SYLLABUS STRUCTURE
(Effective from academic session 2025-26)

FOR THE DEGREE

OF

Master of Science

(Cyber Security)

Four-Semester Full Time Programme

SCHOOL OF BASIC SCIENCES

MANIPAL UNIVERSITY
JAIPUR

INSPIRED BY LIFE

ELIGIBILITY OF THE CANDIDATES:

B.Sc. (Information Technology (IT)/Computer Science (CS)/Electronics) OR Bachelor of Computer Application s (BCA) OR B.Sc. Forensic Science in Cyber Forensic / Digital Forensics / Computer Forensics OR equivalent qualification from recognized University with minimum 50%.

Or

B.E./B.Tech. in all Engineering/Technology Branches

Program specific outcomes for Master of Science (Cyber Security) program:

[PSO.1.]	To work effectively as cybersecurity professionals in both supportive and leadership roles, with a focus on securing digital infrastructure.
[PSO.2.]	To progress successfully in cybersecurity careers by utilizing technical expertise, leadership, communication, and interpersonal skills while adhering to legal, regulatory, and ethical standards.
[PSO.3.]	To adapt to evolving cybersecurity technologies and threats, with a commitment to continuous learning and professional development.

						SECOND SEMESTER					
Course Code	Course Name	L	T	P	C	Course Code	Course Name	L	T	P	C
🟥	Mathematical Foundation to Computer Science	3	1	0	4	🟩	Network Protection and Cryptographic Techniques	3	1	0	4
🟩	Introduction to Computer Networks & Protocols	3	1	0	4	🟩	Automation with Python	3	1	0	4
🟩	Foundations in Cybersecurity	3	1	0	4	🟩	Web Application Security Fundamentals	3	1	0	4
🟩	Programming & Problem-Solving using C	3	1	0	4	🟩	Intrusion Detection Systems	3	1	0	4
🟩	OS and Shell Programming	3	1	0	4	🟦	Program Elective-I	3	0	0	3
🟩	Foundations in Cybersecurity Lab	0	0	2	1	🟩	Automation with Python Lab	0	0	2	1
🟩	Programming & Problem-Solving using C Lab	0	0	2	1	🟩	Intrusion Detection Systems Lab	0	0	2	1
🟩	OS and Shell Programming Lab	0	0	2	1	🟩	Pragmatic Learning	0	0	2	1
					23						23
Total Contact Hours (L + T + P)		(15+5+6)				Total Contact Hours (L + T + P)		(16+5+6)			
THIRD SEMESTER						FOURTH SEMESTER					
🟩	Secure Protocol Design	3	1	0	4	🟩	Major Project	0	0	0	16
🟩	Ethical Hacking and Penetration Testing	3	1	0	4						
🟩	Cyber security Audit and Compliances	3	1	0	4						
🟦	Program Elective-II	3	0	0	3						
🟦	Program Elective-III	3	0	0	3						
🟩	Minor Project	0	0	4	2						
🟩	Secure Protocol Design LAB	0	0	2	1						
🟩	Ethical Hacking and Penetration Testing Lab	0	0	2	1						
					22			0	0	0	16
Total Contact Hours (L + T + P)		(15+3+8)				Total Contact Hours (L + T + P)		00			

Program Electives – I

Introduction to Mobile Computing
Introduction To IoT
Introduction to Cloud Computing

Program Electives – II

Mobile Security
IoT Security
Cloud Security

Program Electives – III

Blockchain Technologies
Security Operations and Incident Response
Data Science

FIRST SEMESTER

XXXXXX: Mathematical Foundation to Computer Science [3 1 0 4]

POSET, Lattices, distributive, and complemented lattices, Boolean Lattice, Uniqueness of Boolean LatticesBoolean expression & function. Mathematical Logic: Statement and notations, connectives, normal forms, well- formed formulas, implication, Tautology, Predicate calculus. Graphs: Introduction, Isomorphism, Sub graphs, Walks, Paths, Circuits, Connectedness, Components, Euler graphs, Hamiltonian paths and circuits, Trees, Properties of trees, Distance and canters in tree, Rooted and binary trees. Trees, Connectivity & PlanaritySpanning 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: Isomorphism, Combinational and geometric graphs, Planer graphs, Different representation of a planer graph. Matrices, Coloring and Directed Graph. Chromatic number, Chromatic partitioning, Chromatic polynomial, Matching, Covering, Four color problem, Directed graphs, Types of directed graphs, Digraphs and binary relations, Directed paths and connectedness, Euler graphs.

References:

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.

XXXXXX: Introduction to Computer Networks & 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

References:

1. W. R Stevens, TCP/IP Illustrated, Volume 1: The Protocols, (2e) Addison-Wesley, 1994.
2. P. Loshin, IPV6 Clearly Explained, (4e) Morgan Kauffman, 2003.
3. B. A. Forouzan, TCP/IP Protocol Suite, (2e) TMH, 2005.

XXXXXX: Foundations in Cybersecurity [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.

References:

1. William Stallings, "Operating Systems: Internals and Design Principles", Prentice Hall, 2009.
2. John Purcell, Robert Kiesling, "Linux: The Complete Reference", Linux System Labs, 1998.
3. Chuck Easttom, "Computer Security Fundamentals", Pearson, 2011.
4. C. J. Date, "An Introduction to Database Systems", Addison-Wesley, 2000.

XXXXXX: 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.

References:

1. Kerninghan & Ritchie “The C programming language”, PHI.
2. Schildt “C: The Complete reference” 4th ed TMH.
3. Cooper Mullish “The Spirit of C”, Jaico Publishing House, Delhi.
4. Kanetkar Y. “Let us C”, BPB.
5. TennenBaum A.M. & others: Data Structures using C & C++; PHI.

XXXXXX: UNIX & 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.

References:

1. W. R. Steven, S. A. Rago “Advanced Programming in the Unix environment”, Addison Wesley, (1e), 2011
2. Y. P. Kanetkar “Unix Shell Programming”. BPB Publication, (1e), 2009.

XXXXXX: FOUNDATIONS IN CYBERSECURITY 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.

XXXXXX: 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.

XXXXXX: UNIX & SHELL PROGRAMMING LAB [3 1 0 4]

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.

References:

1. W. R. Steven, S. A. Rago "Advanced Programming in the Unix environment", Addison Wesley, 2011.
2. Y. P. Kanetkar "Unix Shell Programming". BPB Publication, 2009.

SECOND SEMESTER

XXXXXX: 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.

References:

1. S. Williams, Cryptography and Network Security: Principles and Practices, (6e) Pearson Education, 2013.
2. A. Kahate, Cryptography and Network Security, (4e) Tata Mc-Graw Hill, 2019
3. K. Charlie, Network Security: Private Communication in a Public World, (2e), Pearson Education, 2016.
4. V. Bagad, I. Dhotre, Cryptography and Network Security, (2e), Technical Publications, 2008.
5. B.A. Forouzan, Network Security, (3e), Tata Mc-Graw Hill, 20011.

XXXXXX: 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:

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.

XXXXXX: WEB APPLICATION SECURITY FUNDAMENTALS [3 1 0 4]

Introduction to System Programs & Operating Systems, Evolution of Operating System (mainframe, desktop, multiprocessor, Distributed, Network Operating System, Clustered & Handheld System), Operating system services, Operating system structure, System Call & System Boots, Operating system design & Implementations, System protection, Buffering & Spooling. Types of Operating System: Bare machine, Batch Processing, Real Time, Multitasking & Multiprogramming, time-sharing system. File: concepts, access methods, free space managements, allocation methods, directory systems, protection, organization, sharing & implementation issues, Disk & Drum Scheduling, I/0 devices organization, I/0 devices organization, I/0 buffering, I/O Hardware, Kernel I/O subsystem, Transforming I/O request to hardware operations. Device Driver: Path managements, Sub module, Procedure, Scheduler, Handler, Interrupt Service Routine. File system in Linux & Windows Process: Concept, Process Control Blocks (PCB), Scheduling criteria Preemptive & non-Preemptive process scheduling, Scheduling algorithms, algorithm evaluation, multiple processor scheduling, real time scheduling, operations on processes, threads, inter process communication, precedence graphs, critical section problem, semaphores, classical problems of synchronization. Deadlock: Characterization, Methods for deadlock handling, deadlock prevention, deadlock avoidance, deadlock detection, recovery from deadlock, Process Management in Linux. Memory Hierarchy, Concepts of memory management, MFT & MVT, logical and physical address space, swapping, contiguous and non-contiguous allocation, paging, segmentation, and paging combined with segmentation. Structure & implementation of page table. Concepts of virtual memory, Cache Memory Organization, demand paging, page replacement algorithms, allocation of frames, thrashing, demand segmentation. Unit V Distributed operating system: Types, Design issues, File system, Remote file access, RPC, RMI, Distributed Shared Memory (DSM), Basic Concept of Parallel Processing &Concurrent Programming. Case study of Unix, Linux & Windows.

References:

1. Silberschatz,” Operating system”, Willey Pub.
2. Stuart,” Operating System Principles, Design & Applications”, Cengage Learning.
3. Tannanbaum, “Modern operating system”, PHI Learning.
4. Dhamdhere,” Operating System”, TMH.
6. William stalling, “operating system” Pearson Edu.
7. Deitel & Deitel, “Operating Systems”, Pearson Edu.
8. Flynn & Mchoes, “Operating Systems”, Cengage Learning.
9. Haldar, “Operating System”, Pearson Edu.

XXXXXX: 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.

References:

1. Christopher Kruegel,FredrikValeur, Giovanni Vigna: “IntrusionDetection and Correlation Challenges and Solutions”, 1st Edition,Springer, 2005.
2. Carl Endorf, Eugene Schultz and Jim Mellander “ IntrusionDetection & Prevention”, 1st Edition, Tata McGraw-Hill, 2004.
3. Stephen Northcutt, Judy Novak : “Network Intrusion Detection”, 3rdEdition, New Riders Publishing, 2002.

XXXXXX: 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

References:

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.

XXXXXX: 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, Firwalls , 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.

References:

1. Carl Endorf, Eugene Schultz and Jim Mellander "Intrusion Detection & Prevention", 1st Edition, Tata McGraw-Hill, 2004.
2. Stephen Northcutt, Judy Novak: "Network Intrusion Detection", 3rdEdition, New Riders Publishing, 2002.
3. T. Fahringer, R. Prodan, "A Textbook on Grid Application Development and Computing Environment". 6th Edition,Khanna Publihsers, 2012.

XXXXXX: 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 andsystematic approach.

Course Outcome: At the end of the course, the students will be able to:

- To design, implement and evaluate a project.
- Gain project management skills.
- To learn to work effectively and ethically in a team towards project development.
- To demonstrate the ability to produce a technical document.

Syllabus: 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
- References

XXXXXX: APTITUDE AND TECHNICAL DEVELOPMENT [1 1 0 2]

Section I: Quantitative: Number System, Percentage, Time & Distance, Profit & Loss, Time & Work, Average, Permutation & Combinations, Game Based. Verbal: Sentence Improvement, Sentence Rearrangement, Fill in the Blanks. Logical: Coding & Decoding, Direction, Blood Relation, Puzzle, Series, Statement & Arguments. Mock Interview Preparation and Group Discussion.

Section II: C Programming: C Fundamentals, Function, Array, Pointers, Structure and File Handling. Object Oriented Concepts. Data Structure: Types of Data Structure and their implementation. Program Logic Development and MCQ Solving. DBMS; SQL Queries. Software Engineering: Use case preparation and Implementation. Overview of Operating Systems and Computer Networks.

Program Electives – I

XXXXXX: INTRODUCTION TO MOBILE COMPUTING [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.

References:

1. Jochen Schiller, “Mobile Communications”, Second edition Addison-Wesley, 2008.
2. Ivan Stojmenovic and Cacute, “Handbook of Wireless Networks and Mobile Computing”, Wiley, 2002.

XXXXXX: INTRODUCTION TO IoT [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.

References:

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

XXXXXX: INTRODUCTION TO CLOUD COMPUTING [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.

References:

1. Miller M, Cloud Computing, (8e), Que Publishers 2008.
2. Buyya R K, Cloud Computing: Principles and Paradigms, Wiley Press, (1e), 2011.
3. K Saurabh, Cloud Computing, (2e), Wiley India, 2017
4. V Joysula, M Orr, G Page, Cloud Computing: Automating the Virtualized Data Center: Cisco Press, (1e), 2012.
5. Mei- Ling Liu, “Distributed Computing: Principles and Application”, Pearson Education, Inc. New Delhi, (1e), 2004.

THIRD SEMESTER

XXXXXX: 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- IRDPTransport 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.

References:

1. Jawin: "Networks Protocols Handbook", 3rd Edition, Jawin Technologies Inc., 2005.
2. Bruce Potter and Bob Fleck : "802.11 Security", 1st Edition, O‟Reilly Publications, 2002.

XXXXXX: 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 requirements – Standardized logging criteria – Journal risk and control matrix – Neural networks – Misuse detection and Novelty detection.

References:

1. Kenneth C.Brancik "Insider Computer Fraud" Auerbach Publications Taylor & Francis Group, 2008.
2. AnkitFadia" Ethical Hacking" 2nd Edition Macmillan India Ltd, 2006

XXXXXX: CYBER SECURITY AUDIT AND COMPLIANCES [3 1 0 4]

Information Security Compliance, IT Security Assessment vs IT Security Audit, Compliance and Governance, Scope of IT Compliance Audits. Information Auditing Standards, Risk Management and Compliance, Forensic Auditing.IT Audit Standards and Ethics, Audit Planning, IT Security Assessment, Mapping IT Policies, Security Control Verification, Audit Execution, Audit Report Writing, Risk-Based Audit Planning, Evidence Collection Techniques, Computer-Assisted Audit Tools (CAATs),Reporting Techniques, Audit Quality Assurance (QA), Types of Audits: Compliance within LAN/WAN: Key Devices: Routers, switches, firewalls, proxy servers, honeypots, IDS/IPS. Traffic and Performance Monitoring: Intrusive vs non-intrusive testing. Best Practices for LAN/WAN Compliance. Compliance within Remote Access and Application Domains, Remote Devices: VPNs, workstations, authentication servers. Traffic Monitoring: VPN tunnel monitoring, remote access management. Patch Management: OS and application patch management. Best Practices: Remote access configuration validation, vulnerability management.

References:

1. Auditor’s Guide to IT Auditing by Richard E. Cascarino
2. IT Audit, Control, and Security by Robert R. Moeller
3. Human-Computer Interaction and Cybersecurity Handbook” edited by Abbas Moallem

CA7131: 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.

Course Outcome

- CA7131.1 To demonstrate a depth of knowledge of modern technology.
- CA7131.2 Design Understand about project organization and feasibility analysis in Project Management.
- CA7131.3 To complete an independent project using Software Development Life Cycle.
- CA7131.4 To acquire the skills to communicate effectively and to present ideas clearly and coherently to specific audience in both the written and oral forms.
- CA7131.5 To reflect learning and take appropriate actions to improve entrepreneur skills.

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.

Textbook(s):

1. Prasanna Chandra; Projects- Planning, Analysis, Selection, Financing, Implementation and Review’,VI Edition, Tata Mc Graw Hill.

Reference Book(s):

1. Chaudhary S.; Project Management, Tata Mc Graw Hill
2. Kerzner H.; Project Management, II Edition, CBS Publishers

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, there 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 in 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 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.

Project Synopsis Format

The project synopsis must be prepared and approved with the supervisor's input. The synopsis should include a detailed description of the proposed project and objectives. The synopsis should be prepared as per the following format.

- Title of the project
- Name of the supervisor/project guide
- Project Introduction
- Objectives of the project
- DFD, ER Diagrams
- Project Timeline
- Tools / platform, hardware and software requirement specifications
- References

Project Report Format

The final project report should describe the detailed work completed by the student. The report must be prepared as per the following format.

General Guidelines

- Project Report to be minimum 35 pages. Reports less than 35 pages will be rejected.
- Project report to be maximum 50 - 60 pages (preferred but not mandatory).
- Paper Size: A4; Left = Right = Top = Bottom Margins = 0.7".
- Page Numbering Position: Bottom with right justified and continuous numbering from the Introduction Chapter.
- Use Times New Roman Font with Normal Style, paragraph justified and 1.15 line spacing.
- Paragraph Heading: Times New Roman Font, Bold, Font Size 14; Paragraph Matter: Times New Roman Font, Normal, Font Size 12.
- Sub-paragraphs be appropriately numbered as in 1.1, 1.2, 1.3 etc; Sub-paragraph Heading: Times New Roman Font, Italics, Font Size 12; Sub-paragraph Matter: Times New Roman Font, Normal, Font Size 12.
- Figure captions below Figure with chapter wise numbering.
- Tables captions above Table with chapter wise numbering.
- All references must be listed in the order in which they appear in the report (follow IEEE format for referencing).
- Only hard bound reports will be accepted, colour of the front cover to be in mustard yellow.
- Note: The Cover page color as mentioned above has CMYK Values are C: 00 M:20 Y:75 K:00 & Hex is: FFCC00

Project Report Structure

The following structure should be followed while preparing the final project report.

1. Title Page
2. Certificate of Completion (internal/External)
3. Acknowledgement
4. Table of contents / index with page numbering
5. List of tables
6. List of figures
7. Introduction / objectives of the project
8. System analysis
9. Feasibility study
10. Software and hardware requirement specifications
11. System design (DFD, ER Diagram, Class diagram etc.)
12. Database Schema
13. Project code
14. Screenshot of the project
15. Implementation/deployment details
16. Testing (testing techniques and testing strategies used along with the test data and the errors listed for each test case).
17. Conclusion
18. Future scope and further enhancement of the project
19. Bibliography/ references
20. Appendices (if required)

Note: Reports, tables figures should be properly numbered/labelled. Two hard copies of the project report should be submitted. The soft copy of the project report in PDF should also be submitted along with the hard copy.

XXXXXX: 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.

References:

1. Ralph Oppliger :"SSL and TSL: Theory and Practice", 1st Edition, Arttech House, 2009.
2. Lawrence Harte: "Introduction to CDMA- Network services Technologies and Operations", 1st Edition, Althos Publishing, 2004.
3. Lawrence Harte: "Introduction to WIMAX", 1st Edition, Althos Publishing, 2005.

XXXXXX: 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, Creationof .bat files and insertion, Introduction of automation tools i.e. qualys, ibm appscan, 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/pii data.

References:

1. Kenneth C.Brancik "Insider Computer Fraud" Auerbach Publications Taylor & Francis Group, 2008.
2. AnkitFadia" Ethical Hacking" 2nd Edition Macmillan India Ltd, 2006

Program Electives – II

XXXXXX: 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

References:

1. David Kleidermacher, Mike Kleidermacher, Embedded and Mobile Device Security, O'Reilly Media, 2012.
2. Dominic Chell, Tyrone Erasmus, The Mobile Application Hacker's Handbook, Wiley, 2015.
3. OWASP Mobile Security Project, Mobile Application Security Verification Standard (MASVS) (Online Resource).

XXXXXX: IOT SECURITY [3 0 0 3]

Overview of IoT: Ecosystem, applications, and architectures (Perception, Network, Application layers). IoT Protocols: MQTT, CoAP, AMQP, Bluetooth, ZigBee, LoRaWAN. 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

References:

1. Madhusanka Liyanage, Andrei Gurtov, IoT Security: Advances in Authentication, 2020.
2. Fei Hu, Internet of Things Security: Principles and Practice, CRC Press, 2016.
3. NIST Cybersecurity Framework for IoT (Online Resource).

XXXXXX: 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.

References:

1. Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy, O'Reilly Media, 2009.
2. Vic (J.R.) Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics, Elsevier, 2011.
3. J.R. Rittinghouse, James F. Ransome, Cloud Computing: Implementation, Management, and Security, CRC Press, 2017.

Program Electives – III

XXXXXX: BLOCKCHAIN TECHNOLOGIES [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 etc, 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.

References:

1. Kumar Saurabh, Ashutosh Saxena, Blockchain Technology: Concepts and Applications, Wiley, 2020.
2. Daniel Drescher, Blockchain Basics, A Non-Technical introduction in 25 steps, Apress, 2017.

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

Introduction to Security Operations, Security Operations Centres (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, behaviour-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

References:

1.Incident Response & Computer Forensics" by Kevin Mandia, Chris Prosise, and Matt Pepe
2.The Practice of Network Security Monitoring" by Richard Bejtlich
3.Blue Team Handbook: Incident Response Edition" by Don Murdoch
4.The Art of Security Operations Center: A Practical Guide" by Joseph Muniz, Gary McIntyre, and Nadhem AlFardan

XXXXXX: 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.

References:

1. Andrew Wolf, Machine Learning Simplified: A Gentle Introduction to Supervised Learning, themlsbook.com, 2022.
2. Peter Bruce and Andrew Bruce, Practical Statistics for Data Scientists, Publisher(s): O'Reilly Media, Inc., 2017.

FOURTH SEMESTER

CA7270: MAJOR PROJECT [0 0 0 16]

Introduction: Each student shall carry out an industry level project in this semester. The project will be carried out under the supervision of a teacher of 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.

Course Outcome

- CA7270.1 To demonstrate in-depth knowledge and application of development technology.
- CA7270.2 Understand about project organization and project management.
- CA7270.3 To complete an independent project using software development life cycle.
- CA7270.4 To acquire the skills to communicate effectively and to present ideas clearly and coherently to specific audience in both written and oral forms.
- CA7270.5 To reflect learning and take appropriate actions to improve entrepreneurship skills.

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 in 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 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.

Project Synopsis Format

The project synopsis must be prepared and approved with the supervisor's input. The synopsis should include a detailed description of the proposed project and objectives. The synopsis should be prepared as per the following format.

- Title of the project
- Name of the supervisor/project guide
- Project Introduction
- Objectives of the project
- DFD, ER Diagrams
- Project Timeline
- Tools / platform, hardware and software requirement specifications
- References

Project Report Format

The final project report should describe the detailed work completed by the student. The report must be prepared as per the following format.

General Guidelines

- Project Report to be minimum 35 pages. Reports less than 35 pages will be rejected.
- Project report to be maximum 50 - 60 pages (preferred but not mandatory).
- Paper Size: A4; Left = Right = Top = Bottom Margins = 0.7”.
- Number of hard bound copies – Two (2)
- Page Numbering Position: Bottom with right justified and continuous numbering from the Introduction Chapter.
- Use Times New Roman Font with Normal Style, paragraph justified and 1.15 line spacing.
- Paragraph Heading: Times New Roman Font, Bold, Font Size 14; Paragraph Matter: Times New Roman Font, Normal, Font Size 12.
- Sub-paragraphs be appropriately numbered as in 1.1, 1.2, 1.3 etc; Sub-paragraph Heading: Times New Roman Font, Italics, Font Size 12; Sub-paragraph Matter: Times New Roman Font, Normal, Font Size 12.
- Figure captions below Figure with chapter wise numbering.
- Tables captions above Table with chapter wise numbering.
- All references must be listed in the order in which they appear in the report (follow IEEE format for referencing).
- Only hard bound reports will be accepted, colour of the front cover to be in mustard yellow (refer format).
- Note: The Cover page color as mentioned above has CMYK Values are C:00 M:20 Y:75 K:00 & Hex is: FFCC00

Project Report Structure

The following structure should be followed, to whatever extent possible, while preparing the final project report.

- Title Page
- Certificate of Completion (Internal/External)
- Abstract
- Acknowledgement
- List of tables
- List of figures
- Table of contents (with page numbering)
- Introduction

    - Company Profile
    - Existing System and Need for System
    - Scope of Work
    - Operating Environment - Hardware and Software
- System Analysis and Design
    - Feasibility study
    - Software and hardware requirement specifications
    - Data Flow Diagram (DFD)
    - Functional Decomposition Diagram (FDD)
    - Entity Relationship Diagram (ERD)
    - Data Dictionary
    - Table Design
    - Code Design
    - Menu Tree
    - Menu Screens
    - Input Screens
    - Test Procedures and Implementation
- Project code
- Screenshots of the project
- Implementation/deployment details
- Conclusion
- Future scope of the project
- Drawbacks and Limitations
- Bibliography/ References
- Annexures (if required)

Note: Reports, tables figures should be properly numbered/labelled. Two hard copies of the project report should be submitted. The soft copy of the project report in PDF should also be submitted along with the hard copy

New Courses Introduced: Not Applicabel

C. Attendance

A minimum of 75% Attendance is required to be maintained by a student to be qualified for taking up the End Semester examination. The allowance of 25% includes all types of leaves including medical leaves.

D. Examination Pattern

Criteria	Description	Maximum Marks
Internal Assessment (Summative)	Sessional Exam I (Close/Open Book)	30
	In class Quizzes and Assignments, every semester, students must obtain some type of certification, either through Swayam or another platform such as Coursera, etc. One SWAYAM Certification is required for the complete program, Activity feedbacks (Accumulated and Averaged)	30
End Term Exam (Summative)	End Term Exam (Close/Open Book)	40
	Total	100

Make up Assignments (Formative)	Students who miss a class will have to report to the teacher about the absence. A makeup assignment on the topic taught on the day of absence will be given which has to be submitted within a week from the date of absence. No extensions will be given on this. The attendance for that particular day of absence will be marked blank, so that the student is not accounted for absence. These assignments are limited to a maximum of 5 throughout the entire semester.
Homework/ Home Assignment/ Activity Assignment (Formative)	There are situations where a student may have to work in home, especially before a flipped classroom. Although these works are not graded with marks. However, a student is expected to participate and perform these assignments with full zeal since the activity/ flipped classroom participation by a student will be assessed and marks will be awarded.

E. Minimum for pass

As per the university norms.

F. Number of attempts

As per the university norms.

G. Reference list of books & journals

To be provided along with the detailed syllabus.

H. Collaborations with other department Institutions

Only faculty required from Department of English, Mathematics to teach Technical Communication, Mathematics papers and Environmental Science respectively.

Else Experts required for following Core Subject starting from semester 1

- Foundations in Cybersecurity
- Intrusion Detection Systems
- Secure Protocol Design
- Ethical Hacking and Penetration Testing
-

Expert in Department

S.NO	Expert Name	Domain
1	Dr. Devershi Pallavi Bhatt	Information Security
2	Dr. Linesh Raja	Wireless Networking
3	Dr. Kuntal Gaur	Software Defined Network
4	Dr. Pragya Vaishnav	Security

I. Industry placements/Internships

"The provision of a summer internship is made available for MSc (CS) students after completing Semester 2. The duration of the internship is a minimum of 30 days. In Semester 3, all students are required to complete a minor project based on the skills developed during the internship. Following Semester 3, there is a provision of mandatory 6-month industry internship to further build practical expertise."

J. Prospects & Placements

The Institution's placement cell, industry collaborators, and alumni network will facilitate placements and internships in roles such as cybersecurity analysts, penetration testers, and security engineers. The course targets placements and internships in top companies like Capgemini, Palo Alto Networks, Oracle, Publicis Sapient, Wipro, SAP Labs, and Infosys, in domains such as finance, government, defense, and healthcare.

Industry Feedback Inclusion

First Semester:

- Based on industry recommendations, it is suggested to include a course on **Operating Systems and Shell Programming** to provide students with essential foundational knowledge.
- Additionally, we have incorporated a module on **Introduction to Computer Networks & Protocols**. This module aims to elucidate how the internet and various devices—both personal and network—function collaboratively to facilitate internet connectivity, with a focus on understanding IP protocols.

Second Semester:

- In response to industry feedback, we will be adding **Automation with Python** as a key course to equip students with valuable automation skills.
- Furthermore, we will include a course on **Web Application Security Fundamentals** to address the critical need for knowledge in securing web applications against vulnerabilities.

Third Semester:

- For Program Electives II and III, it is recommended to add the following courses, both of which hold significant industry relevance and demand:
  - Mobile Security Fundamentals
  - Security Operations and Incident Response

Note: Detailed discussion of mail has been attached in Annexure II