AICTE MODEL CURRICULUM
FOR
POST GRADUATE DEGREE COURSE
M.TECH
in
COMPUTER NETWORKS & INFORMATION SECURITY
[W.E.F. 2021-22]

DEPARTMENT OF
COMPUTER SCIENCE AND SYSTEMS
ENGINEERING
AU COLLEGE OF ENGINEERING (AUTONOMOUS)
ANDHRA UNIVERSITY
VISAKHAPATNAM-530 003
ANDHRA UNIVERSITY: : VISAKHAPATNAM

M.Tech.

Computer Networks & Information Security

Course Structure and Scheme of Valuation w.e.f. 2021-22

### I-SEMESTER

<table>
<thead>
<tr>
<th>Code</th>
<th>Name of the subject</th>
<th>Periods/week</th>
<th>Max. Marks</th>
<th>Total</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Theory</td>
<td>Lab</td>
<td>Ext.</td>
<td>Int.</td>
</tr>
<tr>
<td>MTCNIS11</td>
<td>Mathematical Foundations For Cryptography</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS12</td>
<td>TCP/IP</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS13</td>
<td>Elective-I</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS14</td>
<td>Elective-II</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS15</td>
<td>Research Methodology &amp; IPR</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCST16</td>
<td>Organizational Behavior (Audit Course)</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS17</td>
<td>TCP/IP Lab</td>
<td>3</td>
<td>-</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>MTCNIS18</td>
<td>Network Simulation &amp; IoT Lab</td>
<td>3</td>
<td>-</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>18</strong></td>
<td><strong>6</strong></td>
<td><strong>520</strong></td>
<td><strong>280</strong></td>
</tr>
</tbody>
</table>

**Elective-I:** Virtual Private Networks/Machine Learning/Unix Network Programming

**Elective II:** Cloud Computing/Distributed Operating Systems/IoT

### II-SEMESTER

<table>
<thead>
<tr>
<th>Code</th>
<th>Name of the subject</th>
<th>Periods/week</th>
<th>Max. Marks</th>
<th>Total</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Theory</td>
<td>Lab</td>
<td>Ext.</td>
<td>Int.</td>
</tr>
<tr>
<td>MTCNIS21</td>
<td>Mobile-Adhoc Networks</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS22</td>
<td>Computer Security</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS23</td>
<td>Elective-III</td>
<td>3</td>
<td>3</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS24</td>
<td>Elective-IV</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCST25</td>
<td>Entrepreneurship (Audit Course)</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS26</td>
<td>Wireless Networks Lab</td>
<td>-</td>
<td>3</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>MTCNIS27</td>
<td>Application Security Lab</td>
<td>-</td>
<td>3</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>MTCNIS28</td>
<td>Mini Project With Seminar</td>
<td>-</td>
<td>3</td>
<td>-</td>
<td>100</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>15</strong></td>
<td><strong>9</strong></td>
<td><strong>450</strong></td>
<td><strong>350</strong></td>
</tr>
</tbody>
</table>

**Elective III:** Web Application Security/Android-IoS Security/IoT Security

**Elective IV:** Digital Forensics/Sensor Networks/Intrusion Detection System (IDS)
### III-SEMESTER

<table>
<thead>
<tr>
<th>Code</th>
<th>Name of the subject</th>
<th>Periods/week</th>
<th>Max. Marks</th>
<th>Total</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Theory</td>
<td>Lab</td>
<td>Ext.</td>
<td>Int.</td>
</tr>
<tr>
<td>MTCNIS 31</td>
<td>Elective-V</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS 32</td>
<td>Open Elective</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS33</td>
<td>Dissertation-I / Industrial project</td>
<td>-</td>
<td>100</td>
<td>-</td>
<td>100</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td>6</td>
<td>-</td>
<td>240</td>
<td>60</td>
</tr>
</tbody>
</table>

**Elective V:** Malware Analysis/Block chain Technologies/Software Defined Networks  
**Open Elective:** Business Analytics /4G-5G Mobile Communication Networks/ Operation Research

### IV-SEMESTER

<table>
<thead>
<tr>
<th>Code</th>
<th>Name of the subject</th>
<th>Periods/week</th>
<th>Max. Marks</th>
<th>Total</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Theory</td>
<td>Lab</td>
<td>Ext.</td>
<td>Int.</td>
</tr>
<tr>
<td>MTCNIS41</td>
<td>Dissertation- II</td>
<td>-</td>
<td>-</td>
<td>100</td>
<td>-</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td>-</td>
<td>-</td>
<td>100</td>
<td>-</td>
</tr>
</tbody>
</table>
Programme Education Objectives (PEO)
PEO1: To drive the students to achieve excellence in research and professional career.
PEO2: To promote creative thinking and innovative mindset for solving societal problems.
PEO3: To help exhibit adaptive and agile skills in the core area of Information Security & Networks to meet the technical and managerial challenges.
PEO4: To demonstrate interpersonal skills, professional ethics to work in a team to make a positive impact on society and sustenance.

Programme Specific Outcomes (PSO)
PSO 1: Ability to understand the design and implementation of Computer Networks and Information Security algorithms and infrastructure.
PSO 2: Ability to apply standard practices related to Networks and Security Technologies and follow professional ethics.
PSO 3: Ability to apply mathematical and algorithmic models and handle projects involving hardware and software related to Networks and Security and follow agile methods.
PSO 4: Ability to propose research and applicability of innovative ideas related to Networks and Security and be able to write reports.

Programme Outcomes (PO)
PO1: To acquire essential knowledge of relevant mathematics and algorithms basics.
PO2: To understand, model and find solutions for engineering problems to help achieve sustainable development.
PO3: To be able to design systems, components and products useful to enhance quality of human life while using internet and related devices.
PO4: To be able to apply knowledge in Computer Engineering to solve research problems and publish in high impact journals/conferences.
PO5: To be able to use open-source networking and security tools and networking equipment.
PO6: To be able to understand societal, health, cultural, safety and legal issues in context of network and security domain.
PO7: To be able to understand the impact of network and security technology-based solutions in a global, economic, environmental and societal context.
PO8: To understand professional and ethical responsibility.
PO9: To excel as an individual and as a team member in achieving a common goal.
PO10: To communicate effectively with research and academic communities in both written and oral formats.
PO11: To acquire knowledge of contemporary issues in QOS, cyber-attacks, preventive measures, and data safety.
PO12: To gain appropriate skills and be a continuous learner for professional and career advancement.
Course Objectives:
In this course, we will be introduced to basic mathematical principles and functions that form the foundation for cryptographic and cryptanalysis methods. These principles and functions will be helpful in understanding symmetric and asymmetric cryptographic methods examined in our course. It is recommended that you have a basic knowledge of computer science and basic math skills such as algebra and probability.
To make the student learn different encryption techniques along with hash functions, MAC, digital signatures, and their use in various protocols for network security and system security.
- To understand basics of Cryptography and mathematical foundations.
- To be able to secure a message over insecure channel by various means.
- To learn about how to maintain the Confidentiality, Integrity, and Availability of a data.
- To understand various protocols for network security to protect against the threats in the networks.

Course Outcomes:
After successful completion of the course, the learners would be able to
- Provide security of the data over the network.
- Do research in the emerging areas of cryptography and network security.
- Implement various networking protocols.
- Protect any network from the threats in the world.
- Apply numerical methods and Mathematical Foundations to solve the complex engineering Problems.
Course Objectives:

- The objective of a TCP/IP course is to provide a comprehensive understanding of the TCP/IP protocol suite, including its architecture, protocols, and services.
- The course should cover topics such as IP addressing, subnetting, routing, TCP and UDP protocols, domain names, network security, and network troubleshooting.
- The goal is to equip students with the knowledge and skills necessary to design, implement, and manage TCP/IP-based networks.

Course Outcomes:

By the end of this course, students will gain the following knowledge and skills:

- Understanding of Networking Fundamentals: Students will gain an understanding of basic networking concepts, such as the OSI & TCP/IP models.
- Details of Network layer protocols (such as IP, ARP, RARP, ICMP etc.,)
- Knowledge of TCP/IP Protocols: Students will develop an understanding of the core concepts of the TCP and IP protocols, including data segmentation, flow control, congestion control and error detection.
- IP Routing Skills: Students will learn how to configure and implement IP routing, including the use of static and dynamic routing protocols (such as BOOTP, DHCP).
- TCP Connection Management Skills: Students will gain experience in managing TCP connections, including the three-way handshake and flow control.
- Knowledge of Application Protocols: Students will develop an understanding of commonly used application protocols that run over TCP/IP, such as HTTP, SNMP, FTP, IP Multicasting, MPLS and DNS.
- A good understanding of the other advanced protocols such as FINGER protocol, MOBILE IP, WHOIS protocol, TCPDUMP, GOPHER, VERONICA etc.,
## Course Objectives:

- To Learn About the Different Layers, Encapsulation, Addressing, Routing of Tcp/Ip Model.
- To Learn About Virtual Private Network, Its Components, Workflow, Tunneling, Architecture, Advantages and Disadvantages and Different Protocols
- To Learn About Secure Sockets Layer (Ssl), Its Protocols, Its Security, Secure Socket Shell (Ssh) And About Light Weight Vpn
- To Learn About Vpn Applications in Business and Industry

## Course Outcomes:

- Gain Knowledge About Vpn, Device Level and Network Level Components Of Vpn, Steps For All Kinds Of Vpn Configurations, Process By Which Vpn Packets Reach Their Intended Destinations, And Different Protocols Like Ip-In-Ip Tunnels, Point To Point Tunneling, Generic Routing Encapsulation, Secure Shell, Layer 2 Tunneling Etc.
- Gain Knowledge About Secure Socket Shell, Sshv1, Sshv2, Lightweight Vpn.
- Gain Knowledge About Building Vpn Using Ssh
- Gain Knowledge to Establish Vpn In Business And Industry Establishments.
MTCNIS13 ELECTIVE-I MACHINE LEARNING

<table>
<thead>
<tr>
<th>Instruction: 3Periods/week,</th>
<th>Time: 3 Hours</th>
<th>Credits: 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
<td>Total: 100 Marks</td>
</tr>
</tbody>
</table>

Course Objectives:
Machine Learning course will
- Develop an appreciation for what is involved in learning from data.
- Study a wide variety of learning algorithms.
- Demonstrate how to apply a variety of learning algorithms to data.
- Demonstrate how to perform evaluation of learning algorithms and model selection.

Course Outcomes:
After the completion of the course, student will be able to
- Understand the distribution and diversity of Data.
- Extract features useful for building predictive models.
- Gain knowledge on Supervised and unsupervised Learning techniques.
- Analyze Statistical learning techniques and Logistic Regression
- Select appropriate Support Vector Machines and Perceptron Algorithm
- Compare the performance of different learning models.

MTCNIS13 ELECTIVE-I UNIX NETWORK PROGRAMMING

<table>
<thead>
<tr>
<th>Instruction: 3Periods/week,</th>
<th>Time: 3 Hours</th>
<th>Credits: 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
<td>Total: 100 Marks</td>
</tr>
</tbody>
</table>

Course Objectives:
- To understand inter process and inter-system communication.
- To understand socket programming in its entirety.
- To understand usage of TCP/UDP / Raw sockets.
- To understand how to build network applications.

Course Outcomes:
- To write socket API based programs.
- To design and implement client-server applications using TCP and UDP sockets.
- To analyse network programs.
### ELECTIVE-II  CLOUD COMPUTING

**MTCNIS14**

<table>
<thead>
<tr>
<th>Instruction: 3 Periods/week,</th>
<th>Time: 3 Hours</th>
<th>Credits: 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
<td>Total: 100 Marks</td>
</tr>
</tbody>
</table>

**Course objectives:**
- To import fundamental concepts in cloud computing.
- To understand the concept of Virtualization and cloud data storage.
- To learn cloud Application Development and cloud Governance.
- To gain competence in Map Reduce and Hadoop Overview.

**Course Outcomes:**
- Identify the architecture and infrastructure of cloud computing.
- Develop applications for cloud computing.
- Design and implement a novel cloud computing application.

### ELECTIVE-II  DISTRIBUTED OPERATING SYSTEMS

**MTCNIS14**

<table>
<thead>
<tr>
<th>Instruction: 3 Periods/week,</th>
<th>Time: 3 Hours</th>
<th>Credits: 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
<td>Total: 100 Marks</td>
</tr>
</tbody>
</table>

**Course objectives:**
- Understand how computational power of multiple computing systems distributed remotely can solve complex problems and importance of replication of data in distributed systems.
- Understand the core concepts of distributed operating systems including process management, synchronization, memory management and file systems.
- Apply various distributed algorithms related to clock synchronization, concurrency control, deadlock detection, load balancing, etc.

**Course outcomes:**
By the end of the course, the student will be able to:
- Identify the core concepts of distributed systems and understand the design principles and architectures for distributed systems.
- Understand client-server organizations in distributed systems and how processes in different machines exchange information through group communication.
- Analyze fault tolerance and recovery in distributed systems.
- Understand the design and implementation of distributed file systems.
ELECTIVE-II  INTERNET OF THINGS

MTCNIS14

<table>
<thead>
<tr>
<th>Instruction: 3 Periods/week,</th>
<th>Time: 3 Hours</th>
<th>Credits: 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
<td>Total: 100 Marks</td>
</tr>
</tbody>
</table>

Course Objectives:
- Vision and Introduction to Internet of Things (IoT).
- Understand IoT Market perspective.
- Data and Knowledge Management and use of Devices in IoT Technology.
- Understand Real World IoT Design Constraints, Industrial Automation and Commercial.

Course Outcomes:
At the end of the course, student will be able to:
- Explain in a concise manner how the general Internet as well as Internet of Things work.
- Understand constraints and opportunities of wireless and mobile networks for Internet of Things.
- Use basic sensing and measurement and tools to determine the real-time performance of network of devices.
- Develop prototype models for various applications using IoT technology.

RESEARCH METHODOLOGY AND IPR
Common for MTech (CST, IT, CN&IS, AI&ML)

MTCNIS15

<table>
<thead>
<tr>
<th>Instruction: 3 Periods/week,</th>
<th>Time: 3 Hours</th>
<th>Credits: 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
<td>Total: 100 Marks</td>
</tr>
</tbody>
</table>

Course Objectives:
- To provide students a comprehensive knowledge about IPR.
- The students will learn the procedure of obtaining Patents, Copyrights, Trademarks & Industrial Design.
- To enable the students to know about various IP rights its recognition and protection.
- To provide knowledge on various types of IP databases.

Course Outcomes:
On successful completion of this course student will be able to
- Distinguish and explain various forms of IPRs like trade mark, copy right, Geo tagged etc.
- Know and identify the methods to fit one's own intellectual work in particular form of IPRs.
- Apply statutory provisions to protect particular form of IPRs.
- Understand current and emerging issues relating to the intellectual property and its protection.

### MTCNIS16

**ORGANIZATIONAL BEHAVIOR (Audit Course)**
Common for MTech (CST, IT, CN&IS, AI&ML)

<table>
<thead>
<tr>
<th>Instruction: 3Periods/week,</th>
<th>Time: 3 Hours</th>
<th>Credits: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
<td>Total: 100 Marks</td>
</tr>
</tbody>
</table>

**Course Objectives:**
- To understand the basic concepts of organizational behavior, its foundations and importance.
- To enable students to have a basic perspective of Motivation and Motivation theories.
- To acquaint the students about group behavior in organizations, including communication, leadership conflicts and organizational change and how these are linked to an impact organizational performance.

### MTCNIS17

**TCP/IP LAB**

<table>
<thead>
<tr>
<th>Instruction: 3Periods/week,</th>
<th>Time: 3 Hours</th>
<th>Credits: 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
<td>Total: 100 Marks</td>
</tr>
</tbody>
</table>

**Course Objectives:**
A TCP/IP Lab course is designed to provide hands-on experience and practical skills in working with TCP/IP networks. The objective of this course is to enable students to:
- *Apply theoretical knowledge of TCP/IP protocols:* Students will have the opportunity to apply their understanding of the IP addressing concepts in a hands-on lab environment.
- *Configure and Troubleshoot IP addresses:* Students will gain experience in
configuring and troubleshooting IP addressing protocols.

- **Simulate Real-World Network Scenarios:** Students will have the opportunity to simulate real-world networking scenarios, such as network design, security, and troubleshooting, in a controlled laboratory environment.

- **Learn Network Monitoring and Analysis Techniques:** Students will learn how to monitor and analyze network traffic using network monitoring and analysis tools, such as ireshark or tcpdump.

- **Collaborate with Peers:** Students will have the opportunity to collaborate with their peers on lab assignments and projects, allowing them to develop teamwork skills and share knowledge and experience.

**Course Outcomes:**

By the end of this course, students will achieve the following:

- **Practical Knowledge of TCP/IP Protocols:** Students will have practical experience in applying their understanding of the IP addressing concepts in a laboratory environment.

- **Ability to Configure and Troubleshoot IP Networks:** Students will be able to configure and troubleshoot IP addressing using CIDR notation.

- **Proficiency in Networking Tools and Techniques:** Students will have developed proficiency in using networking hardware and software, such as network simulation tools and configuring Apache web server and DNS server on windows system to run python networking scripts.

- **Confidence in Network Monitoring and Analysis:** Students will have the ability to monitor and analyze TCP/IP network traffic using network monitoring and analysis tools, such as Wireshark and tcpdump.

- **Teamwork and Collaboration Skills:** Students will have developed teamwork and collaboration skills through working on lab assignments and projects with their peers.

- **By the end of a TCP/IP Lab course, students should be well-prepared to work with TCP/IP networks in a practical setting and have a solid foundation for further study and certification in the field of networking.**

---

<table>
<thead>
<tr>
<th>MTCNIS18</th>
<th>NETWORK SIMULATION &amp;IOT LAB</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Instruction:</strong> 3Periods/week, <strong>Time:</strong> 3 Hours</td>
<td><strong>Credits:</strong> 2</td>
</tr>
<tr>
<td><strong>Internal:</strong> 30 Marks</td>
<td><strong>External:</strong> 70 Marks</td>
</tr>
</tbody>
</table>

**Course Objectives:**

- To Identify and make familiar to the control element in the design of communication protocols for WSNs.

- To Understand the hardware platforms and software frameworks used in functioning
of various wireless sensor Networks (WSN).

- To Understand the concept of routing for sending the data from one node to another node evaluating the results through trace analysis and graphical visualization.
- To Provide in-depth knowledge of estimating of parameter measures and testing process of the wireless communication system.

Course Outcomes:
- Ability to get familiarized with the protocol design requirements, suitable algorithms and state-of-the-art cloud platform to meet industrial requirements.
- Ability to establish networks with an attempt to reduce issue of broadcast and flooding techniques.
- Proactive in understanding the routing protocol’s function and their implementation on data transmission delay and bandwidth.
- Ability to implement hardware and software for wireless sensor networks in everyday life.
- Ability to be able to contribute appropriate algorithms to improve existing or to develop new WSN applications.

<table>
<thead>
<tr>
<th>MTCNIS21</th>
<th>MOBILE-ADHOC NETWORKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instruction: 3 Periods/week</td>
<td>Time: 3 Hours</td>
</tr>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
</tr>
<tr>
<td>Credits: 3</td>
<td>Total: 100 Marks</td>
</tr>
</tbody>
</table>

Course Objectives:
- To understand the concepts of mobile adhoc networks
- To understand the concepts of wireless LANs, wireless adhoc networks, types and their routing protocols
- To introduce students to mobile communications and mobile computing
- To understand basics of Mobile Data Networks, MANETs and other wireless technologies

Course outcomes:
By the end of the course, the student should be able to demonstrate:
- Ability to understand the state-of-the-art research in the emerging subject of Mobile Adhoc Networks
- Explain basics, standards and topologies of wireless LANs.
- Understand basics, types, routing protocols and applications of wireless adhoc networks.
- Understand basics of Mobile Data Networks, MANETs and other wireless technologies

MTCNIS22 | COMPUTER SECURITY |
Course Objectives:
- Introduction of the issues in network security- its need and importance, taxonomy, and terminology.
- Exploration of different types of security threats and remedies.
- Understanding of Internet security protocols and standards

Course Outcomes:
By the end of the course, the student should be able to:
- Realize the need for and importance of network and data security on the Internet and in the distributed environments.
- Identify the different types of network security issues and their remedies.
- Implementation of some Internet security protocols and standards
Course Objectives:
This course describes different components of Android applications and iOS Applications.
- Identifies possible vulnerabilities and Security issues in both the platforms.
- Identifies and helps in practicing defensive programming techniques to protect the users of Android and iOS applications from the common attacks.
- Secure coding examples

Course Outcomes:
At the end of this course Students will
- Identify various risks related to Android and iOS applications.
- Understand the structure of Android and iOS files.
- Understand the Android security model and the protections provided by the Android OS.
Understand the iOS security model and the protections provided by the iOS.

<table>
<thead>
<tr>
<th>MTCNIS23</th>
<th>ELECTIVE-III</th>
<th>IoT SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instruction: 3Periods/week,</td>
<td>Time: 3 Hours</td>
<td>Credits: 3</td>
</tr>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
<td>Total: 100 Marks</td>
</tr>
</tbody>
</table>

Course Objectives:
- Able to understand the IoT security issues and IoT Security architecture.
- Identifies the vulnerability on the Internet of Things.
- To gain Knowledge of IoT privacy concerns
- To be familiar with the IoT incident response and Forensic Analysis.

Course Outcomes:
At the end of this course Students will
- Identify various threats and security requirement for IoT devices.
- Understand the Firmware Security and Physical layer security in IoT devices.
- Understand the Identity and Access Management Solutions for the IoT.
- Understand the Cloud Security for the IoT and IoT incident response.

<table>
<thead>
<tr>
<th>MTCNIS24</th>
<th>ELECTIVE-IV</th>
<th>DIGITAL FORENSICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instruction: 3Periods/week,</td>
<td>Time: 3 Hours</td>
<td>Credits: 3</td>
</tr>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
<td>Total: 100 Marks</td>
</tr>
</tbody>
</table>

Course Objectives:
To understand digital forensics basics and tools for conducting forensics of digital devices.
To understand the digital forensic systems and services
To understand various techniques of data acquisition and identification analysis
To understand about processing the crime scene and preserving digital evidence and gain skills required for a digital crime investigator.

Course Outcomes:
• To be able to learn various basics of digital forensics and investigation and the challenges involved in evidence collection, incidence response.
• To learn various Cyber Laws and understand the legal requirements before performing digital investigation.
• To learn methods and tools to backup, recover, preserve evidence.
• To learn various methods to collect evidence from applications, network, hard disk, main memory and be able to generate reports.
• To be able to research using the skills learned and implement or update Cyber forensics methods.

<table>
<thead>
<tr>
<th>MTCNIS24</th>
<th>ELECTIVE-IV SENSOR NETWORKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instruction: 3 Periods/week,</td>
<td>Time: 3 Hours</td>
</tr>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
</tr>
</tbody>
</table>

Course Objectives:
• To understand the concepts of sensor networks
• To understand the MAC and transport protocols for ad hoc networks
• To understand the security of sensor networks
• To understand the applications of adhoc and sensor networks

Course Outcomes:
By the end of the course, the student will be able to demonstrate:
• Ability to understand the state-of-the-art research in the emerging subject of Ad Hoc and Wireless Sensor Networks
• Ability to solve issues in real-time application development based on ASN.
• Ability to conduct further research in the domain of ASN.

<table>
<thead>
<tr>
<th>MTCNIS24</th>
<th>ELECTIVE-IV INTRUSION DETECTION SYSTEM (IDS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instruction: 3 Periods/week,</td>
<td>Time: 3 Hours</td>
</tr>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
</tr>
</tbody>
</table>
**Course Objectives:**
- Understand when, where, how, and why to apply Intrusion Detection tools and techniques to improve the security posture of an enterprise.
- Apply knowledge of the fundamentals and history of Intrusion Detection to avoid common pitfalls in the creation and evaluation of new Intrusion Detection Systems.
- Analyze intrusion detection alerts and logs to distinguish attack types from false alarms.
- Apply the knowledge to the architecture, configuration, and analysis of specific intrusion detection systems.

**Course Outcomes:**
- Understand modern concepts related to Intrusion Detection System.
- Compare alternative tools and approaches for Intrusion Detection through quantitative analysis to determine the best tool or approach to reduce risk from intrusion.
- Identify and describe the parts of all intrusion detection systems and characterize new and emerging.

<table>
<thead>
<tr>
<th>MTCNIS25</th>
<th>ENTREPRENEURSHIP (AUDIT COURSE)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instruction: 3Periods/week,</td>
<td>Time: 3 Hours</td>
</tr>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
</tr>
</tbody>
</table>

**Course Objectives:**
- To familiarize the students with the concepts of Management.
- To relate the concepts of Management with industrial organizations.
- To explain the factors affecting productivity and how productivity can be increased in an Industrial undertaking.
- To set forth a basic framework for understanding Entrepreneurship.

**Course Outcomes:**
On completion of the course, the students will be able to:
- Understand the roles, skills, and functions of management.
- Distinguish the different types of business organizations.
- Identify the factors involved in Production Operations Management.
- Diagnose organizational problems and take suitable decisions.
- Establish good Human Resource Management practices.
- Acquire necessary knowledge and skills required for organizing and carrying out entrepreneurial activities.
WIRELESS NETWORKS LAB

Instruction: 3Periods/week, Time: 3 Hours Credits: 2

Internal: 30 Marks External: 70 Marks Total: 100 Marks

Course Objectives:

- The objective of this course is to provide students an overview of Wireless Sensor Networks.
- The students learn issues and challenges related to WSN design, and implementation.
- The course provides required knowledge to students to build real-time WSN applications.
- To study the evolving wireless technologies and standards.

Course Outcomes:

After successfully completing the course student will be able to

- Keep himself updated on latest wireless technologies and trends in the communication field.
- To understand the architectures of various access technologies such as 3G, 4G, Wi-Fi etc.
- To understand various protocols and services provided by next generation networks.
- Understand the transmission of voice and data through various networks.

APPLICATION SECURITY LAB

Instruction: 3Periods/week, Time: 3 Hours Credits: 2

Internal: 30 Marks External: 70 Marks Total: 100 Marks

Course Objectives:

- Recognize common web application security vulnerabilities and how to determine if they are present in web applications.
- Recognize web application design assumptions and how to exploit them.
- Be familiar with the capabilities of various Browser Proxies
- Be familiar with the capabilities of various Penetration Testing tools.
- Be prepared to detect Access Control Vulnerabilities
- Be prepared to detect SQL Injection Vulnerabilities
- Be prepared to detect Cross-Site Scripting (XSS) Vulnerabilities
- Be prepared to detect Authentication and Session Vulnerabilities
Be prepared to test web application security.

**Course Outcomes:**

- Identify the vulnerabilities in the web applications.
- Identify the various types of threats and mitigation measures of web applications.
- Apply the security principles in developing a reliable web application.
- Use industry standard tools for web application security.
- Apply penetration testing to improve the security of web applications.

<table>
<thead>
<tr>
<th>MTCNIS31</th>
<th>ELECTIVE-V MALWARE ANALYSIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instruction: 3 Periods/week,</td>
<td>Time: 3 Hours</td>
</tr>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
</tr>
</tbody>
</table>

**Course Objectives:**

- To understand the impact of malwares during cyber-attacks.
- To be able to classify malwares through analysis and use tools for detection.
- To learn malware propagation and their containment
- To prevent malwares from affecting the network resources and digital assets using tools

**Course Outcomes:**

- Know various types of malwares, their impact and understand their behaviors.
- Perform different malware analysis techniques on samples using static and dynamic methods.
- Understand malware attack mechanisms, use tools to detect and to contain their propagation.
- Understand Windows based malwares and apply the learned techniques to reduce risks and malware attacks.
- Able to research using the skills learned and implement or update Cyber Security methods for reducing risks due to cyber-attacks through malwares.

<table>
<thead>
<tr>
<th>MTCNIS31</th>
<th>ELECTIVE-V BLOCK CHAIN TECHNOLOGIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instruction: 3 Periods/week,</td>
<td>Time: 3 Hours</td>
</tr>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
</tr>
</tbody>
</table>

**Course Objectives:**
To understand the basic concepts block chain technology and to explore the driving force behind the crypto currency Bitcoin.

To understand about the different methods of Decentralization using Block Chain and different Bitcoins and Alternative Coins.

To understand about Ethereum and applications using Smart contracts and Block Chain Applications

**Course Outcomes:**
At the end of the course the student will be able to:

- Understand the types, benefits, and limitation of block chain.
- Explore the block chain decentralization and cryptography concepts.
- Enumerate the Bitcoin features and its alternative options.
- Describe and deploy the smart contracts.

<table>
<thead>
<tr>
<th>MTCNIS31</th>
<th>ELECTIVE-V SOFTWARE DEFINED NETWORKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instruction: 3 Periods/week, Time: 3 Hours</td>
<td>Credits: 3</td>
</tr>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
</tr>
</tbody>
</table>

**Course Objectives:**

- Understand the evolution of Software Defined Networks (SDN) and its interoperability.
- Examine the characteristics of SDN and its devices and controllers.
- Understand the OpenFlow specifications and its limitations.
- Comparison of SDN, Overlays and APIs.
- Design of network virtualization tunnels and offloading flows in data centers.
- Design and development of switch and controller in SDN applications.

**Course Outcomes:**

- Analyze the implications of SDN for research and innovation data centers.
- Brief the OpenFlow basics and optical transport protocols.
- Develop the tunneling and path technologies for real world data center.
- Implementation of the access control for the campus and traffic engineering for service providers.
- Simulation and testing of SDN in open-source cloud software.
- Implementation of switch and controller in SDN applications

| MTCNIS32 | OPEN ELECTIVE: BUSINESS ANALYTICS |
Course objectives:
- To introduce students to problem solving with Business Analytics and the use of spreadsheets for descriptive analytics, data queries and visualization
- To introduce students to statistical sampling, sampling distributions, confidence intervals and statistical inference
- To familiarize students with various types of regression including simple linear regression and multiple linear regression
- To introduce students to key concepts in statistical forecasting models for time series data.
- To familiarize students with predictive decision modeling, model analysis and developing spreadsheet applications including building linear optimization models on spreadsheets.

Course outcomes:
After completion of the course the student should be able to:
- Describe data and models used for Business Analytics and apply various descriptive analytic techniques to analyze data.
- Estimating population parameters, interval estimates, construct confidence intervals and perform hypothesis testing.
- Estimate and interpret the parameters of simple linear regression and multiple linear regressions.
- Apply forecasting models for various time series data including stationary time series, time series with linear trend and time series with seasonality.
- Implement models on spreadsheets, develop user-friendly applications and build linear optimization models on spreadsheets.
duality and complementary slackness

- Perform sensitivity analysis to determine the direction and magnitude of change of a model’s optimal solution as the data change.
- Solve specialized linear programming problems like the transportation and assignment problems.
- Solve network models like the shortest path, minimum spanning tree, and maximum flow problems.
- Understand the applications of basic methods for, and challenges in integer programming

**Course Outcomes:**
By the end of the course, the student will be able to:

- Students will be able to describe characteristics and scope of OR.
- Students will be able to define and formulate mathematical problems.
- Students will be able to select optimal problems solving techniques for a given problem using LP.
- Students will be able to formulate and solve transportation, travelling salesman and transshipment problems.
- Students will be able to formulate and solve optimization problems related to job/ work assignments.
- Students will be able to demonstrate and solve simple models of Game theory.
- Students will be able to evaluate optimum solution using dynamic programming for different applications.
- Students will be able to choose / devise appropriate queuing model for practical application.
- Students will be able to solve different problems related to Network.

<table>
<thead>
<tr>
<th>MTCNIS32</th>
<th>OPEN ELECTIVE: 4G-5G MOBILE COMMUNICATION NETWORKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instruction: 3Periods/week, Time: 3 Hours</td>
<td>Credits: 3</td>
</tr>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
</tr>
</tbody>
</table>

**Course Objectives:**

- Understand the 5G and beyond broadband networks.
- Analysis the emerging technologies in Software Defined radio and Mobile IP networks.
- Determine the capacity of multi-gigabit wireless networks and High-speed networks.
- Evaluate the energy harvesting tags and low power networks.
- Ability to understand the working of Wi-Fi fingerprinting and RF sensing.
- Understand the wireless technologies for Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V).
Course Outcomes:

- Summarize the spectrum regulation and standards of broadband network.
- Explain the need of adaptive techniques and resource management for 4G networks.
- Evaluate the QoS requirements for SDR and IP Networks.
- Develop the visible light indoor localization and RF sensing networks.
- Explain the necessity of backscatter communication protocols for IoT.
- Design the smart phone localization and drone networks and implement networks through simulation.
AICTE MODEL CURRICULUM
FOR
POST GRADUATE DEGREE COURSE
M.TECH
in
COMPUTER NETWORKS & INFORMATION SECURITY
[W.E.F. 2021-22]

DEPARTMENT OF
COMPUTER SCIENCE AND SYSTEMS
ENGINEERING
AU COLLEGE OF ENGINEERING (AUTONOMOUS)
ANDHRA UNIVERSITY
VISAKHAPATNAM-530 003
# ANDhra University: Visakhapatnam

## M.Tech.

### Computer Networks & Information Security

Course Structure and Scheme of Valuation w.e.f. 2021-22

## I-SEMESTER

<table>
<thead>
<tr>
<th>Code</th>
<th>Name of the subject</th>
<th>Periods/week</th>
<th>Max. Marks</th>
<th>Total</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Theory</td>
<td>Lab</td>
<td>Ext.</td>
<td>Int.</td>
</tr>
<tr>
<td>MTCNIS11</td>
<td>Mathematical Foundations For Cryptography</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS12</td>
<td>TCP/IP</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS13</td>
<td>Elective-I</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS14</td>
<td>Elective-II</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCST15</td>
<td>Research Methodology &amp; IPR</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCST16</td>
<td>Organizational Behavior (Audit Course)</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS17</td>
<td>TCP/IP Lab</td>
<td>3</td>
<td>50</td>
<td>50</td>
<td>100</td>
</tr>
<tr>
<td>MTCNIS18</td>
<td>Network Simulation &amp; IoT Lab</td>
<td>3</td>
<td>50</td>
<td>50</td>
<td>100</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>18</strong></td>
<td><strong>6</strong></td>
<td><strong>520</strong></td>
<td><strong>280</strong></td>
</tr>
</tbody>
</table>

**Elective I:** Virtual Private Networks/Machine Learning/Unix Network Programming

**Elective II:** Cloud Computing/ Distributed Operating Systems/IoT

## II-SEMESTER

<table>
<thead>
<tr>
<th>Code</th>
<th>Name of the subject</th>
<th>Periods/week</th>
<th>Max. Marks</th>
<th>Total</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Theory</td>
<td>Lab</td>
<td>Ext.</td>
<td>Int.</td>
</tr>
<tr>
<td>MTCNIS21</td>
<td>Mobile-Adhoc Networks</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS22</td>
<td>Computer Security</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS23</td>
<td>Elective-III</td>
<td>3</td>
<td>3</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS24</td>
<td>Elective-IV</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCST25</td>
<td>Entrepreneurship (Audit Course)</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS26</td>
<td>Wireless Networks Lab</td>
<td>-</td>
<td>3</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS27</td>
<td>Application Security Lab</td>
<td>-</td>
<td>3</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>MTCNIS28</td>
<td>Mini Project With Seminar</td>
<td>-</td>
<td>3</td>
<td>-</td>
<td>100</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>15</strong></td>
<td><strong>9</strong></td>
<td><strong>450</strong></td>
<td><strong>350</strong></td>
</tr>
</tbody>
</table>

**Elective III:** Web Application Security/Android-IoS Security/IoT Security

**Elective IV:** Digital Forensics/Sensor Networks/Intrusion Detection System (IDS)
### III-SEMESTER

<table>
<thead>
<tr>
<th>Code</th>
<th>Name of the subject</th>
<th>Periods/week</th>
<th>Max. Marks</th>
<th>Total</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Theory</td>
<td>Lab</td>
<td>Ext.</td>
<td>Int.</td>
</tr>
<tr>
<td>MTCNIS 31</td>
<td>Elective-V</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS 32</td>
<td>Open Elective</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS33</td>
<td>Dissertation-I / Industrial project</td>
<td>-</td>
<td>-</td>
<td>100</td>
<td>-</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td>6</td>
<td>-</td>
<td>240</td>
<td>60</td>
</tr>
</tbody>
</table>

**Elective V:** Malware Analysis/Block chain Technologies/Software Defined Networks  
**Open Elective:** Business Analytics /4G-5G Mobile Communication Networks/ Operation Research

### IV-SEMESTER

<table>
<thead>
<tr>
<th>Code</th>
<th>Name of the subject</th>
<th>Periods/week</th>
<th>Max. Marks</th>
<th>Total</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Theory</td>
<td>Lab</td>
<td>Ext.</td>
<td>Int.</td>
</tr>
<tr>
<td>MTCNIS41</td>
<td>Dissertation- II</td>
<td>-</td>
<td>-</td>
<td>100</td>
<td>-</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td>-</td>
<td>-</td>
<td>100</td>
<td>-</td>
</tr>
</tbody>
</table>
MTCNIS11 MATHEMATICAL FOUNDATIONS FOR CRYPTOGRAPHY

**Instruction:** 3 Periods/week
**Time:** 3 Hours
**Credits:** 3

| Internal: 30 Marks | External: 70 Marks | Total: 100 Marks |

**UNIT I:** Introduction and classical cryptography
Overview of Cryptography and Security (Text Book, Reference 1), Cryptographic Attacks, services and mechanisms, Mathematics of Cryptography (Reference 2)

**UNIT II:** Secret key cryptography
Mathematics for Symmetric Key Cryptography (Reference 2), Encryption, Stream ciphers, Block ciphers, Chosen plaintext attacks (Text Book)

**UNIT III:** Integrity and Hashing
Message integrity, Message integrity from universal hashing, Message integrity from collision resistant hashing, Authenticated encryption (Text Book)

**UNIT IV:** Public key cryptography
Mathematics for Asymmetric Cryptography (Reference 2), Public key tools, Public key encryption, Chosen ciphertext secure public-key encryption, Digital signatures (Text Book)

**UNIT V:** Modern Cryptographic methods
Fast signatures from one-way functions, Elliptic curve cryptography and pairings, Post-quantum cryptography: lattices and isogenies, Analysis of number theoretic assumptions (Text Book)

**UNIT VI:** Protocols
Protocols for identification and login, Identification and signatures from sigma protocols (Text Book)

**UNIT VI:** Cryptographic Proofs
Proving properties in zero-knowledge, Modern proof systems, Authenticated key exchange, Two-party and multi-party secure computation (Text Book)

**Text Book:** A Graduate Course in Applied Cryptography (V 0.5) by D. Boneh and V. Shoup, available free online.

**References:**
Introduction to Modern Cryptography (3rd edition), Jonathan Katz and Yehuda Lindell
Cryptography and Network Security 3/e, Behrouz A. Forouzan, Debdeep Mukhopadhyay
UNIT I: Review Of Important Networking Concepts: Networking and architectures of TCP/IP and OSI reference models

UNIT II: Address Resolution Protocol (ARP) and RARP, IP Protocol, IP addresses, Overview of ICMP, PING and Trace route, BOOTP and DHCP, IP Forwarding, Congestion Control in the NW layer

UNIT III: Dynamic Routing Protocols: RIP, OSPF

UNIT IV: Transport Protocols: TCP and UDP- Connection Management, Flow Control and Congestion Control

UNIT V: LAN Switching, NAT, DHCP

UNIT VI: Domain Name System, IP Multicasting, SNMP, IPV6, MPLS, MOBILE IP, TCP/IP SECURITY

UNIT VII: Introduction to FINGER Protocol, WHOIS Protocol

UNIT VIII: Other Protocols: WAIS, GOPHER, VERONICA, TCPDUMP

TEXT BOOKS:

REFERENCE BOOKS:
UNIT 1 : Introduction to VPN
TCP/IP overview: Layering, Encapsulation, Addressing, IP, UDP, TCP, ICMP, NAT and Private IP Addresses, IPv6, Routing

UNIT 2 : VPN Security
What is VPN, VPN Components, VPN Workflow, Tunneling, Intranet, Extranet, Remote Access Types of VPN’s, VPN Architecture, Advantages & Disadvantages

UNIT 3 : Tunnels
Introduction, IP-in-IP tunnels, PPPoE, GRE, PPTP, L2TP, MPLS

UNIT 4 : SSL & SSH
SSL-Introduction, SSL Protocol, SSL on wire, Open SSL, SSL Security
SSH-Introduction, SSH V1, SSH V2, Building VPN’s with SSH

UNIT 5 : Light weight VPN
Introduction, VTun, CIPE, Tinc, Open VPN

UNIT 6 : IPsec
IPsec Architecture, Protocols, IPsec Modes, Security Associations
AH- AH Header, Sequence Numbers, AH Processing, Tunnel mode, AH with IPV6
ESP-Header, Tunnel Mode, ESP with IPV6

UNIT 7 : Applications of VPN
Applications of VPN, Application of VPN in industries and business

References:
1. VPN’s Illustrated Tunnels, VPN’s and IPsec by Jon.c,Snader
UNIT 1:  **Introduction:** Introduction to Machine Learning, learning task- illustration, Approaches to Machine Learning, Machine Learning algorithms- Theory, Experiment in biology and Psychology.

UNIT 2:  **Concept Learning:** Introduction, Concept Learning Task- Notation, Concept Learning Search, Version spaces, Candidate Elimination Algorithm, Inductive Bias, Biased hypothesis Space, Unbiased Learner, Bias-free Learning, Active queries, Mistake bound/PAC model – basic results. Overview of issues regarding data sources, success criteria

UNIT 3:  **Decision Tree Learning:** Decision Tree Representation, Basic decision Tree Learning, Inductive bias in Decision tree Learning, Issues in Decision Tree Learning, Minimum Description Length Principle, Occam's razor, Learning with active queries

UNIT 4:  **Neural Network Learning:** Neural Network Representation, Problems for Neural Network Learning, Perceptions and gradient descent, Multi-Layer Network and Back propagation Algorithm, Illustrative Example of Back Propagation Algorithm- Face Recognition, Advanced Topics in ANN.

UNIT 5:  **Bayesian Approaches:** Basics of Bayes Theorem and Concept Learning, Expectation Maximization, Minimum Description Length Principle, Navie Bayes Classifier, Bayesian Belief Networks, EM Algorithm, K-Means Algorithm, Hidden Markov Models Instance-Based Techniques; Lazy vs. eager generalization, k nearest neighbor, Locally Weight Representation, Case-based Reasoning

UNIT 6:  **Analytical Learning:** Inductive and Analytical Learning problems, Learning with perfect Domain Theory, Explanation Based Learning, Inductive Bias in EBL, Search Control Knowledge with EBL, Inductive- Analytical Approaches to Learning, Using prior Knowledge for Initialize the Hypothesis, and Altering Search objective, FOCL Algorithm.

UNIT 7:  **Genetic Algorithms:** Representation of Hypothesis as GA,, Genetic Operators, Fitness function and Selection, Hypothesis Space search, Genetic Programming, Models of Evolution and Learning, Parallelizing GA, Different search methods for induction

**Text Books:**
2. The Elements of Statistical Learning, Trevor Hastie, Robert Tibshirani & Jerome Friedman, Springer Verlag, 2001

**Reference Books:**
2. Neural Networks for Pattern Recognition, Chris Bishop, Oxford University Press,
Course Objectives
1. To understand inter process and inter-system communication.
2. To understand socket programming in its entirety.
3. To understand usage of TCP/UDP / Raw sockets.
4. To understand how to build network applications.

Course Outcomes:
1. To write socket API based programs.
2. To design and implement client-server applications using TCP and UDP sockets.
3. To analyse network programs.

UNIT - I
Introduction to Network Programming: UNIX standards, OSI model, TCP and UDP & TCP connection establishment and Format, Buffer sizes and limitation, standard internet services, Protocol usage by common internet application.

UNIT - II
Socket: Elementary sockets introduction, Address structures, value – result arguments, Byte ordering and manipulation function and related functions.
Elementary TCP sockets – Introduction, Socket, connect, bind, listen, accept, fork and exec functions, concurrent servers. Close function, getsockname and getpeername functions.

UNIT - III
TCP Client/Server: Introduction, TCP Echo server functions, Normal start up, Normal termination and POSIX signal handling, Termination of server process, Crashing and Rebooting of server host, shutdown of server host.
I/O Multiplexing: Introduction, I/O Models, select function, Batch input and buffering, shutdown function, poll function, TCP Echo server.
Socket options: introduction, getsockopt and setsockopt functions. Socket states, Generic socket option, IPV6 socket option, ICMPV6 socket option, IPV6 socket option and TCP socket options.

UNIT – IV
Elementary UDP sockets: Introduction, UDP Echo server functions, lost datagram, summary of UDP example, Lack of flow control with UDP, determining outgoing interface with UDP.
Name and Address conversions: DNS, gethost by Name function, Re-entrant function, obsolete IPv6 Address lookup functions, and other networking information.

UNIT - V
Advanced I/O Functions-Introduction, Socket Timeouts, recv and send Functions, readv and writev Functions, recvmsg and sendmsg Functions, Ancillary Data, How Much Data Is Queued?, Sockets and Standard I/O, Advanced Polling.
UNIT - VI

**Broadcasting**- Introduction, Broadcast Addresses, Unicast versus Broadcast, dg_cli Function Using Broadcasting, Race Conditions.

**Multicasting**- Introduction, Multicast Addresses, Multicasting versus Broadcasting on A LAN, Multicasting on a WAN, Multicast Socket Options, mcast join and Related Functions, dg_cli Function Using Multicasting, Receiving IP Multicast Infrastructure Session Announcements, Sending and Receiving, SNTP: Simple Network Time Protocol.

UNIT – VII

**Raw Sockets**- Introduction, Raw Socket Creation, Raw Socket Output, Raw Socket Input, Ping Program, Traceroute Program, An ICMP Message Daemon,


**Text Book:**

**References:**
1. UNIX Systems Programming using C++ T CHAN, PHI.
2. UNIX for Programmers and Users, 3rd Edition Graham GLASS, King abls, Pearson Education.
Detailed Syllabus for M.Tech (CN & IS) First Semester

MTCNIS14 ELECTIVE-II CLOUD COMPUTING

Instruction: 3 Periods/week  
Time: 3 Hours  
Credits: 3

Internal: 30 Marks  
External: 70 Marks  
Total: 100 Marks

Course objectives:
1. To import fundamental concepts in the area of cloud computing.
2. To understand the concept of Virtualization and cloud data storage.
3. To learn cloud Application Development and cloud Governance.
4. To gain competence in Map Reduce and Hadoop Overview.

Course Outcomes:
1. Identify the architecture and infrastructure of cloud computing.
2. Develop applications for cloud computing.
3. Design and Implement a novel cloud computing application.

Syllabus:

UNIT 1: Introduction to cloud computing: Cloud computing components, Infrastructure services, storage applications, database services – introduction to Saas, Paas, Iaas, Idaas, data storage

UNIT 2: Virtualization: enabling technologies, types of virtualization, server virtualization, desktop virtualization, memory virtualization, application and storage virtualization-tools and products available for virtualization

UNIT 3: SAAS and PAAS: Getting started with Saas, SaaS solutions, SOA, PaaS and benefits.

UNIT 4: Iaas and Cloud data storage: understanding Iaas, improving performance for load balancing, server types within Iaas, utilizing cloud based NAS devices, cloud based data storage, and backup services, cloud based block storage and database services

UNIT 5: Cloud Application development: Client server distributed architecture for cloud designing cloud based solutions, coding cloud based applications, traditional Apps vs cloud Apps, client side programming, server side programming overview-fundamental treatment of web application frameworks.

UNIT 6: Cloud Governance and economics: Securing the cloud, disaster recovery and business continuity in the cloud, Managing the cloud, migrating to the cloud, governing and evaluating the clouds business impact and economics,

UNIT 7: Inside Cloud: Introduction to MapReduce and Hadoop-over view of big data and its impact on cloud

Text Books:
2. Hadoop Map Reduce cookbook, Srinath Perera and Thilina Gunarathne, Packt publishing

Reference Book:
Detailed Syllabus for M.Tech (CN & IS) First Semester

**ELECTIVE-II**
**DISTRIBUTED OPERATING SYSTEMS**

<table>
<thead>
<tr>
<th>Instruction: 3 Periods/week</th>
<th>Time: 3 Hours</th>
<th>Credits: 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
<td>Total: 100 Marks</td>
</tr>
</tbody>
</table>

**Unit-1:** Introduction to Distributed Systems, What is a Distributed System?, Hardware concepts, Software concepts, Design issues.

**Unit-2:** Communication in Distributed Systems Lay red Protocols, ATM networks, The Client – server model, Remote Procedure call, Group communication.

**Unit-3:** Synchronization in Distributed System, Clock Synchronization, Mutual Exclusion, Election algorithms, Atomic transactions, Deadlocks in Distributed Systems.

**Unit-4:** Process and processors in Distributed System threads, System Models, Processors allocation, Scheduling in Distributed System, Fault tolerance, Real time Distributed System.

**Unit-5:** Distributed File Systems, Distributed File System Design, Distributed File System implementation, Trends in Distributed File System.

**Unit-6:** Distributed Shared Memory, Introduction, What is Shared memory?, Consistency models, Page based Distributed Shared memory, Shared – variable Distributed Shared memory, Object based Distributed Shared Memory.

**Text Book:**
Distributed Operating Systems, Andrew S. Tanenbanm

**Reference Book:**
Advanced Concepts in Operating Systems, Makes Singhal and Niranjan G. Shivaratna

UNIT 2: Prototyping connected objects. Open-source prototyping platforms.

UNIT 3: Integrating internet services. XML and JSON. HTTP APIs for accessing popular Internet services (Facebook, Twitter, and others). Practical activities. IoT Application Development: Application Protocols MQTT, REST/HTTP, CoAP, MySQL

UNIT 4: Overview of IoT supported Hardware platforms such as: Raspberry pi, ARM Cortex Processors, Arduino and Intel Galileo boards.

UNIT 5: Ubiquitous computing, applications of IOT, Virtualization of network resources and physical devices in IOT.

UNIT 6: Internet of Things Standardization M2M Service Layer Standardization OGC Sensor Web for IoT

Text Book:

Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems
author. Marina Ruggieri H, River Publishers Series In Communications
### Detailed Syllabus for M.Tech (CN & IS) First Semester

**MTCNIS15 RESEARCH METHODOLOGY AND IPR**

<table>
<thead>
<tr>
<th>Instruction: 3 Periods/week</th>
<th>Time: 3 Hours</th>
<th>Credits: 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
<td>Total: 100 Marks</td>
</tr>
</tbody>
</table>

**Unit 1:** Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem. Scope and objectives of research problem. Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations

**Unit 2:** Effective literature studies approaches, analysis Plagiarism, Research ethics,

**Unit 3:** Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee


**Unit 6:** New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs.

**References:**

2. Wayne Goddard and Stuart Melville, “Research Methodology: An Introduction”
MTNIS16 ORGANIZATIONAL BEHAVIOR (Audit Course)
Common for M.Tech (CST, IT, CN&IS, AI&ML)

Instruction: 3 Periods/week  Time: 3 Hours  Credits: 0
Internal: 30 Marks  External: 70 Marks  Total: 100 Marks

UNIT I: Organizational Behavior: Concept of Organization - Concept of Organizational Behavior - Nature of Organizational Behavior - Role of Organizational behavior - Disciplines contributing to Organizational Behavior.

UNIT II: Motivation: Definition - Nature of Motivation - Role of Motivation - Theories of Motivation: Maslow's Need Hierarchy Theory, Herzberg's Motivation Hygiene Theory and McGregor's Theory X and Theory Y.

UNIT III: Group Dynamics: Meaning - Concept of Group - Types of groups - Formal and Informal groups - Group development - Group cohesiveness and factors affecting group cohesiveness.

UNIT IV: Leadership: Concept of Leadership - Difference between Leadership and Management - Importance of Leadership - Leadership styles: Autocratic leadership, Participative leadership and Free Rein leadership.

UNIT V: Communication: Meaning - Communication Process - Forms of communication: Oral, Written and Non-Verbal communication - Direction of communication: Downward, Upward and Horizontal communication.


Text Books:
1. L.M. Prasad: Organizational Behavior, Sultan Chand & Sons, New Delhi - 110002

Reference Books:
Name of practical:

1. To implement allocation of IP address.
2. To configure internet IP address
3. To assign IP address using CIDR
4. To configure APACHE server
5. To decode header fields of IP datagram
6. To decode header fields of TCP header.
7. To configure a DNS server
8. Identify, download & install open source tools related to TCP/IP.
9. Compile and test TTCP
Network Simulation Lab:
1. Performance Analysis of AODV using OPNET
2. Performance Analysis of DSR using NS2
3. Performance Analysis of ZRP using NS3
4. Performance Analysis of WiMax Using OPNET
5. Performance Analysis of Wireless Local Area Network using OPNET
6. Performance Analysis of MAC Protocols using OPNET

Internet of Things Lab:
1. Performance Analysis of QoS Metrics of IEEE 802.15.4 protocol using Cooja Simulator
2. Performance Analysis of QoS Metrics 6LowPAN protocol using Cooja Simulator
3. Performance Analysis of QoS Metrics RPL protocol using Cooja Simulator
4. Performance Analysis of QoS Metrics MQTT protocol using Cooja Simulator
5. Performance Analysis of QoS Metrics AMQP protocol using Cooja Simulator

Detailed Syllabus for M.Tech (CN & IS) Second Semester
UNIT 1: **Introduction**: Introduction to Wireless Networks, Various Generations of Wireless Networks, Virtual Private Networks - Wireless Data Services, Common Channel Signaling, Various Networks for Connecting to the Internet, Blue tooth Technology, Wifi-Wi Max- Radio Propagation mechanism, Pathloss Modeling and Signal Coverage

UNIT 2: **Wireless Local Area Networks**: Introduction-WLAN topologies-IEEE 802.11 Standards ,MAC Protocols, Comparison of 802.11 a,b,g and n Standards, HIPER LAN , ZigBee 802.15.4, Wireless Local Loop


UNIT 4: **Mobile Communications**: Introduction to cellular concept, Frequency Reuse, Handoff, GSM: Mobile services, System architecture, Radio interface, Protocols, Localization and calling, Handover, Security, and New data services, Introduction to mobile computing, novel applications, limitations, and architecture.

UNIT 5: **Mobile Data Networks**: Location/mobility management, Mobile IP, Dynamic routing protocols, Location-based protocols, Emerging topics: sensor networking, Data-Oriented CDPD network, GPRS and higher data rates, Short messaging service in GSM.


UNIT 7: **Other Wireless Technologies**: Introduction, IEEE 802.15.4 and Zigbee, General Architecture, Physical Layer, MAC layer, Zigbee, WiMAX and IEEE 802.16, Layers and Architecture, Physical Layer, OFDM Physical layer.


**Text Books:**

**References:**

**Detailed Syllabus for M.Tech (CN & IS) Second Semester**
UNIT 1: User Authentication and Database Security
The Need for Database Security, Database Management Systems, Relational Databases, SQL Injection Attacks, Database Access Control, Inference, Database Encryption, Data Center Security

UNIT 2: Access Control
Access Control Principles, Subjects, Objects, and Access Rights, Discretionary Access Control, Example: UNIX File Access Control, Role-Based Access Control, Attribute-Based Access Control, Identity, Credential, and Access Management, Trust Frameworks, Case Study: RBAC System for a Bank

UNIT 3: Malicious Software

UNIT 4: Network Attacks and Prevention
Denial-of-Service Attacks, Distributed Denial-of-Service Attacks, Application-Based Bandwidth Attacks, Defenses Against Denial-of-Service Attacks, Responding to a Denial-of-Service Attack Intruders, Intrusion Detection, Analysis Approaches, Host-Based Intrusion Detection, Network-Based Intrusion Detection, Honeypots, Snort, Need for firewalls, types of firewalls, IPS

UNIT 5: Software and OS Security

UNIT 6: Security Management issues
IT security management and Risk Management, IT Security Controls, plans and procedures, Physical and Infrastructure Security

UNIT 7: Security Auditing, legal and ethical aspects
Security auditing architecture, Security audit trail, implementing the logging function, audit trail analysis, security information and event management, Cybercrime and computer crime, intellectual property, privacy and ethical issues

Text Book:
   Reference Book
Unit 1: Web Application Security and Core Defense mechanisms,

Unit 2: Web Application Technologies and mapping applications,
HTTP Protocol, Web functionality, Encoding Schemes, Mapping the Application: Enumerate the content and Functionality, Analysing the application

Unit 3: Client side and Authentication Attacks Bypassing,
Client-side controls: Transmitting data via the client, Capturing the user data- HTML Forms and Browser extensions, Handling client side data securely. Attacking Authentication: Authentication Technologies, Design flaws in authentication, Implementation flaws in authentication, securing authentication.

Unit 4: Session management attacks and Access,
Controls Session States, weaknesses in Token generation and Session Token handling. Securing session management Common vulnerabilities and attacking access controls, securing access controls.

Unit 5: Attacking Data stores and Back end components,
Bypassing logging, Injecting into SQL: Exploiting Basic Vulnerability, Injecting into different statement types, Finding SQL Injection Bugs, Fingerprinting the database, The UNION Operator, Extracting data, Bypassing filters, Second order SQL Injection, Attack escalation, SQL exploitation tools, preventing SQL Injection, Injecting OS commands, manipulating file paths, Injecting into backend HTTP requests

Unit 6: Attacking Users
XSS- reflected, stored and DOM, XSS attack payloads and delivery mechanisms. Finding and exploiting XSS vulnerabilities and preventing, CSRF basic examples, Client side injection attacks like HTTP header injection, Cookie Injection attacks, Attacking Browsers: logging keystrokes, stealing browser history and search queries, w numerating currently used applications, port scanning, exploiting browser bugs, DNS rebinding, browser exploitation and Man in the middle attacks.

Unit 7: Attacking Application Server and architecture
Attacking Application Architecture, Attacking the application server, Approaches to code review, Signatures of common vulnerabilities

Text Book:

Reference:
2. Web Security Basics, by Shweta Bhasin, Prima Tech

Detailed Syllabus for M.Tech (CN & IS) Second Semester
Course Objectives:
This course describes different components of Android applications and iOS Applications
1) Identifies possible vulnerabilities and Security issues in both the platforms
2) Identifies and helps in practising defensive programming techniques to protect the users of Android and iOS applications from the common attacks.
3) Secure coding examples

Course Outcomes: At the end of this course Students will
1) Identify various risks related to Android and iOS applications.
2) Understand the structure of Android and iOS files.
3) Understand the Android security model and the protections provided by the Android OS.
4) Understand the iOS security model and the protections provided by the iOS.

Part-I Android Security
1. Introduction to Android App Development

2. Android Architecture and packet Management

3. Device Security & NFC

Part -II - iOS Security
4. The iOS Fundamentals & Security Model

5. iOS Application Anatomy

6. iOS Security testing

7. Mobile Privacy Concerns
Dangers of Unique Device Identifiers, Solutions from Apple, Rules for Working with Unique Identifiers, Mobile Safari and Do Not Track Header, Cookie Acceptance Policy, Monitoring Location and Movement, Managing Health and Motion Information, Managing Health and Motion Information.

Text Book:
1. Android Security Internals- An In-Depth Guide to Android’s Security Architecture Author: Nikolay
Elenkov, no starch press (Chapters 1,2,3,10,11 from text book)  (For Part 1-Chapters 1,2, 3 from Syllabus)
2. iOS Application Security- The Definitive Guide for Hackers and Developers, Authors : David Thiel, no starch press (Chapters 1,3, 4, 14 from text book) (For Part II - Chapters 4,5,6,7 from Syllabus)

Reference:

UNIT 1: Introduction: Securing the Internet of Things, security requirements in IoT architecture, security in enabling technologies, security concerns in IoT applications.

UNIT 2: Security Architecture in the Internet of Things: Security Requirements in IoT, Insufficient Authentication/Authorization, Insecure Access Control, Threats to Access Control, Privacy, And Availability, Attacks Specific to IoT.


UNIT 5: Mitigating IoT Privacy Concerns: Mitigating IoT Privacy Concerns, Privacy challenges introduced by the IoT, Guide to performing an IoT PIA, Privacy by design, Privacy engineering recommendations.

UNIT 6: Cloud Security for the IoT: Cloud Security for the IoT, The role of the cloud in IoT systems, The concept of the fog, Threats to cloud IoT services, Cloud-based security services for the IoT.

UNIT 7: IoT Incident Response and Forensic Analysis: IoT Incident Response and Forensic Analysis, Threats to both safety and security, Defining, planning, and executing an IoT incident response, Detection and analysis, IoT forensics

Textbooks:

References:

Detailed Syllabus for M.Tech (CN&IS) Second Semester
Detailed Syllabus for M.Tech (CN & IS) Second Semester

**Unit 1 Introduction**
Introduction of Cybercrime: Types, The Internet spawns crime, Worms versus viruses, Computer's roles in crimes, Introduction to digital forensics, Introduction to Incident - Incident Response Methodology

**Unit 2 Initial Response and Forensic Duplication**
Initial Response & Volatile Data Collection from Windows system - Initial Response & Volatile Data Collection from Unix system - Forensic Duplication: Forensic Duplicates as Admissible Evidence, Forensic Duplication Tool Requirements, Creating a Forensic Duplicate/Qualified Forensic Duplicate of a Hard Drive.

**Unit 3 Preserving and Recovering Digital Evidence**

**Unit 4 Evidence Handling**
Types of Evidence, Challenges in evidence handling, Overview of evidence handling procedure.

**Unit 5 Network Forensics**
Intrusion detection; Different Attacks in network, analysis Collecting Network Based Evidence - Investigating Routers - Network Protocols - Email Tracing - Internet Fraud.

**Unit 6 System Investigation**

**Unit 7 Cyber Laws and Global and Indian Contexts**
Constitutional law, Criminal law, Civil law, Administrative regulations, Local laws, State laws, Federal laws, International laws, Criminal versus civil cases, Vicarious liability, Computer related laws CFAA, DMCA, CAN Spam

**Text Books**

**Reference Books**
2. Cyber Forensics by Dejey and Murugan, Oxford University Press
UNIT 1: **Introduction**: The vision of Ambient Intelligence, Application examples, Types of applications, Challenges for Wireless Sensor Networks (WSNs), Sensor networks vs Enabling Technologies for WSNs, **Single node architecture**: Hardware components, Energy consumption of sensor nodes, Some examples of sensor nodes, Operating systems and execution environments.

UNIT 2: **Network architecture**: Sensor network scenarios, Optimization goals and figures of merit, Design principles for WSNs.

UNIT 3: **Physical layer and transceiver design considerations in WSNs**: 
- **MAC Protocols**: Fundamentals of (wireless) MAC protocols, Low duty cycle protocols and wakeup concepts, Contention-based protocols, Schedule-based protocols, The IEEE 802.15.4 MAC protocol, How about IEEE 802.11 and Bluetooth.

UNIT 4: **Link layer protocols**: Fundamentals: tasks and requirements, Error control, Framing, Link management.

UNIT 5: **Naming and addressing**: Fundamentals, Address and name management in wireless sensor networks, Assignment of MAC addresses, Content-based and geographic addressing.

UNIT 6: **Routing protocols**: The many faces of forwarding and routing, Energy-efficient unicast, Broadcast and multicast, Geographic routing.

UNIT 7: **Data-centric and content-based networking**: Introduction, Data-centric routing, Data aggregation, Data-centric storage.

UNIT 8: **Transport layer and Quality of Service**: The transport layer and QoS in wireless sensor networks, Coverage and deployment, Reliable data transport, Single packet delivery, Block delivery, Congestion control and rate control.

**TEXT BOOK:**


**Detailed Syllabus for M.Tech (CN & IS) Second Semester**
MT-CNIS-24 ELECTIVE-IV INTRUSION DETECTION SYSTEM (IDS)

<table>
<thead>
<tr>
<th>Instruction: 3 Periods/week</th>
<th>Time: 3 Hours</th>
<th>Credits: 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
<td>Total: 100 Marks</td>
</tr>
</tbody>
</table>

Course Objectives:
1. Understand when, where, how, and why to apply Intrusion Detection tools and techniques in order to improve the security posture of an enterprise.
2. Apply knowledge of the fundamentals and history of Intrusion Detection in order to avoid common pitfalls in the creation and evaluation of new Intrusion Detection Systems.
3. Analyze intrusion detection alerts and logs to distinguish attack types from false alarms.
4. Apply the knowledge to the architecture, configuration, and analysis of specific intrusion detection systems.

Course Outcomes
• Understand modern concepts related to Intrusion Detection System.
• Compare alternative tools and approaches for Intrusion Detection through quantitative analysis to determine the best tool or approach to reduce risk from intrusion.
• Identify and describe the parts of all intrusion detection systems and characterize new and emerging technologies.

Unit 1. Introduction
Basic Concepts of Security, Introduction to Intrusions, Need of Intrusion Detection, Classification of Intrusion Detection Systems, Sources of Vulnerabilities, Attacks against various security objectives, Countermeasures of attacks.

Unit II. Intrusion Detection and Prevention Technologies:
Host-based intrusion detection system (HIDS), Network-based IDS, Information Sources for IDS, Host and Network Vulnerabilities and Countermeasures. Intrusion detection techniques, misuse detection: pattern matching, rule-based and state-based anomaly detection: statistical based, machine learning based, data mining based hybrid detection.

Unit III. IDS and IPS Architecture:

Unit IV. Alert Management and Correlation Data fusion:
Alert correlation, Pre-process, Correlation Techniques, Post-process, Alert Correlation architectures. Cooperative Intrusion Detection, Cooperative Discovery of Intrusion chain, Abstraction-based Intrusion Detection, Interest-based communication and cooperation, agent-based cooperation.

Text Book:

References
UNIT 1: Basic Concepts of Management: Management:-Definition, Nature and Importance; Functions of the Management; Levels of Management; F.W Taylor's Scientific Management; Henry Fayol's Principles of Management.


UNIT 3: ProductionandoperationsManagement: Plantlocation-Factorstobeconsidered in the selection of Plant location; Break - even analysis- Significance andmanagerialapplications;ImportanceofProductionPlanningandControlanditsFunctions;Human Resource Management and Functions of Human Resource Manager (in brief); Functions of Marketing; Methods of Raising Finance.


Textbooks:

Reference Books:
2. Sheela,P.,andJagadeswaraRao,K.,Entrepreneurship,ShreePublishingHouse,Guntur,
Experiment 1:
Installation of One Simulator.

Experiment 2:
Implementing Epidemic Routing

Experiment 3:
Performing Average Hop Count of various Routing Protocols

Experiment 4:
Performing the delivery probability of various Routing protocols

Experiment 5:
Switching the LED on/off in octabrix LED

Experiment 6:
Understanding working of octabrix in light conditions

Experiment 7:
Implementing LED color patterns in Octabrix

Experiment 8:
Implementing cloud integration with Octabrix

Experiment 9:
To study the behavior AODV Routing Protocol

Experiment 10:
To study the behavior DSR Routing Protocol

Experiment 11:
To study the behavior OLSR Routing Protocol

Experiment 12:
To study the behavior GRP Routing Protocol

---

Detailed Syllabus for M.Tech (CN & IS) Second Semester

MTCNIS27 APPLICATION SECURITY LAB

<table>
<thead>
<tr>
<th>Instruction: 3 Periods/week</th>
<th>Time: 3 Hours</th>
<th>Credits: 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal: 30 Marks</td>
<td>External: 70 Marks</td>
<td>Total: 100 Marks</td>
</tr>
</tbody>
</table>
LAB Exercises limited to the following scope

**Cycle 1:**
1. Install Kali Linux and study the use of burpsuite and metasploit
2. Learn about NMAP and scan open ports in a target server
3. Find the softwares and their version details in the open ports
4. Find vulnerabilities in any one of the softwares installed in the target server system.
5. Learn about the wireshark tool and analyse the packets in a given interface.

**Cycle 2:**
1. Visit OWASP and learn more about web based vulnerabilities.
2. Implement SQL Injection Attacks
3. Implement Cross site Request Forgery Attack
4. Implement Cross site Scripting Attack
5. Implement Command Injection Attacks
### III SEMESTER

<table>
<thead>
<tr>
<th>Code</th>
<th>Name of the subject</th>
<th>Periods/week</th>
<th>Max. Marks</th>
<th>Total</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Theory</td>
<td>Lab</td>
<td>Ext.</td>
<td>Int.</td>
</tr>
<tr>
<td>MTCNIS31</td>
<td>Elective-V</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS32</td>
<td>Open Elective</td>
<td>3</td>
<td>-</td>
<td>70</td>
<td>30</td>
</tr>
<tr>
<td>MTCNIS3</td>
<td>Dissertation-I / Industrial project</td>
<td>-</td>
<td>-</td>
<td>100</td>
<td>-</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>6</td>
<td>-</td>
<td>240</td>
<td>60</td>
</tr>
</tbody>
</table>

**Elective V:** Malware Analysis/Block chain Technologies/Software Defined Networks

**Open Elective:** Business Analytics/4G-5G Mobile Communication Networks/ Operation Research
UNIT 1: Introduction
Introduction to malware, OS security concepts, malware threats, evolution of malware, malware
types viruses, worms, rootkits, Trojans, bots, spyware, adware, logic bombs, malware analysis,
static malware analysis, dynamic malware analysis.

UNIT 2: Static Analysis
X86 Architecture- Main Memory, Instructions, Opcodes and Endianness, Operands, Registers,
Simple Instructions, The Stack, Conditionals, Branching, Rep Instructions, C Main Method and
Offsets. Antivirus Scanning, Fingerprint for Malware, Portable Executable File Format, The PE
File Headers and Sections, The Structure of a Virtual Machine.

UNIT 3: Dynamic Analysis
Live malware analysis, dead malware analysis, analyzing traces of malware- system-calls,
apicalls, registries, network activities.

UNIT 4: Anti-dynamic analysis
Analysis techniques anti-VM, runtime-evasion techniques, , Malware Sandbox, Monitoring with
Process Monitor, Packet Sniffing with Wireshark.

UNIT 5: Attack mechanisms
Downloader, Backdoors, Credential Stealers, Persistence Mechanisms, Privilege Escalation,
Covert malware launching- Launchers, Process Injection, Process Replacement, Hook Injection,
Detours, APC injection.

UNIT 6: Malware Detection Techniques
Signature-based techniques: malware signatures, packed malware signature, metamorphic and
polymorphic malware signature Non-signature based techniques: similarity-based techniques,
machine-learning methods, invariant inferences.

UNIT 7: kernels and Rootkits
Intro to Kernel – Kernel basics, Windows Kernel API, Windows Drivers, Kernel Debugging - ,
Rootkit Techniques- Hooking, Patching, Kernel Object Manipulation ,Rootkit Anti-forensics

TEXT BOOK:
2. Learning Malware Analysis: Explore the Concepts, Tools, and Techniques to Analyze and
Investigate Windows Malware by Monnappa K A

REFERENCES
1. Jamie Butler and Greg Hoglund, “Rootkits: Subverting the Windows Kernel”, Addison-Wesley,
2005
**Course Objectives:**
1. To understand the basic concepts block chain technology and to explore the driving force behind the crypto currency Bitcoin.
2. To understand about the different methods of Decentralization using Block Chain and different Bitcoins and Alternative Coins.
3. To understand about Ethereum and applications using Smart contracts and Block Chain Applications

**Course Outcomes:**
At the end of the course the student will be able to:
1. Understand the types, benefits and limitation of block chain.
2. Explore the block chain decentralization and cryptography concepts.
3. Enumerate the Bitcoin features and its alternative options.
4. Describe and deploy the smart contracts

**Syllabus:**

**UNIT 1: BlockChain and its History:**

**UNIT 2: Decentralization and Consensus Algorithms:**
Decentralization using blockchain, Methods of decentralization, Routes to decentralization, Decentralized organizations, Distributed systems, Distributed ledger, Merkle tree, structure of a block, Consensus Algorithms- Proof of Work, Proof of Stack, Proof of Burn, Proof of Elapsed Time, Proof of Activity, Proof of Concept.

**UNIT 3: Bitcoin and Alternative Coins:**

**UNIT 4: Ethereum and smart contracts:**
Ethereum Architecture, solidity programming basics, Smart Contract, Deploying Smart Contracts, Integration with UI.

**UNIT 5: Blockchain Applications:**

**Textbooks:**

**References:**
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Instructions</th>
<th>Time</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTCNIS31</td>
<td>ELECTIVE-V SOFTWARE DEFINED NETWORKS</td>
<td>3 Periods/week</td>
<td>3 Hours</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internal: 30 Marks</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>External: 70 Marks</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Total: 100 Marks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


UNIT IV. Alternative Definitions of SDN: Potential Drawbacks of Open SDN, SDN via APIs, SDN via Hypervisor-Based Overlays, SDN via Opening Up the Device, Network Functions Virtualization and Alternatives Overlap and Ranking.

UNIT V. SDN in the Data Center: Data Center Demands, Tunnelling Technologies for the Data Center, Path Technologies in the Data Center, Ethernet Fabrics in the Data Center, SDN Use Cases in the Data Center, Comparison of Open SDN, Overlays, and APIs, Real-World Data Center Implementations


Text Books:

Reference:
SDN - Software Defined Networks by Thomas D. Nadeau & Ken Gray, O'Reilly, 2013

Detailed Syllabus for M.Tech (CN & IS) Third Semester
MTCNIS32 OPEN ELECTIVE: BUSINESS ANALYTICS

<table>
<thead>
<tr>
<th>Instruction:</th>
<th>3 Periods/week</th>
<th>Time: 3 Hours</th>
<th>Credits: 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal:</td>
<td>30 Marks</td>
<td>External: 70 Marks</td>
<td>Total: 100 Marks</td>
</tr>
</tbody>
</table>

Course objectives:
1. To introduce students to problem solving with Business Analytics and the use of spreadsheets for descriptive analytics, data queries and visualization
2. To introduce students to statistical sampling, sampling distributions, confidence intervals and statistical inference
3. To familiarize students with various types of regression including simple linear regression and multiple linear regression
4. To introduce students to key concepts in statistical forecasting models for time series data
5. To familiarize students with predictive decision modeling, model analysis and developing spreadsheet applications including building linear optimization models on spreadsheets.

Course outcomes:
After completion of the course the student should be able to:
1. Describe data and models used for Business Analytics and apply various descriptive analytic techniques to analyze data
2. Estimating population parameters, interval estimates, construct confidence intervals and perform hypothesis testing
3. Estimate and interpret the parameters of simple linear regression and multiple linear regressions
4. Apply forecasting models for various time series data including stationary time series, time series with linear trend and time series with seasonality
5. Implement models on spreadsheets, develop user-friendly applications and build linear optimization models on spreadsheets.

Syllabus
UNIT 1. Foundations of Business Analytics: Evolution of Business Analytics, Scope, data and models for Business Analytics, problem solving with Business Analytics, Analytics on spreadsheets, Excel functions for Database queries, Add-ons for Business Analytics. Descriptive Analytics: Data visualization, creating charts in MS Excel, Data Queries, Tables, sorting and filtering, Data summarization with statistics, Data exploration using Pivot tables

UNIT 2. Statistical Sampling: methods, estimating population parameters, sampling error, sampling distributions, interval estimates, confidence intervals, using confidence intervals for decision making, prediction intervals Statistical Inference: Hypothesis testing, one-sample Hypothesis testing, two-tailed test of Hypothesis for mean, two-sample Hypothesis testing, Analysis of variance, chi-square test for independence

UNIT 3. Trendliness and Regression: Modelling Relationships and trends in data, Simple linear regression, least squares regression, regression on analysis of variance, testing hypothesis for regression coefficients, Confidence intervals for regression coefficients, Residual analysis and regression assumptions, Multiple linear regression, building regression models, regression with categorical independent variables with two or more levels, regression with nonlinear terms, advanced techniques for regression modelling

UNIT 4. Forecasting Techniques: Qualitative and judgemental forecasting, statistical forecasting models, forecasting models for stationery time series, forecasting models for time series with linear trend, forecasting models for time series with seasonality, selecting appropriate time-series-based forecasting models, regression forecasting with casual variables, practice of forecasting

UNIT 5. Spreadsheet modeling and Analysis: Strategies for predictive decision modelling, Implementing models on spreadsheet, spreadsheet applications in Business analytics, Model assumptions, complexity and realism, developing user-friendly applications, analyzing uncertainty
and model assumptions, model analysis using analytics solver platform

UNIT 6. Linear Optimization & Applications: Building Linear Optimization Models on spreadsheets, solving Linear Optimization models, Graphical interpretation of linear optimization, Using optimization models of prediction and insight, Types of constraints in optimization models, process selection models, Blending Models, Portfolio Investment models

Text Book

Reference Book

Detailed Syllabus for M.Tech (CN & IS) Third Semester
MTCNIS32 OPEN ELECTIVE: OPERATION RESEARCH
Instruction: 3 Periods/week  Time: 3 Hours  Credits: 3
Internal: 30 Marks  External: 70 Marks  Total: 100 Marks
UNIT I: Overview of Operations Research, Types of OR Models, Phases of Operations Research—OR Techniques, Introduction to Linear Programming, Formulation of Linear Programming Problem, Graphical Solution; Graphical Sensitivity Analysis

UNIT II: Standard Form of LPP, Basic Feasible Solutions, Unrestricted Variables, Simplex Algorithm, Artificial Variables, Big M Method, Two Phase Simplex Method, Degeneracy, Alternative Optimal, Unbounded Solutions, Infeasible Solutions, Primal And Dual Problems And Their Relations, Dual Simplex Method

UNIT III: Transportation Problem as LPP, Initial Solutions, North West Corner Rule, Lowest Cost Method, Vogels Approximation Method, Optimum Solutions of TPP, Degeneracy in Transportation, Transportation Algorithms


UNIT VI: Replacement Problems—Individual And Group Replacement Policy, Reliability & System Failure Problems, Inventory-Factors Effecting Inventory—EOQ, Inventory Problems With and Without Shortages, Inventory Problems With Price Breakups, Multi Item Deterministic Problems, Probabilistic Inventory Problems

UNIT VII: Game Theory: Two Person Zero Sum Games, Mixed Strategy Games and Their Algorithms.

Text Books:

Detailed Syllabus for M.Tech (CN & IS) Third Semester

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Type</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTCNIS32</td>
<td>OPEN ELECTIVE: 4G-5G MOBILE COMMUNICATION NETWORKS</td>
<td>Time: 3 Hours</td>
<td>Credits: 3</td>
</tr>
<tr>
<td></td>
<td>Internal: 30Marks</td>
<td>External: 70 Marks</td>
<td>Total: 100Marks</td>
</tr>
</tbody>
</table>
Unit-1: Introduction

Unit-2: Emerging Technologies for 4G

Unit 3: Multi-gigabit wireless networks
Next generation (5G) wireless technologies- Upper Gigahertz and Terahertz wireless Communications: Millimeter wave networking- Directionality and beam forming- Mobility and signal blockage- IEEE 802.11ad (60 GHz WLAN) MAC and PHY overview: Visible light communication- High-speed networking using LEDs - IEEE 802.15.7 PHY and MAC overview Sensing through visible light- Visible light indoor localization and positioning

Unit 4: Indoor localization and RF sensing
Smartphone localization - WiFi fingerprinting - protocols and challenges - Non-WiFi localization - Device-free sensing with radio frequency - Mining wireless PHY channel state information- Device free localization and indoor human tracking - Activity and gesture recognition through RF.

Unit 5: Low-power networking
Backscatter communication - Radio Frequency Identification (RFID) technology overview – Energy harvesting tags and applications- Internet-of-Things (IoT) - IoT protocol overview - CoAP and MQTT - IPv6 networking in low-power PANs (6LoWPAN)

Unit 6: Future mobile networks
Drone networking - Multi-UAV networks, architectures and civilian applications-Communication challenges and protocols for micro UAVs- Connected and autonomous cars - Wireless technologies for Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communications – Automotive surrounding sensing with GHz and THz signals.

Unit 7: Instructional Activities
Survey minimum of four 5G wireless networks for wireless communication and carry out simulation of those networks.

Text Books:
References Books:

Hyperlinks:
1. https://www.amazon.in/4G-LTE-Advanced-Pro-Road-5G-ebook/dp/B01IUACTDM
3. https://www.theiet.org/resources/books/telecom/5gwire.cfm?
5. https://www.researchgate.net/publication/311896317_Ultra-reliable_communication_in_a_factory_environment_for_5G_wireless_networks_Link_level_and_deployment_study