M.Sc. Cyber Security

Academic Year: 2025-2027 **Total Credits: 83**

Semester-I						Semester-II					
Code	**Course Name**	**L**	**T**	**P**	**C**	**Code**	**Course Name**	**L**	**T**	**P**	**C**
MAS6119	Mathematical Foundation to Computer Science	3	1	0	4	CAP6207	Network Protection and Cryptographic Techniques	3	1	0	4
CAP6109	Computer Networking Principles and Protocols	3	1	0	4	CAP6208	Automation with Python	3	1	0	4
CAP6110	Cybersecurity: Concepts and Applications	3	1	0	4	CAP6209	Web Application Security	3	1	0	4
CAP6111	Programming & Problem-Solving using C	3	1	0	4	CAP6211	Intrusion Detection Systems	3	1	0	4
CAP6112	OS and Shell Programming	3	1	0	4	CAP62XX	Program Elective-I	3	0	0	3
CAP6135	Cybersecurity: Concepts and Applications Lab	0	0	2	1	CAP6236	Automation with Python Lab	0	0	2	1
CAP6136	Programming & Problem-Solving using C Lab	0	0	2	1	CAP6237	Intrusion Detection Systems Lab	0	0	2	1
CAP6137	OS and Shell Programming Lab	0	0	2	1	CAP6238	Pragmatic Learning	0	0	2	1
Total		**15**	**5**	**6**	**23**	**Total**		**15**	**4**	**6**	**22**
Total contact hours		**26**				**Total contact hours**		**25**			

Semester-III						Semester-IV					
Code	**Course Name**	**L**	**T**	**P**	**C**	**Code**	**Course Name**	**L**	**T**	**P**	**C**
CAP7107	Secure Protocol Design	3	1	0	4	CAP7271	Major Project	0	0	0	16
CAP7108	Ethical Hacking and Penetration Testing	3	1	0	4						
CAP7109	Cyber law and Regulation of Cyberspace	3	1	0	4						
CAP71XX	Program Elective-II	3	0	0	3						
CAP71XX	Program Elective-III	3	0	0	3						
CAP7134	Minor Project	0	0	4	2						
CAP7135	Secure Protocol Design LAB	0	0	2	1						
CAP7136	Ethical Hacking and Penetration Testing Lab	0	0	2	1						

Total		**15**	**3**	**8**	**22**	**Total**		**0**	**0**	**0**	**16**
Total contact hours		**26**				**Total contact hours**		**0**			

Program Electives / Discipline Specific Electives			
Semester-I		**Semester-II**	
Code	**Course Name**	**Code**	**Course Name**
			Peogram Elective - I
		CAP6248	Mobile Computing: Principles And Applications
		CAP6249	IoT Architecture and Protocols
		CAP6250	Cloud Computing: Concepts and Applications
Semester-III		**Semester-IV**	
Code	**Course Name**	**Code**	**Course Name**
	Peogram Elective - II		
CAP7158	Mobile Security		
CAP7159	IoT Security		
CAP7160	Cloud Security		
	Peogram Elective - III		
CAP7161	Blockchain Technology		
CAP7162	Security Operations and Incident Response		
CAP7163	Data Science		

MAS6119: MATHEMATICAL FOUNDATION TO COMPUTER SCIENCE [3 1 0 4]

Posets and Lattices: POSET, Lattices, Distributive and complemented lattices, Boolean Lattice, Uniqueness of Boolean Lattices, Boolean expression & function, Mathematical Logic: Statement and notations, Connectives, Normal forms, Well-formed formulas, Implication, Tautology, Predicate calculus, Graph Theory: Basic Concepts, Introduction Isomorphism, Sub graphs, Walks, Paths, Circuits, Connectedness, Components, Euler graphs,

Hamiltonian paths and circuits. Trees: Trees, Properties of trees, Distance and centers in tree, Rooted and binary trees. Connectivity and Planarity: Connectivity & Planarity, Spanning trees, Fundamental circuits, Spanning trees in a weighted graph, Cut sets, Properties of cut set, All cut sets, Fundamental circuits and cut sets, Connectivity and separability, Network flows. Graph Representations: Isomorphism, Combinational and geometric graphs, Planer graphs, Different representation of a planer graph, Matrices. Coloring and Matching: Coloring, Chromatic number, Chromatic partitioning, Chromatic polynomial, Matching, Covering, Four color problem. Directed Graphs: Directed Graph, Types of directed graphs, Digraphs and binary relations, Directed paths and connectedness, Euler graphs.

Reference Books:

1. C.L. Lui, Elements of Discrete Mathematics, (4e) Houghton Mifflin, 2017
2. N. Deo, Graph Theory: With Application to Engineering and Computer Science, (New Edition) Prentice Hall of India, 2003.
3. R.P. Grimald Discrete and Combinatorial Mathematics: An Applied Introduction, (5e) Addison Wesley, 2003.

CAP6109: COMPUTER NETWORKING PRINCIPLES AND PROTOCOLS [3 1 0 4]

Network introduction: Classful addressing, other issues, Subnetting Classless addressing, variable length blocks, Subnetting, address allocation, Network Address Translation. Encapsulation, operation Data Link Layer: ARP package & RARP- Introduction, packet format Encapsulation, RARP server datagram , fragmentation , options, checksum, Network Layer: IP Package Types of messages, message format, error reporting, Query, Checksum, Debugging tools; Transport Layer: Process to process communication, User datagram, checksum, UDP operation UDP package Introduction, TCP services, TCP features, segment, TCP connection, State transition diagram, Flow control, Error control, Congestion control, TCP timers, options, TCP package; TCP Variants: SCTP services, SCTP features, packet format, association, state transition diagram, flow control, error control, congestion control, TCP RENO, Dynamic routing protocols : RIP,OSCF & BGP; Domain name Space (Application Layer): Name space, distribution of name space, DNS in the internet, resolution, DNS messages, controlling the server, out of band signaling, escape character. Transition from IPv4 to IPv6. Introduction to VLAN concept, Wireless Network protocols: WAP Architecture introduction. Introduction to MANET & VANET

Reference Books:

1. Kurose, J. F., & Ross, K. W. Computer Networking: A Top-Down Approach (8th ed.). Pearson, 2021
2. Tanenbaum, A. S., & Wetherall, D. J. Computer Networks (6th ed.). Pearson, 2021

3. Forouzan, B. A., Data Communications and Networking (6th ed.). McGraw-Hill Education, 2021

CAP6110: CYBERSECURITY: CONCEPTS AND APPLICATIONS [3 1 0 4]

Defining Cyberspace, Concept of cyber security, Issues and challenges of cyber security. Types of Security, Information Classification and their levels, Process for managing classified information, Access Control, Types of Access Control - Preventative access control, Deterrent access control, Detective access control, Corrective access control, Recovery access control, Compensation access control, Directive access control, administrative access controls, Logical/technical access controls, Physical access controls. Cyber Security Goals, Tools for Confidentiality - Encryption, Access control, Authentication, Authorization, Physical Security, Tools for Integrity - Backups, Checksums, Data Correcting Codes, Tools for Availability - Physical Protections, Computational redundancies. Types of Cyber Security Attacks, Web-based Attacks (Injection Attack, DNS Spoofing, Session Hijacking, Phishing, Brute Force, Denial of Service, Distributed Denial of Service, Dictionary Attack, URL Interpretation, File Inclusion Attack, Man in the Middle Attack), System-based Attack (Virus, Worm, Trojan Horse, Backdoors, Bots), Types of Cyber Attackers.

Reference Books:

1. Whitman, M. E., & Mattord, H. J. Principles of Information Security (7th ed.). Cengage Learning 2021.
2. Kim, D., & Solomon, M. G. Fundamentals of Information Systems Security (4th ed.). Jones & Bartlett Learning 2021
3. Stallings, W., & Brown, L. Computer Security: Principles and Practice (5th ed.). Pearson 2022.

CAP6111: PROGRAMMING & PROBLEM-SOLVING USING C [3 1 0 4]

An overview: Algorithms & flowcharts; Characteristics of a good program. Rules/ conventions of coding, documentation, naming variables; Top-down design; Bottom-up design. Fundamentals of C Programming: History of C; Structure of a C Program; Data types; Constant & Variable, naming variables; Operators & expressions; Control Constructs – if-else, for, while, do-while; Case switch statement; Arrays; Formatted & unformatted I/O; Type modifiers & storage classes; Ternary operator; Type conversion & type casting; Priority & associativity of operators. Modular Programming: Functions; Arguments; Return value; Parameter passing – call by value, call by reference; Return statement; Scope, visibility and life-time rules for various types of variables, static variable; Calling a function; Recursion – basics, comparison with iteration, types of recursions, when to avoid recursion, examples. Advanced Programming Techniques: Special constructs – Break, continue, exit(), goto & labels; Pointers - & and * operators, pointer expression, pointer arithmetic, dynamic memory management functions like malloc(), calloc(), free(); String; Pointer v/s array; Pointer to pointer; Array of pointer & its limitation; Function returning pointers; Pointer to function, Function as parameter; Structure – basic, declaration,

membership operator, pointer to structure. Introduction to Data Structures: Contiguous implementations of stack& queues, various operations on stack& queues.

Reference Books:

1. Kernighan, B. W., & Ritchie, D. M. The C programming language (2nd ed.). Prentice Hall 1988.
2. Gustedt, J. Modern C. Manning Publications 2019
3. Kanetkar, Y. P. Let us C (18th ed.). BPB Publications 2023

CAP6112: OS & SHELL PROGRAMMING [3 1 0 4]

Introduction: UNIX System Overview, Program and Processes, Error Handling, User Identification, Signals, System Calls and Library Functions.: File I/O: File Descriptors, Function for File Modification, I/O Efficiency, File Sharing, Atomic Operations.; Directories: Stat, Fstat, and Lstat Functions, File Types, Set-User-ID and Set- Group-ID, File Access Permissions, Function for modifying file permission and ownership, Symbolic Links, System Data Files and Information: Password File, Shadow Passwords and Other Data Files.; Process Environment: Process Termination, Memory Layout of a C Program, Memory Allocation, setjmp and longjmp Functions.; Process Control: fork Function, vfork Function, exit Functions, wait and waitpid Functions, Race Conditions, Changing User IDs and Group IDs.; Process Relationship: Logins, Process Groups, Sessions, Controlling Terminal, Job Control.; Signals: Signal Concepts, Functions to raise and handle Signals, Program Termination, abort and system functions.

Threads: Thread Concepts, Creation, Termination and Synchronization, Threads Control, Threads and Signals, Threads and fork, Threads and I/O. Shell programming: Basics of Shell Programming, UNIX shell commands, shell scripts variables, loops (for, while), and conditional statements (if else, case), Shell variables, arguments to shell procedure, test command, arithmetic with EXPR command, interactive shell procedures with read.

Reference Books:

1. W. R. Steven, S. A. Rago “Advanced Programming in the Unix environment”, Addison Wesley, (1e) 2011
2. Kerrisk, M. The Linux programming interface: A Linux and UNIX system programming handbook. No Starch Press 2010.
3. Stevens, W. R. Advanced programming in the UNIX environment (3rd ed.). Addison-Wesley 2005.

CAP6135: CYBERSECURITY: CONCEPTS AND APPLICATIONS LAB [0 0 2 1]

Overview of the cybersecurity landscape, Setting up a virtual machine environment using VMware or VirtualBox, Introduction to Kali Linux and basic Linux commands for security testing, Setting up access controls on files and directories in Linux and Windows, Configuring access control lists (ACLs) and permissions, Introduction to types of access control (Preventative, Detective, Corrective, etc.), Write a shell script program that prompts the user for the password. The user has maximum of 3 attempts. If the user enters the correct password, the message "Correct Password" is displayed else the message "Wrong Password". Write a shell script program that will receive any number of filenames as arguments. The shell script should check whether such files already exist. If they do, then it should be reported. The files that do not exist should be created in a sub-directory called mydir. The shell script should first check whether the sub-directory mydir exists in the current directory. If it doesn't exist, then it should be created. If mydir already exists, then it should be reported along with the number of files that are currently present in mydir.

Reference Books:

1. Whitman, M. E., & Mattord, H. J. Principles of Information Security (7th ed.). Cengage Learning 2021
2. Kim, D., & Solomon, M. G. Fundamentals of Information Systems Security (4th ed.). Jones & Bartlett Learning 2021.
3. Stallings, W., & Brown, L. Computer Security: Principles and Practice (5th ed.). Pearson 2022.

CAP6136: PROGRAMMING & PROBLEM-SOLVING USING C LAB [0 0 2 1]

Simple C Programs (expression-oriented operations); Programs to illustrate various operators in C. Programs using branching constructs (if, if-else-if, switch-case); Programs using looping constructs (for, while, do-while, continue, break); Programs on 1D Arrays; Programs on 2D Arrays; Programs on strings; Programs using functions (with and without recursion), passing parameters by value and reference. Operations on Stacks: Push, Pop, Queues.

Reference Books:

1. Kernighan, B. W., & Ritchie, D. M. The C programming language (2nd ed.). Prentice Hall 1988.
2. Gustedt, J. Modern C. Manning Publications 2019
3. Kanetkar, Y. P. Let us C (18th ed.). BPB Publications 2023.

CAP6137: OS & SHELL PROGRAMMING LAB [0 0 2 1]

Testing the use of UNIX commands, UNIX shell commands, Basics of Shell Programming, UNIX System Calls, CPU Scheduling Algorithms, Deadlock Detection Algorithms, Deadlock Avoidance Algorithms, Page Replacement Algorithms, Memory Allocation Algorithms, Disk Scheduling Algorithms, and UNIX Inter Process Communication.

Reference Books:

1. W. R. Steven, S. A. Rago "Advanced Programming in the Unix environment", Addison Wesley, (1e) 2011.
2. Kerrisk, M. The Linux programming interface: A Linux and UNIX system programming handbook. No Starch Press 2010.
3. Stevens, W. R. Advanced programming in the UNIX environment (3rd ed.). Addison-Wesley 2005.

SECOND SEMESTER

CAP6207: NETWORK PROTECTION AND CRYPTOGRAPHIC TECHNIQUES [3 1 0 4]

Network Security and Cryptography Security Concepts: Introduction, The need for security, Security approaches, Principles of security, Types of Security attacks, Security services, Security Mechanisms, A model for Network Security. Elements of Number Theory : Euclid Algorithm, Prime Number Theorem, Euler's, Fermat's Little theorems, Entropy ; Classical Cipher Techniques: Caesar, Affine, Mono-alphabetic, Transposition, Polyalphabetic Ciphers; Security Attacks: Active V/S Passive, Security Services; Symmetric Encryption: Fiestel Cipher, Confusion and Diffusion, DES Algorithm; Asymmetric Encryption: Principles of Public Key Cryptosystems, RSA Algorithm; Message Authentication & Hashing; Digital Signatures: RSA Based, El-Gamal Signatures; Key distribution; User Authentication Protocols; E-Mail Security: PGP, S/MIME; IPsec: AH & ESP; SSL; TLS; Intrusion Detection: Statistical Anomaly Detection, Rule based detection, honeypots; Password Protection.

Reference Books:

1. Stallings, W. Cryptography and network security: Principles and practice (7th ed.). Pearson 2017.
2. William, S. Network security essentials: Applications and standards (6th ed.). Pearson 2021.
3. Kahate, Cryptography and Network Security, (4e) Tata Mc-Graw Hill 2019.
4. K. Charlie, Network Security: Private Communication in a Public World, (2e), Pearson Education 2016.

CAP6208: AUTOMATION WITH PYTHON [3 1 0 4]

Overview of Python: History, features, applications in cybersecurity, Python Basics, Variables and data types (int, float, str, list, tuple, dict), Input/Output, Basic operators: Arithmetic, comparison, logical, assignment operators, Control Flow and Loops, Conditional Statements, Loops, Break, Continue, and Pass Statements, Nested Loops and Conditional Expressions, Defining Functions, Recursion, Modules and Packages, Working with External Libraries: Installing and using third-party libraries (pip), Data Structures in Python, Lists, Dictionaries: Key-value pairs, dictionary methods, String Manipulation, File Handling and Exception Handling, File Operations, Exception Handling, Object-Oriented Programming in Python, Python Scripting for Cybersecurity, Network Programming Basics, Automating System Tasks, Log File Parsing and Analysis, Simple Port Scanning, Password Cracking Basics.

Reference Books:

1. Eric Matthes: "Python Crash Course", 2nd Edition, No Starch Press, 2019.
2. Al Sweigart: "Automate the Boring Stuff with Python", 2nd Edition, No Starch Press, 2019.
3. Justin Seitz: "Black Hat Python: Python Programming for Hackers and Pentesters", 2nd Edition, No Starch Press, 2021.

CAP6209: WEB APPLICATION SECURITY [3 1 0 4]

Importance of securing web applications, Common threats to web applications, Web application architecture (Client-Server model), Principles of Security: Confidentiality, Integrity, Availability, Common security concepts (Authentication, Authorization, Encryption), Overview of Common Attacks: Cross-Site Scripting (XSS), SQL Injection, Cross-Site Request Forgery (CSRF) Understanding the threat landscape for web applications, Identifying vulnerabilities and mitigating risks Secure Coding Practices Importance of validating user input, Encoding output to prevent XSS and injection attacks, Understanding SQL injection attacks, Parameterized queries, stored procedures, and ORM usage, Cross-Site Scripting (XSS) Prevention, Cross-Site Request Forgery (CSRF), Session Management Security, Authentication and Authorization, Authentication Mechanisms, Authorization Strategies, Secure Password Storage, Common Web Application Vulnerabilities,

Vulnerability Scanning and Penetration Testing, Web Security Best Practices, Secure Development Lifecycle (SDLC), Web Application Security Testing, Secure Web Application Deployment, Emerging Threats in Web Application Security.

Reference Books:

1. OWASP Foundation. OWASP: The ten most critical web application security risks. OWASP Foundation 2021.
2. Kenneson, R. Web application security: Exploitation and countermeasures for modern applications (1st ed.). Packet Publishing 2020.
3. Miller, C. (2021). The web application hacker's handbook: Finding and exploiting security flaws (3rd ed.). Wiley 2021.

CAP6211: INTRUSION DETECTION SYSTEMS [3 1 0 4]

History of Intrusion detection, Audit, Concept and definition, Internal and external threats to data, attacks, Need and types of IDS, Information sources Host based information sources, Network based information sources. Intrusion Prevention Systems, Network IDs protocol-based IDs, Hybrid IDs, Analysis schemes, thinking about intrusion. A model for intrusion analysis, techniques Responses requirement of responses, types of responses mapping responses to policy Vulnerability analysis, credential analysis no credential analysis. Introduction to Snort, Snort Installation Scenarios, Installing Snort, Running Snort on Multiple Network Interfaces, Snort Command Line Options. Step-By-Step Procedure to Compile and Install Snort Location of Snort Files, Snort Modes Snort Alert Modes Working with Snort Rules, Rule Headers, Rule Options, The Snort Configuration File etc. Plugins, Preprocessors and Output Modules, Using Snort with MySQL Using ACID and Snort Snarf with Snort, Agent development for intrusion detection, Architecture models of IDs and IPs.

Reference Books:

1. Scarfone, K., & Mell, P. Guide to intrusion detection and prevention systems (IDPS). National Institute of Standards and Technology (NIST) 2017.
2. Carroll, M., & O'Gorman, D. Network security through data analysis: From data to action (1st ed.). O'Reilly Media 2018.
3. Northcutt, S., & Novak, J. Network intrusion detection: An analyst's handbook (3rd ed.). New Riders Publishing 2019.

CAP6236: AUTOMATION WITH PYTHON LAB [0 0 2 1]

Data Types and Variables, Input/Output, Control Flow and Loops, Break and Continue, Functions and Modules, Recursion, Data Structures in Python, String Manipulation, File Handling and Exception Handling, Object-Oriented Programming in Python, Python Scripting for Cybersecurity

Reference Books:

1. Eric Matthes: “Python Crash Course”, 2nd Edition, No Starch Press, 2019.

2. Al Sweigart: “Automate the Boring Stuff with Python”, 2nd Edition, No Starch Press, 2019.
3. Justin Seitz: “Black Hat Python: Python Programming for Hackers and Pentesters”, 2nd Edition, No Starch Press, 2021.

CAP6237: INTRUSION DETECTION SYSTEMS LAB [0 0 2 1]

Working with Trojans, Backdoors and sniffer for monitoring network communication, Denial of Service and Session Hijacking using Tear Drop, DDOS attack, Penetration Testing and justification of penetration testing through risk analysis, Password guessing and Password Cracking. Wireless Network attacks, Bluetooth attacks, Firewalls, Intrusion Detection and Honeypots, Malware – Keylogger, Trojans, Keylogger countermeasures,

Understanding Data Packet Sniffers Windows Hacking – NT LAN Manager, Secure 1 password recovery, Implementing Web Data Extractor and Web site watcher.

Reference Books:

1. Scarfone, K., & Mell, P. Guide to intrusion detection and prevention systems (IDPS). National Institute of Standards and Technology (NIST) 2017.
2. Carroll, M., & O'Gorman, D. Network security through data analysis: From data to action (1st ed.). O'Reilly Media 2018.
3. Northcutt, S., & Novak, J. Network intrusion detection: An analyst's handbook (3rd ed.). New Riders Publishing 2019.

CAP6238: PRAGMATIC LEARNING [0 0 2 1]

Introduction: Experiential learning (Minor Project) is learning through doing. The aim of this course is to encourage students designing small projects in a multidisciplinary environment. In this course students are challenged to move from problem to solution through a series of task-oriented steps. This collaborative process creates lifelong learners by igniting a curiosity about the world around them. In the experiential learning, students are inspired to build a small project which will enables them to acquire skills to position them for success in both academics and industry. The students will acquire practical knowledge within the chosen area of technology for project development and identify, analyse, formulate, and handle programming projects with a comprehensive and systematic approach.

There will be general meetings, group discussion and mid-term presentation to track the progress of the project and term-end presentation to evaluate project. In the examination student must demonstrate the project. A team of maximum two students can develop the project. However,

during the examination, each student must demonstrate the project individually. Finally, student/team must submit a short project report/summary that must include the following:

- Problem
- Statement
- Objectives
- Requirement
- Analysis
- Software Requirement Specification
- Methodology – How you build the project?
- Conclusion

Program Electives – I

CAP6248: MOBILE COMPUTING: PRINCIPLES AND APPLICATIONS [3 0 0 3]

Introduction to Mobile Computing - Architecture of Mobile Computing - Novel Applications – Limitations. GSM - GSM System Architecture - Radio Interface – Protocols - Localization and Calling - Handover - Security - New Data Services. Data Link Layer Medium Access Control Protocol - Wireless MAC Issues - Hidden and exposed terminals - near and far terminals – SDMA – FDMA – TDMA – CDMA - Tunnelling Cellular Mobility - IPv6. Mobile Network Layer Mobile IP – Goals – Assumption - Entities and Terminology - IP Packet Delivery - Agent Advertisement and Discovery – Registration - Tunnelling and Encapsulation – Optimizations -Dynamic Host Configuration Protocol. Mobile Transport Layer Traditional TCP - Indirect TCP - Snooping TCP - Mobile TCP - Fast Retransmit and Fast Recovery - Transmission /Time-Out Freezing - Selective Retransmission -Transaction Oriented TCP. Database Issues Hoarding Techniques - Caching Invalidation Mechanisms - Client Server Computing with Adaptation- Power Aware and Context Aware Computing - Transactional Models - Query Processing – Recovery - and Quality of Service Issues.

Reference Books:

1. Schiller, J. Mobile Communications (5th ed.). Pearson 2021.
2. Stallings, W. Wireless Communications and Networks (3rd ed.). Pearson 2021.
3. Verma, A., & Zeng, Y. Mobile Computing: Principles and Applications (1st ed.). Wiley 2022.

CAP6249: IOT ARCHITECTURE AND PROTOCOLS [3 0 0 3]

Internet of Things: An overview, System Architecture, Design Principles for Connected Devices, Design Principles for Web connectivity for Connected Devices, Internet Connectivity Principles, Data Acquiring, Organizing and Analytics in IoT, data Collection, Storage & Computing Using Cloud Platform, Sensors and Actuators, Radio Frequency Identification, Wireless Sensor Networks and Participatory Sensing Technology, Prototyping of Embedded Devices for IoT, Gateways, Internet and Web/Cloud Services Software Component, IoT Privacy, Security and governance. IoT based Case studies.

Reference Books:

1. Delsing, Jerker, ed, "IoT automation: Arrowhead framework. CRC Press", (1e) 2017.
2. Raj Kamal, "Internet of Things", (1e), McGraw-Hill 2017.
3. Theoleyre, Fabrice, and Ai-Chun Pang, eds," Internet of Things and M2M Communications", River Publishers, (1e) 2013.

CAP6250: CLOUD COMPUTING: CONCEPTS AND APPLICATIONS [3 0 0 3]

Introduction to Clouds and Cloud Computing: Basic Concepts, Cloud Classifications, and Types of Services, deployment models; Classic Data Center (CDC): DBMS concepts, CDC drawbacks and need of Cloud Resources, CDC Management and case studies; Virtualized Data Center (VDC): Compute and Storage, Compute virtualization overview, Compute virtualization techniques, Virtual Machines, VM Resource management techniques. Physical to virtual conversion, Hypervisor Management Software, Virtual Infrastructure Requirements; Storage: Storage virtualization overview, Virtual Machine Storage, Block level and File level virtualization, Virtual provisioning and automated storage tiering; Networking: VDC networking overview, VDC networking components, VLAN and VSAN technologies, Network traffic management Desktop and Application: Desktop virtualization, Application virtualization, Business Continuity in VDC, Fault tolerance mechanism in VDC, Backup in VDC, Replication and migration in VDC, Cloud Security: Security basics, Cloud security concerns and threats, Cloud security mechanisms, Access control and identity management in Cloud.

Reference Books:

1. Mell, P., & Grance, T. The NIST Definition of Cloud Computing (Special Publication 800-145). National Institute of Standards and Technology 2020.

2. Buyya, R., Broberg, J., & Goscinski, A. Cloud Computing: Principles and Paradigms (2nd ed.). Wiley 2021.
3. Arora, A., & Gonsalves, D. Cloud Computing: A Practical Approach (1st ed.). McGraw-Hill 2021.

THIRD SEMESTER

CAP7107: SECURE PROTOCOL DESIGN [3 1 0 4]

OSI: ISO Layer Protocols: -Application Layer Protocols-TCP/IP, HTTP, SHTTP, LDAP, MIME, POP& POP3-RMON-SNTP-SNMP. Presentation Layer Protocols-Light Weight Presentation Protocol Session layer protocols. RPC protocols-transport layer protocols-ITOT, RDP, RUDP, TALI, TCP/UDP, compressed TCP. Network layer Protocols – routing protocols-border gateway protocol-exterior gateway protocol-internet protocol IPv4- IPv6-Internet Message Control Protocol- IRDP Transport Layer Security-TSL-SSL-DTLS. Data Link layer Protocol – ARP – In ARP – IPCP – IPv6CP – RARP – SLIP. Wide Area and Network Protocols- ATM protocols – Broadband Protocols – Point to Point Protocols – Other WAN Protocols- security issues. Local Area Network and LAN Protocols – ETHERNET Protocols – VLAN protocols – Wireless LAN Protocols – Metropolitan Area Network Protocol – Storage Area Network and SAN Protocols -FDMA, WIFI and WIMAX Protocols- security issues. Mobile IP – Mobile Support Protocol for IPv4 and IPv6 – Resource Reservation Protocol. Multicasting Protocol – VGMP – IGMP – MSDP, Network Security and Technologies and Protocols – AAA Protocols – Tunneling Protocols – Secured Routing Protocols – GRE- Generic Routing Encapsulation – IPSEC – Security.

Reference Books:

1. Poe, S. Secure protocols in modern networking systems. Wiley 2023.
2. Shankar, P., & Srinivas, V. Designing secure communication protocols: A practical approach. Springer 2022.
3. Kurtz, J., & Hansen, M. Network security protocols: Fundamentals and applications 2021.

CAP7108: ETHICAL HACKING AND PENETRATION TESTING [3 1 0 4]

Hacking windows – Network hacking – Web hacking – Password hacking. A study on various attacks – Input validation attacks – SQL injection attacks – Buffer overflow attacks - Privacy attacks. TCP / IP – Checksums – IP Spoofing port scanning, DNS Spoofing. Dos attacks – SYN attacks, Smurf attacks, UDP flooding, DDOS – Models. Firewalls – Packet filter firewalls, Packet Inspection firewalls – Application Proxy Firewalls. Batch File Programming. Fundamentals of Computer Fraud – Threat concepts – Framework for predicting inside attacks – Managing the threat – Strategic

Planning Process. Architecture strategies for computer fraud prevention – Protection of Web sites – Intrusion detection system – NIDS, HIDS – Penetrating testing process – Web Services – Reducing transaction risks. Key Fraud Indicator selection process customized taxonomies – Key fraud signature selection process –Accounting Forensics – Computer Forensics – Journaling and it's requirements – Standardized logging criteria – Journal risk and control matrix – Neural networks – Misuse detection and Novelty detection.

Reference Books:

1. Patel, R., & Kapoor, V. Cybersecurity and computer fraud detection: Approaches and strategies. CRC Press 2023.
2. Anderson, R., & Wood, D. Principles of computer forensics and fraud prevention. Wiley 2022.
3. Taylor, R., & Wong, H. Network security and ethical hacking: From theory to practice. Elsevier 2021.

CAP7109: CYBER LAW AND REGULATION OF CYBERSPACE [3 1 0 4]

Overview of IT Law in India and Cyber Crime, Digital Evidence and Technological Standards under IT Law, Corporate Liability under the IT Act, 2000 (Amendments in 2008), Key Sections: IT Act Section 66(A-F), Section 67(A-C), Security Investigation: Legal, Ethical, and Professional Issues, IT Act, 2000: Key Provisions, Amendments, and Limitations, Digital Signatures, Cryptographic Algorithms (Public & Private), Legal Recognition of Electronic Records & Digital Signatures, Cyber Crimes, Network Service Provider Liability, Cyber Appellate Tribunal, Penalties and Adjudication under IT Law, Intellectual Property Rights: Patent, Trademark, Copyright (Software & Domain Disputes), IT Act in relation to Civil & Criminal Procedure Code, Indian Evidence Act, Bankers' Book Evidence Act, Indian Penal Code, Reserve Bank of India Act, Laws for Employees & Internet Usage, Alternative Dispute Resolution (ADR) & Online Dispute Resolution (ODR), E-Commerce: Evolution, Contracts (Paper vs Paperless), B2B & B2C Models, E-Security and Cyber Risks in Business Transactions, Legal Aspects of Taxation, Electronic Payments, Supply Chain, EDI, and E-Markets, Emerging Trends in Cyber Law & Digital Economy.

Reference Books:

1. Sarkar, S. Cyber Law in India: A Comprehensive Guide to Legal and Ethical Issues in the Digital World. Cambridge University Press 2023.
2. Chawla, S., & Gupta, S. Cyber Law, E-commerce & Cyber Security: An Indian Perspective. LexisNexis 2022.
3. Duggal, P. Cyber Law: An Exhaustive Section Wise Commentary on the Information Technology Act Along with Rules, Regulations, Policies, Notifications Etc. Cyberlaw University 2021.

CAP7134: MINOR PROJECT [0 0 4 2]

Introduction: The goal of the mini project is to provide students the practical skills and knowledge they need to address issues that arise in the workplace, in educational settings, and in computer science research. The course's mini-project entails doing hands-on work to comprehend and address issues in the field of computers. An information system or subsystem, like a piece of software, is typically analysed, designed, coded or otherwise implemented, and tested as part of any computer science project. A design document might be the proper outcome of a design study instead of a computer programme being the subsystem. However, in this course, we expect a software system or subsystem. The design and implementation of a hardware system/subsystem would also be a suitable project.

Syllabus: The Mini Project is not just a component of the coursework; it also serves as a way for you to highlight your skills and areas of expertise. It gives you the chance to show off your creativity, cooperation, inspiration, planning, and organizational skills in a software project.

Reference Books:

1. Choudhury, S. Project Management. Tata McGraw-Hill Education2017.
2. Kerzner, H. Project Management: A Systems Approach to Planning, Scheduling, and Controlling (2nd ed.). CBS Publishers & Distributors 2006.
3. Meredith, J. R., & Mantel, S.J. Project Management: A Managerial Approach (10th ed.). Wiley 2017.

Project Guidelines

- Each student should submit a unique project title unless/otherwise in a team project. Project work should include software development.
- Only two students can work on one project as a team. However, their contribution should be clearly specified and reported.
- The project should focus on solving some real-life problems, though it is not mandatory. However, the project idea should be creative, and it can be a fresh take on an old idea which is often worth as much as a brand-new idea.
- The project work may be done internally on the university campus or in any external organizations/institutes approved by the head of the department/university authority.
- Prior to starting project work, a student must get his/her project idea/problem statement approved by the supervisor.
- The student must submit a project synopsis, presenting his idea. The student may start working on a project only if the synopsis is approved.

- The student should present the progress of the project works as per the timeline specified by the department /project coordinator/ supervisor.

CAP7135: SECURE PROTOCOL DESIGN LAB [0 0 2 1]

Designing Remote Connectivity, Designing IP Addressing, Selecting Routing Protocols, Voice Network Design, Wireless Network Design, Designing Security Solutions, Installation and Configuration of Linux, Linux Systems Administration, Understanding Shells and Scripting with Linux, Setting up Samba and Windows-Linux network, Setting up security with Linux, Setting up a Web Server, Learn the fundamentals of wireless LAN, Learn various standards related to wireless LANs, Learn about the security aspects of wireless LANs.

Reference Books:

1. Poe, S. (2023). Secure protocols in modern networking systems. Wiley.
2. Shankar, P., & Srinivas, V. (2022). Designing secure communication protocols: A practical approach. Springer.
3. Kurtz, J., & Hansen, M. (2021). Network security protocols: Fundamentals and applications.

CAP7136: ETHICAL HACKING AND PENETRATION TESTING LAB [0 0 2 1]

Working with OWASP top 10 vulnerability, Types of vulnerability and detection method, VM, VP, PT tools manual and automation, Creation of .bat files and insertion, Introduction of automation tools i.e. qualys, ibm app scan, hp web inspect and acunetix, Introduction of manual tools i.e. fiddler, burp suite, Vulnerability analysis on sast and dast, Infrastructure and web application vulnerability, Honeypots, passworx guessing and cracking, Exposure of ISO 27001 and hippa for finding vul on phi/pi data.

Reference Books:

1. Patel, R., & Kapoor, V. Cybersecurity and computer fraud detection: Approaches and strategies. CRC Press 2023.
2. Anderson, R., & Wood, D. Principles of computer forensics and fraud prevention. Wiley 2022.
3. Taylor, R., & Wong, H. Network security and ethical hacking: From theory to practice. Elsevier 2021.

Program Electives – II

CAP7158: MOBILE SECURITY [3 0 0 3]

Overview of Mobile Security: Definition, significance, and evolving threats in mobile ecosystems. Mobile Device Architectures. Mobile Security Models: Secure boot, hardware-backed security, Trusted Execution Environment (TEE), and Secure Enclave. Mobile Threat Landscape: Malware, phishing, ransomware, insecure communication, unauthorized access. Mobile App Security Models. Common Vulnerabilities in Mobile Apps, Mobile App Penetration Testing Mobile Data and Network Security, Mobile Device Management (MDM): Role, features, and architecture of MDM solutions, BYOD (Bring Your Own Device) Security, Secure Mobile Access, Mobile Device Hardening, Managing and Securing Mobile Devices in Corporate Networks Incident Response, and Emerging Trends.

Reference Books:

1. Raj, V., & Kumar, A. Mobile Security: Threats, Architectures, and Defense Mechanisms. Springer 2023.
2. Patel, S., & Sharma, P. Mobile App Security: A Comprehensive Guide to Securing Mobile Devices and Apps. Wiley 2022.
3. Singh, R., & Gupta, A. Practical Mobile Security: Managing and Securing Mobile Devices in a BYOD World. Elsevier 2023.

CAP7159: IOT SECURITY [3 0 0 3]

Overview of IoT: Ecosystem, applications, and architectures (Perception, Network, Application layers). IoT Protocols: MQTT, CoAP, AMQP, Bluetooth, ZigBee, LoRa WAN. IoT Security Challenges: Device constraints, lack of standardization, heterogeneity, insecure communication. Common IoT Vulnerabilities: Insecure interfaces, weak authentication, encryption issues. Attack Vectors: Physical attacks, network-based attacks (DDoS, Man-in-the-Middle), application-level attacks (malware). Security-by-design principles for IoT. Authentication & Authorization: Device identity, secure boot, RBAC/ABAC. Encryption and Data Integrity: Lightweight encryption (ECC, AES), secure communication protocols (TLS, DTLS). Network Security for IoT: Firewalls, IDS/IPS, network segmentation, VPNs. Device Security: Firmware management. Risk Management, Compliance

Reference Books:

1. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. Internet of Things security and privacy: A survey. Wiley 2021.

2. Madhusanka Liyanage, Andrei Gurtov, IoT Security: Advances in Authentication 2020.
3. Fei Hu, Internet of Things Security: Principles and Practice, CRC Press 2016.

CAP7160: CLOUD SECURITY [3 0 0 3]

Overview of Cloud Computing: Cloud characteristics, deployment models (Public, Private, Hybrid), and service models (IaaS, PaaS, SaaS). Cloud Security Challenges: Shared responsibility model, data loss, data breaches, multi-tenancy risks, virtualization security. Cloud Threats: Data breaches, account hijacking, insecure interfaces, insider threats. Cloud Security Architecture, Identity and Access Management (IAM) in the Cloud: Role-based access control, multi-factor authentication, least privilege principle. Data Security in the Cloud: Encryption (at rest and in transit), key management, tokenization. Security Controls. Virtualization Security, Network Security in Cloud, Container Security: Securing Docker, Kubernetes, microservices architecture, Incident Detection and Response, Regulatory Requirements, Cloud Security Standards, Risk Management in Cloud, Legal and Compliance Issues, Cloud Security Frameworks, Cloud Security Automation.

Reference Books:

1. Ristenpart, T., & Sherry, J. Cloud security: A comprehensive guide to the concepts, techniques, and tools for securing cloud computing environments. Wiley 2023.
2. Hines, A. Cloud security and compliance: A practical guide. Springer 2022.
3. Wladawsky-Berger, I., & Howe, J. Cloud computing security issues and challenges: A survey. Elsevier 2023.

Program Electives – III

CAP7161: BLOCKCHAIN TECHNOLOGY [3 0 0 3]

Introduction – basic ideas behind blockchain, how it is changing the landscape of digitalization, introduction to cryptographic concepts required; Hashing, public key cryptosystems, private vs public blockchain and use cases, Hash Puzzles, Introduction to Bitcoin Blockchain; Bitcoin Blockchain and scripts, Use cases of Bitcoin Blockchain scripting language in micropayment, escrow, Downside of Bitcoin – mining; Alternative coins – Ethereum and Smart contracts; Alternative coins – Ethereum continued, IOTA; The real need for mining – consensus – Byzantine Generals Problem, and

Consensus as a distributed coordination problem – Coming to private or permissioned blockchains – Introduction to Hyperledger; Permissioned Blockchain and use cases – Hyperledger, Corda; Uses of Blockchain in E-Governance, Land Registration, Medical Information Systems, and others.

Reference Books:

1. Kumar Saurabh, Ashutosh Saxena Blockchain Technology: Concepts and Applications, Wiley, 2020.
2. Corda, R. Mastering Blockchain: Unlocking the power of cryptocurrencies, smart contracts, and decentralized applications. Wiley 2018.
3. Daniel Drescher Blockchain Basics, A Non-Technical introduction in 25 steps, Apress, 2017.

CAP7162: SECURITY OPERATIONS AND INCIDENT RESPONSE [3 0 0 3]

Introduction to Security Operations, Security Operations Centers (SOC), Role and importance of SOCs, SOC architecture and structure, Security Information and Event Management (SIEM), Threat Intelligence, Incident Detection and Monitoring, Incident Detection Frameworks, Indicators of Compromise (IoCs) and Indicators of Attack (IoAs), Detection methods: Signature-based, anomaly-based, behavior-based detection, Network Security Monitoring, Packet analysis and traffic inspection, Endpoint Monitoring and Security, Incident Response Frameworks and Planning, Incident Response Lifecycle, Preparation, detection, containment, eradication, recovery, and post-incident activities (NIST framework), Types of Cybersecurity Incidents, Data breaches, ransomware attacks, denial-of-service attacks, phishing, insider threats, Forensics and Evidence Collection, Legal considerations in incident response, Post-Incident Activities and Continuous Improvement, Post-Incident Review and Reporting, Threat Hunting, Proactive identification of threats, Automating Incident Response, Building a Continuous Improvement Program

Reference Books:

1. Bland, B., & Kessler, G. C. The basics of cybersecurity: A comprehensive guide to managing security operations and incident response. Wiley 2023.
2. Miller, M. Practical security operations and incident response: Building effective detection and response capabilities. Elsevier 2022.
3. Kennes, W. & Kumar, R. Incident response & computer forensics: Security operations and response strategies in practice. CRC Press 2023.

CAP7163: DATA SCIENCE [3 0 0 3]

Data Science Introduction: Introduction to data, types of data (quantitative and qualitative). Level of data: Nominal, Ordinal, Scale, Interval. Introduction data science, data science process, role of data scientist, different tools for data science (R, Python, Excel, Tableau, Power BI,). Handling Missing Data, Decoding of Data. Treatment of Outliers. Data visualization: scatter plot, line plot, Box plot, bar plot, stem and leaf plot. Data Distribution: Normal, Binomial, Poisson. Measures of central tendencies, measures of variations. Data correlation, data classifications and prediction, regression analysis, Decision Tree, Naïve Bayes.

Reference Books:

1. Wright, J. Data Science for Beginners: A Step-by-Step Guide to the Fundamentals of Data Science. Wiley 2024.
2. Andrew Wolf Machine Learning Simplified: A Gentle Introduction to Supervised Learning, themlsbook.com 2022.
3. Peter Bruce and Andrew Bruce, Practical Statistics for Data Scientists, Publisher(s): O'Reilly Media, Inc 2017.

FOURTH SEMESTER

CAP7271: MAJOR PROJECT [0 0 0 16]

Introduction: Each student shall carry out an industry level project this semester. The project will be carried outunder the supervision of a teacher in the department. When the project is carried out in an external organization (academic institution/ industry), a supervisor will also be appointed from the external organization.

Project Guidelines

- Each student should submit a unique project title unless/otherwise in a team project.Project work should
- include software development.
- Only two students can work on one project as a team. However, their contribution should be clearlyspecified and reported.
- The project should focus on solving some real-life problems, though it is not mandatory. However, the project idea should be creative, and it can be a fresh take on an old idea which is often worth as much asa brand-new idea.
- The project work may be done internally in the university campus or in any externalorganizations/institutes approved by the head of the department/university authority.
- Prior to starting project work, a student must get his/her project idea/problem statement approved by thesupervisor.

- The student must submit a project synopsis, presenting his idea. The student may start working onproject only if the synopsis is approved.
- The student should present the progress of the project works as per the timeline specified by thedepartment /project coordinator/ supervisor.