<td>-</td>
<td>02</td>
</tr>
<tr>
<td>Total Credits</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total Credit for Semester V+VI+VII+VIII = 20

*To be offered as Honours for Major Disciplines as–*
1. Computer Engineering
2. Electronics and Telecommunication Engineering
3. Electronics Engineering
4. Information Technology

For any other Major Disciplines which is not mentioned above, it may be offered as Minor Degree.
Reference: [https://www.aicte-india.org/sites/default/files/APH%202020%2021.pdf](https://www.aicte-india.org/sites/default/files/APH%202020%2021.pdf) / page 99-100
Savitribai Phule Pune University  
Honours* in Cyber Security  
Third Year of Engineering (Semester V)  
310401: Information and Cyber Security

<table>
<thead>
<tr>
<th>Teaching Scheme:</th>
<th>Credit:</th>
<th>Examination Scheme:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theory: 04 Hours/Week</td>
<td>04</td>
<td>Mid_Semester(TH): 30 Marks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>End_Semester(TH): 70 Marks</td>
</tr>
</tbody>
</table>

Companion Course, if any: - Information and Cyber Security Laboratory

Course Objectives:
- To understand the basics of computer, network and information security.
- To study operating system security and malwares.
- To acquaint with security issues in internet protocols.
- To analyze the system for vulnerabilities.

Course Outcomes:
On completion of the course, learner will be able to–
- Use cryptographic techniques in secure application development.
- Apply methods for authentication, access control, intrusion detection and prevention.
- To apply the scientific method for security assessment
- To develop computer forensics awareness.

Course Contents

<table>
<thead>
<tr>
<th>Unit I</th>
<th>Security Fundamentals</th>
<th>(06 Hours)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Unit II</th>
<th>Modular Arithmetic and Cryptography Basics</th>
<th>(08 Hours)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Unit III</th>
<th>Advanced Cryptography</th>
<th>(08 Hours)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Unit IV</th>
<th>Issues in Security Management and Cyber Laws</th>
<th>(08 Hours)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Unit V</th>
<th>Key Management and Secure Communication</th>
<th>(08 Hours)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Unit VI</th>
<th>Attacks, Malicious Logic and Countermeasures</th>
<th>(08 Hours)</th>
</tr>
</thead>
</table>
Phishing, Password Cracking, Key-loggers and Spywares, Types of Virus, Worms, DoS and DDoS, SQL injection, Buffer Overflow, Spyware, Adware and Ransomware. Antivirus and other security measures

Intrusion Detection System: IDS fundamentals, Different types of IDS. Intrusion Prevention.

<table>
<thead>
<tr>
<th>Learning Resources</th>
</tr>
</thead>
</table>
Savitribai Phule Pune University
Honours* in Cyber Security
Third Year of Engineering (Semester V)
310402: Information and Cyber Security Laboratory

Teaching Scheme | Credit Scheme | Examination Scheme and Marks
--- | --- | ---
Practical: 02 Hours/Week | 01 | Term work: 50 Marks

Guidelines for Laboratory Conduction

- **Lab Assignments:** Following is list of suggested laboratory assignments for reference. Laboratory Instructors may design suitable set of assignments for respective course at their level. **Beyond curriculum assignments and mini-project may be included as a part of laboratory work.** The instructor may set multiple sets of assignments and distribute among batches of students. It is appreciated if the assignments are based on real world problems/applications. The inclusion of few optional assignments that are intricate and/or beyond the scope of curriculum will surely be the value addition for the students and it will satisfy the intellectuals within the group of the learners and will add to the perspective of the learners. For each laboratory assignment, it is essential for students to draw/write/generate flowchart, algorithm, test cases, mathematical model, Test data set and comparative/complexity analysis (as applicable). Batch size for practical and tutorial may be as per guidelines of authority.

- **Term Work**—Term work is continuous assessment that evaluates a student’s progress throughout the semester. Term work assessment criteria specify the standards that must be met and the evidence that will be gathered to demonstrate the achievement of course outcomes. Categorical assessment criteria for the term work should establish unambiguous standards of achievement for each course outcome. They should describe what the learner is expected to perform in the laboratories or on the fields to show that the course outcomes have been achieved. **It is recommended to conduct internal monthly practical examination as part of continuous assessment.**

- **Assessment:** Students’ work will be evaluated typically based on the criteria like attentiveness, proficiency in execution of the task, regularity, punctuality, use of referencing, accuracy of language, use of supporting evidence in drawing conclusions, quality of critical thinking and similar performance measuring criteria.

- **Laboratory Journal**—Program codes with sample output of all performed assignments are to be submitted as softcopy. Use of DVD or similar media containing students programs maintained by Laboratory In-charge is highly encouraged. For reference one or two journals may be maintained with program prints in the Laboratory. As a conscious effort and little contribution towards Green IT and environment awareness, attaching printed papers as part of write-ups and program listing to journal may be avoided. Submission of journal/ term work in the form of softcopy is desirable and appreciated.

Suggested list of assignments
(Use suitable programming language/Tool for implementation)

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Statement of Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Implement Euclid’s algorithm to find the GCD of two integers. Further implement extended Euclidean algorithm to find the multiplicative inverse of the given integer.</td>
</tr>
<tr>
<td>2</td>
<td>Develop the program to implement DES algorithm for encryption and decryption. Assume suitable key.</td>
</tr>
<tr>
<td>3</td>
<td>Develop the program to implement RSA algorithm for encryption and decryption. Assume suitable Private and Public Keys.</td>
</tr>
<tr>
<td>4</td>
<td>Write a program to implement SHA1 algorithm using libraries (API)</td>
</tr>
<tr>
<td>5</td>
<td>Configure and demonstrate use of vulnerability assessment tool like Wireshark or SNORT</td>
</tr>
</tbody>
</table>
### Course Objectives:

- To learn fitting of enterprise information into the broader context of enterprise architecture frameworks.
- To learn an architectural foundation that effectively addresses important business and societal challenges.
- To learn a comprehensive architectural guide that includes architectural principles, architectural patterns, and building blocks and their applications for information-centric solutions.
- To provide methodology that is critical for all business leaders and technologist trying to build an enterprise on the internet.

### Course Outcomes:

On completion of the course, learner will be able to—

- CO1: Explain the concept of the enterprise information architecture.
- CO2: Describe how the domains can be managed within the enterprise though a coherent Information Governance framework.
- CO3: Interpret component model of the EIA Reference Architecture for relevant services with its descriptions and interfaces.
- CO4: Discuss the operational characteristics of the EIA Reference Architecture.
- CO5: Describe the increasing role of enterprise-wide Metadata Management within information-centric use case scenarios.
- CO6: Define enterprise security architecture based on available risk to an enterprise. Discuss various models for enterprise security architecture.

### Course Contents

<table>
<thead>
<tr>
<th>Unit I</th>
<th>Introduction</th>
<th>(08 Hours)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Unit II</th>
<th>Domains and Enterprise information architecture</th>
<th>(08 Hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data domains, Conceptual architecture overview,</td>
<td>EIA reference architecture, architecture principals for EIA, Logical view of EIA reference architecture</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unit III</th>
<th>Enterprise information architecture: Component model</th>
<th>(08 Hours)</th>
</tr>
</thead>
</table>
The component model, component relationship diagram, component description, component interaction diagrams- a deployment scenario

<table>
<thead>
<tr>
<th>Unit IV</th>
<th>Enterprise information architecture: Operational model</th>
<th>(08 Hours)</th>
</tr>
</thead>
</table>

Terminology and definitions, Context of operational model design techniques, service qualities, Standards used for operational model relationship diagram framework of operational patterns

<table>
<thead>
<tr>
<th>Unit V</th>
<th>Metadata and master data management</th>
<th>(08 Hours)</th>
</tr>
</thead>
</table>

Terminology and definitions, business scenarios, component deep dive, component interaction diagram-deployment scenario, service qualities for metadata management, master data management: Terminology, business scenarios, component deep dive, component interaction diagram, service qualities.

<table>
<thead>
<tr>
<th>Unit VI</th>
<th>Enterprise Security Architecture—A Top-down Approach</th>
<th>(08 Hours)</th>
</tr>
</thead>
</table>

SABSA, COBIT and TOGAF and Their Relationships, Using the Frameworks to Develop an Enterprise Security Architecture, A Real-Life Example, Using CMMI to Monitor, Measure and Report the Architecture Development Progress

**Learning Resources**

**Text Books:**

**Reference Books:**

**Online Resources:**
Prof. Jenamani, IIT Kharagpur, E-business, https://nptel.ac.in/courses/110/105/110105083/
Savitribai Phule Pune University  
Honours* in Cyber Security  
Fourth Year of Engineering (Semester VII)  
410401 - Internet of Things and Embedded Security

<table>
<thead>
<tr>
<th>Teaching Scheme:</th>
<th>Credit</th>
<th>Examination Scheme:</th>
</tr>
</thead>
<tbody>
<tr>
<td>TH: 04 Hours/Week</td>
<td>04</td>
<td>Mid_Semester(TH): 30 Marks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>End_Semester(TH): 70 Marks</td>
</tr>
</tbody>
</table>

**Prerequisite Courses, if any:**  
- Fundamentals of Embedded Systems, IoT  
- Basic of Network Security

**Companion Course, if any:**

**Course Objectives:**

- To understand the main threats and attacks in IoT Environment  
- Ability to understand the Security requirements in IoT.  
- To learn security aspects in the design of IoT systems  
- To learn IoT security life cycle  
- To create awareness of IoT security  
- To understand cryptographic security for their IoT implementations and deployments  
- To learn identity and access management for IoT development  
- To understand Identity models for IoT

**Course Outcomes:**  
On completion of the course, learner will be able to–

- CO1- Define IoT security issues and concerns  
- CO2- Identify the main threats and attacks in IoT Environment  
- CO3- Determine secure development methodology for the IoT  
- CO4- Describe IoT security lifecycle management processes  
- CO5– Apply cryptography methods in securing the IoT and embedded system  
- CO6- Determine IoT IAM infrastructure

**Course Contents**

**Unit I**  
**Introduction: Securing the Internet of Things, Vulnerabilities, attacks and countermeasures**  
(08 Hours)

Defining the IoT, IoT uses today, The IoT in the enterprise, The IoT of the future and the need to secure, Primer on threats - The classic pillars of information assurance, Threats, Vulnerability, Risks, vulnerability, and risks; Primer on attacks and countermeasures- Common IoT attack types, Attack trees, Fault (failure) trees and CPS; Today's IoT attacks – attacks; Threat modeling an IoT system

**Unit II**  
**Security Engineering for IoT Development**  
(08 Hours)

Building security in to design and development, Secure design - Security in agile developments, Focusing on the IoT device in operation, Safety and security design - Threat modeling, Privacy impact assessment, Safety impact assessment, Compliance, Security system integration, Processes and agreements, Technology selection – security products and services- IoT device hardware, Selecting an MCU, Selecting a real-time operating system (RTOS), IoT relationship platforms, Cryptographic security APIs, Authentication/authorization
### Unit III: The IoT Security Lifecycle (08 Hours)

The secure IoT system implementation lifecycle, Implementation and integration - IoT security CONOPS document, Network and security integration, System security verification and validation (V&V), Security training, Secure configurations, Operations and maintenance - Managing identities, roles, and attributes, Security monitoring, Penetration testing, Compliance monitoring, Asset and configuration management, Incident management, Forensics, Dispose - Secure device disposal and zeroization, Data purging, Inventory control, Data archiving and records management.

### Unit IV: Cryptographic Fundamentals for IoT Security Engineering (08 Hours)

Cryptography and its role in securing the IoT, Types and uses of cryptographic primitives in the IoT, Encryption and decryption - Symmetric encryption, Asymmetric encryption, Hashes, Digital signatures - Symmetric (MACs), Random number generation, Ciphersuites, Cryptographic module principles, Cryptographic key management fundamentals - Key generation - Key establishment, Key derivation, Key storage, Key escrow, Key lifetime, Key zeroization, Accounting and management, Examining cryptographic controls for IoT protocols - Cryptographic controls built into IoT communication protocols (ZigBee, Bluetooth, Near field communication (NFC)), Cryptographic controls built into IoT messaging protocols – MQTT, CoAP, DDS, REST, Future directions of the IoT and cryptography.

### Unit V: Identity and Access Management Solutions for the IoT (08 Hours)


### Unit VI: Identity management models (08 Hours)


### Learning Resources

**Text Books:**
4. Practical Internet of Things Security, Brian Russell, Drew Van Duren, PACKT Publishing

**Reference Books:**
**Online Resources:**

- Introduction to Industry 4.0 and Industrial Internet of Things
  By Prof. Sudip Misra | IIT Kharagpur, [https://nptel.ac.in/courses/106/105/106105195/](https://nptel.ac.in/courses/106/105/106105195/)

- Cryptography and Network Security By Prof. Sourav Mukhopadhyay | IIT Kharagpur
  [https://onlinecourses.nptel.ac.in/noc21_cs16/preview](https://onlinecourses.nptel.ac.in/noc21_cs16/preview)
Savitribai Phule Pune University
Honours* in Cyber Security
Fourth Year of Engineering (Semester VII)
410402: Risk Assessment Laboratory

<table>
<thead>
<tr>
<th>Teaching Scheme:</th>
<th>Credit</th>
<th>Examination Scheme:</th>
</tr>
</thead>
<tbody>
<tr>
<td>TH: 02 Hours/Week</td>
<td>01</td>
<td>Term work Marks 50</td>
</tr>
</tbody>
</table>

**Prerequisite Courses, if any:**
- Embedded Systems and Internet of Things Security

**Companion Course, if any:**

**Course Objectives:**
- To understand the importance of protecting IoT devices and sensors
- To safeguard the information IoT devices collect.
- To assess the risks associated with IoT device vulnerabilities.
- To learn IoT device is functioning properly safe from attacks.

**Course Outcomes:**

On completion of the course, student will be able to–

CO1- Understand the vulnerabilities associated with IoT devices and sensors

CO2- Apply the knowledge to secure the data, communication with respect to embedded and IoT device.

CO3- Identify the risks associated in the context of application that uses IoT.

**Guidelines for Instructor's Manual**

The instructor's manual is to be developed as a hands-on resource and reference. The instructor's manual need to include prologue (about University/program/ institute/ department/foreword/preface), curriculum of course, conduction and Assessment guidelines, topics under consideration- concept, objectives, outcomes.

**Guidelines for Student's Laboratory Journal**

The laboratory assignments are to be submitted by student in the form of journal. Journal consists of prologue, Certificate, table of contents, and handwritten write-up of each assignment (Title, Objectives, Problem Statement, Outcomes, software and Hardware requirements, Date of Completion, Assessment grade/marks and assessor's sign.

*As a conscious effort and little contribution towards Green IT and environment awareness, attaching printed papers as part of write-ups and program listing to journal may be avoided.*
**Guidelines for Laboratory Conduction**

The instructor may set multiple sets of assignments and distribute among batches of students. It is appreciated if the assignments are based on real world problems/applications. Student should perform at least three experiments from group A, four experiments from group B and, two experiments from C and any one assignment from group D.

**Suggested List of Laboratory Experiments/Assignments**

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th><strong>Group A</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Study of Raspberry-Pi, Beagle (History &amp; Elevation) board, Arduino and other micro controller</td>
</tr>
<tr>
<td>2</td>
<td>Study of different operating systems for Raspberry-Pi /Beagle board. Understanding the process of OS installation on Raspberry-Pi /Beagle board</td>
</tr>
<tr>
<td>3</td>
<td>Study of different sensors:温度 sensor, bio-sensor, IR sensor, chemical sensor(PH), gauge sensor, ultrasonic sensor etc.</td>
</tr>
<tr>
<td>4</td>
<td>Understand the connection and configuration of GPIO and its use in programming. Write an application of the use of LEDs.</td>
</tr>
</tbody>
</table>

| **Group B**                                                                 |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| 5                           | Design and implement program to detect and report invalid login attempts and malicious activities to embedded device.             |
| 6                           | Design and implement the program to secure the communication between the IoT devices.                                             |
| 7                           | Design and implement the program to protect the data stored at IoT device.                                                        |
| 8                           | Design and implement the program for detecting tampering of data at storage at IoT                                                |
| 9                           | Write a program identifying operating system, version and IP address assigned to the device.                                     |
| 10                          | Design and implement the code to authenticate the communication with IoT device.                                                   |

| **Group C**                                                                 |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| 11                          | Install and use open source tools to identifying various types of attacks on IoT device. Analyze the risks associated with the attacks. Write a C++/Java/Python program to identify at least one such attack. |
| 12                          | Design and implement program/ use open source tool to analyze the packets in IoT environment.                                     |
| 13                          | Develop a Real time application like a smart home security.                                                                        |

**Description:** When anyone comes at door the camera module automatically captures his image and send a notification to the owner of the house on his mobile phone using GSM modem.
<table>
<thead>
<tr>
<th>Group D</th>
</tr>
</thead>
</table>
| **14** | Design Real time application like smart home with following requirements: When user enters into house the required appliances like fan, light should be switched ON. Appliances should also get controlled remotely by a suitable web interface. The objective of this application is student should design complete Smart application in group and analyze the risks associated with it. Perform following five steps to risk assessment  
  a. Identify hazards, i.e. anything that may cause harm.  
  b. Decide what it may be harmed, and how?  
  c. Assess the risks and take action.  
  d. Make a record of the findings.  
  e. Review the risk assessment |
| **15** | Design Real time application like a smart home with following requirements: If anyone comes at door the camera module automatically captures his image send it to the email account of user or send notification to the user. Door will open only after user’s approval. The objective of this application is student should design smart home application in group and analyze the risks associated with it.  
  a. Identify the various types of risk like Technical IoT risk, Security and privacy IoT risk, Ethical IoT risk  
  b. Identify Vulnerabilities of IoT devices  
  c. Identify threats and do the threat analysis. |
Savitribai Phule Pune University
Honours* in Cyber Security
Fourth Year of Engineering (Semester VIII)
410403: Information System Management

<table>
<thead>
<tr>
<th>Teaching Scheme</th>
<th>Credit Scheme</th>
<th>Examination Scheme and Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lecture: 04 Hours/Week</td>
<td>04</td>
<td>Mid_Semester (TH): 30 Marks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>End_Semester (TH): 70 Marks</td>
</tr>
</tbody>
</table>

Prerequisites: Basic knowledge of Operating System and Data bases

Companion Course: ---

Course Objectives:
1. The course is blend of Management and Technical field.
2. Discuss the roles played by information technology in today’s business and define various technology architectures on which information systems are built.
3. Define and analyze typical functional information systems and identify how they meet the needs of the firm to deliver efficiency and competitive advantage.
4. Identify the basic steps in systems development.

Course Outcomes:
On completion of the course, learner will be able to–
1. Understand the concepts of Information systems and design the strategies for dealing with competitive forces.
2. Apply Ethical and Social Issues to Information Systems.
4. Identify and evaluate the knowledge. Apply it to the Decision-Making Process.
5. Outline the range of solutions for Systems Development and Organizational Change.

Course Contents

Unit I
Information Systems, Organizations, and Strategy (06 Hours)


#Exemplar/Case Studies
ERP

Unit II
Ethical and Social Issues in Information Systems (09 Hours)


#Exemplar/Case Studies
Kiwan Code Security (SAST), Nmap, Netsparker

Unit III
IT Infrastructure and (09 Hours)
Emerging Technologies


#Exemplar/Case Studies

Windows, Android, iOS, MacOS

Unit IV

Managing Knowledge and Enhancing Decision Making (08 Hours)


#Exemplar/Case Studies

AsinSeed, AVDecision, Expert Choice

Unit V

Building and Managing Systems (08 Hours)


#Exemplar/Case Studies

ASANA, Basecamp, JIRA, Teamwork PM, Microsoft Team

Unit VI

Information Systems Security (08 Hours)


#Exemplar/Case Studies

Norton, Life Lock, Zone Alarm.

Learning Resources

Text Books:

Reference Books:
|-------------------------------|

**e-Books:**

Information Systems for Business and Beyond, David T. Bourgeois Biola University, James L. Smith Shouhong Wang, Joseph Mortati

**MOOC/ Video Lectures available at:** Prof. Kunal Ghosh, Prof. Surojit Mookherjee, Prof. Saini Das, IIT Kharagpur, Management Information System, https://nptel.ac.in/courses/110/105/110105148/
Savitribai Phule Pune University
Honours* in Cyber Security
Fourth Year of Engineering (Semester VIII)
410404: Seminar

<table>
<thead>
<tr>
<th>Teaching Scheme</th>
<th>Credit Scheme</th>
<th>Examination Scheme and Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practical: 02</td>
<td>02</td>
<td>Presentation: 50 Marks</td>
</tr>
<tr>
<td>Hours/Week</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Course Objectives:
- To train the student to independently search, identify and study important topics in computer science.
- To develop skills among students to study and keep themselves up to date of the technological developments taking place in computer science
- To expose students to the world of research, technology and innovation.

Course Outcomes:
On completion of the course, student will be able to
- To train the student to independently search, identify and study important topics in computer science.
- To develop skills among students to study and keep themselves up to date of the technological developments taking place in computer science.
- To expose students to the world of research, technology and innovation

Guidelines for Seminar:
- The department will assign an internal guide under which students shall carry out Hons. seminar work
- In order to select a topic for Hons. Seminar, the student shall refer to various resources like books, magazines, scientific papers, journals, the Internet and experts from industries and research institutes
- The topic selected for Hons. Seminar by the students will be scrutinized and if found suitable, shall be approved by the internal guide
- Student should also explore the tools and technologies available for implementation of selected topic. Student should implement/simulate the seminar work partially/fully for enhancing the practical skill set on topic.
- Student shall submit the progress of his/her Hons. Seminar work to the internal guide.
- The student shall prepare a REPORT on the work done on Hons. Seminar and submit it at the time of presentation.

Evaluation of IT Seminar Work
- During the seminar work, its progress will be monitored, by the internal guide.
- At the end of seminar work, copy of Hons. Seminar Report should be prepared and submitted to department.
- End Examination shall be based on the Report, technical content and Presentation.
- Guidelines for Assessment: Panel of staff members along with a guide would be assessing the seminar work based on these parameters-Topic, Contents and Presentation, implementation, regularity, Punctuality and Timely Completion, Question and Answers, Report, Paper presentation/Publication, Attendance and Active Participation.

References: