# University of Mumbai

No. AAMS_UGS/ICC/2024-25/ 89

**CIRCULAR:-**

Attention of the Principals of the Affiliated Colleges and Directors of the Recognized Institutions and the Head, University Departments is invited to this office circular No. AAMS_UGS/ICC/2023-24/23 dated 08th September, 2023 relating to the NEP UG & PG Syllabus.

They are hereby informed that the recommendations made by the **Ad-hoc Board of Studies in Information Technology** at its meeting held on 03rd June, 2024 and subsequently passed by the Board of Deans at its meeting held on 27th June, 2024 **vide** item No. 6.5 (N) have been accepted by the Academic Council at its meeting held on 28th June, 2024 **vide** item No. 6.5 (N) and that in accordance therewith the **syllabus** for the **M.Sc. (I.T- Security) (Sem. III & IV)** is introduced as per appendix (NEP 2020) with effect from the academic year 2024-25.

(The circular is available on the University's website www.mu.ac.in).

Baliram

MUMBAI – 400 032
20th August, 2024

(Prof.(Dr) Baliram Gaikwad)
I/c Registrar

To

The Principals of the Affiliated Colleges, Directors of the Recognized Institutions and the Head, University Department.

**A.C/6.5(N)/28/06/2024**

Copy forwarded with Compliments for information to:-

1) The Chairman, Board of Deans,
2) The Dean, Faculty of Science &Technology,
3) The Chairman, **Ad-hoc Board of Studies in Information Technology.**
4) The Director, Board of Examinations and Evaluation,
5) The Director, Board of Students Development,
6) The Director,.Department of Information & Communication Technology.
7) The Director, Institute of Distance and Open Learning (IDOL Admin). Vidyanagari.
8) The Deputy Registrar, Admissions, Enrolment, Eligibility & Migration Department (AEM),

| **Copy forwarded for information and necessary action to :-** | |
|---|---|
| 1 | The Deputy Registrar, (Admissions, Enrolment, Eligibility and Migration Dept)(AEM), dr@eligi.mu.ac.in |
| 2 | The Deputy Registrar, Result unit, Vidyanagari drresults@exam.mu.ac.in |
| 3 | The Deputy Registrar, Marks and Certificate Unit,. Vidyanagari dr.verification@mu.ac.in |
| 4 | The Deputy Registrar, Appointment Unit, Vidyanagari dr.appointment@exam.mu.ac.in |
| 5 | The Deputy Registrar, CAP Unit, Vidyanagari cap.exam@mu.ac.in |
| 6 | The Deputy Registrar, College Affiliations & Development Department (CAD), deputyregistrar.uni@gmail.com |
| 7 | The Deputy Registrar, PRO, Fort, (Publication Section), Pro@mu.ac.in |
| 8 | The Deputy Registrar, Executive Authorities Section (EA) eau120@fort.mu.ac.in<br><br>He is requested to treat this as action taken report on the concerned resolution adopted by the Academic Council referred to the above circular. |
| 9 | The Deputy Registrar, Research Administration & Promotion Cell (RAPC), rapc@mu.ac.in |
| 10 | The Deputy Registrar, Academic Appointments & Quality Assurance (AAQA) dy.registrar.tau.fort.mu.ac.in ar.tau@fort.mu.ac.in |
| 11 | The Deputy Registrar, College Teachers Approval Unit (CTA), concolsection@gmail.com |
| 12 | The Deputy Registrars, Finance & Accounts Section, fort draccounts@fort.mu.ac.in |
| 13 | The Deputy Registrar, Election Section, Fort drelection@election.mu.ac.in |
| 14 | The Assistant Registrar, Administrative Sub-Campus Thane, thanesubcampus@mu.ac.in |
| 15 | The Assistant Registrar, School of Engg. & Applied Sciences, Kalyan, ar.seask@mu.ac.in |
| 16 | The Assistant Registrar, Ratnagiri Sub-centre, Ratnagiri, ratnagirisubcentre@gmail.com |

| **Copy for information :-** | |
|---|---|
| 1 | P.A to Hon'ble Vice-Chancellor,<br>vice-chancellor@mu.ac.in |
| 2 | P.A to Pro-Vice-Chancellor<br>pvc@fort.mu.ac.in |
| 3 | P.A to Registrar,<br>registrar@fort.mu.ac.in |
| 4 | P.A to all Deans of all Faculties |
| 5 | P.A to Finance & Account Officers, (F & A.O),<br>camu@accounts.mu.ac.in |

| | |
|---|---|
| 1 | The Chairman, Board of Deans |
| 2 | The Dean, Faculty of Humanities, |
| 3 | Chairman, Board of Studies, |
| 4 | The Director, Board of Examinations and Evaluation,<br>dboee@exam.mu.ac.in |
| 5 | The Director, Board of Students Development,<br>dsd@mu.ac.in@gmail.com DSW direcotr@dsw.mu.ac.in |
| 6 | The Director, Department of Information & Communication Technology, |
| 7 | The Director, Institute of Distance and Open Learning (IDOL Admin),<br>Vidyanagari,<br>director@idol.mu.ac.in |

**AC – 28/06/2024**
**Item No. 6.5 (N)**

# As Per NEP 2020

# University of Mumbai

**Title of the program**

**M.Sc. (IT-Security) (Two Year)**

**Syllabus for**

**Semester – Sem III & IV**
**Ref: GR dated 16th May, 2023 for Credit Structure of PG**

**(With effect from the academic year 2024-25)**

# University of Mumbai

**(As per NEP 2020)**

| Sr. No. | Heading | Particulars |
|---|---|---|
| 1 | **Title of program**<br>**O:_____ B** | **M.Sc. (IT-Security)** |
| 2 | **Scheme of Examination**<br>**R: _____** | **NEP**<br>**50% Internal**<br>**50% External,**<br>**Semester End Examination**<br>**Individual Passing in Internal and External Examination** |
| 3 | **Standards of Passing**<br>**R: _____** | **40%** |
| 4 | **Credit Structure**<br>**R: SP-120B** | **Attached herewith** |
| 5 | **Semesters** | **Sem. III & IV** |
| 6 | **Program Academic Level** | **6.5** |
| 7 | **Pattern** | **Semester** |
| 8 | **Status** | **New** |
| 9 | **To be implemented from Academic Year** | **2024-25** |

**Sign of Chairperson**
**Dr. Mrs. R. Srivaramangai**
**Ad-hoc BoS (IT)**

**Sign of the**
**Offg. Associate Dean**
**Dr. Madhav R. Rajwade**
**Faculty of Science & Technology**

**Sign of Offg. Dean,**
**Prof. Shivram S. Garje**
**Faculty of Science & Technology**

## 5. Credit Structure of the program (Sem-I, II, III & IV)

### Post Graduate Programs in University

**Parishishta 1**

**R. SP-120B**

| Year | Level | Sem (2yr) | Major | | | | RM | OJT/FP | RP | Cum. Cr. | Degree |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 6.5 | Sem III | 2*4+2*2 + 2 | | | 4 | - | - | (607)4 | 22 | PG Degree after 3-yr UG or PG Degree after 4-yr UG |
| | | | Security Breaches and Counter Measures (601) | TH | 4 | Blockchain(606a) **(OR)** Cloud Economics(606b) **(OR)** BioMedical Image Processing(606c) | | | | | |
| | | | Security Breaches and Counter Measures Practical (602) | PR | 2 | | | | | | |
| | | | Offensive Security(603) | TH | 4 | | | | | | |
| | | | Offensive Security Practical(604) | PR | 2 | | | | | | |
| | | | ISA(605) | TH | 2 | | | | | | |
| | | Sem IV | 2*4+2*2 | | | 4 | - | - | (616)6 | 22 | |
| | | | Cyber Forensics(611) | TH | 4 | Augmented Reality & Virtual Reality(615a) **(OR)** Digital Image Forensics(615b) **(OR)** Edge Computing(615c) | | | | | |
| | | | Cyber Forensics Practical(612) | PR | 2 | | | | | | |
| | | | Security Operations Centre(613) | TH | 4 | | | | | | |
| | | | Security Operations Centre Practical(614) | PR | 2 | | | | | | |
| Cum. Cr. For 1 Yr PG Degree | | | 26 | | | 8 | | | 10 | 44 | |
| Cum. Cr. For 2 Yr PG Degree | | | 54 | | | 16 | 4 | 4 | 10 | 88 | |

# Syllabus

## M.Sc. (IT-Security)
## (Sem. III & IV)

# Sem-III

**Programme Name: M.Sc. (IT-Security)**
**Programme Name: M.Sc. (IT-Security)**

| | |
|---|---|
| **Course Code:**601 [Mandatory]<br>**Total Credits:** 04 (60 Lecture Hrs)<br>**University assessment:** 50 marks | **Course Name Security Breaches and Counter Measures** (Theory)<br>**Total Marks:** 100 marks<br>**College/Department assessment:** 50 marks |

**Pre requisite:**

1. Fundamental concept of Networking
2. Fundament concept of Security

**Course Objectives (COs)**

To enable the students to:

CO1: Gain a deep understanding of ethical hacking principles, methodologies, and tools.

CO2: Develop the skills to conduct network scanning, enumeration, system hacking, malware analysis, and sniffing.

CO3: Learn about social engineering tactics, wireless security, and attacks.

CO4: Understand cryptography, security architecture, cloud computing, and IoT principles.

CO5: Be able to apply this knowledge in real-world scenarios, with a focus on ethical and responsible behaviour.

| **MODULE I:** | **(2 CREDITS)** |
|---|---|
| **Unit 1: Introduction of Ethical Hacking, Foundation of Networking and security, Footprinting and Reconnaissance**<br>**a. Ethical Hacking**: Overview of Ethics, Overview of Ethical Hacking, Attack Modeling- Cyber Kill Chain, Attack Lifecycle, MITRE ATT&CK Framework. Methodology of Ethical Hacking-Reconnaissance and Footprinting, Scanning and Enumeration, Gaining Access, Maintaining Access, Covering Tracks.<br>**b. Networking Foundations**: Communications Models- Open Systems Interconnection, TCP/IP Architecture. Topologies- Bus Network, Star Network, Ring Network, Mesh Network, Hybrid. Physical Networking - Addressing, Switching. IP - Headers, Addressing, Subnets, TCP, UDP, Internet Control Message Protocol, Network Architectures - Network Types, Isolation, Remote Access. Cloud Computing - Storage as a Service, Infrastructure as a Service, Platform as a Service, Software as a Service, Internet of Things.<br>**c. Security Foundations:** The Triad- Confidentiality, Integrity, Availability, Parkerian Hexad. Information Assurance and Risk, Policies, Standards, and Procedures – Security Policies, Security Standards, Procedures, Guidelines. Organizing Your Protections. Security Technology- Firewalls, Intrusion Detection Systems, Intrusion Prevention Systems, Endpoint Detection and Response, Security Information and Event Management. Being Prepared - Defense in Depth, Defense in Breadth, Defensible Network Architecture, Logging, Auditing. **Footprinting and Reconnaissance:** Open Source Intelligence- Companies, People, Social Networking- Domain Name System - Name Lookups, Zone Transfers Passive DNS, Passive Reconnaissance, Website Intelligence, Technology Intelligence- Google Hacking, Internet of Things (IoT). | 15 Hrs [OC1, OC2, OC3,OC4] |
| | |
| **Unit 2: Networks Scanning, Enumeration, System Hacking, Malware and Sniffing**<br>**a. Scanning Networks**: Ping Sweeps- using fping, Using MegaPing, Port Scanning- nmap, masscan, MegaPing, Metasploit. Vulnerability Scanning- OpenVAS, Nessus, looking for Vulnerabilities with Metasploit. Packet Crafting and Manipulation- hping, packETH, fragroute. Evasion Techniques- Evasion with nmap, Protecting and Detecting.<br>**b. Enumeration:** Service Enumeration- Countermeasures, Remote Procedure Calls - SunRPC, Remote Method Invocation. Server Message Block- Built-in Utilities, nmap Scripts, NetBIOS Enumerator, Metasploit, Other Utilities, Countermeasures. Simple Network Management Protocol- Countermeasures. Simple Mail Transfer Protocol- | 15 Hrs [OC5, OC6, ] |

| | |
|---|---|
| Countermeasures. Web-Based Enumeration- Countermeasures.<br>**c. System Hacking:** Searching for Exploits, System Compromise. Metasploit Modules- Exploit-DB, Gathering Passwords, Password Cracking- John the Ripper, Rainbow Tables, Kerberoasting. Client-Side Vulnerabilities, Living Off the Land, Fuzzing. Post Exploitation- Evasion, Privilege Escalation, Pivoting, Persistence, Covering Tracks. **Malware:** Malware Types - Virus, Worm, Trojan, Botnet, Ransomware, Dropper, Fileless Malware, Polymorphic Malware. Malware Analysis - Static Analysis, Dynamic Analysis, Automated Malware Analysis. Creating Malware - Writing Your Own, Using Metasploit, Obfuscating. Malware Infrastructure, Antivirus Solutions, Persistence. **Sniffing:** Packet Capture - tcpdump, tshark, Wireshark, Berkeley Packet Filter, Port Mirroring/Spanning. Detecting Sniffers Packet Analysis, Spoofing Attacks - ARP Spoofing, DNS Spoofing, DHCP Starvation Attack, sslstrip, Spoofing Detection. | |
| **MODULE II :** | **(2 CREDITS)** |
| **Unit 3: Principle of Social Engineering, Wireless security and Attack**<br>**a. Social Engineering:** Social Engineering - Pretexting, Social Engineering Vectors, Identity Theft. Physical Social Engineering - Badge Access, Man Traps, Biometrics, Phone Calls, Baiting, Tailgating. Phishing Attacks -Contact Spamming, Quid Pro Quo. Social Engineering for Social Networking. Website Attacks- Cloning, Rogue Attacks, Wireless Social Engineering, Automating Social Engineering.<br>**b. Wireless Security:** Wi-Fi - Wi-Fi Network Types, Wi-Fi Authentication, Wi-Fi Encryption, Bring Your Own Device, Wi-Fi Attacks. Bluetooth - Scanning, Bluejacking, Bluesnarfing, Bluebugging, Bluedump, Bluesmack. Mobile Devices - Mobile Device Attacks<br>**c. Attack and Defence:** Web Application Attacks - OWASP Top 10 Vulnerabilities, WebApplication Protections. Denial-of-Service Attacks - Bandwidth Attacks, Slow Attacks, Legacy. Application Exploitation - Buffer Overflow, Heap Spraying, Application Protections and Evasions. Lateral Movement, Defense in Depth/Defense in Breadth, Defensible Network Architecture, | 15 Hrs [OC7, OC8,] OC10] |
| | |
| **Unit 4: Application of Cryptography, Security Architecture, Cloud Computing and IOT**<br>**a. Cryptography:** Basic Encryption - Substitution Ciphers, Diffie–Hellman. Symmetric Key Cryptography- Data Encryption Standard, Advanced Encryption Standard. Asymmetric Key Cryptography- Hybrid Cryptosystem Nonrepudiation, Elliptic Curve Cryptography. Certificate Authorities and Key Management - Certificate Authority, Trusted Third Party, Self-Signed Certificates. Cryptographic Hashing, PGP and S/MIME, Disk and File Encryption.<br>**b. Security Architecture and Design:** Data Classification, Security Models - State Machine, Biba, Bell–LaPadula, Clark–Wilson Integrity Model. Application Architecture - n-tier Application Design, Service-Oriented Architecture, Cloud-Based Applications, Database Considerations. Security Architecture - Zero-Trust Model.<br>**c. Cloud Computing and the Internet of Things**: Cloud Computing Overview - Cloud Services, Shared Responsibility Model, Public vs. Private Cloud, Grid Computing. Cloud Architectures and Deployment- Responsive Design, Cloud-Native Design, Deployment, Dealing with REST. Common Cloud Threats - Access Management, Data Breach, Web Application Compromise, Credential Compromise, Insider Threat. Internet of Things- Fog Computing. Operational Technology -The Purdue Model.<br>a. | 15 Hrs [OC8, OC9, ] |

**References:**

| Sr. No. | Title | Author/s | Publisher | Edition | Year |
|---|---|---|---|---|---|
| 1. | CEH™ v12 Certified Ethical Hacker Study Guide | Ric Messier | John Wiley & Sons, Inc | | 2023 |

| | | | | | |
|---|---|---|---|---|---|
| **2.** | CEH Certified Ethical Hacker Cert Guide | Michael Gregg Omar Santos | Pearson Education, Inc. | | 2023 |
| **3.** | CEH™ Certified Ethical Hacker All-in-One Exam Guide | Matt Walker | McGraw Hill | Fifth | 2022 |
| **4.** | Ethical Hacking and Countermeasures Version 12 | EC-Council. | EC-Council. | | 2022 |

**Course Outcomes(OCs)**

Upon completion of this course, students will:

**OC 1: Understand Ethical Hacking Principles**: Gain a comprehensive understanding of ethical hacking, including its ethics, methodologies, and attack models such as the Cyber Kill Chain and MITRE ATT&CK Framework.

**OC 2: Grasp Networking Foundations**: Acquire knowledge of communication models (OSI, TCP/IP), network topologies, physical networking, IP fundamentals, and various network architectures, including cloud computing and IoT.

**OC 3: Comprehend Security Foundations**: Learn about the security triad (confidentiality, integrity, availability), risk management, security policies, standards, procedures, and various security technologies such as firewalls, IDS/IPS, and SIEM.

**OC 4: Master Footprinting and Reconnaissance**: Understand the importance of open-source intelligence (OSINT), domain name system (DNS), and passive reconnaissance in security assessments.

**OC 5: Develop Scanning and Enumeration Skills**: Gain practical experience in scanning networks, performing vulnerability scans, and enumerating services, including countermeasure techniques.

**OC 6: Learn System Hacking Techniques**: Acquire skills in exploiting systems, using Metasploit modules, cracking passwords, and understanding malware types and analysis methods.

**OC 7: Understand Social Engineering and Wireless Security**: Learn about social engineering tactics, phishing attacks, wireless security principles, and wireless attacks and defences.

**OC 8: Explore Cryptography and Security Architecture**: Understand basic encryption, symmetric and asymmetric cryptography, certificate authorities, cryptographic hashing, and security models and architectures.

**OC 9: Gain Insight into Cloud Computing and IoT Security**: Learn about cloud computing models, architectures, threats, and security considerations for IoT devices and operational technology.

**OC 10: Enhance Defensive Strategies**: Understand defense-in-depth, defense-in-breadth, and defensible network architecture principles, along with logging and auditing best practices.

**Programme Name: M.Sc. (IT-Security)**

| | |
|---|---|
| **Course Code:**602 [Mandatory]<br>**Total Credits:** 02 (60 Lecture Hrs)<br>**University assessment:** 25 marks | **Course Name:** Security Breaches and Counter Measures Practical<br>**Total Marks:** 50 marks<br>**College/Department assessment:** 25 marks |

**Prerequisite:**

1. Sound knowledge of Netwprking
2. Sound knowledge of concepts in Security principle

**Course Objectives (COs):**

To enable the students to:

a. gaining practical skills in ethical hacking,
b. understand the common attack vectors
c. learn how to identify and exploit vulnerabilities, and developing strategies for securing systems and networks against such attacks

| Prac No | Practical Description | 2 CREDITS (60 hrs) |
|---|---|---|
| 1 | Introduction to Ethical Hacking<br>a. Setting up a secure hacking environment using virtual machines and labs. | 2 hrs [OC1] |
| 2 | **Footprinting and Reconnaissance**<br>a. Perform Footprinting through Search Engines<br>b. Find the Company's Domains and Sub-domains using Netfcraft<br>c. Gather personal information from various social networking sites using Sherlock<br>d. Gather info about target website using Ping command line utilityPerform Email Footprinting<br>e. Mirroring website using HTTrack Web Site Copier<br>f. Perform Whois Footprinting<br>g. Perform DNS Footprinting<br>h. Perform reverse DNS lookup using Reverse IP domain check and DNSRecon<br>i. Perform Network Footprinting<br>j. Perform network tracerouting in Windows and Linux machines<br>k. Footprinting a target using Recon-ng<br>l. Footprinting a target using Maltego<br>m. Footprinting a target using OSINT Framework<br>n. Automated Fingerprinting using FOCA | 10 hrs [OC2] |
| 3 | **Network Scanning**<br>a. UDP and TCP Packet Crafting Techniques using hping3<br>b. Identify Target System's OS with TTL (Time-to-Live) and TCP Windows Sizes using Wireshark<br>c. Basic Network Troubleshooting using MegaPing (Windows)<br>d. Understanding the Basics of Network Scanning using Nmap<br>e. Windows Scanning Tools | 4 hrs [OC3] |
| 4 | **Enumeration**<br>a. Enumeration using Nmap | 4 hrs [OC4] |

| | | |
|---|---|---|
| | b. SNMP Enumeration<br>c. NetBIOS Enumeration<br>d. Enumeration using Metasploit<br>e. SNMP Enumeration<br>f. Advanced IP Scanner | |
| 5 | **Vulnerability Analysis**<br>a. Nessus<br>b. GFI LanGuard<br>c. Nikto<br>d. Nmap<br>e. Searchsploit | 4 hrs<br>[OC5] |
| 6 | **System Hacking**<br>a. NTLM Hash crack<br>b. Rainbow table crack using Winrtgen<br>c. Hash dump with Pwdump7 and crack with Ophcrack<br>d. Hiding file in NTFS stream<br>e. Hiding Data Using White Space Steganography<br>f. Image Steganography using OpenStego and QuickStego<br>g. Demonstrate how to escalate privileges on a victim machine by exploiting its vulnerabilities<br>h. Hacking Windows using Metasploit / Meterpreter - Post-Exploitation | 4 hrs<br>[OC6] |
| 7 | **Malware**<br>a. Create a server using njRAT. And Access the target machine remotely.<br>b. Create a server and Run HTTP Trojan on Windows Server 2012 , Execute the Server from Windows 10 virtual machine and Control Windows 10 machine remotely from Windows Server 2012 | 4 hrs<br>[OC7] |
| 8 | **Sniffing**<br>a. Password Sniffing using Wireshark<br>b. Detect ARP Poisoning using Wireshark<br>c. Cain & Abel – MITM attack tool (via ARP Poisoning)<br>d. MAC Address Spoofing | 4 hrs<br>[OC8] |
| 9 | **Social Engineering**<br>a. Using Social Engineering Toolkit (SET) | 2 hrs<br>[OC9] |
| 10 | **Denial-of-Service**<br>a. Perform a SYN Flooding on a Target Host using hping3<br>b. HTTP Flooding Attack using HOIC (High Orbit Ion Cannon)<br>c. Detect DoS attack using KFSensor and analyze the incoming packet dump using Wireshark | 4 hrs<br>[OC10] |
| 11 | **Session-Hijacking**<br>a. Using ZAP (Zed Attack Proxy) | 3 hrs<br>[OC11] |
| 12 | **Hacking Web Servers**<br>a. ID Server - Webserver Foot printing<br>b. Uniscan - WebServer Fingerprinting (Kali) | 2 hrs<br>[OC12] |

| | | |
|---|---|---|
| | c. Skipfish – WebServer Recon | |
| 13 | **Hacking Web Apps**<br>a. Perform a Brute-force Attack using Burp Suite<br>b. Exploiting web application vulnerabilities like Cross-Site Scripting, Directory Traversal, File Upload, CSRF, SSRF, Command Injection, etc. | 2 hrs<br>[OC12] |
| 14 | **SQL Injection**<br>a. Perform an SQL Injection Attack Against MSSQL to Extract Databases using SQLMap<br>b. BBQSQL | 3 hrs<br>[OC13 |
| 15 | **Hacking Wireless**<br>a. WEP/WPA/WPA2 Cracking using AIRCRACK-NG | 4 hrs<br>[OC14] |
| 16 | **Cryptography**<br>a. Calculate One-way Hashes using HashClac<br>b. Calculate MD5 Hashes using MD5 Calculator<br>c. Perform File Encryption using Advanced Encryption Package<br>d. Encrypt and Decrypt messages using BCText Encoder<br>e. Perform Disk Encryption Using VeraCrypt<br>f. Perform Encryption and Decryption using Cryptool | 4 hrs<br>[OC15] |

**Course Outcomes(OCs)**

Upon completing this course,

**OC1: Setting Up Secure Hacking Environment**: Students will be proficient in setting up secure hacking environments using virtual machines and labs, ensuring safe and legal practice.

**OC2: Footprinting and Reconnaissance**: Students will master techniques for gathering information about targets through diverse methods such as search engines, social networking sites, and specialized tools like Netcraft, Recon-ng, and Maltego.

**OC3: Network Scanning**: Students will understand UDP and TCP packet crafting techniques, identify target system's OS, troubleshoot networks, and utilize scanning tools like Nmap effectively.

**OC4: Enumeration**: Students will learn enumeration techniques using various tools such as Nmap, Metasploit, SNMP, and Advanced IP Scanner to identify and gather information about potential vulnerabilities.

**OC5: Vulnerability Analysis**: Students will gain proficiency in analyzing vulnerabilities using tools such as Nessus, Nikto, and Nmap, enabling them to assess system weaknesses comprehensively.

**OC6: System Hacking**: Students will develop skills in cracking hashes, hiding files, escalating privileges, and exploiting vulnerabilities using tools like Metasploit/Meterpreter, enhancing their ability to penetrate systems ethically.

**0C7: Malware**: Students will learn to create and deploy malware servers like njRAT, enabling them to understand and mitigate the threats posed by malicious software effectively.

**OC8: Sniffing**: Students will understand sniffing techniques, ARP poisoning, MITM attacks, and MAC address spoofing using tools like Wireshark and Cain & Abel, facilitating effective network analysis and security.

**OC9: Social Engineering**: Students will be proficient in using the Social Engineering Toolkit (SET) to exploit human vulnerabilities, enhancing their understanding of the human element in cybersecurity.

**OC10: Denial-of-Service**: Students will learn to perform SYN flooding and HTTP flooding attacks, as well as analyze incoming packet dumps to detect and mitigate DoS attacks effectively.

**OC11: Session Hijacking**: Students will understand session hijacking techniques using tools like ZAP (Zed Attack Proxy), enabling them to identify and prevent session-based attacks.

**OC12: Hacking Web Servers and Web Apps**: Students will be adept at footprinting, fingerprinting, and exploiting vulnerabilities in web servers and applications using tools like Burp Suite, Uniscan, and Skipfish.

**OC13: SQL Injection**: Students will master SQL injection attacks against MSSQL databases using tools like SQLMap and BBQSQL, enhancing their ability to identify and mitigate SQL injection vulnerabilities.
**OC14: Hacking Wireless**: Students will gain skills in cracking WEP/WPA/WPA2 wireless security protocols using AIRCRACK-NG, enabling them to assess and improve wireless network security.
**OC15: Cryptography**: Students will understand various cryptographic techniques such as hashing, file encryption, message encryption/decryption, and disk encryption using tools like HashCalc, VeraCrypt, and Cryptool, enhancing their understanding of data protection mechanisms.

## Programme Name: M.Sc. (IT-Security)

| | |
|---|---|
| **Course Code:** 603 [Mandatory]<br>**Total Credits:** 04 (60 Lecture Hrs)<br>**University assessment:** 50 marks | **Course Name:** Offensive Security (Theory)<br>**Total Marks:** 100 marks<br>**College/Department assessment:** 50 marks |

**Prerequisite:**
A basic understanding of the following concepts would be beneficial:

1. Solid understanding of TCP/IP networking
2. Reasonable Windows and Linux administration experience
3. Familiarity with basic Bash and/or Python scripting
4. Windows 11 instance (VM or Host)

**Course Objectives (COs)**
To enable the students to:

CO1 : Define ethical hacking principles and the legal considerations of penetration testing.
CO2 : Explain the fundamentals of networking, including TCP/IP, network protocols, and network devices.
CO3 : Identify and understand core security concepts like vulnerabilities, threats, and risk management.
CO4 : Conduct thorough information gathering techniques like footprinting and reconnaissance, utilize various tools and techniques to scan networks and identify vulnerabilities.
CO5 : Employ network sniffing techniques to capture sensitive data traffic, Enumerate systems to discover exploitable services, accounts, and resources, Implement social engineering tactics to manipulate human behavior for security breaches.
CO6 : Understand the principles of cryptography and its role in offensive security testing.
CO7 : Assess the security vulnerabilities of wireless networks, analyze the security implications of cloud computing environments and Internet of Things devices.

| **MODULE I: Basics of Offensive Security** | **(2 CREDITS)** |
|---|---|
| **Unit 1: Introduction to Offensive Security**<br>a. Ethical Hacking: Overview of Ethics, Overview of Ethical Hacking, Attack Modeling, Methodology of Ethical Hacking.<br>b. Networking Foundations: Communication Models, Topologies, Physical Networking, IP, TCP, UDP, Internet Control Message Protocol, Network Architectures, Cloud Computing.<br>c. Security Foundations: The Triad, Information Assurance and Risk, Policies, Standards, and Procedures, Organizing your Protections, Security Technology, Being Prepared. | 15 Hrs<br>[OC1, OC3] |
| | |
| **Unit 2: Phases of Offensive Security**<br>a. Footprinting and Reconnaissance: Open-Source Intelligence, Domain Name System, Passive Reconnaissance, Web Intelligence, Technology Intelligence.<br>b. Scanning Networks: Ping Sweeps, Port Scanning, Vulnerability Scanning, Packet Crafting and Manipulation, Evasion Techniques, Protecting and Detecting.<br>c. Enumeration: Service Enumeration, Remote Procedure Calls, Server Message Block, Simple Network Management Protocol, Simple Mail Transfer Protocol, Web-Based Enumeration.<br>d. System Hacking: Searching for Exploits, System Compromise, Gathering Passwords, Password Cracking, Client-side Vulnerabilities, Living off the Land, Fuzzing, Post Exploitation. | 15 Hrs<br>[OC2, OC3, OC4] |
| **MODULE II: Attack Vectors in Offensive Security** | **(2 CREDITS)** |

| | |
|---|---|
| **Unit 3: Basic Attack Vectors**<br>a. Malware: Malware Types, Malware Analysis, Creating Malware, Malware Infrastructure, Antivirus Solutions, Persistence.<br>b. Sniffing: Packet Capture, Detecting Sniffers, Packet Analysis, Spoofing Attacks.<br>c. Social Engineering: Social Engineering, Physical Social Engineering, Phishing Attacks, Social Engineering for Social Networking, Website Attacks, Wireless Social Engineering, Automating Social Engineering.<br>d. Cryptography: Basic Encryption, Symmetric Key Cryptography, Asymmetric Key Cryptography, Certificate Authorities and Key Management, Cryptographic Hashing, PGP and S/MIME, Disk and File Encryption. | 15 Hrs [OC2, OC4, OC6] |
| | |
| **Unit 4: Advanced Attack Vectors**<br>a. Wireless Security: Wi-Fi, Bluetooth, Mobile Devices.<br>b. Attack and Defence: Web Application Attacks, Denial-of-Service Attacks, Application Exploitation, Lateral Movement, Defence in Depth / Defence in Breadth, Defensible Network Architecture.<br>c. Cloud Computing and Internet of Things: Cloud Computing Overview, Cloud Architectures and Deployment, Common Cloud Threats, Internet of Things, Operational Technology. | 15 Hrs [OC2, OC4, OC5, OC6] |
| | |

**References:**

| Sr. No. | Title | Author/s | Publisher | Edition | Year |
|---|---|---|---|---|---|
| 1. | CEH v12 Certified Ethical Hacker Study Guide | Ric Messier | Sybex | | 2023 |
| 2. | Penetration testing - A Hands-On Introduction to Hacking | Georgia Weidman | No Starch Press | | 2014 |
| 3. | Ethical Hacking and Penetration Testing Guide | Rafay Baloch | CRC Press | First | 2014 |

**Course Outcomes(OCs)**

OC1. Students will be able to ethically conduct penetration testing engagements.
OC2. Students will gain the skills to identify and exploit vulnerabilities in various systems.
OC3. Students will develop a strong understanding of network security concepts.
OC4. Students will be adept at utilizing various tools and techniques for offensive security assessments.
OC5. Students will be able to implement security best practices for cloud, wireless, and IoT environments.
OC6. Students will demonstrate critical thinking and problem-solving skills in a security context.

**Programme Name: M.Sc. (IT-Security)**

| | |
|---|---|
| **Course Code:** 604 [Mandatory]<br>**Total Credits:** 02 (60 Lecture Hrs)<br>**University assessment:** 25 marks | **Course Name:** Offensive Security Practical<br>**Total Marks:** 50 marks<br>**College/Department assessment:** 25 marks |

**Pre requisite:**
A basic understanding of the following concepts would be beneficial:

1. Solid understanding of TCP/IP networking
2. Reasonable Windows and Linux administration experience
3. Familiarity with basic Bash and/or Python scripting
4. Windows 11 instance (VM or Host)

**Course Objectives (COs):**
To enable the students to:
CO1: Understand and apply a structured ethical hacking methodology for penetration testing engagements.
CO2: Develop skills in gathering information about a target organization using OSINT techniques.
CO3: Master network scanning techniques to identify vulnerabilities and prioritize targets.
CO4: Learn how to enumerate information from a system to identify potential entry points.
CO5: Learn how to capture and analyze network traffic to identify vulnerabilities.

| Prac No | Practical Description | 2 CREDITS (60 hrs) |
|---|---|---|
| 0 | Setting up the Lab and Virtual Environment:<br>a. Install VMWare/VirtualBox<br>b. Setup Kali Linux<br>c. Create target machines – Windows XP, Windows 7 | 4 [OC 1, OC 2, OC 3] |
| 1 | Perform Footprinting and Reconnaissance (Passive Information Gathering):<br>a. Windows/Linux Command Line Utilities<br>b. Whois Enumeration<br>c. Google Hacking<br>d. Netcraft<br>e. Recon-ng<br>f. Shodan<br>g. Searching for Email Addresses | 7 [OC 1, OC 2, OC 3] |
| 2 | Perform Footprinting and Reconnaissance (Active Information Gathering):<br>a. DNS Enumeration<br>b. Port Scanning<br>c. SMB Enumeration<br>d. NFS Enumeration | 6 [OC 1, OC 2, OC 3] |
| 3 | Perform Footprinting and Reconnaissance (User Information Gathering):<br>a. Email Harvesting<br>b. Password Dumps<br>c. OSINT Framework<br>d. Maltego | 6 [OC 1, OC 2, OC 3] |
| 4 | Capturing Traffic and Network Discovery<br>a. Wireshark<br>b. TCPdump | 6 [OC 4, OC 5] |

| | | |
|---|---|---|
| | c. ARP Cache Poisoning<br>d. DNS Cache Poisoning<br>e. SSL Attacks<br>f. SSL Stripping<br>g. Kismet<br>h. The Dude | |
| 5 | Vulnerability Scanning<br>a. Nessus<br>b. Nmap<br>c. Metasploit<br>d. OpenVAS | 7<br>[OC 6] |
| 6 | Web Application Scanning<br>a. Nikto<br>b. DIRB<br>c. Burpsuite<br>d. SQLInjection<br>e. w3af<br>f. OWASP ZAP | 7<br>[OC 6] |
| 7 | Password Cracking Tools / Password Attacks<br>a. Winrtgen<br>b. PWDump<br>c. THC-Hydra<br>d. John the Ripper<br>e. Hashcat<br>f. Ophcrack<br>g. Cain and Abel | 8<br>[OC 7, OC 8] |
| 8 | Social Engineering<br>a. The Social-Engineer Toolkit<br>b. Spear Phishing Attacks<br>c. Web Attacks<br>d. Mass Email Attacks | 5<br>[OC 9, OC 10] |
| 9 | Privilege Escalation<br>a. Windows Privilege Escalation<br>b. Linux Privilege Escalation | 5<br>[OC 11, OC 12] |

**References:**


| Sr. No. | Title | Author/s | Publisher | Edition | Year |
|---|---|---|---|---|---|
| 1. | CEH v12 Certified Ethical Hacker Study Guide | Ric Messier | Sybex | | 2023 |
| 2. | Penetration testing - A Hands-On Introduction to Hacking | Georgia Weidman | No Starch Press | | 2014 |
| 3. | Ethical Hacking and Penetration Testing Guide | Rafay Baloch | CRC Press | First | 2014 |


**Course Outcomes (OCs)**:
Upon completing this course, the student will be able to:

| | |
|---|---|
| OC 1. | Understand offensive security fundamentals & gain knowledge of virtual environment setup. |
| OC 2. | Proficient in passive and active information gathering techniques using various tools |
| OC 3. | Understand the importance of user information gathering and its role in penetration testing |
| OC 4. | Learn to capture and analyze network traffic & gain expertise in ARP and DNS cache poisoning techniques for network discovery. |
| OC 5. | Understand SSL attacks, including SSL stripping, and their implications for network security |
| OC 6. | Understand the process of exploiting vulnerabilities and launching attacks using various tools available. |
| OC 7. | Gain proficiency in password cracking techniques & |
| OC 8. | Understand the importance of strong password policies and the implications of weak passwords in cybersecurity. |
| OC 9. | Learn about social engineering techniques and tools for exploiting human vulnerabilities. |
| OC 10. | Understand spear phishing attacks, web attacks, and mass email attacks, and their impact on organizational security. |
| OC 11. | Understand privilege escalation techniques for both Windows and Linux systems. |
| OC 12. | Learn about gaining and maintaining access to compromised systems, exploring post-exploitation techniques, and evading detection. |

## Programme Name: M.Sc. (IT-Security)

| | |
|---|---|
| **Course Code:** [Mandatory]<br>**Total Credits:** 02 (30 Lecture Hrs)<br>**University assessment:** 25 marks | **Course Name**: **Information Security Auditing**<br>**Total Marks:** 50 marks<br>**College/Department assessment:** 25 marks |

**Pre-requisite:**

- Sound knowledge of Information Systems in general

**Course Objectives (COs):**

To enable the students to:

CO 1. Understand various information security policies in place.

CO 2. Assess an organization based on the needs and suggest the requisite information security policies to be deployed.

CO 3. Audit the organization across relevant policies and assist the organization in implementing such policies along with suggesting improvements.

| **MODULE I:** | **(2 CREDITS)** |
|---|---|
| **Unit 1:**<br>**a) Secrets of a Successful Auditor -** Understanding the Demand for IS Audits, Understanding Policies, Standards, Guidelines, and Procedures , Understanding Professional Ethics, Understanding the Purpose of an Audit , Differentiating between Auditor and Auditee, Roles Implementing Audit Standards, Auditor Is an Executive Position, Understanding the Corporate Organizational Structure<br>**b) Governance -** Strategy Planning for Organizational Control, Overview of Tactical Management , Planning and Performance, Overview of Business Process Reengineering, Operations Management<br>**c) Audit Process -** Understanding the Audit Program, Establishing and Approving an Audit Charter, Preplanning specific Audits, Performing an Audit Risk Assessment, Determining Whether an Audit Is Possible, Performing the Audit, Gathering Audit Evidence | 15 Hrs<br>[OC1, OC2, OC3] |
| **Unit 2:**<br>**a) System Implementation and Operations -** Understanding the Nature of IT Services, Performing IT Operations Management, Performing Capacity Management, Using Administrative Protection, Performing Problem Management, Monitoring the Status of Controls, Implementing Physical Protection<br>**b) Protecting Information Assets -** Understanding the Threat, Using Technical Protection<br>**c) Business Continuity and Disaster Recovery -** Debunking the Myths , Understanding the Five Conflicting Disciplines Called Business Continuity, Defining Disaster Recovery, Defining the Purpose of Business Continuity, Uniting Other Plans with Business Continuity, Understanding the Five Phases of a Business Continuity Program, Understanding the Auditor Interests in BC/DR Plans | [OC1, OC4, OC5] |

**References:**

**Books and References:**

| Sr. No. | Title | Author/s | Publisher | Edition | Year |
|---|---|---|---|---|---|
| 1. | CISA®: Certified Information Systems Auditor | David Cannon | SYBEX | Fourth Edition | 2016 |
| 2. | CISA Review Manual 27th Edition | | ISACA | | 2019 |
| 3. | CISA Certified Information Systems Auditor All-in-One Exam Guide, Fourth Edition, | | O'Reilly | 4th Edition | 2019 |

**Course Outcomes (OCs):**

Upon completing this course, the student will be able to:

OC1: Understand various information security policies and process flow, Ethics of an Information security Auditor.

OC2: Understand various information systems in an organization, their criticality and various governance and management policies associated with them.

OC3: Critically analyse various operational strategies like asset management, data governance etc. and suggest requisite changes as per organizations requirements with improvements.

OC4: Understand the information flow across the organization and identify the weak spots, and also suggest improvements to strengthen them.

OC5: Come up with strong strategies to protect information assets and Come up with an efficient business Continuity plan, disaster recovery strategy

## Programme Name: M.Sc. (IT-Security)

| | |
|---|---|
| **Course Code:606a** [Elective]<br>**Total Credits:** 04 (60 Lecture Hrs)<br>**University assessment:** 50 marks | **Course Name:** Blockchain (Theory)<br>**Total Marks:** 100 marks<br>**College/Department assessment:** 50 marks |

**Pre requisite:**
A basic understanding of the following concepts would be beneficial:

1. Computer networks and distributed systems
2. Cryptography fundamentals

**Course Objectives (COs)**
To enable the students to:

CO1: Explain the fundamental concepts and underlying technologies of blockchain.
CO2: Analyse the benefits and challenges associated with blockchain adoption.
CO3: Analyse the potential benefits and limitations of blockchain in different use cases.
CO4: Critically evaluate the role of blockchain in addressing the double-spending problem and ensuring secure ownership.
CO5: Become familiar with leading blockchain platforms like Bitcoin and Ethereum, along with their functionalities.
CO6: Explore the emerging trends in blockchain, including Web3 and Hyperledger.

| **MODULE I: Fundamentals of Blockchain** | **(2 CREDITS)** |
|---|---|
| **Unit 1: Technical Foundations and Need for Blockchain**<br>a. Thinking in Layers and Aspects: Layers of a Software System, Considering Two Layers at the Same Time, Integrity.<br>b. Seeing the Big Picture: A Payment System, Two Types of Software Architecture, The Advantages of Distributed Systems, The Disadvantages of Distributed Systems, Distributed Peer-to-Peer Systems, Mixing Centralized and Distributed Systems, Identifying Distributed Systems, The Purpose of the Blockchain.<br>c. Recognizing the Potential: How a Peer-to-Peer System Changed a Whole Industry, The Potential of Peer-to-Peer Systems, Terminology, and the Link to the Blockchain.<br>d. Discovering the Core Problem: Trust and Integrity in Peer-to-Peer Systems, The Core Problem to Be Solved by the Blockchain.<br>e. Disambiguating the Term: Four ways to define the blockchain, Provisional Definition, The Role of Managing Ownership.<br>f. Understanding the Nature of Ownership, Ownership and Witnesses, Foundations of Ownership, A Short Detour to Security, Purposes and Properties of a Ledger, Ownership and the Blockchain.<br>g. Spending Money Twice: The Double Spending Problem, How to Solve the Double Spending Problem. | 15 Hrs [OC1, OC2, OC3, OC4] |
| | |

| | |
|---|---|
| **Unit 2: Working of Blockchain**<br>a. Planning the Blockchain: Starting Point, The Path to Follow.<br>b. Documenting Ownership: The Goal, The Challenge, The Idea, A Short Detour to Inventory and Transaction Data, How It Works, Importance of Ordering, Integrity of the Transaction History.<br>c. Hashing Data: The Goal, How it Works, Trying It Out Yourself, Patterns of Hashing Data.<br>d. Hashing in the Real World: Comparing Data, Detecting Changes in Data, Referring to Data in a Change-Sensitive Manner, A Schematic Illustration, Storing Data in a Change-Sensitive Manner, Causing Time-Consuming Computations.<br>e. Identifying and Protecting User Accounts: A gentle introduction to cryptography, A Short Detour to Cryptography, Symmetric Cryptography, Asymmetric Cryptography, Asymmetric Cryptography in the Real World, Asymmetric Cryptography in the Blockchain.<br>f. Authorizing Transactions: Utilizing the digital equivalent to handwritten signatures, A Short Detour to Digital Signatures, How It Works, Why It Works.<br>g. Storing Transaction Data: Building and maintaining a history of transaction data, Transforming a Book into a Blockchain-Data-Structure, The Blockchain-Data-Structure, Storing Transactions in the Blockchain-Data-Structure. | 15 Hrs [OC2, OC3, OC4, OC5] |
| **MODULE II : Blockchain Frameworks** | **(2 CREDITS)** |
| **Unit 3: Cryptocurrencies**<br>a. Introducing Bitcoin: Bitcoin, Digital keys and Addresses, Transactions, Blockchain, Mining.<br>b. Ethereum 101: Introduction, Ethereum – bird's eye view, The Ethereum network, Components of the Ethereum ecosystem. | 15 Hrs [OC3, OC4, OC5, OC6] |
| | |
| **Unit 4: Web3 and Hyperledger**<br>a. Introducing Web3: Web3, Contract Deployment, POST requests, The HTML and JavaScript frontend, Development frameworks.<br>b. Hyperledger: Projects under Hyperledger, Hyperledger as a protocol, The reference architecture, Fabric, Sawtooth Lake, Corda. | 15 Hrs [OC3, OC4, OC5, OC7, OC8] |

**References:**

| Sr. No. | Title | Author/s | Publisher | Edition | Year |
|---|---|---|---|---|---|
| 1. | Blockchain Basics – A Non-Technical Introduction in 25 steps | Daniel Drescher | Apress | First | 2017 |
| 2. | Mastering Blockchain | Imran Bashir | Packt Publishing | Second | 2018 |
| 3. | Bitcoin and Cryptocurrency Technologies - A Comprehensive Introduction | Arvind Narayanan, et.al. | Princeton University Press | First | 2016 |
| 4. | Hands-On Blockchain with Hyperledger | Nitin Gaur, et.al. | Packt Publishing | First | 2018 |

**Course Outcomes (OCs)**

OC 1. Describe the layered architecture of blockchain systems and their interconnectedness.

OC 2. Explain the process of registering and managing ownership on a blockchain network.
OC 3. Explain the double-spending problem and how blockchain technology addresses it.
OC 4. Describe the process of designing and implementing a blockchain network, including data ownership, hashing, and transaction authorization.
OC 5. Evaluate the security features employed in blockchain systems for user authentication and transaction authorization.
OC 6. Explain the fundamentals of Bitcoin and Ethereum, including their architecture and core functionalities.
OC 7. Explain the concept of Web3 and its role in building decentralized applications.
OC 8. Describe the functionalities, purpose, and applications of Hyperledger Projects in blockchain ecosystems.

## Programme Name: M.Sc. (IT-Security)

| | |
|---|---|
| **Course Code:** (606b) [Elective]<br>**Total Credits:** 04 (60 Lecture Hrs)<br>**University assessment:** 50 marks | **Course Name:** Cloud Economics (Theory)<br>**Total Marks:** 100 marks<br>**College/Department assessment:** 50 marks |

**Pre requisite:**

1. Basic knowledge of Cloud Computing.

**Course Objectives (COs)**

To enable the students to:

**CO1:** Understand cloud computing models, deployment strategies, and business impact metrics.

**CO2:** Master FinOps fundamentals, including data-driven decisions, real-time feedback, and team collaboration.

CO3: Develop skills in managing cloud expenses through usage reduction, rightsizing, and commitment-based discounts.

**CO4:** Integrate FinOps strategies with sustainability and broader business objectives, fostering a cost-aware culture.

**CO5:** Implement FinOps in containerized and serverless architectures, optimizing costs and collaborating effectively with engineering teams.

| **MODULE I:** | **(2 CREDITS)** |
|---|---|
| **Unit 1:**<br>a. **What Is Cloud Computing? —The Journey to Cloud -** Cloud Computing Defined NIST Definition of Cloud Computing, Characteristics, Clouds Cloud Service Models, Cloud Deployment Models, **Metrics That Matter—What You Need to Know -** Business Value Measurements, Indirect Metrics, Direct Metrics, Other Direct Metrics. **Sample Case Studies—Applied Metrics**-Total Cost of Ownership, Software Licensing: SaaS, TCO with Software as a Service, Software as a Service Cost Comparison Disaster Recovery and Business Continuity: IaaS Cost-Benefit Analysis for Server Virtualization, Disaster Recovery and Business Continuity (IaaS) -Summary Platform as a Service. **The Cloud Economy—The Human-Economic Impact of Cloud Computing** - Technological Revolutions and Paradigm Change, The Course of Human Development, The United Nations Human Development Index, Cloud Computing as an Economic Enabler, Cloud Computing and Unemployment, Cloud Computing and the Environment Meritocratic Applications of Cloud Computing, Alternative Metrics and Measures of Welfare, The Economic Future of Cloud Computing.<br>**b. Introducing FinOps** -What Is FinOps? Defining the Term "FinOps", The FinOps Hero's Journey, Where Did FinOps Come from? Data-Driven Decision Making, Real-Time Feedback (aka the "Prius Effect"), Core Principles of FinOps , When Should You Start FinOps? , Starting with the End in Mind: Data-Driven Decision Making **, Why FinOps?** - Use Cloud for the Right Reasons, Cloud Spend Keeps Accelerating, The Impact of Not Adopting FinOps, Informed Ignoring: Why Start Now? **Cultural Shift and the FinOps Team** - Deming on Business Transformation, Who Does FinOps? Why a Centralized Team? The FinOps Team Doesn't Do FinOps, The Role of Each Team in FinOps, Executives and Leadership, Engineering and Developer, Finance Procurement and Sourcing Product or Business Teams FinOps Practitioners A New Way of Working Together, Where Does Your FinOps Team Report? Understanding Motivations, Engineers, Finance People, Executives and Leadership, Procurement and Sourcing People, FinOps Throughout Your Organization Hiring for FinOps, FinOps Culture in Action, Difficulty Motivating People Is Not New, Contributors to Action, Detractors from Action, Tipping the Scales in Your Favor,<br>c. **The Language of FinOps** - Defining a Common Lexicon , Defining the Basic Terms, Defining Finance Terms for Cloud Professionals , Abstraction Assists Understanding , Cloud Language Versus Business Language , Creating a Universal Translator Between Your | 15 Hrs<br>[OC1,OC2] |

| | |
|---|---|
| DevOps and Finance Teams , The Need to Educate All the Disciplines , Benchmarking and Gamification , Anatomy of the Cloud Bill- Types of Cloud Bill , Cloud Billing Complexity , Basic Format of Billing Data, Time, Why Do You Punish Me?, Sum of the Tiny Parts , A Brief History of Cloud Billing Data , The Importance of Hourly Data , A Month Is Not a Month , A Dollar Is Not a Dollar , Two Levers to Affect Your Bill , Who Should Avoid Costs and Who Should Reduce Rates? , Centralizing Rate Reduction , Why You Should Decentralize Usage Reduction . | |
| | |
| **Unit 2:**<br>**a. Adopting FinOps**- A Confession , Different Executive Pitches for Different Levels , Starting Pitch , Advancing Pitch , Sample Headcount Plan for Advancing a FinOps Team , Pitching the Executive Sponsor , Playing to Your Audience, Key Personas That the Driver Must Influence , CEO Persona , CTO/CIO Persona , CFO Persona , Engineering Lead Persona , Roadmap for Getting Adoption of FinOps - Stage 1: Planning for FinOps in an Organization , Stage 2: Socializing FinOps for Adoption in an Organization , Stage 3: Preparing the Organization for FinOps , Type of Alignment to the Organization , Full Time, Part Time, Borrowed Time: A Note on Resources, A Complex System Designed from Scratch Never Works , **The FinOps Foundation Framework**- An Operating Model for Your Practice , The Framework Model - Principles , Personas , Maturity , Phases , Domains and Capabilities - Structure of a Domain , Structure of Capabilities , Adapting the Framework to Fit Your Needs , Connection to Other Frameworks/Models .<br>**b. The UI of FinOps**-Build Versus Buy Versus Native- When to Use Native Tooling, When to Build, Why to Buy, Operationalized Reporting, Data Quality, Perfect Is the Enemy of Good, Report Tiering, Rolling Out Changes, The Universal Report, Accessibility, Color, Visual Hierarchy, Usability and Consistency, Language, Consistency of Color and Visual Representation ,Recognition Versus Recall, Psychological Concepts ,Anchoring Bias ,Confirmation Bias , The Von Restorff Effect , Hick's Law , Perspectives on Reports -Personas Maturity Multicloud , Putting Data in the Path of Each Persona - Data in the Path of Finance , Data in the Path of Leadership , Data in the Path of Engineers ,Connecting FinOps to the Rest of the Business Seek First to Understand, **The FinOps Lifecycle**- The Six Principles of FinOps -#1: Teams Need to Collaborate, #2: Decisions Are Driven by the Business Value of Cloud, #3: Everyone Takes Ownership of Their Cloud Usage, #4: FinOps Reports Should Be Accessible and Timely, #5: A Centralized Team Drives FinOps, #6: Take Advantage of the Variable Cost Model of the Cloud. The FinOps Lifecycle-Inform, Optimize, Operate. Considerations, Where Do You Start? You Don't Have to Find All the Answers.<br>**c. The FinOps Lifecycle**- The Six Principles of FinOps -#1: Teams Need to Collaborate, #2: Decisions Are Driven by the Business Value of Cloud, #3: Everyone Takes Ownership of Their Cloud Usage, #4: FinOps Reports Should Be Accessible and Timely, #5: A Centralized Team Drives FinOps, #6: Take Advantage of the Variable Cost Model of the Cloud. The FinOps Lifecycle-Inform, Optimize, Operate. Considerations, Where Do You Start? You Don't Have to Find All the Answers. Inform Phase: Where Are You Right Now-Data Is Meaningless Without Context, Seek First to Understand, Organizational Work During This Phase, Transparency and the Feedback Loop, Benchmarking Team Performance, What Great Looks Like. Allocation: No Dollar Left Behind- Why Allocation Matters, Amortization: It's Accrual World, Creating Goodwill and Auditability with Accounting, The "Spend Panic" Tipping Point, Spreading Out Shared Costs, Chargeback Versus Showback, A Combination of Models Fit for Purpose, Accounts, Tagging, Account Organization Hierarchies, The Showback Model in Action, Chargeback and Showback Considerations. **Tags, Labels, and Accounts**, - Tag- and Hierarchy-Based Approaches , Getting Started with Your Strategy , Communicate Your Plan , Keep It Simple , Formulate Your Questions , Comparing the Allocation Options of the Big Three , Comparing Accounts and Folders Versus Tags and Labels , Organizing Accounts and Projects into Groups , Tags and Labels: The Most Flexible Allocation Option , Using Tags for Billing , Getting Started Early with Tagging | 15 Hrs<br>[OC2, OC3] |

| | |
|---|---|
| , Deciding When to Set Your Tagging Standard , Picking the Right Number of Tags , Working Within Tag/Label Restrictions, Maintaining Tag Hygiene , Reporting on Tag Performance , Getting Teams to Implement Tags , Accurate Forecasting- The State of Cloud Forecasting, Forecasting Methodologies, Forecasting Models, Cloud Forecasting Challenges, Manual Versus Automated Forecasts, Inaccuracies, Granularity, Forecast Frequency, Communication, Future Projects, Cost Estimation, Impacts of Cost Optimization on Forecasts, Forecast and Budgeting, The Importance of Managing Teams to Budgets. | |
| **MODULE II :** | **(2 CREDITS)** |
| **Unit 3:**<br>**a. Optimize Phase**: Adjusting to Hit Goals- Why Do You Set Goals? , The First Goal Is Good Cost Allocation ,Is Savings the Goal? , The Iron Triangle: Good, Fast, Cheap ,Hitting Goals with OKRs -OKR Focus Area #1: Credibility ,OKR Focus Area #2: Maintainable ,OKR Focus Area #3: Control ,Goals as Target Lines ,Budget Variances ,Using Less Versus Paying Less .Using Less: Usage Optimization-The Cold Reality of Cloud Consumption, Where Does Waste Come from? ,Usage Reduction by Removing/Moving ,Usage Reduction by Resizing (Rightsizing) ,Common Rightsizing Mistakes ,Relying on Recommendations That Use Only Averages or Peaks ,Failing to Rightsized Beyond Compute ,Not Addressing Your Resource "Shape" ,Not Simulating Performance Before Rightsizing ,Hesitating Due to Reserved Instance Uncertainty ,Going Beyond Compute: Tips to Control Cloud Costs, Block Storage ,Object Storage, Networking ,Usage Reduction by Redesigning ,Scaling ,Scheduled Operations ,Effects on Reserved Instances ,Benefit Versus Effort ,Serverless Computing ,Not All Waste Is Waste ,Maturing Usage Optimization ,Advanced Workflow: Automated Opt-Out Rightsizing, Tracking Savings. Paying Less: Rate Optimization-Compute Pricing, On-Demand/Pay-As-You-Go, Spot Resource Usage, Commitment-Based Discounts, Storage Pricing, Volume/Tiered Discounts, Usage-Based, Time-Based, Negotiated Rates, Custom Pricing, Seller Private Offers, BYOL Considerations.<br>**b. Understanding Commitment-Based Discounts**-Introduction to Commitment-Based Discounts, Commitment-Based Discount Basics ,Compute Instance Size Flexibility, Conversions and Cancellations ,Overview of Usage Commitments Offered by the Big Three ,Amazon Web Services ,What Does an RI Provide?,AWS Commitment Models,AWS Reserved Instance ,Member Account Affinity .Standard Versus Convertible RIs ,Instance Size Flexibility ,AWS Savings Plans ,Savings Bundles ,Microsoft Azure ,Azure Reservations ,Instance Size Flexibility, Azure Savings Plans ,Google Cloud ,Google Committed Use Discounts ,Paying for Cores, Not Hours, in Google ,Google Billing and Sharing CUDs ,Google Billing Account and Ownership ,Applying Google CUDs in a Project ,Google Flexible Committed Use Discounts.<br>**c. Building a Commitment-Based Discount Strategy**- Common Mistakes ,Steps to Building a Commitment-Based Discount Strategy ,Step 1: Learn the Fundamentals of Each Program ,Step 2: Understand Your Level of Commitment to Your Cloud Service Provider ,Step 3: Build a Repeatable Commitment-Based Discount Process ,Step 4: Purchase Regularly and Often, Step 5: Measure and Iterate ,Step 6: Allocate Up-Front Commitment Costs Appropriately ,How to Manage the Commitment Strategy ,Purchasing Commitments Just-in-Time ,When to Rightsize Versus Commit ,The Zone Approach ,Who Pays for Commitments? , Strategy Tips . | 15 Hrs<br>[OC4, OC,<br>] |
| | |
| **Unit 4:**<br>a. **Sustainability: FinOps Partnering with GreenOps**-What Are Cloud Carbon Emissions? Scope 1, 2, and 3 Emissions Are Cloud Providers Green? -Access, Completeness, Granularity, Partnering with Engineers on Sustainability, FinOps and GreenOps Better Together? GreenOps Remediations, Avoid FinOps Working Against GreenOps. Operate: Aligning Teams to Business Goals- Achieving Goals, Staffing and Augmenting Your FinOps Team, Processes, Onboarding, Responsibility, Visibility, | 15 Hrs<br>[OC5, OC6,] |

| | |
|---|---|
| Action, How Do Responsibilities Help Culture? Carrot Versus Stick Approach, Handling Inaction, Putting Operate into Action.<br>**Automating Cost Management**-What Is the Outcome You Want to Achieve? Automated Versus Manual Tasks, Automation Tools, Costs, Other Considerations, Tooling Deployment Options, Automation Working, Together, Integration, Automation Conflict, Safety and Security, how to Start, what to Automate, Tag Governance, Scheduled Resource Start/Stop, Usage Reduction. Metric-Driven Cost Optimization-Core Principles, Automated Measurement, Targets, Achievable Goals, Data Driven, Metric-Driven Versus Cadence-Driven Processes, Setting Targets, Taking Action, Bring It All Together,<br>b. **FinOps for the Container World**-Containers 101, The Move to Container Orchestration, The Container FinOps Lifecycle, Container Inform Phase, Cost Allocation, Container Proportions, Tags, Labels, and Namespaces, Container Optimize Phase ,Cluster Placement ,Container Usage Optimization ,Server Instance Rate Optimization ,Container Operate Phase ,Serverless Containers . Partnering with Engineers to Enable FinOps-Integrating Us with Them, What's on the Mind of the Engineer? ,Constraints and the Solving of Hard Problems ,Principles for Enabling Cost-Efficient Engineering -#1: Maximize Value Rather Than Reduce Cost ,#2: Remember That We Are on the Same Team ,#3: Prioritize Improving Communication ,#4: Introduce Financial Constraints Early in the Product Development ,#5: Enablement, Not Control ,#6: Leadership Support Isn't Helpful, It Is Essential ,Data in the Path of the Engineer ,Models for Partnering with Engineering Teams ,Direct Contribution ,Indirect Collaboration ,Indirect Collaboration with Targeted Contribution . Connectivity to Other Frameworks-Total Cost of Ownership, working with Other Methodologies and Frameworks, Find Out Who's Out There, Make Friends and Share Goals, Share Influence, Terminology, and Processes, Share Infrastructure, Share Knowledge. FinOps Nirvana: Data-Driven Decision Making-Unit Economics and Metrics -Unit Economics Don't Have to Be About Revenue, Calculating Unit Economic Metrics, Spending Is Fine, Wasting Is Not, Activity-Based Costing, Coming Back to the Iron Triangle, What's Missing from the Equation? When Have You Won at FinO**ps?** | |

**References:**

| Sr. No. | Title | Author/s | Publisher | Edition | Year |
|---|---|---|---|---|---|
| | The Economics of Cloud Computing | Bill Williams | Cisco Press | | 2012 |
| 0. | Cloud FinOps Collaborative, Real-Time Cloud Value Decision Making | J.R. Storment and Mike Fuller | O'Reilly Media, Inc | Second | 2023 |
| 0. | Efficient Cloud FinOps: A Practical Guide to Cloud Financial Management and Optimization with AWS, Azure, and GCP | Alfonso San Miguel Sánchez and Danny Obando García | Packt Publishing | | 2024 |
| 0. | Measuring the Business Value of Cloud Computing (Palgrave Studies in Digital Business & Enabling Technologies) | Theo Lynn, John G. Mooney, Pierangelo Rosati, Grace Fox | Springer Nature Switzerland AG | First | 2020 |
| 0. | | | | | |

**Course Outcomes(OCs)**

Upon completing this course, students will gain:

OC1: A comprehensive understanding of cloud computing, its service and deployment models, and key metrics for evaluating cloud economics.

OC2: Insights into the principles and practices of FinOps, including data-driven decision-making, cost

optimization, and organizational alignment.

OC3: Practical knowledge on adopting and implementing FinOps within an organization, focusing on executive pitching, cultural shifts, and framework application.

OC4Skills to optimize cloud usage and spending through effective goal setting, usage, and rate optimization strategies.

OC5: Awareness of sustainability in cloud operations and the integration of FinOps with GreenOps for environmentally friendly practices.

OC6: Proficiency in automating cost management processes and applying FinOps principles in containerized environments, fostering collaboration between engineering and finance teams for optimized cloud spending.

## Programme Name: M.Sc. (IT-Security)

| | |
|---|---|
| **Course Code:** (606c) [Elective]<br>**Total Credits:** 04 (60 Lecture Hrs)<br>**University assessment:** 50 marks | **Course Name:** BioMedical Image Processing (Theory)<br>**Total Marks:** 100 marks<br>**College/Department assessment:** 50 marks |

**Pre requisite:**

1. Sound Knowledge fundament concept of Digital Image Processing
2. Sound knowledge of concepts in probability, statistics & mathematics
3. Sound knowledge of Machine Learning and Deep Learning techniques

**Course Objectives (COs)**

To enable the students to:

CO1: Gain in-depth knowledge of medical image analysis techniques.

C02: Understand various machine learning and deep learning models used in healthcare applications.

CO3: Develop skills in signal processing, image processing, and data analysis.

CO4: Learn to apply advanced algorithms for disease detection and diagnosis.

CO5: Enhance problem-solving abilities and critical thinking skills in the context of healthcare and medical imaging.

CO6: Explore future research directions and potential applications in the field of medical image analysis.

| **MODULE I:** | **(2 CREDITS)** |
|---|---|
| **Unit 1: Introduction to Medical Image Analysis, Image Denosing Technique**<br>**a. An Introduction to Medical Image Analysis in 3D**: Introduction, Comparison Between 2D and 3D Techniques in Medical Imaging, Importance of 3D Medical Image, Medical Imaging Types and Modalities, Computer Vision System Works in 3D Image Analysis, Various Techniques in 3D Image Processing in Medical Imaging, Types of Medical Imaging Compressed by 3D Medical Visualization ,3D Ultrasound Shortens. The Imaging Development Conclusion<br>**b. Automated Epilepsy Seizure Detection from EEG Signals Using Deep CNN Model**: Introduction **Materials and Methodology** – Dataset, Normalization, Convolution Neural Network (CNN). **Result and Discussions** - Experiment 1: 10-Fold Cross Validation on 90:10 Ratio, Experiment 2: Training and Testing Ratio Variation, Conclusion<br>**c. Medical Image De-Noising Using Combined Bayes Shrink and Total Variation Techniques**: Introduction, Literature Review, **Theoretical Analysis**- Median Modified Wiener Filter, Wavelet Transform, Dual Tree Complex Wavelet Transform, Sure Shrink, Bayes Shrink, Neigh Shrink, DTCWT Based De-Noising Using Adaptive Thresholding. Total Variation Technique. Pixel Level DTCWT Image Fusion Technique. **Performance Evaluation Parameters** - Peak Signal to Noise Ratio, Structural Similarity Index Matrix. Methodology, Results and Discussion, Conclusions and Future Scope | 15 Hrs [OC1, OC2,OC 11 OC12] |
| | |
| **Unit 2: Medical Image Diagnosis, Medical Image Fusion and Medical Image Applications**<br>a. **Detection of Nodule and Lung Segmentation Using Local Gabor XOR Pattern in CT Images**: Introduction, Histories, Concepts. Causes **for Lung Cancer**- Smoking, Familial Predisposition Lung Diseases, Prior Tale Containing Stroke Cancer, Air Pollution, Exposure as Far as Engine Exhaust, Types Containing Tumour, Signs and Symptoms of Lung Cancer. **Solution Methodology with Mathematical Formulations** - Feature Extraction**,** Modified Area Starting to Be Algorithm**,** Gridding**,** Selection of Seed Point**.** Morphological Operation**, Conclusions** and Future Work<br>b. **Medical Image Fusion Using Adaptive Neuro Fuzzy Inference System**: Introduction **Overview**-Digital Image, Types of Digital Images -Binary Images, Grayscale Image, Color Image. **Medical Imaging Type** - CT Images, MRI Image. **Image Fusion** -Some Meanings of Fusion, Applications of Image Fusion, Medical Image Fusion. Literature | 15 Hrs [OC3**,** OC4, OC5, OC 11 OC12] |

| | |
|---|---|
| Survey -A Brief History about Literature Survey. **Solution Methodology** -Fuzzy Logic, Fuzzy Set, Membership Functions, Fuzzy Inference System. **Proposed Methodology** - Applying to ANFIS, ANFIS Rule, RULES: Merge Color Channel, **Result and Discussion** - Simulation Result, Performance Analysis. Conclusion and Future Scope, Future Scope<br>c. **Medical Imaging in Healthcare Applications**: Introduction **Image Modalities** - PET Scan, Ultrasound, MRI Scan, CT Scan. Recent Trends in Healthcare Technology, Scope for Future Work, Conclusions **Classification of Diabetic Retinopathy by Applying an Ensemble of Architectures**: **Introduction** - Literature Survey. **Method and Data** - Dataset Used, Augmentation of Dataset, Partition of Dataset, Evaluation Metrics, Method. Results. Conclusion | |
| **MODULE II :** | **(2 CREDITS)** |
| **Unit 3: Compression and decompression techniques, different machine learning technique for detection of various diseases .**<br>**a. Compression of Clinical Images Using Different Wavelet Function**: Introduction: Background and Need of Compression, Terminology Utilized for Implementation. **Proposed Algorithm** -Calculation for Picture Compression Utilizing Wavelet Input Image Compression Decompression and Filters Compression Image Reconstruction, Performance Analysis **Implementation and Result**- Analysis of CT Scan Images Wavelet Haar Function Is Used. Conclusion<br>**b. PSO-Based Optimized Machine Learning Algorithms for the Prediction of Alzheimer's Disease**: Introduction, **Related Work**- Material and Methods. Proposed Workflow Database Data Pre-processing. **Particle Swarm Optimization (PSO) Techniques** - Machine Learning Models Experimental Results, Discussion, Conclusion<br>**c. Parkinson's Disease Detection Using Voice Measurements**: Introduction. **Literature Survey** - Parkinson's Syndromes**,** Symptoms**,** Causes**,** Threat Causes**,** Complications**. Methodologies Used in Present Work** - Machine Learning (ML) and Artificial Intelligence (AI)**,** Ensemble Learning**,** Advantages**,** Data Drive Machine Learning**,** Architecture. Proposed System **Testing**- Type of Testing**,** Integration Testing**,** Functional Testing**, Conclusion** and Future Enhancements | 15 Hrs [**OC6,** OC7, OC8, OC 11 OC12] |
| | |
| **Unit 4: Different machine learning technique for Speech Impairment, Lung and Nodule.**<br>**a. Speech Impairment Using Hybrid Model of Machine Learning**: Introduction, Types **of Classifier**, Naive Bayes (Classifier), Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Decision Tree Random Forest, XGBoost, Extra Trees. Related Work. Proposed Work, Results and Discussions, Conclusion<br>**b. Advanced Ensemble Machine Learning Model for Balanced BioAssays:** Introduction, Related Work, Proposed Work, Ensemble Classification. **Experimental Investigation**- Dataset Report, Experimental Setting, **Results** - Assessment of Results, Assessment of the Model on the Dataset. Conclusion<br>**c. Lung Segmentation and Nodule Detection in 3D Medical Images Using Convolution Neural Network:** Introduction, Review of Literature **Rationale of the Study** - Morphological Processing of the Digital Image, Objectives of Study **Proposed Methodology** -Evaluation Results for Medical Image Handling, False Positive Rate (FPR), False Negative Rate (FNR), Sensitivity, Specificity, Accuracy, Expected Outcome of Research Work, Conclusion and Future work | 15 Hrs [**OC9,** OC10, OC 11 OC12] |

**References:**

| Sr. No. | Title | Author/s | Publisher | Edition | Year |
|---|---|---|---|---|---|
| | Artificial Intelligence and Machine Learning in 2D/3D Medical | Rohit Raja, Sandeep Kumar, Shilpa Rani, and K. Ramya Laxmi | CRC Press | First | 2021 |

| | | | | | |
|---|---|---|---|---|---|
| | Image Processing | | | | |
| 1. | Biomedical Signal and Image Processing with Artiϐicial Intelligence | Chirag Paunwala, Mita Paunwala, Rahul Kher, Falgun Thakkar, Heena Kher, Mohammed Atiquzzaman and Norliza Mohd. Noor | EAI/Springer Innovations in Communication and Computing | | 2023 |
| 1. | Digital Image Processing for Medical Applications | G. Dougherty | Cambridge University Press | | 2009 |
| 1. | Medical Image Analysis | Atam P. Dhawan | John Wiley & Sons, Inc | Second | 2011 |

**Course Outcomes(OCs)**

Upon completing this course, students will:

**OC1: Understand 3D Medical Image Analysis**: Learn the differences between 2D and 3D techniques, the importance of 3D medical imaging, and various processing techniques.

**OC2: Develop Skills in Deep Learning**: Gain proficiency in using Deep Convolutional Neural Networks (CNN) for automated epilepsy seizure detection and medical image de-noising.

**OC3: Learn Image Processing Techniques**: Acquire knowledge in nodule detection, lung segmentation, and medical image fusion using advanced methods like Gabor XOR pattern and Adaptive Neuro Fuzzy Inference System (ANFIS).

**OC4: Enhance Knowledge in Healthcare Applications**: Understand the application of medical imaging in healthcare, recent trends, and the classification of diabetic retinopathy using ensemble architectures.

**OC5: Master Compression Techniques**: Learn about compression of clinical images using different wavelet functions and its implementation for CT scan images.

**OC6: Explore Predictive Models**: Gain insights into the prediction of Alzheimer's disease using PSO-based optimized machine learning algorithms and Parkinson's disease detection using voice measurements.

**OC7: Develop Machine Learning Skills**: Acquire skills in classifier models (e.g., Naive Bayes, SVM, KNN) for speech impairment detection and ensemble classification for balanced bioassays.

**OC8: Gain Practical Experience**: Apply learned concepts through methodologies, experimental results, and discussions in various medical imaging and disease detection scenarios.

**OC9: Analyze Performance Metrics**: Evaluate performance using metrics like Peak Signal to Noise Ratio, Structural Similarity Index Matrix, False Positive Rate (FPR), False Negative Rate (FNR), Sensitivity, Specificity, and Accuracy.

**OC10: Explore Future Scope**: Understand the future scope and potential enhancements in medical image analysis, disease detection, and healthcare applications.

**OC11: Develop Critical Thinking**: Enhance problem-solving abilities and critical thinking skills in the context of medical imaging and healthcare technology.

**OC11: Prepare for Research and Innovation**: Be prepared for further research and innovation in the field of medical image analysis, machine learning, and healthcare technology.

# Sem-IV

## Programme Name: M.Sc. (IT-Security)

| | |
|---|---|
| **Course Code:** 611 [Mandatory]<br>**Total Credits:** 04 (60 Lecture Hrs)<br>**University assessment:** 50 marks | **Course Name:** Cyber Forensics (Theory)<br>**Total Marks:** 100 marks<br>**College/Department assessment:** 50 marks |

**Prerequisite:**
A basic understanding of the following concepts would be beneficial:

1. Computer Fundamentals
2. Basics of Networking
3. Fundamentals of Operating Systems
4. Cryptography & Hashing Techniques

**Course Objectives (COs)**
To enable the students to:

CO 1 : Understand the basics of cyber forensics and its procedures.
CO 2 : Examine the different file system and its structure.
CO 3 : Discuss principles & various tools of file carving.
CO 4 : Introduces file signature searching forensics and keyword forensics.
CO 5 : Discusses data hiding fundamentals and detection methods.
CO 6 : Gains knowledge on various advanced forensics analysis techniques like timeline analysis, log analytics.
CO 7 : Examine Android, GPS & SIM card Forensics.
CO 8 : Understand malware analysis & ransomware analysis
CO 9 : Gain knowledge of image forgery detection, steganography & steganalysis.

| **MODULE I: Basics of Cyber Forensics & Digital Evidence Capturing** | **(2 CREDITS)** |
|---|---|
| **Unit 1: Introduction to Cyber Forensics & File Systems**<br>a. **Introduction to Computer/Cyber Forensics**: History, Challenges and Risks, Introduction to computer forensics and its importances, Digital Evidence, Computer Forensics Procedures and techniques, types of computer forensics.<br>b. **Building a Forensics Workstation**: The Sleuth Kit and Autopsy Forensic Browser, Virtualization, Building Up Forensics Workstation with Kali Linux.<br>c. **Volume Analysis**: Hard Disk Geometry & Disk Partitioning, Volume Analysis.<br>d. **Examining FAT File System**: File System Overview, FAT File Systems.<br>e. **Deleted File Recovery in FAT**: Principles of File Recovery, File Creation and Deletion in FAT File System. | 15 Hrs [OC1, OC2, OC3] |
| **Unit 2: File Systems & Digital Evidence Capturing**<br>a. **Examining the NTFS File System**: New Technology File System, The Master File Table, NTFS Indexing, NTFS Advanced Features.<br>b. **Deleted File Recovery in NTFS**: File Creation & Deletion in NTFS File Systems, Deleted File Recovery in NTFS File System.<br>c. **File Carving**: Principles of File Carving, File Carving Tools – Foremost, Scalpel, TestDisk and Photorec.<br>d. **File Signature searching forensics**: Introduction, File Signature Search Process, File Signature Search using hfind.<br>e. **Keyword Forensics**: Forensic Keyword Searching Process, Grep and Regular Expressions, Case Study. | 15 Hrs [OC3, OC4, OC5] |
| **MODULE II : Cyber Forensics Analysis and Advanced Topics** | **(2 CREDITS)** |
| **Unit 3: Cyber Forensic Analysis**<br>a. **Timeline Analysis**: Principle of Timeline Analysis, Timeline Analysis Process, Forensic Timeline Analysis Tools, Case Study.<br>b. **Data Hiding & Detection**: Data Hiding Fundamentals, Data Hiding and Detection Office Open XML Documents.<br>c. **Log Analysis**: System Log Analysis, Security Information and Event Management | 15 Hrs [OC6, OC7, OC8, OC9] |

| | |
|---|---|
| Systems, Implementing SIEMS.<br>d. **Android Forensics**: Mobile Phones Fundamentals, Mobile Device Forensic Investigation.<br>e. **GPS Forensics**: The GPS System, GPS Evidentiary Data, Case Study. | |
| **Unit 4: Advanced Cyber Forensics**<br>a. **SIM Cards Forensics**: The Subscriber Identification Module, SIM Architecture, Security, Evidence Extraction, Case Study.<br>b. **Introduction to Malware Analysis**: Malware, viruses, worms, Essential Skills and Tools for Malware Analysis, List of Malware Analysis Tools and Techniques, Case Study.<br>c. **Ransomware Analysis**: Patterns of Ransonware, Notorious Ransomware, Cryptographic and Privacy-Enhancing Techniques as Malware Tools, Case Study.<br>d. **Image Forgery Detection**: Digital Image Processing Fundamentals, Image Forgery Detection.<br>e. **Steganography and Steganalysis**: Steganography and Steganalysis Basis, Steganography Techniques and Steganography Tools, Steganalytic Techniques and Steganalytic Tools. | 15 Hrs [OC9,OC10, OC11] |

**References:**

| Sr. No. | Title | Author/s | Publisher | Edition | Year |
|---|---|---|---|---|---|
| 1. | Introductory Computer Forensics: A Hands-on Practical Approach | Xiaodong Lin | Springer | | 2018 |
| 2. | Digital Forensics and Incident Response | Gerard Johansen | Packt | Second | 2020 |
| 3. | Practical Cyber Forensics | Niranjan Reddy | Apress | | 2019 |

**Course Outcomes(OCs)**

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

| | |
|---|---|
| OC 1 | Understand the foundational principles of computer forensics. |
| OC 2 | Set up and configure a forensics workstation using tools. |
| OC 3 | Conduct volume analysis, disk partitioning, and examine file systems. |
| OC 4 | Utilize file carving tools for data recovery. |
| OC 5 | Perform file signature searching and keyword forensics using tool. |
| OC 6 | Analyze timelines of digital events using specialized tools and methodologies. |
| OC 7 | Detect hidden data within various file formats. |
| OC 8 | Analyze system logs and implement Security Information and Event Management Systems (SIEMS). |
| OC 9 | Conduct forensic investigations on mobile devices (Android), GPS data and Sim card. |
| OC 10 | Analyze malware, including viruses, worms, and ransomware, using specialized tools and techniques. |
| OC 11 | Detect image forgeries and employ steganographic techniques for data hiding and detection. |

## Programme Name: M.Sc. (IT-Security)

| | |
|---|---|
| **Course Code:** 612 [Mandatory]<br>**Total Credits:** 02 (60 Lecture Hrs)<br>**University assessment:** 25 marks | **Course Name:** Cyber Forensics Practical<br>**Total Marks:** 50 marks<br>**College/Department assessment:** 25 marks |

**Prerequisite:**
A basic understanding of the following concepts would be beneficial:

1. Computer Fundamentals
2. Basics of Networking
3. Fundamentals of Operating Systems
4. Cryptography & Hashing Techniques

**Course Objectives (COs):**
To enable the students to:
CO1: Understand the importance of creating a forensic image & learn to create a bit-stream copy of a digital device.
CO2: Recover extract deleted & hidden files from a forensic image using data carving techniques.
CO3: Learn how file systems work.
CO4: Examine the Windows Registry to identify user activity, installed software, and other information.
CO5: Learn how to acquire and analyze volatile memory from a computer to identify running processes, loaded drivers, and other information.
CO6: Understand how to perform e-mail forensics, mobile foresnics.
CO7: Examine the internet artifact analysis.
CO8: Gain knowledge of network analysis.
CO9: Learn how to acquire and analyze volatile memory from a computer.

| Prac No | Practical Description | 2 CREDITS (60 hrs) |
|---|---|---|
| 1. | Creating a Forensic Image using tools like FTK Imager, Guymager, dd (command-line tool), etc. Use minimum three tools. | 3 [OC 1] |
| 2. | Use data carving tools like FTK Imager, Autopsy, Scalpel, etc. to recover deleted or hidden data from a digital device. Use minimum three tools. | 6 [OC 2] |
| 3. | File System Analysis using tools like FTK Imager, Autopsy, Scalpel, etc. Use minimum three tools. | 6 [OC 3] |
| 4. | Extract and analysis registry data using tools like FTK Imager, Autopsy, Registry Explorer, etc. Use minimum three tools. | 6 [OC 4] |
| 5. | Perform network forensics using tools like Wireshark, NetworkMiner, tcpdump, etc. Use minimum three tools. | 6 [OC 5] |
| 6. | Study volatile memory from a computer to identify running processes, loaded drivers, and other information using tools like Volatility Framework, FTK Imager, rekall tool, redline, etc. Use minimum three tools. | 6 [OC 6] |
| 7. | Examine email files to identify senders, recipients, attachments, and other information using tools like FTK Imager, EnCase Forensic Toolkit, MailX (command-line tool), etc. Use minimum three tools. | 3 [OC 7] |
| 8. | Study internet artifact analysis to examine web browsing history, chat logs, and other internet artifacts to identify user activity using FTK Imager, EnCase Forensic Toolkit, Firefox Cache Viewer (command-line tool), etc. Use minimum three tools. | 6 [OC 8] |

| | | |
|---|---|---|
| 9. | Understand how to extract and analyze data from mobile devices using mobile forensics tools like Cellebrite UFDR, Oxygen Forensic Detective, XRY, Andriller, etc. Use minimum three tools. | 6 [OC 9] |
| 10. | Study malware behaviour and classification using tools like IDA Pro, Ghidra, Cuckoo Sandbox, etc. Use minimum three tools. | 6 [OC 10] |
| 11. | Using tools like Test Disk, Recuva, PhotoRec, etc. recover the deleted or corrupted files from storage media. Use minimum three tools. | 6 [OC 11] |

**References:**

| Sr. No. | Title | Author/s | Publisher | Edition | Year |
|---|---|---|---|---|---|
| 1. | Introductory Computer Forensics: A Hands-on Practical Approach | Xiaodong Lin | Springer | | 2018 |
| 2. | Digital Forensics and Incident Response | Gerard Johansen | Packt | Second | 2020 |
| 3. | Practical Cyber Forensics | Niranjan Reddy | Apress | | 2019 |

**Course Outcomes(OCs)**

Upon completing this course, the student will be able to:

| | |
|---|---|
| OC 1 | Create a forensic image of a storage device using a forensic imaging tool. They will understand the importance of using a write-blocker to prevent data from being overwritten. |
| OC 2 | Identify file signatures for various file types & utilize data carving tools to scan a forensic image for specific file signatures. |
| OC 3 | Describe the structure of common file systems & use Autopsy, FTK Investigator, or Scalpel to carve deleted files from a forensic image. |
| OC 4 | Explain the function of the Windows Registry & extract the relevant information using tools. |
| OC 5 | Use different network analysis tools to capture network capture & identifying compromised devices. |
| OC 6 | Explain the concept of memory forensics and its importance in digital investigations. |
| OC 7 | Use forensic tools to examine email files and identify information about senders, recipients, attachments, and the content of emails. |
| OC 8 | Examine internet artifacts and identify user activity, such as websites visited, searches conducted, and online chats. |
| OC 9 | Acquire data from mobile devices and analyze the data to identify contacts, call logs, text messages, photos, videos, and other information. |
| OC 10 | Identifying potential malware characteristics using static and dynamic analysis techniques. |
| OC 11 | Use different data recovery tools for recovery of deleted files, uncovering hidden information & preserving lost data. |

| | |
|---|---|
| **Course Code:** (615a) [Elective]<br>**Total Credits:** 02 (30 Lecture Hrs)<br>**University assessment:** 25 marks | **Course Name:** Security Operations Centre (Theory)<br>**Total Marks:** 50 marks<br>**College/Department assessment:** 25 marks |

## Programme Name: M.Sc. (IT-Security)

| | |
|---|---|
| **Course Code:** (615a) [Elective]<br>**Total Credits:** 04 (60 Lecture Hrs)<br>**University assessment:** 50 marks | **Course Name:** Augmented Reality & Virtual Reality (Theory)<br>**Total Marks:** 100 marks<br>**College/Department assessment:** 50 marks |

**Pre requisite: Nil**

**Course Objectives (COs)**

To enable the students to:

CO1: To learn background of VR including a brief history of VR, different forms of VR and related technologies, and broad overview of some of the most important concepts

CO2: To provide background in perception to educate VR creators on concepts and theories of how we perceive and interact with the world around us

CO3: To make learner aware of high-level concepts for designing/building assets and how subtle design choices can influence user behavior

CO4: To learn about art for VR and AR should be optimized for spatial displays with spatially aware input devices to interact with digital objects in true 3D

CO5: Walkthrough of VRTK, an open source project meant to spur on cross-platform development

| **MODULE I:** | **(2 CREDITS)** |
|---|---|
| **Unit 1:** Introduction: What Is Virtual Reality, A History of VR, An Overview of Various Realities, Immersion, Presence, and Reality Trade-Offs, The Basics: Design Guidelines, Objective and Subjective Reality, Perceptual Models and Processes, Perceptual Modalities | 15 Hrs<br>[OC1, OC2] |
| | |
| **Unit 2:** Perception of Space and Time, Perceptual Stability, Attention, and Action, Perception: Design Guidelines, Adverse Health Effects, Motion Sickness, Eye Strain, Seizures, and Aftereffects, Hardware Challenges, Latency, Measuring Sickness, Reducing Adverse Effects, Adverse Health Effects: Design Guidelines | 15 Hrs<br>[OC1, OC3] |
| **MODULE II :** | **(2 CREDITS)** |
| **Unit 3:** Content Creation, Concepts of Content Creation, Environmental Design, Affecting Behavior, Transitioning to VR Content Creation, Content Creation: Design Guidelines, Interaction, Human-Centered Interaction, VR Interaction Concepts, Input Devices, Interaction Patterns and Techniques, Interaction: Design Guidelines | 15 Hrs<br>[OC4, OC5] |
| | |
| **Unit 4:** Virtual Reality Toolkit: Open Source Framework for the Community, Data and Machine Learning Visualization Design and Development in Spatial Computing, Character AI and Behaviors, The Virtual and Augmented Reality Health Technology Ecosystem | 15 Hrs<br>[OC1,OC6] |

**Books and References:**

| Sr. No. | Title | Author/s | Publisher | Edition | Year |
|---|---|---|---|---|---|
| 1. | The VR Book, Human Centered Design for Virtual Reality | Jason Jerald | ACM Books | 1st | 2016 |
| 2. | Creating Augmented and Virtual Realities | Erin Pangilinan, Steve Lukas, Vasanth Mohan | O'Reilly | 1st | 2019 |
| 3. | Virtual reality with VRTK4 | Rakesh Baruah | APress | 1st | 2020 |

**Course Outcomes(OCs)**

1. Understand the basic concepts of Virtual, Augmented & Mixed Reality.
2. Understand the concepts involved in making a VR system
3. Understand the impact that VR systems would have on users
4. Understand the concepts in implement VR systems
5. Use tools to create simple VR applications
6. Understand the different tools available for creating VR applications

**Programme Name: M.Sc. (IT-Security)**

| | |
|---|---|
| **Course Code:** (615b) [Elective]<br>**Total Credits:** 04 (60 Lecture Hrs)<br>**University assessment:** 50 marks | **Course Name:** Digital Image Forensics (Theory)<br>**Total Marks:** 100 marks<br>**College/Department assessment:** 50 marks |

**Prerequisites:**

1. Fundamental knowledge of Digital Image Processing

**Course Objectives:**

- To understand describe the origin of computer forensics and the relationship between law enforcement and industry.
- Describe electronic evidence and the computing investigation process.
- Extracting Digital Evidence from Images and establishing them in court of Law.
- Enhancing images for investigation and various techniques to enhance images.
- Interpret and present Evidences in Court of Law.

| **Details** | **Lectures/Outcomes** |
|---|---|
| **Module I** | |
| **Unit I**<br>a) History of Forensic Digital Enhancement<br>b) Establishing Integrity of Digital Images for Court | **15**<br>**[OC1]** |
| **Unit II**<br>a) Color Modes and Channel Blending to Extract Detail<br>b) Multiple Image Techniques | **15**<br>**[OC2]** |
| **Module II** | |
| **Unit III**<br>a) Fast Fourier Transform: Background Pattern Removal<br>b) Contrast Adjustment Techniques | **15**<br>**[OC3, OC4]** |
| **Unit IV**<br>a) The Approach: Developing Enhancement Strategies for Images Intended for Analysis<br>b) Digital Imaging in the Courts, Interpreting and Presenting Evidence | **15**<br>**[OC4, OC5]** |

**References:**

| Sr. No. | Title | Author/s | Publisher | Edition | Year |
|---|---|---|---|---|---|
| 1. | Forensic Digital Image Processing: Optimization of Impression Evidence | Brian Dalrymple, Jill Smith | CRC Press | | 2018 |

| | | | | | |
|---|---|---|---|---|---|
| 2. | Forensic Uses of Digital Imaging | John C. Russ, Jens Rindel, P. Lord | Taylor & Francis Group | 2nd | 2016 |

**Course Outcomes(OCs):**

**On completion of this course, students will be able to:**

OC1 Relate computer forensics and its relationship between law enforcement and industry.
OC2 Prepare lectronic evidence and the computing investigation process.
OC3 Extract Digital Evidence from Images and establishing them in court of Law.
OC4 Enhance the images for investigation.
Make it available with the report that interprets and presents Evidences in Court of Law.

## Programme Name: M.Sc. (IT-Security)

| | |
|---|---|
| **Course Code:** (615c) [Elective]<br>**Total Credits:** 04 (60 Lecture Hrs)<br>**University assessment:** 50 marks | **Course Name:** Edge Computing (Theory)<br>**Total Marks:** 100 marks<br>**College/Department assessment:** 50 marks |

**Pre requisite:**

1. Sound Knowledge of Cloud Computing, Distributed Computing and Parallel Computing
2. Sound Knowledge of Cryptographic techniques.
3. Fundamental concept of Blockchain, IOT and Artificial Intelligence Techniques

**Course Objectives (COs)**

To enable the students to:

CO1: Gain a comprehensive understanding of computing paradigms, including edge computing and its essentials.
CO2: Learn about edge analytics and its applications in various domains.
CO3: Understand edge data storage security and blockchain integration with edge computing systems.
CO4: Explore real-world use cases and case studies of edge computing.
CO5: Master machine learning techniques for data science applications at the edge.
CO6: Develop insights into security considerations and future trends in edge computing

| **MODULE I:** | **(2 CREDITS)** |
|---|---|
| **Unit 1:**<br>a. **Computing Paradigms** : Introduction to Computing , The Major Impacts of Computing Parallel Computing , Shared Memory Systems , Distributed Memory Systems , Hybrid Model , Distributed Computing ,Cluster Computing High-Performance Clusters , Load Balancing Clusters High-Availability Clusters , Utility Computing , Grid Computing , Cloud Computing , Characteristics of Cloud Environments , Cloud Models , Cloud Services Models , Cloud Deployment Models , Other Computing Paradigms , Ubiquitous Computing ,Jungle Computing , Fog Computing , Osmotic Computing , Research Directions<br>b. **Edge Computing and Its Essentials**: Introduction: Edge Computing Architecture- Edge Devices, Edge Server Cluster, Cloud Server, Background Essentials: IoT Devices - Mobile Phone-Based Sensors, Medical Sensors, Neural Sensors, Environmental and Chemical Sensors, Radio Frequency Identification, Actuators, Networking Architecture, Network Management and Control- Orchestration, Edge Computing State-of-the-Art Interfaces and Devices. Middleware- Hydra, Aura, TinyDB, FiWare, Application Interfaces. Edge Computing Simulators - PureEdgeSim, IoTSim Edge, iFogSim , EdgeCloudSim , Research Directions<br>c. **Edge Analytics**: Types of Data, Data Analytics, Goals of Data Analytics, Domains Benefiting from Big Data Analytics, Real-Time Applications of Data Analytics, Phases of Data Analytics- Data Collection and Pre-Processing, Machine Learning-Model Building, Performance Evaluation, Types of Data Analytics- Descriptive Analytics, Diagnostic Analytics, Predictive Analytics, Prescriptive Analytics. Edge Data Analytics, Potential of Edge Analytics Architecture of Edge Analytics, Machine Learning for Edge Devices. Edge Analytics: Case Study, Research Challenges and Future Research Directions | 15 Hrs [OC1, OC2, OC3] |
| | |
| **Unit 2:**<br>a. **Edge Data Storage Security**: Data Security, Data Confidentiality- Identity-Based Encryption Attribute-Based Encryption, Proxy Re-encryption, Functional Encryption, Honey Encryption, Searchable Encryption. Homomorphic Encryption -Types of Homomorphic Encryption Basic Functions of Homomorphic Encryption. | 15 Hrs [OC4, OC5, OC6] |

| | |
|---|---|
| Authentication, Single-Domain Authentication, Cross-Domain Authentication, Handover Authentication, Privacy-Preserving Schemes, Data Privacy, Location Privacy, Identity Privacy, Edge-Based Attack Detection and Prevention, Conclusions and Future Research Directions<br>b. **Block chain and Edge Computing Systems**: History of Blockchain, Distributed Ledger Technology, Role of P2P Architecture in Blockchain , Blockchain Cryptography , Characteristics of Blockchain , Benefits and Limitations of Blockchain , Types of Blockchain, Blockchain Architecture and Fundamentals , Blockchain behind Bitcoin Network , Transaction Validation , Mining and Block Structure , Consensus Mechanisms , Smart Contracts Blockchain Platforms. , Ethereum Hyperledger ,Polkadot Network ,Edge Computing with Blockchain ,Internet of Things and Blockchain ,System Design, Case Studies , Research Challenges and Future Research Directions<br>c. **Edge Computing Use Cases and Case Studies** : Use Cases Edge Computing High-Potential, Gaming ,Content Delivery , Financial Sector , Augmented Reality , Healthcare Sector , Realization of Edge Computing in Healthcare Ensuring, Storage Security - Devices and Setup Case Study I: Pulse Oximeter to Detect ARD in Edge Serve , Pulse Oximetry ,Oxygen Delivery (DO2 Oxygen Consumption (VO2) , Acute Respiratory Distress Syndrome , Analysis in Edge Server , Case Study II: Blood Pressure Monitor to Predict Hypotension in Edge Server Mean Arterial Pressure , Edge Server Analysis on MAP , Case Study III: Body Composition Scale to Detect Heat Index in Edge Server Heat Index , Heat Index Analysis in Edge Server Use Case - Edge Computing/Analytics in Industrial , IOT , Conclusions and Open Research Challenges | |
| **MODULE II :** | **(2 CREDITS)** |
| **Unit 3:**<br>a. **Edge Computing Use Case Examples**: Problems Resolved by Edge Computing, Use Case: IOT Gateway, Use Case: Smart City Surveillance, Use Case: Vehicle Telematics, Use Case: Video Streaming Services. Edge systems componentry: Hardware Architecture, Different Classes of Edge, Everything Connected Through Embedded Systems. Communication Hardware - SCADA, Networking Topologies, Personal Area Networks, Local Area Networks, Wide Area Networks<br>b. **Software and system frameworks**: Typical Edge Functions and Services - Security and Hardening Remote Management and Monitoring, Interconnectivity and Networking, Software Provisioning and Upgradability, Reliability and Robustness, Operating System. Software Architecture. Frameworks - EdgeX Foundry, Microsoft Azure IOT Edge. Digital Twins, The Fog and The Mist, System Architecture – One Architecture to Rule Them All, Probably Not. Connecting things (networking and communications): A Typical Edge System in Your Home, Communication Systems Differences, Radio Spectrum Near Range Communication (PAN)- Bluetooth, NFC and RFI, Meshes (Zigbee PAN). Near Range Communication Use Cases. Long Range Communication- 5G and Cellular LoRaWAN, Satellite Communication<br>c. **Edge protocols:** The language of Edge machines: Network Layering and the Basics of the OSI Model, Diving Deep into TCP/IP Networking], Industrial IOT Communications, The Language of Factory Machines, Message-Orientated, Stream-Orientated, and RESTful Protocols, The Most Prevalent Edge Communication Standard: MQTT, Alternative protocols: CoAP and AMPQ, Protocol Comparison | 15 Hrs [OC6, OC7, OC8] |
| | |
| **Unit 4: Machine Learning for Data Science**<br>a. **Making the Edge work through AI:** The Purpose for Clouds with Edge Computing, Work on the Cloud and the Edge, Edge Workloads - Edge Patterns. Example Workload Organization - Situational Awareness Applications, Machine Learning for the Edge, Rules and Decision Systems, Time-Series Analysis, Proportional Integral Derivative Controllers, Probabilistic Analysis System, Deep Learning Models, Federated Machine Learning, Training in the Cloud, Inference at the Edge, Proper Use of Machine Learning | 15 Hrs [OC9, OC10 OC11] |

| | |
|---|---|
| b. **Security at the Edge:** Types of Security Vulnerabilities, The Most Pervasive Internet Hack: Mirai - Mirai, Grand Theft Auto, Credit Card Fraud: Through the HVAC Supplier, Security Architecture, Hardware Security, Software Security, Communications and Network Security, Physical Security, Final Thoughts on Security<br>c. **Edge computing futures and predictions:** Capitalizing on Edge Computing, Regulations and Standards for IOT and Edge Computing, Future of Edge Computing-Pervasive Edge Computing, Smart Concrete, AR/VR, Immersive Interactions and Synthetic Sensing, Devices that Understand You, Industrial and Systems Control, Innovation in Sensors and Electronics, Batteries and Energy Harvesting, MECs, Democratized Communication Systems, Video Gaming and Entertainment | |

**References:**

| Sr. No. | Title | Author/s | Publisher | Edition | Year |
|---|---|---|---|---|---|
| | EDGE COMPUTING Fundamentals, Advances and Applications | K. Anitha Kumari G. Sudha Sadasivam D. Dharani M. Niranjanamurth | CRC Press | First | 2022 |
| 2. | MEAP Edition Manning Early Access Program Edge Computing A friendly introduction Version 3 | Perry Lea | Manning Publications | Version 3 | 2023 |
| 1. | Fog and Edge Computing Principles and Paradigms | Rajkumar Buyya and Satish Narayana Srirama | John Wiley & Sons, Inc | first | 2019 |
| 2. | Edge Computing: A Primer | Jie Cao Quan Zhang Weisong Shi | Springer | | 2018 |

**Course Outcomes(OCs)**

**Upon completion of this course:**

**OC1: Comprehensive Understanding of Computing Paradigms:** Students will gain a deep understanding of various computing paradigms, including parallel computing, distributed systems, cloud computing, and emerging paradigms like edge, fog, and osmotic computing.

**OC2: Proficiency in Edge Computing Essentials:** Students will become proficient in the fundamentals of edge computing, including its architecture, devices, networking, and middleware. They will also learn about state-of-the-art interfaces, simulators, and future directions in edge computing research.

**OC3: Expertise in Edge Analytics:** Through studying edge analytics, students will learn about different types of data, data analytics goals, and real-time applications. They will gain hands-on experience in data collection, preprocessing, machine learning model building, and performance evaluation for edge devices.

**OC4: Knowledge of Edge Data Storage Security:** Students will understand various aspects of data security in edge computing, including encryption techniques, authentication mechanisms, privacy-preserving schemes, and edge-based attack detection and prevention methods.

**OC5: Understanding of Blockchain Integration with Edge Computing:** Students will explore the history, architecture, and fundamentals of blockchain technology, as well as its integration with edge computing systems. They will learn about blockchain platforms, use cases, and research challenges in the context of edge computing.

**OC6: Ability to Apply Edge Computing in Real-World Scenarios:** Students will analyze and discuss various use cases and case studies where edge computing demonstrates high potential, such as gaming, content delivery,

financial sectors, augmented reality, and healthcare. They will gain insights into realizing edge computing in healthcare and ensuring storage security in edge devices.

**OC7: Understanding the framework of IOT applications, fog computing and communication protocol: Students** completing the software and system frameworks section will understand edge functions, security, networking, and software provisioning. They'll master remote management, familiarize with EdgeX Foundry and Azure IoT Edge, and grasp concepts like digital twins and fog computing. They'll also learn about communication protocols from Bluetooth to 5G

**OC8: Familiarity with Edge Systems Componentry and Protocols:** Students will become familiar with the hardware architecture, communication hardware, and different classes of edge systems. They will also learn about edge protocols, networking topologies, and communication standards for edge devices.

**OC9: Proficiency in Machine Learning for Data Science at the Edge:** Through studying machine learning for data science at the edge, students will gain expertise in various machine learning techniques applicable to edge devices, including time-series analysis, deep learning models, federated machine learning, and proper use of machine learning for inference at the edge.

**OC10: Awareness of Security Considerations at the Edge:** Students will understand different types of security vulnerabilities and security architectures relevant to edge computing. They will learn about hardware security, software security, communication security, and physical security measures to mitigate risks at the edge.

**OC11: Insights into the Future of Edge Computing:** Students will gain insights into the future trends and predictions in edge computing, including pervasive edge computing, smart infrastructure, immersive interactions, innovation in sensors and electronics, and democratized communication systems. They will also understand the regulatory and standardization aspects for IoT and edge computing

## Evaluation Scheme

**Theory courses of 4 credits:** Total marks 100. Out of the total, 50 % each for internal and external evaluation.

**A. Internal Evaluation (30m + 10m + 10m = 50 Marks )**

The internal assessment marks shall be awarded as follows:

1. **30 marks (Any one of the following):**
   a. Written Test of 30 Marks
   b. SWAYAM (Advanced Course) of minimum 20 hours and certification exam completed or
   c. NPTEL (Advanced Course) of minimum 20 hours and certification exam completed or
   d. Valid International Certifications (Prometric, Pearson, Certiport, Coursera, Udemy and the like)
   e. Certification marks of one completed exam shall be awarded to one course only. For four courses, the students will have to complete four certifications.
   (Note: Only those certification/courses suggested by the department shall be deemed valid, Student cannot do any certification on their own)
2. **10 marks**
   10 marks from every course (Two 4 credits mandatory courses, one 2 credits mandatory course, one 4 credits elective course) coming to a total of 40 marks, shall be awarded on publishing of research paper in UGC approved / Other Journal with plagiarism less than 15%. The marks can be awarded as per the impact factor of the journal, quality of the paper, importance of the contents published, social value.
3. **10 marks**
   Open Book examination based on problem solving related to the respective subject.

**i. Suggested format of Question paper of 30 marks for the written test.**

| | | |
|---|---|---|
| Q1. | Attempt *any two* of the following: | 16 marks |
| a. | | |
| b. | | |
| c. | | |
| d. | | |
| | | |
| Q2. | Attempt *any two* of the following: | 14 marks |
| a. | | |
| b. | | |
| c. | | |
| d. | | |

**B. External Examination: (50 marks) Duration : 2 hrs**

| | | |
|---|---|---|
| | All questions are compulsory | |
| Q1 | (Based on all units) Attempt *any two* of the following: | 10 marks |
| a. | Unit 1 | |
| b. | Unit 2 | |
| c. | Unit 3 | |
| d. | Unit 4 | |
| | | |
| Q2 | (Based on Unit 1) Attempt *any two* of the following: | 10 marks |
| Q3 | (Based on Unit 2) Attempt *any two* of the following: | 10 marks |
| Q4 | (Based on Unit 3) Attempt *any two* of the following: | 10 marks |
| Q5 | (Based on Unit 4) Attempt *any two* of the following: | 10 marks |

**Theory courses of 2 credits:** Total marks 50. Out of the total, 50 % each for internal and external evaluation.

**A. Internal Evaluation (25 Marks)**

The internal assessment marks shall be awarded as follows:

1. 10 marks from every course (Two 4 credits mandatory courses, One 2 credits mandatory course, One 4 credits elective course) coming to a total of 40 marks, shall be awarded on publishing of research paper in UGC approved / Other Journal with plagiarism less than 15%. The marks can be awarded as per the impact factor of the journal, quality of the paper, importance of the contents published, social value.
2. 10 marks - Open Book examination based on problem solving related to the respective subject.
3. 5 marks - Assignment/Group discussion.

**B. External Examination: (25 marks) Duration : 1 hr**

| | | |
|---|---|---|
| | All questions are compulsory | |
| Q1 | (Based on Unit 1) Attempt *any two* of the following: | 13 marks |
| Q2 | (Based on Unit 2) Attempt *any two* of the following: | 12 marks |

**Practical courses of 2 credits:** Total marks 50. Out of the total, 50 % each for internal and external evaluation.

**A. Practical Evaluation Internal (25 marks)**

| | | |
|---|---|---|
| 1. | Performance during all practical sessions | 10 |
| 2. | Problem solving with the acquired programming skills | 10 |
| 3. | Viva Voce | 5 |

**B. Practical Evaluation External (25 marks)**

A Certified copy of hard-bound journal is essential to appear for the practical examination.

| | | |
|---|---|---|
| 1. | Practical Question | 15 |
| 2. | Journal | 5 |
| 3. | Viva Voce | 5 |

**Sign of Chairperson**
**Dr. Mrs. R. Srivaramangai**
**Ad-hoc BoS (IT)**

**Sign of the**
**Offg. Associate Dean**
**Dr. Madhav R. Rajwade**
**Faculty of Science & Technology**

**Sign of Offg. Dean**,
**Prof. Shivram S. Garje**
**Faculty of Science & Technology**