

As Per NEP 2020

University of Mumbai



Syllabus for Major Vertical – 1, 4 & 5

Name of the Programme – B.E. (Computer Science & Engineering – Cyber Security)

Faculty of Engineering

Board of Studies in Information Technology

U.G. Third Year Programme	Exit Degree	B.Sc. Tech Engineering- <u>Computer Science & Engineering – Cyber Security.</u>
Semester	V & VI	
From the Academic Year	2026-27	

University of Mumbai



(As per NEP 2020)

Sr. No.	Heading	Particulars
1	Title of program O: _____	<u>B.E. (Computer Science & Engineering – Cyber Security)</u>
2	Exit Degree	<u>B.Sc. Tech Engineering – Computer Science & Engineering – Cyber Security.</u>
3	Scheme of Examination R: _____	NEP 40% Internal 60% External, Semester End Examination Individual Passing in Internal and External Examination
4	Standards of Passing R: _____	40%
5	Credit Structure R: _____	Attached herewith
6	Semesters	Sem. V & VI
7	Program Academic Level	5.5
8	Pattern	Semester
9	Status	New
10	To be implemented from Academic Year	2026-27

Sd/-
Dr. Vaishali D. Khairnar
BoS Chairman - Information Technology
Faculty of Technology

Sd/-
Dr. Deven Shah
Associate Dean
Faculty of Science & Technology

Sd/-
Prof. Shivram S. Garje
Dean
Faculty of Science & Technology

Preamble

To meet the challenge of ensuring excellence and NEP 2020 policy in engineering education, the issue of quality needs to be addressed, debated, and taken forward systematically. Accreditation is the principal means of quality assurance in higher education. The major emphasis of the accreditation process is to measure the outcomes of the program that is being accredited. In line with this Faculty of Science and Technology (in particular Engineering) of the University of Mumbai has taken the lead in incorporating the philosophy of NEP 2020 education in the process of curriculum development.

The third-year engineering course consists of a core and elective training program to impart scientific and logical thinking training to learners in general, with a choice of course selection from the program core course, program elective course, multidisciplinary minor, IKS, PCE and vocational skill-enhanced course. Simultaneously, the objectives of NEP 2020 demand nurturing the core program, elective program, communication skills and skills required for the Computer Science & Engineering - Cyber Security Branch of engineering in the learner. Keeping this in view, a pool of courses is offered in Core Courses covering fundamentals required to understand core and modern engineering practices and emerging trends. Elective courses are offered to the learners to understand the concepts of emerging technology. This will help with the holistic development of learners through interdisciplinary skills development and mobility among other departments as real-time solutions. Considering the shift in pedagogy and the convenience of a stress-free learning process, a choice-based subject pool is offered in the coursework under the heads of Computer Science & Engineering - Cyber Security in Engineering for open electives and multidisciplinary minor courses in sem V and VI. Essentially, to give a glimpse of trends in the industry under vocational and enhanced skill practices, the pool is offered to nurture and develop creative skills in contemporary industrial practices. Criteria met in the structure is the opportunity for learners to choose the course of their interest in all disciplines.

Program Core Course and Program Elective Courses Cover Computer Science & Engineering - Cyber Security core and elective courses. Also, MDM is where a pool of subjects is given for selection. In addition to this learner will have IKS and PCE courses. Considering the present scenario, diverse choices need to be made available to fulfil the expectation of a learner to aspire for a career in the field of current trends of Technology and interdisciplinary research. The IKS course will be program-specific, which can be achieved in Undergraduate training by giving an objective viewpoint to the learning technology, from ascent time and how it was learned and the process and transitioning a learner from a rote learner to a creative professional. For this purpose, PCE is introduced in the First Semester to orient a communication skills to become skilled professionals for placement and higher education entrance exams. Considering the NEP-2020 structure of award of Certificate after U.G. First Year, U. G. Diploma after the Second Year and B.Sc. Tech Engineering after the Third Year at multiple exit-point pools of Vocational skills, is arranged to give exposure to the current Industry practices.

The faculty resolved that course objectives and course outcomes are to be clearly defined for every core and elective course so that all faculty members in affiliated higher education institutes understand the depth and approach of the course to be taught to the learners, which will enhance the learners' learning process. NEP 2020 grading system enables a much-needed shift in focus from teacher-centric to continuous-based learner-centric education since the workload estimated is based on the investment of time in learning and not in teaching. It also focuses on the holistic development of the learners through mobility and continuous evaluation, which will enhance the quality of education. Credit assignment for courses is based on a 15-week teaching-learning process for NEP 2020; however, the content of courses is to be taught in 12-13 weeks, and the remaining 2-3 weeks are to be utilized for revision, self learning, tutorial, guest lectures, coverage of content beyond the syllabus, etc.

There was a concern that in the present system, the third-year syllabus must not be heavily loaded for the learner and it is of utmost importance that the learner entering into the third year of an engineering course should feel at ease by lowering the burden of syllabus and credits. This is necessary for a learner to get accustomed to the new environment of a college and to create a bond between the teacher and the learner. The present curriculum will be implemented for the Third Year of Engineering from the academic year 2026-27. Subsequently, this system will be carried forward for Final Year Engineering in the academic years 2027-28, respectively.

Sd/-

Dr. Vaishali D. Khairnar
BoS-Chairman-Information Technology
Faculty of Technology

Sd/-

Dr. Deven Shah
Associate Dean
Faculty of Science & Technology

Sd/-

Prof. Shivram S. Garje
Dean
Faculty of Science & Technology

B.Sc. Tech Engineering (Computer Science & Engineering -Cyber Security).

Credit Structure (Sem. V & VI)

	R: _____ C									
Level	Semester	Major		Minor	OE	VSC, SEC (VSEC)	AEC, VEC, IKS	OJT, FP, CEP, CC,RP	Cum. Cr. / Sem.	Degree/ Cum. Cr.
		Mandatory	Electives							
5.5	V	PCC501:3 PCC502:3 PCC503:3 PCL501: 1 PCL502:1 PCL503:1	PEC501:3 PEL501:1	MDC:3 MDL:1	OE:2	--	IKS: 2	--	24	B.Sc. Tech Engineering (Computer Science & Engineering – Cyber Security) 48
	R: _____ D									
	VI	PCC601:3 PCC602:3 PCL601:1 PCL602:1	PEC601:3 PEC602:3 PEL601:1 PEL602:1	MDC: 3 MDL:1	--	VSEC:2	AEC: 2	--	24	
	Cum Cr.	20	12	8	2	2	2+2	--	48	

Exit option: Award of BSc. Tech Engineering with 138 credits and additional 4 credits core **one** theory subject with 3 credits and **one** lab with 1 credit from one final year from where they want to take Exit degree. Along with theory and practical course student must compulsory do internship for **one month or 160 hours** which internship is equal to 4 credits.

[Abbreviation - OE – Open Electives, VSC – Vocation Skill Course, SEC – Skill Enhancement Course, (VSEC), AEC – Ability Enhancement Course, VEC – Value Education Course, IKS – Indian Knowledge System, OJT – on Job Training, FP – Field Project, CEP – Continuing Education Program, CC – Co-Curricular, RP – Research Project]

Sem. – V & VI

T.E. Computer Science & Engineering - Cyber Security Scheme

Program Structure for Third Year of Computer Science & Engineering -Cyber Security
UNIVERSITY OF MUMBAI (With Effect from 2026-2027)

SEMESTER V

Course Code	Course Description	Teaching Scheme (Contact Hours)			Credit Assigned			
		Theory	Practical	Tutorial	Theory	Tutorial	Practical	Total Credits
2445111	Computer Networks	3	--	--	3	--	--	3
2445112	Cryptography and Network Security	3	--	--	3	--	--	3
2445113	Web Application and Database Security	3	--	--	3	--	--	3
2445114X	PEC-1	3	--	--	3	--	--	3
MDC501	Multidisciplinary minor	3	--	--	3	--	--	3
2445115	Computer Networks Lab	--	2	--	--	--	1	1
2445116	Cryptography and Network Security Lab	--	2	--	--	--	1	1
2445117	Web Application and Database Security Lab	--	2	--	--	--	1	1
2445118X	PEL-1	--	2	--	--	--	1	1
MDL501	Multidisciplinary minor	--	2@	--	--	--	1	1
OECL501	To be taken from the bucket provided by the University from other Faculty	2#	--	---	2	--	--	2
2345511	Indian Knowledge System as per Group A	--	2*+2	--	--	--	2	2
Total		17	14	00	17	00	07	24

* Two hours of practical class to be conducted for full class as demo/discussion.

Theory / Tutorial 1 credit for 1 hour and Practical 1 credit for 2 hours

Institute shall offer a course for Open Elective from Science/Commerce/Management stream bucket provided by the University of Mumbai.

@ Institute shall offer a course for MDM from other Engineering Boards Group.

Course Code	Course Description
24451141	Artificial Intelligence
24451142	Fundamentals of IoT
24451143	Internet Programming
24451144	Software Engineering and Agile Practices
Lab Code	Lab Description
24451181	Artificial Intelligence Lab
24451182	Fundamentals of IoT Lab
24451183	Internet Programming Lab

course Code	Course Description	Examination scheme							
		Internal Assessment Test (IAT)			End Sem. Exam Marks	End Sem. Exam Duration (Hrs)	Term Work (Tw)	Oral & Pract.	Total
		IAT-I	IAT-II	Total (IAT-I) + IAT-II)					
2445111	Computer Networks	20	20	40	60	2	--	--	100
2445112	Cryptography and Network Security	20	20	40	60	2	--	--	100
2445113	Web Application and Database Security	20	20	40	60	2	--	--	100
2445114X	PEC-1	20	20	40	60	2	--	--	100
MDC501	Multidisciplinary minor	20	20	40	60	2	--	--	100
2445115	Computer Networks Lab	--	--	--	--	--	25	--	25
2445116	Cryptography and Network Security Lab	--	--	--	--	--	25	25	50
2445117	Web Application and Database Security Lab	--	--	--	--	--	25	25	50
2445118X	PEL-1	--	--	--	--	--	25	25	50
MDL501	Multidisciplinary minor	--	--	--	--	--	25	25	50
OECL501	To be taken from the bucket provided by the University from other Faculty	--	--	--	--	--	50	--	50
2345511	Indian Knowledge System as per Group A						50	--	50
Total		100	100	200	300	10	225	100	825

Program Structure for Third Year of Computer Science & Engineering - Cyber Security
UNIVERSITY OF MUMBAI (With Effect from 2026-2027)

SEMESTER VI

Course Code	Course Name	Teaching Scheme (Contact Hours)				Credits Assigned			
		Theory	Practical	Tutorial	Total	Theory	Practical	Tutorial	Total
2446111	Blockchain Technology	3	--	--	03	3	--	--	03
2446112	Cyber Forensics & Incident Response	3	--	--	03	3	--	--	03
2446113X	PEC-2	3	--	--	03	3	--	--	03
2446114X	PEC-3	3	--	--	03	3	--	--	03
MDC601	Multidisciplinary Minor Course	3	--	--	03	3	--	--	03
2446115	Blockchain Technology Lab	--	2	--	02	--	2	--	01
2446116	Cyber Forensics & Incident Response Lab	--	2	--	02	--	2	--	01
2446117X	PEL-2	--	2	--	02	--	1	--	01
2446118X	PEL-3	--	2	--	02	--	1	--	01
MDL601	Multidisciplinary Minor Lab	--	2@	--	02	--	1	--	01
2446411	Innovation Lab (Mini Project)	--	4	--	04	--	1	--	02
2996511	Professional Skill	--	2* + 2	--	04	--	1	--	02
Total		15	18	00	33	15	09	00	24

* Two hours of practical class to be conducted for full class as demo/discussion.

Theory / Tutorial 1 credit for 1 hour and Practical 1 credit for 2 hours

@ Institute shall offer a course for MDM from other Engineering Boards.

Course Code	Course Description
24461131	Cyber Threat Intelligence and Risk Management
24461132	ML & DL for Security Analytics
24461133	IoT Device Security & Embedded Systems
24461134	DevOps and CI/CD Automation
24461141	Malware Analysis
24461142	Information Security Management Systems (ISMS)
24461143	Cloud Computing and Security
24461144	User Interface Design with Security
Lab Code	Lab Description
24461171	Cyber Threat Intelligence and Risk Management Lab
24461172	ML & DL for Security Analytics Lab
24461173	IoT Device Security & Embedded Systems Lab
24461174	DevOps and CI/CD Automation Lab
24461181	Malware Analysis Lab
24461182	Information Security Management Systems (ISMS) Lab
24461183	Cloud Computing and Security Lab
24461184	User Interface Design with Security Lab

Course Code	Course Name	Examination Scheme							
		Internal Assessment Test (IAT)			End Semester Exam Marks	End Semester Exam Duration (Hrs)	Term Work (TW)	Oral & Practical	Total
		IAT-I	IAT-II	Total (IAT-I) + IAT-II)					
2446111	Blockchain Technology	20	20	40	60	2	--	--	100
2446112	Cyber Forensics & Incident Response	20	20	40	60	2	--	--	100

2446113X	PEC-2	20	20	40	60	2	--	--	100
2446114X	PEC-3	20	20	40	60	2	--	--	100
MDC601	Multidisciplinary Minor Course	20	20	40	60	2	--	--	100
2446115	Blockchain Technology Lab	--	--	--	--	--	25	25	50
2446116	Cyber Forensics & Incident Response Lab	--	--	--	--	--	25	25	50
2446117X	PEL-2	--	--	--	--	--	25	25	50
2446118X	PEL-3	--	--	--	--	--	25	25	50
MDL601	Multidisciplinary Minor Lab	--	--	--	--	--	25	25	50
2446411	Innovation Lab (Mini Project)	--	--	--	--	--	50	--	50
2996511	Professional Skill	--	--	--	--	--	25	--	25
Total		100	100	200	300	10	200	200	825

Vertical – 1

Major

DRAFT

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
2445111	Computer Networks	3	---	---	3	---	---	3

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
2445111	Computer Networks	20	20	40	60	02	---	---	100

Course Objective: Students will be able to learn:

Sr. No.	Course Objectives
1	Study the basic taxonomy and terminology of the computer networking, enumerate the layers of OSI model and TCP/IP model.
2	Study the fundamentals and basics of Physical layer and data link layer concepts, design issues, and protocols.
3	Gain core knowledge of Network layer routing protocols and IP addressing, Transport layer services, and protocols.
4	Study Session layer protocols and Presentation layer paradigms and protocols.
5	Acquire knowledge of Application layer and Protocols.
6	Acquire insights on Authentication, Access Control and Threat Mitigation

Course Outcomes: On successful completion of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Explain communication protocols, layered network architectures and network topologies	L2
2	Apply Physical and Data Link Layer concepts and protocols.	L3
3	Analyze routing protocols and design appropriate IP addressing schemes for given network scenarios.	L4
4	Analyze session and presentation layer protocols and paradigms and evaluate their role in communication efficiency.	L4
5	Evaluate application layer protocols based on performance and functionality.	L5
6	Assess the effectiveness of authentication mechanisms, access control models, and threat mitigation strategies in network security architectures.	L5

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mappings
0	Prerequisites	Prerequisite Concepts and Course Introduction	02	-
1	Introduction to Computer Networks	Definition of a Computer Network; Components of a computer network: Classification of networks, network types, Network topologies, networking devices, Networks Software; Protocol hierarchy, Design issues for the layers, Service Primitives, OSI Reference Model and TCP/IP Reference Model Self Learning Topics: Physical Media (Coaxial, Twisted-Pair, Fiber-Optic, Serial Cables)	05	CO1
2	Physical Layer and Data Link layer	Switching Techniques; Comparison of switching techniques; Multiplexing: FDM, TDM, WDM, Hamming code, Flow and Error Control Self Learning Topics: IEEE 802.11, CSMA/CD vs CSMA/CA	06	CO2
3	Network-Layer & Transport Layer	Introduction: Network-Layer Services, Packet Switching, Network-Layer Performance, Network Layer Protocols: IPv4 Datagram Format, IPv4 Addresses, Forwarding of IP Packets, ICMPv4, Internet Protocol Version 6 (IPv6) Transport-Layer Protocols, User Datagram Protocol: User Datagram, UDP Services, UDP Applications, TCP Services, Features and Segment, TCP Timers, TCP Flow control (sliding Window), Subnetting Self Learning Topics: NAT, VPNs	08	CO3
4	Session Layer and Presentation Layer	Session layer design issues, Session Layer protocol - Remote Procedure Call (RPC), Sockets, Compression: Lossless Compression, Lossy Compression, Huffman Coding, Adaptive Huffman Compression, TLS/SSL. Self Learning Topics: Piggybacking, Speech Compression	06	CO4
5	Application Layer	DNS: Name Space, Resource Record and Types of Name Server. HTTP, SMTP, SSH, FTP, DHCP Self Learning Topics: SNMP, Electronic mail	05	CO5
6	Network Security Concepts	Authentication and Access Control: Security Filtering, Managing User Account and Password Security, User-Authentication Methods (Public Key Infrastructure (PKI), Kerberos, Authentication, Authorization, and	07	CO6

		Accounting(AAA), Network Access Control(NAC), Network Threats and Mitigation: Recognizing SecurityThreats, Understanding Mitigation Techniques, Policies and Procedures,Physical and Hardware Security, Defining Firewalls, Firewall Technologies,IDS/IPS. Self Learning Topics: Network troubleshooting and Network Scanners.		
--	--	--	--	--

Note: No questions will be asked in the end-semester exam from self-study topics. However, students are encouraged to explore these topics for a better understanding of the subject.

Text Books:

Textbooks:	
1	Behrouz A. Forouzan, Forouzan Mosharrat , Computer Networks: A Top down Approach, McGraw Hill education.
2	Andrew S Tanenbaum, Computer Networks -, 4th Edition, Pearson Education.
3	James F. Kurose, Keith W. Ross, Computer Networking, A Top-Down Approach Featuring the Internet,6th edition, Addison Wesley
Reference Books:	
1	Behrouz A. Forouzan, Data communications and Networking, Fifth edition TMH 2013.
2	Larry L.Peterson, Bruce S.Davie, Computer Networks: A Systems Approach, Second Edition The Morgan Kaufmann Series in Networking
Access to software and virtual labs:	
1	Network Simulator ns2
2	https://www.nsnam.org/
3	https://www.coursera.org/learn/computer-networkin

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

- IAT will consist of two compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I the remaining syllabus content must be covered in the IAT-II.

End Semester Theory Examination:

- Question Paper will comprise a total of **six questions each carrying 15 marks. Question 1** will be **compulsory** and should **cover the maximum contents of the syllabus.**

- **Remaining questions** will be **mixed in nature**. (Part (a) and part (b) of each question must be from different modules. For example, if Q2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules).
- A total of **four questions** need to be answered.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
2445112	Cryptography and Network Security	3	---	---	3	---	---	3

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
2445112	Cryptography and Network Security	20	20	40	60	02	---	---	100

Course Objective: Students will be able to learn:

Sr. No.	Course Objectives
1	The basic concepts of computer and Network Security.
2	Various cryptographic algorithms including secret key management and different authentication techniques.
3	Different types of malicious Software and its effect on the security.
4	Various secure communication standards including IPsec, SSL/TLS and email.
5	The Network management Security and Network Access Control techniques in Computer Security.
6	Different attacks on networks and infer the use of firewalls and security protocols.

Course Outcomes: On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Explain security goals, attacks, services, mechanisms, and apply number theory in classical cryptography.	L2 – Understand
2	Apply symmetric and asymmetric cryptographic techniques for secure communication and key management.	L3 – Apply
3	Analyze cryptographic hash functions and digital signature schemes for ensuring integrity and authentication.	L4 – Analyze

4	Evaluate authentication protocols and secure communication protocols used in modern networks.	L5 – Evaluate
5	Analyze network-level attacks and recommend appropriate defense mechanisms.	L4 – Analyze
6	Design secure network architectures using firewalls, IDS, NAC, and network management security principles.	L6 – Create

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mappings
0	Prerequisite	Basic concepts of Computer Networks (TCP/IP model, OSI model), Operating Systems (process, memory, access control), Fundamentals of Discrete Mathematics (modular arithmetic basics).	2	-
1	Security Fundamentals & Classical Cryptography	Computer Security vs Network Security, CIA Triad, Security Services & Mechanisms, Types of Attacks (Passive & Active), OSI Security Architecture, Network Security Model. Number Theory: Modular Arithmetic, Euclidean Algorithm, Fermat's Theorem, Euler's Theorem. Classical Encryption Techniques: Monoalphabetic & Polyalphabetic substitution (Vigenere, Playfair, Hill cipher), Transposition techniques (Keyed & Keyless). Introduction to Steganography. Self Study Topics: Zero Trust Security Architecture Advanced Persistent Threats (APT) and Cyber Kill Chain, Public Key Infrastructure (PKI) and Digital Certificates, Elliptic Curve Cryptography (ECC) basics	8	CO1
2	Symmetric & Asymmetric Cryptography and Key Management	Symmetric Cipher Model, Block Cipher Principles, Modes of Operation (ECB, CBC, CFB, OFB, CTR), DES, Double DES, Triple DES, AES, Stream Ciphers (RC4). Public Key Cryptography Principles, RSA Algorithm, Knapsack Cryptosystem (conceptual), Diffie-Hellman Key Exchange. Key Distribution: KDC, Needham-Schroeder Protocol, Kerberos Authentication Protocol. Digital Certificates: X.509, Public Key Infrastructure (PKI). Self Study Topics: Lightweight cryptography for IoT (e.g., PRESENT, SPECK), Post-Quantum Cryptography (lattice-based, hash-based methods), Blockchain-based key management and cryptographic systems, Homomorphic Encryption and Secure Multi-Party Computation	11	CO2
3	Cryptographic Hash Functions & Digital Signatures	Properties of Secure Hash Functions, MD5, SHA-1 (limitations), SHA-256, SHA-512, MAC, HMAC, CMAC. Digital Signatures: RSA Signature, DSS. Attacks on Digital Signature. Self Study Topics: Cryptographic hash collisions and real-world attacks (e.g., MD5/SHA-1), Post-quantum digital signature schemes (e.g., lattice-based signatures),	5	CO3

		Blockchain hashing and Merkle Trees, Hash-based authentication in modern protocols (e.g., OAuth, JWT)		
4	Authentication Protocols & Secure Communication	User Authentication (Password-based, Challenge-Response, Multi-factor), Remote User Authentication Protocols. SSL Architecture, Transport Layer Security (TLS), HTTPS, Secure Shell (SSH). IPSec Architecture (AH, ESP), VPN concepts. Secure Email: PGP, S/MIME. Self Study Topics: Biometric authentication systems and behavioral biometrics, Zero Trust Authentication and Identity Management (IAM), TLS 1.3 enhancements and forward secrecy, Secure Access Service Edge (SASE) and modern VPN architectures	7	CO4
5	Network Attacks & Defense Mechanisms	TCP/IP Vulnerabilities (Layer-wise), Network Attacks: Packet Sniffing, ARP Spoofing, IP Spoofing, Port Scanning. DoS Attacks (SYN Flood, UDP Flood, ICMP Flood), Distributed DoS (DDoS). Malicious Software: Worms, Viruses, Trojan Horse, Rootkits, Keyloggers, Phishing, SPAM, Backdoors. SQL Injection, Buffer Overflow. Self Study Topics: Advanced Persistent Threats (APT) and multi-stage attack lifecycle, Zero-day vulnerabilities and exploit development basics, AI/ML in cyber attacks and defense (adversarial attacks, anomaly detection), Cloud security threats and container vulnerabilities	8	CO5
6	System Security & Network Management Security	Firewall Design Principles, Characteristics & Types of Firewalls (Packet Filtering, Stateful Inspection, Application-Level Gateway). Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS). Network Access Control (NAC): Principle Elements, Enforcement Methods, Implementation & Use Cases. SNMPv3 Security. Self Study Topics: Next-Generation Firewalls (NGFW) and Unified Threat Management (UTM), Security Information and Event Management (SIEM) systems, Zero Trust Network Access (ZTNA), Network Behavior Anomaly Detection (NBAD) using AI/ML	6	CO6

Note: No questions will be asked in the end-of-semester exam from self-study topics. However, students are encouraged to explore these topics for a better understanding of the subject.

Text Books:

Textbooks:	
1	William Stallings, Cryptography and Network Security, Principles and Practice, 6th Edition, Pearson Education, March 2013.
2	Behrouz A. Ferouzan, "Cryptography & Network Security", Tata Mc Graw Hill.
3	Mark Stamp's Information Security Principles and Practice, Wiley

4	Bernard Menezes, “Cryptography & Network Security”, Cengage Learning
Reference Books:	
1	Applied Cryptography, Protocols, Algorithms and Source Code in C, Bruce Schneier, Wiley.
2	Cryptography and Network Security, Atul Kahate, Tata Mc Graw Hill.
3	www.rsa.com
Access to software and virtual labs:	
1	https://swayam.gov.in/
2	https://nptel.ac.in/
3	https://www.coursera.org/

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

- IAT will consist of two compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I the remaining syllabus content must be covered in the IAT-II.

End Semester Theory Examination:

- Question Paper will comprise a total of **six questions each carrying 15 marks. Question 1** will be **compulsory** and should **cover the maximum contents of the syllabus**.
- **Remaining questions** will be **mixed in nature**. (Part (a) and part (b) of each question must be from different modules. For example, if Q2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules).
- A total of **four questions** need to be answered.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
2445113	Web Application and Database Security	3	---	---	3	---	---	3

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
2445113	Web Application and Database Security	20	20	40	60	02	---	---	100

Course Objective: Students will be able to learn:

Sr. No.	Course Objectives
1	Understand security principles related to web applications and databases
2	Identify vulnerabilities in web and database-driven applications
3	Learn secure coding practices for web applications
4	Apply authentication and authorization mechanisms
5	Understand database security models and access control
6	Analyze and mitigate common web and database attacks

Course Outcomes: On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive Levels of
---------	-----------------	---------------------

		Attainment as per Bloom's Taxonomy
1	Explain web and database security concepts	L2
2	Analyze common web vulnerabilities	L4
3	Design secure web applications	L6
4	Apply authentication and authorization techniques	L4
5	Implement database security mechanisms	L3
6	Evaluate threats and security controls	L3

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mapping
0	Introduction to Security	Introduction to security concepts, CIA Triad (Confidentiality, Integrity, Availability), security goals, basics of threat modeling, identification of attack surface, overview of OWASP and OWASP Top 10	02	CO1
1	Web Application Architecture & Threats	Web application architecture, client-server and multi-tier architecture, HTTP and HTTPS protocols, cookies and sessions, session management concepts, same-origin policy, common architectural threats Self-Learning Topics: OWASP recommendations for secure web application development	06	CO1
2	Web Application Vulnerabilities	Web application vulnerabilities, SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), file inclusion attacks, command injection, improper input validation Self-Learning Topics: Case studies on web application vulnerabilities ; OWASP-based prevention techniques for common attacks	06	CO2
3	Secure Web Application Design	Secure web application design principles, Secure SDLC, security requirements in SDLC phases, input validation techniques, output encoding, secure session management, secure error handling Self-Learning Topics: Secure error-handling methods in web systems	07	CO3

4	Authentication & Authorization	Authentication and authorization concepts, password security, hashing and salting, multi-factor authentication, OAuth basics, role-based access control (RBAC), common authentication flaws Self-Learning Topics: Basics of OAuth and RBAC, Common authentication and authorization vulnerabilities	04	CO4
5	Database Security Fundamentals	Database security concepts, database threats, access control mechanisms, user roles and privileges, views, encryption of data, database auditing and logging Self-Learning Topics: Access control using roles, privileges, and views	08	CO5
6	Advanced Web & Database Security	Stored procedure security, secure database backup and recovery, NoSQL database security issues, security testing tools, vulnerability assessment and penetration testing basics Self-Learning Topics: Basics of security testing, vulnerability assessment, and penetration testing, Stored procedure vulnerabilities and secure coding practices	08	CO6
Note: No questions will be asked in the end-semester exam from self-study topics. However, students are encouraged to explore these topics for a better understanding of the subject				

Text Books:

Textbooks:	
1	Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India
2	William Stallings, Computer Security: Principles and Practice, Pearson India
3	B. B. Meshram & M. S. Obaidat, Information and Network Security, Wiley India
4	Ankit Fadia, Web Hacking: Attacks and Defense, Macmillan India
Reference Books:	
1	Michael E. Whitman & Herbert J. Mattord, Principles of Information Security, Cengage Learning
2	Dafydd Stuttard & Marcus Pinto, The Web Application Hacker's Handbook, Wiley

3	Ivan Ristic, Web Application Security, O'Reilly Media
4	Pavan Duggal, Cyber Law in India, Saakshar Law Publications
Access to software and virtual labs:	
1	https://owasp.org
2	https://portswigger.net/
3	https://developer.mozilla.org
4	https://www.meity.gov.in

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

- IAT will consist of two compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I the remaining syllabus content must be covered in the IAT-II.

End Semester Theory Examination:

- Question Paper will comprise a total of **six questions each carrying 15 marks. Question 1** will be **compulsory** and should **cover the maximum contents of the syllabus**.
- **Remaining questions** will be **mixed in nature**. (Part (a) and part (b) of each question must be from different modules. For example, if Q2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules).
- A total of **four questions** need to be answered.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24451141	Artificial Intelligence	3	---	---	3	---	---	3

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24451141	Artificial Intelligence	20	20	40	60	02	---	---	100

Course Objective: Students will be able to learn:

Sr. No.	Course Objectives
1	Provide foundational knowledge of Artificial Intelligence, its evolution, core concepts, sub-areas, and emerging trends.
2	Develop understanding of intelligent agents, their environments, rational behavior, and problem formulation techniques for search-based solutions
3	Introduce various problem-solving strategies including uninformed, informed, local,

	and adversarial search algorithms.
4	Build the ability to represent knowledge formally using logic and perform reasoning under certain and uncertain conditions.
5	Familiarize students with AI planning techniques and different learning paradigms including reinforcement and statistical learning.
6	Create awareness about AI applications across domains and emphasize ethical considerations such as fairness, bias, transparency, and societal impact.

Course Outcomes: On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Explain the fundamental concepts of Artificial Intelligence including its history, foundations, components of intelligent systems, sub-areas, and current trends.	L2
2	Analyze intelligent agents, their environments, rationality, structures, and apply problem formulation concepts for search-based problem solving.	L4
3	Apply appropriate uninformed, informed, local, and adversarial search algorithms to solve complex AI problems and evaluate their performance.	L3
4	Represent knowledge using propositional and first-order logic and perform logical inference using resolution, unification, forward and backward chaining under certain and uncertain environments.	L3
5	Demonstrate understanding of AI planning techniques and various learning paradigms including reinforcement learning and statistical learning approaches.	L2
6	Assess AI applications across domains and evaluate ethical issues such as bias, fairness, transparency, and societal impact in AI systems.	L5

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mappings
---------	----------------	------------------	-------	-------------

1	Introduction to Artificial Intelligence	Introduction, History of Artificial Intelligence, Intelligent Systems: Categorization of Intelligent System, Components of AI Program, Foundations of AI, Sub-areas of AI, Applications of AI, Current trends in AI. Self Learning Topics: Weak AI vs Strong AI, Explainable AI (XAI), Generative AI	04	CO1
2	Intelligent Agents	Agents and Environments, The concept of rationality, The nature of environment, The structure of Agents, Types of Agents, Learning Agent. Solving problem by Searching: Problem Solving Agent, Formulating Problems, Example Problems. Self Learning Topics: Multi-agent systems, Autonomous agents in robotics	04	CO2
3	Problem Solving	Uninformed Search Methods: Breadth First Search (BFS), Depth First Search (DFS), Depth Limited Search, Depth First Iterative Deepening (DFID), Informed Search Methods: Greedy best first Search, A* Search, Memory bounded heuristic Search. Local Search Algorithms and Optimization Problems: Hill climbing search Simulated annealing, Genetic algorithms. Adversarial Search: Game Playing, Min-Max Search, Alpha Beta Pruning. Self Learning Topics: Travelling Salesman Problem using Genetic Algorithm, Real world applications of simulated annealing	10	CO3
4	Knowledge and Reasoning	Knowledge based Agents, Brief Overview of propositional logic, First Order Logic: Syntax and Semantic, Inference in FOL, Forward chaining, backward Chaining. Knowledge Engineering in First-Order Logic, Unification, Resolution, Uncertain Knowledge and Reasoning: Uncertainty, Representing knowledge in an uncertain domain, The semantics of belief network, Simple Inference in belief network. Self Learning Topics: Expert systems and rule-based systems, Bayesian Networks applications, Probabilistic reasoning vs logical reasoning	12	CO4
5	Planning and Learning	The planning problem, Planning with state space search, Partial order planning, Hierarchical planning, Conditional Planning. Learning: Forms of Learning, Theory of Learning, PAC learning. Introduction to statistical learning (Introduction only) Introduction to reinforcement learning: Learning from Rewards, Passive Reinforcement Learning, Active reinforcement Learning Self Learning Topics: Machine learning vs reinforcement learning, Applications of AI planning in robotics, Applications of reinforcement learning in gaming	05	CO5

6	AI Applications and Ethical Considerations	Brief overview of AI applications in various domains (NLP, Computer Vision, Robotics). Ethical considerations in AI development, Bias, fairness, and transparency, Social implications of AI. Self Learning Topics: AI in Natural Language Processing (Chatbots, Voice Assistants), AI in Computer Vision (Face recognition, Object detection), AI in education	04	CO6
---	--	---	----	-----

Note: No questions will be asked in the end-semester exam from self-study topics. However, students are encouraged to explore these topics for a better understanding of the subject.

Text Books:

Sr. No.	Book Name
1	Stuart J. Russell and Peter Norvig, " <i>Artificial Intelligence: A Modern Approach</i> ", Fourth Edition" Pearson Education, 2020.
2	Saroj Kaushik, " <i>Artificial Intelligence</i> ", Cengage Learning, First edition, 2011
3	George F Luger, " <i>Artificial Intelligence</i> " Low Price Edition, Fourth edition, Pearson Education.,2005

Reference Books:

Sr. No.	Book Name
1	Nils J. Nilsson, Principles of Artificial Intelligence, Narosa Publication.
2	Deepak Khemani, A First Course in Artificial Intelligence, McGraw Hill Publication
3	Patrick H. Winston, Artificial Intelligence, 3rd edition, Pearson Education.
4	Elaine Rich and Kevin Knight, " <i>Artificial Intelligence</i> ", Third Edition, McGraw Hill Education,2017.

Online Resources Web Link:

Sr. No.	Web Link
1	https://onlinecourses.nptel.ac.in/noc22_cs56/preview
2	https://nptel.ac.in/courses/106105077
3	https://altair.com/altair-rapidminer
4	https://shorturl.at/jM33J
5	https://shorturl.at/MZgOv https://shorturl.at/K8Vlr https://shorturl.at/21koY https://rb.gy/b19n5

6	https://shorturl.at/i53iD https://shorturl.at/uSJdT

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

- IAT will consist of two compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I the remaining syllabus content must be covered in the IAT-II.

End Semester Theory Examination:

- Question Paper will comprise a total of **six questions each carrying 15 marks. Question 1** will be **compulsory** and should **cover the maximum contents of the syllabus**.
- Remaining questions** will be **mixed in nature**. (Part (a) and part (b) of each question must be from different modules. For example, if Q2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules).
- A total of **four questions** need to be answered.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24451142	Fundamentals of IOT	3	---	---	3	---	---	3

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24451142	Fundamentals of IOT	20	20	40	60	02	---	---	100

Course Objective: Students will be able to learn:

Sr. No.	Course Objectives
1	Understand concepts, functional blocks, and communication methodologies relevant to the Internet of Things (IoT).
2	Identify and explain various components of IoT systems and their roles in real-world applications.
3	Compare and implement various communication protocols used in IoT for device-to-device and device-to-cloud communication.
4	Understand and apply various methods for data handling in IoT-based systems, including data acquisition, processing, and cloud integration.
5	To understand the Design Methodology in IoT through case studies.
6	To understand IoT systems through case studies.

Course Outcomes: On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Understand the basic concepts, functional blocks, and communication methodologies relevant to IoT and identify real-life problems suitable for IoT-based automation.	L1
2	Identify and select appropriate IoT components including sensors, actuators, controllers, and hardware platforms for designing specific IoT solutions.	L2
3	Compare various IoT communication protocols and explore their applicability in remote access and control using cloud platforms.	L3
4	Understand and apply various data handling methods in IoT-based applications including storage, processing, and retrieval on cloud services.	L4
5	Design basic applications based on IoT using specific components.	L5
6	Introduce various security issues in IoT	L6

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mappings
1	Introduction to IoT	Definition and Characteristics of IoT, IoT Protocols, IoT Functional Blocks, IoT Communication Models, IoT Communication APIs: REST and Web Sockets, IoT Enabling Technologies, Self Learning Topics Introduction to M2M and Difference between IoT and M2M	07	CO1
2	Components (Things) in IoT	Components (Things) in IoT, Sensor Technology, Examples of Sensors - DHT, PIR, IR, Ultrasonic	07	CO2

		etc, Actuators - Motor, Relay, servo motor etc. Applications of RFID and WSN in IoT, Self Learning Topics Exemplary Device:-R-Pi and its Interfaces, PCDuino, Beagle Bone.		
3	Data Handling in IoT	IoT Data Management and Compute Stack : Fog Computing , Edge Computing. IoT and Data Analytics: Defining IoT Analytics, IoT Analytics challenges, IoT analytics for the cloud, Strategies to organize Data for IoT Analytics, Managing Data lakes, The data retention strategy, visualization and Dash boarding Self Learning Topics Introduction to Cloud Computing, Virtualization, Cloud Models and Cloud Services	05	CO3
4	Design Principles for Web Connectivity	Design Principles for Web Connectivity, Communication Technologies – A Comparison, Edge to Cloud Protocol: Web Communication Protocols for Connected Devices: CoRE Environment, CoAP, LWM2M, MQTT, XMPP, HTTP and SOAP Protocols, Self Learning Topics LPWAN Fundamentals: LORA and NB-IoT.	07	CO4
5	IOT Design Methodology	IoT Architecture: Drivers Behind New Network Architectures - Scale, Security, Constrained Devices and Networks, Data, Legacy, Device Support, The IoT World Forum (IoTWF) Standardized Architecture: Layer 1-7, IT and OT Responsibilities in the IoT. Self Learning Topics Additional IoT Reference Models	05	CO5
6	IOT Case Studies & Security	Case Studies: Home Automation (Smart lighting, home intrusion detection), Case Studies: on Smart Cities (Smart Parking), Self Learning Topics Case Studies: Environment (Weather monitoring, weather reporting BoT) Security Issues of IoT	08	CO6

Text Books:

Textbooks:	
1	Arshdeep Bahga and Vijay Madiseti, "Internet of Things: A Hands-on Approach, Universities Press.
2	Raj Kamal, " Internet of Things: Architecture and Design Principles", McGraw Hill Education ,First edition

3	David Hanes ,Gonzalo Salgueiro"IoT Fundamentals Networking Technologies, Protocols and Use Cases for Internet of Things", Cisco Press, Kindle 2017 Edition
4	Andrew Minter , "Analytics for the Internet of Things(IoT)", Kindle Edition
Reference Books:	
1	Adrian McEwen, Hakim Cassimally, : Designing the Internet of Things", Paperback, First Edition.
2	Yashavant Kanetkar, Shrirang Korde: Paperback "21 Internet of Things (IOT) Experiments", BPB Publications.
Access to software and virtual labs:	
1	https://nptel.ac.in/courses/106105166
2	https://mqttlabs.iotsim.io/readonly/
3	https://ifttt.com/

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

- IAT will consist of two compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I the remaining syllabus content must be covered in the IAT-II.

End Semester Theory Examination:

- Question Paper will comprise a total of **six questions each carrying 15 marks. Question 1** will be **compulsory** and should **cover the maximum contents of the syllabus**.
- Remaining questions** will be **mixed in nature**. (Part (a) and part (b) of each question must be from different modules. For example, if Q2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules).
- A total of **four questions** need to be answered.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24451143	Internet Programming	3	---	---	3	---	---	3

Course Code	Course Name	Theory			Term Work	Pract / Oral	Total
		Internal Assessment	End Sem	Exam Duration			

		IAT-I	IAT-II	IAT-I + IAT-II	Exam	(in Hrs)			
24451143	Internet Programming	20	20	40	60	02	---	---	100

Course Objective: Students will be able to learn:

Sr. No.	Course Objectives
1	To orient students to Web Programming fundamental.
2	To expose students to JavaScript to develop interactive web page development
3	To orient students to Basics of REACT along with installation
4	To expose students to Advanced concepts in REACT
5	To orient students to Fundamentals of node.js
6	To expose students to node.js applications using express framework.

Course Outcomes: On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Select protocols or technologies required for various web applications.	L2,L4
2	Apply JavaScript to add functionality to web pages.	L2,
3	Design front end application using basic React.	L4,L5,L6
4	Design front end applications using functional components of React.	,L6
5	Design back-end applications using Node.js.	L5,L6
6	Construct web based Node.js applications using Express	L4,L5,L6

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mappings
0	Prerequisite	Introduction and basics of HTML, CSS	02	-
1	Web programming fundamentals	Working of web browser, HTTP protocol, HTTPS, DNS, TLS, XML introduction, Json introduction, DOM, URL, URI, REST API. Self-learning Topics: : Nginx server	03	CO1
2	Java script	Introduction to ES6, Difference between ES5 and ES6. Variables, Condition, Loops, Functions, Events, Arrow functions, Setting CSS Styles using JavaScript, DOM manipulation, Classes and Inheritance. Iterators and Generators, Promise, Client-server communication, Fetch Self-learning Topics: Asynchronous JavaScript, JSON	06	CO2
3	React fundamentals	Installation, Installing libraries, Folder and file structure, Components, Component lifecycle, State and Props, React Router and Single page applications, UI design, Forms, Events,	07	CO3

		Animations, Best practices. Self-learning Topics: React vs Angular vs Vue		
4	Advanced React	Functional components- Refs, Use effects, Hooks, Flow architecture, Model-View-Controller framework, Flux, Bundling the application. Web pack. Self-learning Topics: React Native	07	CO4
5	Node.js	Environment setup, First app, Asynchronous programming, Callback concept, Event loops, REPL, Event emitter, Networking module, Buffers, Streams, File system, Web module. Self-learning Topics: Node.js with MongoDB.	07	CO5
6	Express	Introduction, Express router, REST API, Generator, Authentication, sessions, Integrating with React. Self-learning Topics: Commercial deployment.	07	CO6

Note: No questions will be asked in the end-semester exam from self-study topics. However, students are encouraged to explore these topics for a better understanding of the subject.

Text Books:

Textbooks:	
1	Rediscovering JavaScript, Master ES6, ES7, and ES8, By Venkat Subramaniam · 2018
2	Learning React Functional Web Development with React and Redux, Alex Banks and Eve Porcello, O'Reilly
3	Learning Redux, Daniel Bugl, Packt Publication
4	Learning Node.js Development, Andrew Mead, Packt Publishing
5	RESTful Web API Design with Node.js 10, Valentin Bojinov, Packt Publication

Reference Books:

1	Web Development with Node and Express, Ethan Brown, O'Reilly
---	--

Access to software and virtual labs:

1	https://reactjs.org/tutorial/tutorial.html
2	https://react-redux.js.org/introduction/quick-start
3	https://webpack.js.org/

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

- IAT will consist of two compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I the remaining syllabus content must be covered in the IAT-II.

End Semester Theory Examination:

- Question Paper will comprise a total of **six questions each carrying 15 marks. Question 1** will be **compulsory** and should **cover the maximum contents of the syllabus**.
- **Remaining questions** will be **mixed in nature**. (Part (a) and part (b) of each question must be from different modules. For example, if Q2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules).
- A total of **four questions** need to be answered.

DRAFT

Course	Course Name	Teaching Scheme	Credits Assigned
--------	-------------	-----------------	------------------

Code		(Contact Hours)			Theory	Pract.	Tut.	Total
		Theory	Pract.	Tut.				
24451144	Software Engineering and Agile Practices	3	---	---	3	---	---	3

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24451144	Software Engineering and Agile Practices	20	20	40	60	02	---	---	100

Course Objective: Students will be able to learn:

Sr. No.	Course Objectives
1	To provide comprehensive knowledge of software engineering principles.
2	To describe and analyze requirements, and perform planning and scheduling.
3	To develop software solutions using behavioral and structural UML diagrams, and effectively utilize tools for creating and modeling these diagrams
4	To apply testing and ensure quality in software solutions.
5	To introduce Agile software development concepts, principles, and methodologies, and contrast them with traditional models while emphasizing agile values, team practices, and ethics.
6	To understand Agile project and product management concepts and compare them with traditional models, while gaining hands-on knowledge of JIRA for managing agile projects.

Course Outcomes: On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Explain software engineering principles and software development models.	L2
2	Analyse requirements to prepare software plans, schedules, and track project progress.	L4

3	Design UML diagrams based on software requirements and apply appropriate tools to create and model these diagrams.	L6
4	Analyse the quality of software solutions through testing.	L4
5	Apply Agile methods such as Scrum, XP, Crystal, FDD, and ASD to design, develop, test, and manage software effectively in dynamic environments.	L3
6	Apply Agile project management practices and effectively use JIRA tools to plan, track, administer, and control software development projects.	L3

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mappings
0	Prerequisites	Prerequisite Concepts and Course Introduction.	02	-
1	Software Engineering and Foundations	Software Engineering Myths, Software Process, Generic Process Model, SDLC. Prescriptive Process Models: The Waterfall Model, Incremental Models, Evolutionary Process Models: RAD and Spiral Model. Self-Learning Topics: Study how SDLC differs in: Embedded systems (real-time constraints), Web applications (continuous updates), Mobile apps (versioning & deployment)	06	CO1
2	Requirement Analysis Software Cost Estimation	Software Requirements: Functional & Non-Functional, Software Documentation: Analysis and Modelling, Software Requirement Specification (SRS). Software Project Estimation: LOC, FP, and Cost Estimation Techniques. Project Scheduling & Tracking, Gantt Chart, PERT/CPM Self-Learning Topics: Software Engineering Myths: Management myths, Customer myths, Developer myths	06	CO2
3	UML Diagrams	Design Concepts, Data Flow Diagram, Use Case Diagrams, Activity Diagrams. State Charts, Sequence Diagrams, Class and Component Diagrams, Popular UML Tools Criteria for Choosing UML Tools, Tools for Collaborative UML Designing, Advanced Features in UML Tools Self-Learning Topics: Case Studies like : Online Examination System, ATM System, Hospital management System	07	CO3

4	Software Testing	Software Quality Testing: Strategic Approach, Strategies for Conventional Software. Types of Dynamic Testing: White Box and Black Box Testing, Alpha and Beta Testing. Self-Learning Topics: Selenium	04	CO4
5	Agile Methodology	Agile Management - Agile Software Development - Traditional Model vs. Agile, Model - Classification of Agile Methods - Agile Manifesto and Principles - Agile Team, Interactions - Ethics in Agile Teams - Agility in Design, Testing - Agile Documentations Agile Drivers, Capabilities and Values SCRUM, Crystal, Feature Driven Development, Adaptive Software Development - Extreme Programming: Method Overview, Lifecycle, Work Products, Roles and Practices. Self-Learning Topics: Role of QA in Agile, SAFe, LeSS	08	CO5
6	Agile Management and Software Tool	Agile Project Management – Traditional Model versus RAD model for project management – Task planning and effort tracking – The project manager's new work – Agile Development Management – Agile product Management. Introduction to JIRA – JIRA Version – JIRA Cloud Instance Setup – JIRA Administration: Creating a New User and Group – Permission Levels – Global Permission – Project Roles and Permissions - JIRA Schemes: Issue Types, Screens, Custom Fields, and Workflow. Self-Learning Topics: Trello, Asana, Azure DevOps	08	CO6

Note: No questions will be asked in the end-semester exam from self-study topics. However, students are encouraged to explore these topics for a better understanding of the subject.

Text Books:

Textbooks:	
1	R. Pressman, Software Engineering: A Practitioner's Approach, McGraw Hill.
2	R. Mall, Fundamentals of Software Engineering, PHI.
3	Robert C. Martin, "Agile Software Development, Principles, Patterns and Practices", First International Edition, Prentice Hall.
4	David J. Anderson and Eli Schragenheim, —Agile Management for Software Engineering: Applying the Theory of Constraints for Business Results, Prentice Hall, 2003.

Reference Books:

1	P. Jalote, An Integrated Approach to Software Engineering, Narosa Publication.
2	I. Sommerville, Software Engineering, Addison-Wesley.
3	Kevin C. Desouza, —Agile Information Systems: Conceptualization, Construction, and Managementll, Butterworth-Heinemann, 2007.

Access to software and virtual labs:

1	https://onlinecourses.nptel.ac.in/noc20_cs68/preview
2	https://www.coursera.org/specializations/software-development-lifecycle
3	https://www.youtube.com/watch?v=wEr6mwquPLY

Assessment:**Internal Assessment Test (IAT) for 20 marks each:**

- IAT will consist of two compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I the remaining syllabus content must be covered in the IAT-II.

End Semester Theory Examination:

- Question Paper will comprise a total of **six questions each carrying 15 marks. Question 1** will be **compulsory** and should **cover the maximum contents of the syllabus**.
- **Remaining questions** will be **mixed in nature**. (Part (a) and part (b) of each question must be from different modules. For example, if Q2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules).
- A total of **four questions** need to be answered.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
2445115	Computer Networks Lab	---	2	---	---	1	---	1

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
2445115	Computer Networks Lab	---	---	---	---	---	25	--	25

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
1	To understand and use basic networking commands in Linux for network configuration and topologies
2	To design and configure computer networks using IP addressing, subnetting, and static routing
3	To analyze network protocols and traffic at different layers of the TCP/IP model
4	To analyze and study different networking protocols
5	To perform network discovery and monitoring, network behaviour using standard network analysis tools & simulators.
6	Analyze access control and threats

Lab Outcomes: Upon completion of the course students will be able to:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment (Bloom's Taxonomy)
LO1	Use Linux networking commands for network configuration and diagnostics	L3
LO2	Design and configure networks using IP addressing, subnetting, and routing	L4
LO3	Analyze TCP/IP protocol operations using packet analysis tools	L4
LO4	Implement network services (DNS, FTP, DHCP)	L4
LO5	Design and simulate enterprise network topologies	L5
LO6	Implement and test network security configurations for Access control & Threat Mitigation	L5

Hardware & Software Requirements:

Hardware Requirement: Intel Core i3 / i5 Minimum 4-8 GB ram 256 GB SSD or 500 GB HDD	Software requirement: Network Simulators -NS2 Protocol Analysis Tools- Wireshark Virtualization Software
---	---

DETAILED SYLLABUS:

Sr. No.	Experiment List	Hours	LO Mappings
0	Lab Prerequisites.	02	-
1	Use basic networking commands in Linux (ping, tracer, nslookup, netstat, ARP, RARP, ip, ifconfig, dig, route)	02	LO1
2	To design and implement different network topologies(Star, Bus, Ring, Mesh) and configure it for static routing protocol using packet tracer(e.g. Cisco Packet Tracer)	02	LO2,LO5
3	To practice IP addressing, subnetting, and address classification(e.g.,Cisco Packet Tracer)	02	LO2
4	To configure static and dynamic routing between networks (e.g.,Cisco Packet Tracer)	02	LO2
5	To understand encapsulation and operation OSI layer and TCP/IP layers using Wireshark.	02	LO3
6	Demonstrate the encapsulation process and interpret packet headers using a network protocol analyzer.(Use Wireshark).	02	LO3
7	Perform File Transfer and Access using FTP	02	LO4
8	Network Design for an organization using the following concepts: 1. Addressing (IP Address Assignment), 2. Naming (DNS) 3. Routing	04	LO2,3,4,5
9	To secure a network using Access Control Lists and simulate a basic firewall.	02	LO6

10	To scan,monitor,and optimize network performance (NMAP Tool).	02	LO6
----	---	----	-----

Text Books:

Textbooks:	
1	A.S. Tanenbaum, Computer Networks,4th edition Pearson Education
2	B.A. Forouzan, Data Communications and Networking, 5th edition, TMH
3	James F. Kurose, Keith W. Ross, Computer Networking, A Top-Down Approach Featuring the Internet,6th edition, Addison Wesley
Reference Books:	
1	S.Keshav,An Engineering Approach To Computer Networking, Pearson
2	Natalia Olifer & Victor Olifer,Computer Networks: Principles, Technologies & Protocols for Network Design, Wiley India, 2011.
3	Larry L.Peterson, Bruce S.Davie, Computer Networks: A Systems Approach, Second Edition ,The Morgan Kaufmann Series in Networking
Access to software and virtual labs:	
1	https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer
2	https://www.coursera.org/projects/data-forwarding-computer-networks
3	https://www.edx.org/course/ilabx-the-internet-masterclass

Assessment:

Term Work: Term work shall consist of at least 10-12 Practical based on above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiments) + 5 Marks (Assignments) + 5 Marks (Attendance)

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
2445116	Cryptography and Network Security Lab	---	2	---	---	1	---	1

Course Code	Course Name	Theory Internal Assessment			End Sem Exam	Exam Duration (in Hrs)	Term Work	Pract / Oral	Total
		IAT-I	IAT-II	IAT-I + IAT-II					
2445116	Cryptography and Network Security Lab	---	---	---	---	---	25	25	50

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
1	To implement classical and modern symmetric cryptographic techniques.
2	To implement and analyze asymmetric cryptography, key exchange and digital signature schemes.
3	To apply cryptographic hash functions and authentication mechanisms.
4	To explore network reconnaissance, packet analysis and port scanning tools.
5	To scan networks for vulnerabilities and simulate common attacks.
6	To configure and demonstrate firewall, IDS/IPS and secure communication protocols.

Lab Outcomes: Upon completion of the course students will be able to:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Implement classical and symmetric cryptographic algorithms.	L2, L3
2	Implement public key cryptosystems and key exchange mechanisms.	L3

3	Demonstrate hashing and digital signature mechanisms for authentication.	L3, L4
4	Use network reconnaissance and packet analysis tools effectively.	L2, L3
5	Perform vulnerability scanning and simulate network attacks.	L3, L4
6	Implement classical and symmetric cryptographic algorithms.	L2, L3

Hardware & Software Requirements:

Hardware Requirement: Intel Core i3 / i5 Minimum 4-8 GB ram 256 GB SSD or 500 GB HDD	Software requirement: Protocol Analysis Tools Virtualization Software
---	---

DETAILED SYLLABUS:

Sr. No.	Experiment List	Hours	LO Mappings
0	Lab Prerequisites: Installation of Virtual Machine, Kali Linux setup, OpenSSL installation	2	-
1	Implement Classical Ciphers: Caesar, Vigenere, Playfair, Hill Cipher using Python	2	LO1
2	Implement Transposition Cipher (Keyed & Keyless) and perform frequency analysis attack	2	LO1
3	Implement AES encryption and demonstrate different block cipher modes using OpenSSL/Python	2	LO1
4	Implement RSA algorithm and analyze key generation, encryption and decryption	2	LO2
5	Implement Diffie-Hellman Key Exchange and analyze secure key establishment	2	LO2
6	Implement SHA-256 and HMAC using Python/OpenSSL and verify message integrity	2	LO3
7	Study and simulate Digital Signature using RSA and verify signature authenticity	2	LO3
8	Study network reconnaissance tools: WHOIS, nslookup, dig, traceroute	2	LO4
9	Perform network scanning using Nmap (TCP scan, UDP scan, OS detection, Port scan)	2	LO4
10	Perform vulnerability scanning using Nessus / OpenVAS	2	LO5

Text Books:

Textbooks:	
1	William Stallings, Cryptography and Network Security, Principles and Practice, 6th Edition, Pearson Education, March 2013.
2	Applied Cryptography, Protocols, Algorithms and Source Code in C, Bruce Schneier, Wiley.
3	Cryptography and Network Security, Atul Kahate, Tata Mc Graw Hill.

Reference Books:

1	Bernard Menezes, "Cryptography & Network Security", Cengage Learning.
2	Mark Stamp's Information Security Principles and Practice, Wiley
Access to software and virtual labs:	
1	https://www.dcode.fr/frequency-analysis
2	https://www.cloudflare.com/learning/ssl/what-is-hmac/
3	https://www.stationx.net/nmap-cheat-sheet/

Assessment:

Term Work: Term work shall consist of at least 10-12 Practical based on above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiments) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above list of Practical.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
2445117	Web Application and Database Security Lab	---	2	---	---	1	---	1

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
2445117	Web Application and Database Security Lab	---	---	---	---	---	25	25	50

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
1	Develop a comprehensive understanding of the evolving threat landscape in web applications and databases.
2	Gain proficiency in the fundamental principles of securing web applications, covering authentication, authorization, session management, and secure coding practices.
3	Explore foundational concepts and best practices for securing databases, focusing on access control, encryption, and secure database design.
4	Learn and apply various security testing techniques for web applications and databases, including penetration testing, vulnerability scanning, and code reviews.

5	Explore foundational concepts and best practices for securing databases, focusing on access control, encryption, and secure database design.
6	Understand and implement secure software development lifecycle methodologies, integrating security practices throughout the entire development process

Lab Outcomes: Upon completion of the course students will be able to:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Define cybersecurity concepts, list common web application threats (SQL Injection, XSS, CSRF), and identify security misconfigurations in web development.	L1
2	Describe security protocols (HTTPS, TLS/SSL, PKI) and explain authentication and authorization mechanisms such as 2FA, SSO, RBAC, OAuth, and OpenID Connect.	L1,L2
3	Implement secure coding practices such as input validation, output encoding, and database access control, and demonstrate secure communication in applications.	L1,L2
4	Analyze risks in web and database applications, categorize security threats, compare different vulnerability testing methods, and distinguish between secure and insecure system configurations	L3
5	Assess encryption methods, access control policies, and database security measures, and validate incident response strategies for handling security incidents.	L3,L4
6	Design and develop secure web/database applications by integrating authentication, encryption, backup/recovery, and incident response mechanisms	L4,L5

Hardware & Software Requirements:

Hardware Requirement: Intel Core i3 / i5 Minimum 4-8 GB ram 256 GB SSD or 500 GB HDD	Software requirement: Virtualization support enabled in the BIOS; this is sometimes called Intel Virtualization Technology (also known as Intel VT) or AMD-V
---	---

DETAILED SYLLABUS:

Sr. No.	Experiment List	Hours	LO Mappings
0	Lab Prerequisites.	02	-
1	Study and demonstration of common web application vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF) using a vulnerable web application.	02	LO1
2	Study and implementation of secure communication protocols such as HTTPS, SSL/TLS, and understanding Public Key Infrastructure (PKI) using browser and server configurations.	02	LO1,LO2
3	Implementation and comparison of authentication and authorization mechanisms including 2FA, Single Sign-On (SSO), Role-Based Access Control (RBAC), OAuth, and OpenID Connect.	02	LO1,LO2
4	Implementation of secure coding practices such as input validation, output encoding, and prevention of SQL injection in a web	02	LO1,LO2

	application.		
5	Design and demonstration of secure communication between client and server using encryption and secure session management techniques.	02	LO3
6	Implementation and analysis of encryption techniques for data at rest and data in transit, including password hashing and database encryption.	02	LO3,LO4
7	Design and development of a secure web/database application by integrating authentication, authorization, encryption, backup and recovery mechanisms.	02	LO4,LO5
8	Implementation of backup, recovery, and logging mechanisms along with incident response integration for a secure web/database system.	02	LO5
9	Create on login server with 2-factor authentication. Use one pre-defined python script for this.	02	LO6
10	Collect Log Events from Windows Server by using Log Parser tool.	04	LO6

Text Books:

Textbooks:	
1	The Web Application Hacker's Handbook", Dafydd Stuttard, Wiley India Pvt. Ltd.
2	" Database Security" , S.Castano, M. Fugini, G. Martella,P. Samarati, Addison-Wesley.
3	"Database Security " Alfred Basta, Melissa Zgola, Cengage Publication, 2012
Reference Books:	
1	Deane Brker, Web Content Management: Systems, Features, and Best Practices, O'Reilly & Associates incorporated, 2016
Access to software and virtual labs:	
1	https://owasp.org/www-community/attacks/xss/
2	https://www.geeksforgeeks.org/secure-coding-practices/

Assessment:

Term Work: Term work shall consist of at least 10-12 Practical based on above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiments) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above list of Practical.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24451181	Artificial Intelligence Lab	---	2	---	---	1	---	1

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24451181	Artificial Intelligence Lab	---	---	---	---	---	25	25	50

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
---------	----------------

1	Enable students to formulate real-world AI problems and analyze intelligent agent characteristics using PEAS and environment properties.
2	Develop the ability to model and implement classical AI problems using PROLOG and basic problem-solving techniques.
3	Provide practical exposure to implementing and comparing various search algorithms including uninformed, informed, adversarial, and local search methods.
4	Train students to design and implement knowledge-based systems using logical inference, first-order logic, and probabilistic reasoning models.
5	Familiarize students with AI planning techniques using PDDL and reinforcement learning approaches for decision-making.
6	Encourage development of AI applications such as chatbots and promote understanding of ethical considerations in AI systems.

Lab Outcomes: Upon completion of the course students will be able to:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Identify and formulate real-world AI problems, define PEAS descriptors, and analyze environment properties for intelligent system design.	L4
2	Model and implement basic AI problems using PROLOG and search-based problem-solving approaches.	L3
3	Implement and analyze uninformed, informed, adversarial, and local search algorithms to solve complex AI problems.	L4
4	Develop knowledge-based systems using propositional logic, first-order logic, inference mechanisms, and Bayesian networks to reason under certainty and uncertainty.	L6
5	Design and implement AI planning problems using PDDL and apply reinforcement learning techniques for decision-making.	L6
6	Design and develop AI applications such as chatbots while considering ethical aspects of fairness, bias, and transparency.	L6

Hardware & Software Requirements:

Hardware Requirement: • Computer with Intel i5 / Ryzen 5 or higher • Minimum 8 GB RAM • 256 GB SSD • Internet connectivity	Software requirement: Python 3.x (with NumPy, Pandas, Matplotlib, Scikit-learn) SWI-Prolog (for logic programming experiments) PDDL planner such as Fast Downward or Planning.Domains Jupyter Notebook / VS Code (Optional) TensorFlow / Keras for ML experiments
--	---

DETAILED SYLLABUS:

Star (*) marked experiments are compulsory.			
Sr. No	Name of the Experiment	Hours	LO
1*	Identify and formulate an appropriate real world problem statement relevant to AI and define its PEAS descriptor and various properties of the environment.	02	LO1

2*	Implement Family Tree / Tower of Hanoi / Water Jug Problem in PROLOG	02	LO1
3*	Implement any one of the uninformed Searching algorithms (BFS / DFS / DLS / IDDFS) by identifying and analyzing the given problem to reach the goal state.	02	LO3
4*	Implement A* search algorithm by identifying and analyzing the given problem to reach the goal state.	02	LO3
5*	Implement Adversarial search for Game playing algorithms.	02	LO3
6*	Implement Local Search algorithm for optimization : Hill climbing search / Genetic Algorithm	02	LO3
7	Develop a program to perform logical inference using: • Truth table method • Forward chaining • Backward chaining	02	LO4
8*	To create a knowledge base for a Rule based Expert System in a real world scenario using FOL in PROLOG.	02	LO4
9	Design and implement a Belief Network (Bayesian Network) to model reasoning under uncertainty for a real-world problem domain (e.g., medical diagnosis, weather prediction, or fault detection).	02	LO4
10	Identify, analyze, implement a planning problem using PDDL	02	LO5
11	Implement passive or active reinforcement learning.	02	LO5
12*	Implement a basic text classification system (e.g., spam detection or sentiment analysis) using machine learning techniques.	02	LO6
13	Design and implement a rule-based or simple ML-based chatbot for a specific domain (college enquiry / healthcare / banking).	02	LO6

Useful Links	
1	https://www.analyticsvidhya.com/blog/2023/05/emerging-trends-in-ai-and-machine-learning
2	https://influencermarketinghub.com/ai-trends
3	https://www.forbes.com/sites/bernardmarr/2023/02/28/beyond-chatgpt-14-mind-blowing-ai-tools-everyone-should-be-trying-out-now/
Tools and Articles	
4	https://rb.gy/b19n5r
5	https://rb.gy/9z3p1z
6	https://microsoft.github.io/AI-For-Beginners/

Assessment:

Term Work: Term work shall consist of at least 10-12 Practical based on above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiments) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above list of Practical.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24451182	Fundamentals of IoT Lab	---	2	---	---	1	---	1

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24451182	Fundamentals of IoT Lab	---	---	---	---	---	25	25	50

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
1	To interface various sensors and collect real-time data using IoT hardware platforms
2	To transmit and visualize sensor data on cloud-based IoT platforms
3	To control IoT devices remotely using workflow-based and mobile applications
4	To understand and implement publish–subscribe communication using MQTT protocol
5	To integrate voice assistants and automation services with IoT systems
6	To design end-to-end IoT applications using cloud services and notification mechanisms

Lab Outcomes: Upon completion of the course students will be able to:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment (Bloom's Taxonomy)
LO1	Interface sensors and acquire real-time environmental data	L3
LO2	Publish and visualize IoT data on cloud platforms	L4
LO3	Control and monitor IoT devices remotely using applications and dashboards	L4
LO4	Implement MQTT-based publish–subscribe communication for IoT applications	L6
LO5	Integrate voice control and automation services with IoT devices	L6
LO6	Develop complete IoT systems using cloud services and push notifications	L6

Hardware & Software Requirements:

Hardware Requirement:	Software requirement:
-----------------------	-----------------------

Intel Core i3 / i5 Minimum 4-8 GB ram 256 GB SSD or 500 GB HDD Arduino / ESP32 / Raspberry Pi code	Arduino IDE Cisco Packet Tracer (IoT Mode) Firebase
---	---

DETAILED SYLLABUS:

Sr. No.	Experiment List	Hours	LO Mappings
0	Lab Prerequisites.	02	-
1	Interfacing Various Sensors like LDR, ultrasonic, DHT etc (data collection) and pushing data on to Thingspeak Cloud	02	LO1
2	Controlling IoT devices/sensors remotely using Node-red and Rpi. Studying Application of MQTT in node red	02	LO2
3	Control a LED Remotely & Monitor Temperature values with a Raspberry Pi using Node-RED	02	LO2
4	Controlling IoT devices using Blynk App.	02	LO3
5	ESP8266 Voice Control With Google Assistant and Adafruit IO and IFTTT.	02	LO3
6	Implementing Publish-Subscribe model using MQTT protocol and DHT11 sensor	02	LO1,LO4
7	Google Firebase :- controlling LED using Android App	02	LO2
8	Publishing sensor data from ESP32 to AWS IoT Cloud.	02	LO5
9	To send Push notification to IoT device (R-Pi to Smart Phone)	02	LO5
10	Google Assistant Controlled Switch Using NodeMCU	02	LO5

Text Books:

Textbooks:	
1	Arshdeep Bahga and Vijay Madisetti, "Internet of Things: A Hands-on Approach, Universities Press.
2	Raj Kamal, " Internet of Things: Architecture and Design Principles", McGraw Hill Education ,First edition
3	Andrew Minter , "Analytics for the Internet of Things(IoT)", Kindle Edition
Reference Books:	
1	Adrian McEwen, Hakim Cassimally, : Designing the Internet of Things", Paperback, First Edition.
2	Yashavant Kanetkar, Shrirang Korde: Paperback "21 Internet of Things (IOT) Experiments", BPB Publications.
Access to software and virtual labs:	
1	https://www.arduino.cc/en/Tutorial/BuiltInExamples/Blink
2	https://randomnerdtutorials.com/esp32-dht11-dht22-temperature-humidity/

Assessment:

Term Work: Term work shall consist of at least 10-12 Practical based on above list. Also, Term

work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiments) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above list of Practical.

DRAFT

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24451183	Internet Programming Lab	---	2	---	---	1	---	1

Course Code	Course Name	Theory				End Sem Exam	Exam Duration (in Hrs)	Term Work	Pract / Oral	Total
		Internal Assessment								
		IAT-I	IAT-II	IAT-I +						

				IAT-II					
24451183	Internet Programming Lab	---	---	---	---	---	25	25	50

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
1	To Acquire knowledge and Skills for creation of Web Site considering both client- and server-side Programming.
2	To create Web application using tools and techniques used in industry.
3	To learn the characteristics of RIA
4	To Demonstrate Amazon/Google or Yahoo mashup
5	To be well versed with XML and web services Technologies.
6	To be familiarized with open source Frameworks for web development.

Lab Outcomes: Upon completion of the course students will be able to:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Design a basic web site using HTML5 and CSS3 to demonstrate responsive web design.	L1
2	Implement dynamic web pages with validation using JavaScript objects by applying different event handling mechanism.	L1
3	Use AJAX Programming Technique to develop RIA	L2
4	Build RESTful backend applications using Node.js and Express framework.	L2
5	Build well-formed XML Document and implement Web Service using Java.	L2,L3
6	Deploy full-stack web applications, implementing authentication, session management, and frontend-backend communication.	L2,L3

Hardware & Software Requirements:

Hardware Requirement: PC With following Configuration 1. Intel Core i3/i5/i7 Processor 2. 4 GB RAM 3. 500 GB Harddisk 1.	Software requirement: Windows or Linux Desktop OS 2. HTML5 compatible web browsers(Chrome, Opera, Firefox, Safari etc) 3. HTML,CSS editors like Dreamweaver, Notepad++ etc. 4. Netbeans or Eclipse IDE 5. XAMPP
---	---

DETAILED SYLLABUS:

Sr. No.	Experiment List	Hours	LO Mappings
0	Lab Prerequisites.	02	-
1	To study the fundamentals of web programming including the	02	LO1

	working of a web browser, HTTP and HTTPS protocols, DNS, TLS, and the structure of URLs and URIs.		
2	To create and validate XML documents and JSON data formats and to understand the differences between XML and JSON.	02	LO5
3	To demonstrate Document Object Model (DOM) manipulation using JavaScript by accessing, modifying, and styling HTML elements dynamically.	02	LO2
4	To implement asynchronous programming in JavaScript using callbacks, promises, async/await, and to perform client-server communication using the Fetch API.	02	LO2
5	To set up a React development environment and develop a basic React application using functional components while understanding the project folder structure.	02	LO2
6	To implement state and props in React components, handle forms and events, and develop a single-page application using React Router.	02	LO2
7	To develop a backend application using Node.js and Express framework and implement RESTful web services.	02	LO4
8	To integrate a React frontend with an Express backend, implement authentication and session management, and deploy the application using a web server or cloud platform.	02	LO4
9	Developing RIA using AJAX including -A browser built-in XMLHttpRequest object (to request data from a web server) and JavaScript and HTML DOM (to display or use the data) Building Amazon/Yahoo /Google Web Mashups for the website..	02	LO3
10	Mini Project	04	LO1-6

Text Books:

Textbooks:	
1	Responsive Web Design by Example Beginner's Guide by Thoriq Firdaus, PACKT
2	Responsive Web Design with HTML5 and CSS3 PACKT
Reference Books:	
1	Learning React: Functional Web Development with React and Redux, By Alex Banks,Eve Porcello O'Reilly, 2017.
2	Advanced Internet Technologies (includes practicals) ,Deven Shah ,Dreamtech publication
Access to software and virtual labs:	
1	https://www.freecodecamp.org/news/learn-full-stack-development-html-css-javascript-node-js-mongodb/?utm_source=chatgpt.com
2	https://www.w3schools.com/nodeJs/nodejs_bootcamp.asp?utm_source=chatgpt.com
3	https://www.coursera.org/specializations/javascript-programming-with-react-node-

Assessment:

Term Work: Term work shall consist of at least 10-12 Practical based on above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiments) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above list of Practical.

DRAFT

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24451184	Software Engineering and	---	2	---	---	1	---	1

	Agile Practices Lab							
--	----------------------------	--	--	--	--	--	--	--

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24451184	Software Engineering and Agile Practices Lab	---	---	---	---	---	25	25	50

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
1	To understand the principles of software engineering and software development life cycle
2	To apply requirements analysis and software design techniques
3	To understand and practice Agile software development methodologies
4	To apply project planning, estimation, and risk management techniques
5	To use software engineering tools for modeling and documentation
6	To develop teamwork and communication skills through Agile practices

Lab Outcomes: Upon completion of the course students will be able to:

Sr. No.	Lab Outcomes	Cognitive Levels (Bloom's Taxonomy)
LO1	Analyze software requirements and prepare requirement documents	L4
LO2	Design software using modeling techniques	L4
LO3	Apply Agile principles and practices	L3
LO4	Use project management and version control tools	L3
LO5	Develop software artifacts using Agile methods	L6
LO6	Demonstrate teamwork and presentation skills in software projects	L6

Hardware & Software Requirements:

Hardware Requirement: • PC with a minimum i3 Processor or equivalent • 8 GB RAM	Software requirement: • Ubuntu / Windows OS • Any IDE (Eclipse / VS Code / IntelliJ) • Git and GitHub / GitLab • UML Modeling Tool (StarUML / Draw.io)
---	--

DETAILED SYLLABUS:

Sr. No.	Experiment List	Hours	LO Mapping
0	Lab Prerequisites: Overview of Software Engineering concepts and Agile methodology	2	–
1	Case study: Software Development Life Cycle (SDLC) models	2	LO1
2	Requirement Analysis and Preparation of SRS Document	2	LO1
3	Software Design using UML Diagrams (Use Case, Class Diagram)	2	LO2
4	Introduction to Agile Manifesto and Scrum Framework	2	LO2
5	Sprint Planning and User Story Creation	2	LO3
6	Version Control using Git and GitHub	2	LO4
7	Agile Estimation Techniques (Story Points, Planning Pker)	2	LO5
8	Continuous Integration and Agile Testing Basics	2	LO5
9	Mini Project using Agile Practices	2	LO6
10	Project Demonstration, Documentation, and Viva	4	LO6

Text Books:

Textbooks:	
1	Ian Sommerville, Software Engineering, Pearson
2	Roger S. Pressman, Software Engineering: A Practitioner's Approach, McGraw Hill
3	Ken Schwaber, Agile Project Management with Scrum, Microsoft Press
Reference Books:	
1	Robert C. Martin, Agile Software Development: Principles, Patterns, and Practices
2	Alistair Cockburn, Agile Software Development
Access to software and virtual labs:	

1	https://agilemanifesto.org
2	https://www.scrum.org
3	https://www.atlassian.com/agile
4	https://git-scm.com
5	https://www.uml-diagrams.org

Assessment:

Term Work: Term work shall consist of at least 10-12 Practical based on above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiments) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above list of Practical.

Sem. – VI

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
2446111	Blockchain Technology	3	---	---	3	---	---	3

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
2446111	Blockchain Technology	20	20	40	60	02	---	---	100

Course Objectives: Students will be able to learn:

Sr. No.	Course Objectives
1	Understand the fundamental concepts, architecture, and components of Blockchain Technology.
2	Explain the working principles of Bitcoin and cryptocurrency mechanisms.
3	Comprehend the architecture and workflow of public blockchain platforms such as Ethereum.

4	Develop smart contracts using Solidity programming language.
5	Examine private blockchain frameworks and enterprise-level blockchain solutions.
6	Explore blockchain tools and real-world applications across various domains.

Course Outcomes: On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Describe the basic concepts, components, and types of Blockchain.	L2
2	Explain the working of Bitcoin, transactions, mining, and consensus mechanisms.	L3
3	Apply the concepts of Ethereum to perform basic transactions and explore its architecture.	L2
4	Develop simple Smart Contracts using Solidity programming.	L4
5	Compare and evaluate Private Blockchain frameworks and consensus algorithms.	L2
6	Design basic blockchain-based solutions for real-world applications.	L4

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mappings
01	Introduction to Blockchain	What is a blockchain, Origin of blockchain, Foundation of blockchain: Hashing, Merkle trees Components of blockchain, Block in blockchain, Types of blockchain: Public, Private and Consortium, Consensus Protocols, Limitations and Challenges of blockchain Self-Learning: Real-world use cases of blockchain	07	CO1
02	Bitcoin Blockchain	Transactions in blockchain, Double spending problem, UTXO, Cryptocurrency wallets: Hot and cold wallets, Cryptocurrency usage. Consensus in Bitcoin, Proof-of-Work (PoW), Proof-of-Burn (PoB), Proof-of-Stake (PoS) and Proof-of-Elapsed Time (PoET), Bitcoin mining terminologies, Mining difficulty, Altcoins and Tokens Self-Learning: Legal and regulatory issues related to cryptocurrencies	07	CO2
03	Public Blockchain	Introduction to Public Blockchain, Ethereum and its Components, Ethereum block structure, Architecture and Workflow, Comparison between Bitcoin and Ethereum Types of test-networks used in Ethereum, Transferring Ethers using Metamask, Ethereum frameworks, Exploring etherscan.io and ether block structure Self-Learning: Role of MetaMask in Ethereum transactions	07	CO3

04	Smart Contracts Programming	Introduction to Smart Contracts, Working of a Smart Contract, Components of Smart Contract, Smart Contract Approaches. Introduction to Solidity Programming: Data types, Functions in Solidity, Visibility Quantifiers, Inheritance, Error Handling Self-Learning: Applications of smart contracts in real-world systems	07	CO4
05	Private Blockchain	Introduction to Private Blockchain, Need of Private Blockchain, Smart Contract in a Private Environment, State Machine in Smart Contract, Consensus Algorithms for Private Blockchain - PAXOS and RAFT, Byzantine Faults: Byzantine Fault Tolerant (BFT) and Practical BFT Introduction to Hyperledger: Tools and Frameworks, Hyperledger Fabric Architecture, Comparison between Hyperledger Fabric & Ethereum, Components of Hyperledger Fabric: MSP, Chain Codes. Self-Learning: Real-world case studies using Hyperledger Fabric	07	CO5
06	Tools & Application	Tools: Corda, Ripple, Quorum and DeFi Applications: Supply Chain Management, Blockchain with IoT, Blockchain with Cyber Security Self-Learning: Ripple and cross-border payment systems	05	CO6

Note: No questions will be asked in the end-semester exam from self-study topics. However, students are encouraged to explore these topics for a better understanding of the subject.

Text Books:

Textbooks:

- | | |
|---|---|
| 1 | Chandramouli Subramanian, Asha A. George, Abhillash K.A. and Meena Karthikeyan, Blockchain Technology, Universities Press |
| 2 | Andreas M. Antonopoulos, Dr. Gavin Wood, Mastering Ethereum, Building Smart Contract and Dapps, O'reilly Publication |

Reference Books:

- | | |
|---|--|
| 1 | Imran Bashir, Mastering Blockchain, 3rd ed., Packt Publishing. |
| 2 | Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press. |
| 3 | Yathish R and Tejaaswini N, Blockchain for Beginners, SPD Publication |

Access to software and virtual labs:

- | | |
|---|---|
| 1 | NIST Cryptographic Standards and Guidelines (NIST). |
|---|---|

2	Ethereum Documentation (https://ethereum.org/developers/).
3	Solidity Documentation (https://docs.soliditylang.org/).
4	Hyperledger Fabric Documentation (https://hyperledger-fabric.readthedocs.io/).
5	OpenZeppelin Contracts Library (https://docs.openzeppelin.com/contracts/).

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

- IAT will consist of two compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I the remaining syllabus content must be covered in the IAT-II.

End Semester Theory Examination:

- Question Paper will comprise a total of **six questions each carrying 15 marks. Question 1** will be **compulsory** and should **cover the maximum contents of the syllabus**.
- **Remaining questions** will be **mixed in nature**. (Part (a) and part (b) of each question must be from different modules. For example, if Q2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules).
- A total of **four questions** need to be answered.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
2446112	Cyber Forensics & Incident Response	3	---	---	3	---	---	3

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
2446112	Cyber Forensics & Incident Response	20	20	40	60	02	---	---	100

Course Objective: Students will be able to learn:

Sr. No.	Course Objectives
1	Understand fundamental concepts of cyber security and threat landscape
2	Identify various types of cyber attacks and security incidents
3	Apply incident response lifecycle for handling cyber incidents
4	Analyze logs, alerts, and digital evidence during incidents
5	Understand legal, ethical, and compliance aspects of cyber security

6	Develop practical skills using tools for detection, response, and analysis
---	--

Course Outcomes: On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
CO1	Explain cyber security concepts and threats	L2
CO2	Analyze different types of cyber attacks	L4
CO3	Design and apply incident response strategies	L6
CO4	Analyze security logs and incidents	L4
CO5	Apply cyber laws and ethical principles	L3
CO6	Use tools for incident response and forensics	L3

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mappings
0	Introduction to Cyber Security	Overview of Cyber Security including objectives, importance in modern digital infrastructure, and security principles. Detailed explanation of CIA Triad with practical examples. Understanding threat landscape, evolving cyber threats, attack surface, types of attackers (script kiddies, cybercriminals, hacktivists, nation-state actors), and current security challenges in organizations. Self-Learning Topics: • Study major cyber-attack case studies such as WannaCry and SolarWinds. • Explore OWASP Top 10 vulnerabilities. • Review basics of Firewalls, IDS/IPS and antivirus tools. • Analyze recent cyber security news reports.	2	—

1	Cyber Threats & Attacks	Comprehensive study of malware types including viruses, worms, trojans, spyware, rootkits and their working mechanisms. Understanding phishing, spear phishing and social engineering techniques. Detailed study of ransomware attacks, lifecycle and impact. Concept of DoS and DDoS attacks with attack methods. Insider threats and web-based attacks such as SQL Injection, XSS and CSRF. Understanding various attack vectors and exploitation techniques. Self-Learning Topics: • Research ransomware lifecycle in real-world attacks. • Analyze phishing simulation examples. • Review recent DDoS incidents.	6	CO1
2	Incident Response Fundamentals	Definition and characteristics of a security incident. Classification and categories of incidents. Goals and objectives of Incident Response (IR). Structure of Incident Response Team (IRT), roles and responsibilities of team members. Importance of documentation and communication during incidents. Self-Learning Topics: • Study NIST Incident Response framework. • Review CERT-In guidelines.	6	CO2
3	Digital Evidence & Acquisition	Types of Digital Evidence (volatile & non-volatile), Evidence Handling Procedures, Disk Imaging & Cloning Techniques, Live vs Dead Acquisition, Hashing (MD5, SHA) and Integrity Verification, Write Blockers and Forensic Soundness, Tools: Autopsy, EnCase, FTK, Wireshark, Kali Linux Forensic Tools Self-Learning: Comparison of popular forensic tools: Autopsy, EnCase, FTK, Case studies on evidence tampering and integrity preservation	7	CO3
4	Mobile & Cloud Forensics	Mobile Device Forensics (Android, iOS), Data Extraction using ADB, App Forensics (WhatsApp, SMS, Call Logs), Cloud Forensics Concepts, Challenges in Cloud Investigations Self-Learning: Legal and jurisdictional issues in cloud forensics, Forensic analysis of social media and messaging apps	4	CO4

5	Network Forensics	Network Traffic Analysis, Packet Capturing (Wireshark), Log Analysis (Firewall, webserver, windows, IDS/IPS), Email & Web Forensics, Attack Detection Techniques Self-Learning: Case studies on malware, ransomware, and DDoS detection through network forensics	8	CO5
6	Legal, Ethical & Emerging Trends	Overview of IT Act 2000 and relevant cyber laws. Understanding privacy issues, regulatory compliance requirements and ethical considerations in cyber security. Incident response in cloud environments and IoT ecosystems. Emerging trends including AI in cyber security and Zero Trust Architecture, Evidence Admissibility in Court, Privacy & Data Protection Laws, Compliance Standards (ISO 27001, HIPA, GDPR basics). Self-Learning Topics: • Study case examples under IT Act. • Review GDPR and global privacy regulations. • Explore AI-based security solutions.	8	CO6

Note: No questions will be asked in the end-semester exam from self-study topics. However, students are encouraged to explore these topics for a better understanding of the subject.

Text Books:

Textbooks:	
1	Incident Response & Computer Forensics – Chris Prosise & Kevin Mandia ISBN: 0074041966
2	Cyber Security and Threats: Concepts, Methodologies, Tools and Applications – Information Resources Management Association
3	The Basics of Digital Forensics – John Sammons ISBN: 0128006469
Reference Books:	
1	Cyber Security Essentials – William Stallings & Lawrie Brown
2	Network Security Essentials – William Stallings
3	Computer Security: Principles and Practice – William Stallings
4	Practical Malware Analysis – Michael Sikorski & Andrew Honig

5	Applied Incident Response & Forensics – Jeremy Faircloth
Access to software and virtual labs:	
1	IBM Cybersecurity Analyst (Coursera)
2	Splunk Fundamentals
3	TryHackMe Cyber Defense Path
4	NPTEL Cyber Security (for deep theory)

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

- IAT will consist of two compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I the remaining syllabus content must be covered in the IAT-II.

End Semester Theory Examination:

- Question Paper will comprise a total of **six questions each carrying 15 marks. Question 1** will be **compulsory** and should **cover the maximum contents of the syllabus.**
- **Remaining questions** will be **mixed in nature.** (Part (a) and part (b) of each question must be from different modules. For example, if Q2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules).
- A total of **four questions** need to be answered.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24461131	Cyber Threat Intelligence and Risk Management	3	---	---	3	---	---	3

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24461131	Cyber Threat Intelligence and Risk Management	20	20	40	60	02	---	---	100

Course Objective: Students will be able to learn:

Sr. No.	Course Objectives
1	To introduce the core concepts of Cyber Threat Intelligence (CTI) and its importance in modern cybersecurity defense.
2	To understand the cyber threat intelligence lifecycle and its role in risk management frameworks.
3	To teach methods of collecting, analyzing, and operationalizing threat intelligence data.
4	To integrate CTI with enterprise risk assessment and mitigation strategies.
5	To enable learners to apply CTI techniques using frameworks such as MITRE ATT&CK, Kill Chain, and industry tools.
6	To prepare students to design and implement intelligence-led defense strategies for complex organizational environments.

Course Outcomes: On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Explain the fundamentals of cyber threat intelligence and its relevance in securing digital assets.	L2
2	Describe the threat intelligence lifecycle and differentiate between types of threat intelligence.	L2,L4
3	Collect, process, and analyze threat data from diverse sources to identify adversary tactics and techniques.	L4
4	Integrate threat intelligence into risk assessment frameworks such as ISO 31000 and NIST RMF and prioritize risks accordingly.	L3,L4
5	Apply intelligence-driven defense strategies using frameworks like MITRE ATT&CK and Cyber Kill Chain to improve incident response.	L3
6	Evaluate and mitigate risks using CTI tools, risk treatment strategies, and governance mechanisms in real-world scenarios.	L5

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mappings
0	Prerequisites	Basic understanding of cybersecurity fundamentals, computer networks, operating systems, and risk management concepts.	02	-
1	Introduction to Cyber Threat Intelligence	Definitions and purpose of CTI Difference between data, information, and intelligence Importance of CTI in cybersecurity defense Types of cyber threats (APT, ransomware, phishing, insider threats) Role of CTI in organizational risk reduction Self-Learning Topics: Evolution of cyber threat intelligence, Intelligence-led security vs traditional security approaches	08	CO1
2	Threat Intelligence Lifecycle & Frameworks	Planning & direction in CTI Collection: OSINT, internal logs, sensor data Processing, analysis, dissemination, and feedback Intelligence requirements and quality measurements CTI frameworks: MITRE ATT&CK, Diamond Model, Kill Chain Self-Learning Topics: Comparison of CTI frameworks, Intelligence maturity models	07	CO2
3	Sources & Tools for Threat Intelligence	Threat intelligence platforms (TIPs) Tools: SIEM, SOAR, EDR/XDR Indicators of compromise (IOCs) and threat feeds Automated data collection and enrichment Open source and commercial intelligence sources Self-Learning Topics: Overview of popular open-source CTI tools, Threat feed formats (STIX, TAXII)	07	CO3

4	Risk Management and Integration with CTI	Introduction to risk management frameworks (ISO 31000, NIST RMF) Identifying assets, threats, vulnerabilities Qualitative vs quantitative risk assessment Mapping intelligence findings to risk prioritization Risk treatment: acceptance, mitigation, transfer, avoidance Self-Learning Topics: Threat-informed risk management (TIRM), Risk scoring and heat maps	07	CO4
5	Operationalizing Threat Intelligence	Role of CTI in Security Operations Centers (SOC) Applying CTI to incident detection and response Threat actor profiling Threat hunting based on intelligence Case studies of real threats and remediation Self-Learning Topics: Intelligence-driven SOC workflows, Proactive vs reactive threat hunting	06	CO5
6	Governance, Compliance & Emerging Trends	Cyber intelligence governance and policies Regulatory compliance and reporting requirements, HIPAA and GDPR compliance Intelligence sharing mechanisms (ISACs, CERTs) Emerging trends: machine learning in CTI, automation, AI integration Self-Learning Topics: Legal and ethical issues in threat intelligence, Global threat intelligence sharing initiatives	04	CO6

Note: No questions will be asked in the end-semester exam from self-study topics. However, students are encouraged to explore these topics for a better understanding of the subject.

Text Books:

- A. Dehghantanha, M. Conti, and T. Dargahi, Cyber Threat Intelligence, Springer.
- R. M. Lee, M. J. Assante, and T. Conway, Applied Cyber Threat Intelligence, O'Reilly Media.
- K. Scarfone and P. Mell, Guide to Cyber Threat Information Sharing, NIST Special Publication.
- S. Miller, Practical Cyber Threat Intelligence, Packt Publishing.

References:

- M. Ahmad, Incident Response with Threat Intelligence, Packt Publishing.
- S. Trim and M. Lee, Cyber Security Management and Strategic Intelligence, Routledge.
- A. Kott and B. McEwen, Cyber Defense and Situational Awareness, Springer.
- R. Behl and A. Behl, Cyber Risk Management, McGraw-Hill Education.

Online References:

Sr. No.	Website Name
---------	--------------

1	MITRE ATT&CK® Framework – https://attack.mitre.org
2	OASIS STIX™ / TAXII™ Specifications – https://www.oasis-open.org/standards
3	Coursera: <i>Cyber Threat Intelligence</i> – https://www.coursera.org/learn/basics-of-cyber-threat-intelligence

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

- IAT will consist of two compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I the remaining syllabus content must be covered in the IAT-II.

End Semester Theory Examination:

- Question Paper will comprise a total of **six questions each carrying 15 marks. Question 1** will be **compulsory** and should **cover the maximum contents of the syllabus**.
- Remaining questions** will be **mixed in nature**. (Part (a) and part (b) of each question must be from different modules. For example, if Q2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules).
- A total of **four questions** need to be answered.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24461132	ML & DL for Security Analytics	3	---	---	3	---	---	3

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24461132	ML & DL for Security Analytics	20	20	40	60	02	---	---	100

Course Objectives: Students will be able to learn:

Sr. No.	Course Objectives
1	To understand fundamentals of Machine Learning and Deep Learning concepts in security domains.
2	To explore data preprocessing and feature engineering techniques for security datasets.
3	To implement supervised and unsupervised learning algorithms for threat detection.
4	To analyze deep learning architectures for cybersecurity applications.
5	To evaluate model performance and optimize ML/DL models for security analytics.
6	To study ethical, privacy, and emerging trends in AI-driven security systems.

Course Outcomes: On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Explain ML/DL fundamentals and their role in security analytics.	L2
2	Apply preprocessing and feature engineering techniques to security datasets.	L3
3	Develop supervised and unsupervised models for intrusion and malware detection.	L6
4	Analyze deep learning architectures for network and anomaly detection.	L4
5	Evaluate and optimize model performance using validation metrics.	L5
6	Design AI-based solutions addressing ethical and privacy challenges in cybersecurity.	L6

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mappings
0	Prerequisites	Fundamentals of Probability and Statistics. Introduction to Machine Learning Concepts. Basics of Computer Networks and Cybersecurity	02	-
1	Introduction to ML & Security Analytics	Overview of Cybersecurity Analytics. Types of Security Threats (Malware, Phishing, DDoS, Intrusion). Role of AI/ML in Security Systems. ML Workflow for Security Applications. Security Datasets (KDD Cup, NSL-KDD, CICIDS). Challenges in Security Data (Imbalanced, Noisy, High-Dimensional). Self-Learning Topics: AI-Driven Threat Intelligence and Predictive Security Analytics. Adversarial Machine Learning in Cybersecurity.	06	CO1
2	Data Preprocessing & Feature Engineering for Security	Data Cleaning and Transformation of Log Files. Feature Extraction from Network Traffic. Encoding Categorical Security Data. Handling Imbalanced Datasets (SMOTE, Resampling). Dimensionality Reduction using PCA. Feature Selection Techniques. ML Pipeline for Security. Self-Learning Topics: Deep Feature Representation Learning for Security Data. Feature Selection Techniques for High-Dimensional Security Logs.	06	CO2
3	Supervised Learning for Threat Detection	Classification Algorithms: Logistic Regression, Decision Trees. Random Forest & Ensemble Methods. Support Vector Machines for IDS. Case	06	CO3

		Study: Intrusion Detection System. Model Training and Validation Techniques. Self-Learning Topics: User and Entity Behavior Analytics (UEBA). Ensemble Methods in Security: Gradient Boosting (XGBoost, LightGBM).		
4	Unsupervised Learning & Anomaly Detection	Clustering Techniques (K-Means, DBSCAN). Anomaly Detection Methods. Isolation Forest. Autoencoders for Security Analytics. Network Traffic Behavior Analysis. Self-Learning Topics: Graph-Based Anomaly Detection in Network Security. One-Class SVM for Intrusion Detection. Self-Supervised Learning for Cybersecurity Anomaly Detection.	06	CO4
5	Deep Learning for Security Analytics	Introduction to Neural Networks. CNN for Malware Image Classification. RNN/LSTM for Sequential Log Analysis. Deep Autoencoders for Fraud Detection. Transfer Learning in Cybersecurity. Graph Neural Networks (GNN) for Security. Self-Learning Topics: Transformer Models for Network Traffic Analysis. Deep Reinforcement Learning for Autonomous Cyber Defense. Federated Deep Learning for Privacy-Preserving Security Analytics.	06	CO5
6	Model Optimization, Ethics & Emerging Trends	Evaluation Metrics (Precision, Recall, F1, ROC-AUC). Hyperparameter Tuning (Grid Search, Cross-Validation). Adversarial Attacks and Robust AI. Privacy-Preserving ML (Federated Learning). Explainable AI in Security. NLP Pipeline for Security. Dark Web and OSINT Mining. Cybersecurity Knowledge Graphs. Large Language Models in Security. Legal and Ethical Issues in AI-based Security Systems. Bias and Fairness in Security AI. SOC Workflows and MLOps for Security. Self-Learning Topics: Vulnerability Intelligence: NLP on CVE descriptions for severity classification, Log Analysis and SIEM Integration.	07	CO6

Total : 39

Note: No questions will be asked in the end-semester exam from self-study topics. However, students are encouraged to explore these topics for a better understanding of the subject.

Textbooks:

1	Pramod Gupta, Naresh Kumar Sehgal, John M. Acken--Introduction to Machine Learning with Security: Theory and Practice Using Python in the Cloud, Springer, 2024.
2	Richard Gwashy Young--Artificial Intelligence and Machine Learning in Cybersecurity: A Comprehensive Guide to Improving Cybersecurity Protocol, Productivity Press, 2026.
3	Marwan Omar-- Machine Learning for Cybersecurity: Innovative Deep Learning Solutions, Springer, 2022.
4	Tony Thomas, Athira P. Vijayaraghavan, Sabu Emmanuel--Machine Learning Approaches in Cyber Security Analytics, Springer, 2020.
5	Brij B. Gupta, Quan Z. Sheng (Editors)--Machine Learning for Computer and Cyber Security: Principles, Algorithms, and Practices, CRC Press, 2019.

Reference Books:

1	Mark Stamp, Martin Jureček--Machine Learning, Deep Learning and AI for Cybersecurity, Springer, 2025.
2	Kutub Thakur, Al-Sakib Khan Pathan--Transforming Cybersecurity with Machine Learning, CRC Press, 2026.
3	Ian Goodfellow, Yoshua Bengio, Aaron Courville-- Deep Learning, MIT Press.
4	Aurélien Géron--Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow, O'Reilly Media.

Online References:

1	NIST Cybersecurity AI Resources- https://www.nist.gov/cybersecurity
2	MIT OpenCourseWare – Artificial Intelligence / Machine Learning, https://ocw.mit.edu
3	Google Machine Learning Crash Course-- https://developers.google.com/machine-learning/crash-course
4	Coursera – Machine Learning by Andrew Ng-- https://www.coursera.org/learn/machine-learning
5	Kaggle – Security & ML Datasets and Tutorials-- https://www.kaggle.com

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

- IAT will consist of two compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I the remaining syllabus content must be covered in the IAT-II.

End Semester Theory Examination:

- Question Paper will comprise a total of **six questions each carrying 15 marks. Question 1** will be **compulsory** and should **cover the maximum contents of the syllabus**.
- **Remaining questions** will be **mixed in nature**. (Part (a) and part (b) of each question must be from different modules. For example, if Q2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules).
- A total of **four questions** need to be answered.

DRAFT

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24461133	IoT Device Security & Embedded Systems	3	---	---	3	---	---	3

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24461133	IoT Device Security & Embedded Systems	20	20	40	60	02	---	---	100

Course Objective: Students will be able to learn:

Sr. No.	Course Objectives
1	Understand the architectural building blocks of IoT devices and embedded systems.
2	Learn about security challenges, vulnerabilities, and risks inherent in IoT and embedded environments.
3	Analyze communication protocols and secure design principles for IoT devices.
4	Apply techniques for vulnerability assessment and penetration testing specific to IoT and embedded systems.
5	Design secure architectures and countermeasures for IoT device security.
6	Evaluate mitigation strategies against real-world IoT threats and attacks.

Course Outcomes: On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Explain the architecture of IoT devices and embedded systems, and identify common security vulnerabilities.	L2
2	Analyze threats, attacks, and risks associated with IoT and embedded environments.	L4
3	Apply security principles for secure provisioning, authentication, and firmware integrity in IoT devices.	L3
4	Evaluate communication protocols used in IoT (e.g., MQTT, CoAP) and design secure communication solutions.	L5
5	Implement vulnerability assessment, penetration testing, and risk mitigation strategies for embedded IoT systems.	L3
6	Design secure IoT device architectures incorporating countermeasures and emerging best practices.	L6

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mappings
0	Prerequisites	Prerequisite Concepts and Course Introduction.	02	-
1	Introduction to Embedded Systems & IoT Architectures	Embedded systems basics, microcontrollers, sensors & actuators Introduction to IoT: evolution, characteristics, building blocks IoT device lifecycle, resource constraints and design implications Self-Learning Topics: Basics of IoT architecture and low-power embedded system design	08	CO1
2	Security Challenges & Vulnerabilities in IoT Devices	IoT threat model, common vulnerabilities, risk assessment frameworks Case studies: botnets (Mirai), smart home device attacks Hardware security threats: side-channel, physical tampering Self-Learning Topics: Common IoT security vulnerabilities and real-world attack case studies	05	CO2
3	Secure Provisioning, Firmware & Identity Management	Secure boot, firmware updates and integrity Device identity, trusted platform modules (TPM), secure elements Authentication frameworks (PKI, certificates, token-based) Self-Learning Topics: Secure boot, device identity, and firmware update mechanisms	08	CO3
4	Secure Communication Protocols & Network Security	IoT communication protocols: MQTT, CoAP, HTTP/HTTPS Encryption, authentication, key management in constrained networks Wireless IoT network security (Zigbee, BLE, Wi-Fi) Self-Learning Topics: Security features of IoT communication protocols and wireless networks	06	CO4
5	Vulnerability Assessment & Penetration Testing	Static and dynamic analysis of embedded code Tools and techniques for IoT device scanning Penetration testing of IoT ecosystems and remediation strategies Self-Learning Topics: IoT vulnerability assessment and penetration testing techniques	06	CO5
6	Designing Secure IoT Embedded Systems	Secure architectural patterns, edge computing security Secure firmware and hardware design best practices	06	CO6

		Emerging trends: blockchain for IoT security, AI-based defense Self-Learning Topics: Secure-by-design approaches and emerging trends in IoT security		
--	--	---	--	--

Note: No questions will be asked in the end-semester exam from self-study topics. However, students are encouraged to explore these topics for a better understanding of the subject.

Text Books:

- Sunil Cheruvu, Anil Kumar, Ned Smith, David M. Wheeler, Demystifying Internet of Things Security, Apress / Springer Nature — secure device/edge platform security.
- Raj Kamal, Embedded Systems SoC, IoT, AI & Real Time Systems, McGraw-Hill Education — embedded systems with IoT and real-time focus.
- Benjamin Aziz, Alvaro Arenas, Bruno Crispo (Eds.), Engineering Secure Internet of Things Systems, IET/CRC Press — embedded IoT system security engineering.

References:

- Kersten Heins, *Trusted Cellular IoT Devices: Design Ingredients and Concepts*, Springer — secure IoT device design elements.
- Olivier Markowitch, Jean-Michel Dricot (Eds.), *IoT Security: Threat Detection, Analysis and Defense*, MDPI Books — emerging defense methods.
- Adesh Kumar, Surajit Mondal, Gaurav Verma, Prashant Mani (Eds.), *Embedded Devices and Internet of Things: Technologies and Application*, CRC Press — embedded-IoT technologies.
- Saad Motahhir & Yassine Maleh (Eds.), *Security Engineering for Embedded and Cyber-Physical Systems*, CRC Press — embedded and CPS security design.

Online References:

Sr. No.	Website Name
1	Internet of Things Security ScienceDirect – IoT security attacks, tools, techniques, and defenses overview: https://www.sciencedirect.com/book/9780443337598/internet-of-things-security
2	Survey: Security and privacy issues in IoT (arXiv) – free academic paper on IoT security challenges: https://arxiv.org/abs/1903.00846
3	Security of the IoT: Vulnerabilities & countermeasures (arXiv) – layered view on IoT vulnerabilities and protections: https://arxiv.org/abs/1910.13312

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

- IAT will consist of two compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I the remaining syllabus content must be covered in the IAT-II.

End Semester Theory Examination:

- Question Paper will comprise a total of **six questions each carrying 15 marks. Question 1** will be **compulsory** and should **cover the maximum contents of the syllabus**.

- **Remaining questions** will be **mixed in nature**. (Part (a) and part (b) of each question must be from different modules. For example, if Q2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules).
- A total of **four questions** need to be answered.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24461134	DevOps and CI/CD Automation	3	---	---	3	---	---	3

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24461134	DevOps and CI/CD Automation	20	20	40	60	02	---	---	100

Course Objective: Students will be able to learn:

Sr. No.	Course Objectives
1	To provide knowledge of software engineering discipline.
2	To understand and analyze Process Models in software design .
3	To understand DevOps practices which aim to simplify Software Development Life Cycle.
4	To understand different Version Control tools.
5	To familiarize with Jenkins build & test software Applications..
6	To familiarize with testing tools.

Course Outcomes: On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Understand and demonstrate the basic principles of software engineering.	L2
2	Analyze, evaluate Process Models in software design.	L4
3	To understand the fundamentals of DevOps engineering and be fully proficient with DevOps terminologies, concepts, benefits, and deployment options.	L3
4	To be aware of different Version Control tools.	L2

5	Apply Jenkins to Build, Deploy and Test the Software Applications	L2
6	To be aware of different testing tools.	L2

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mapping s
0	Prerequisite	Concepts of Data Communication including transmission media, network topologies, OSI and TCP/IP models, types of networks, basic networking devices and protocols. Self-Learning Topics: • Review OSI and TCP/IP models in detail. • Study basic networking commands (ping, tracer, ipconfig).	02	---
1	Introduction To Software Engineering	Software Engineering fundamentals, software process framework activities, Capability Maturity Model (CMM) and maturity levels, advanced trends in software engineering including DevOps, CI/CD, and Microservices. Self-Learning Topics: • Study real-world software development lifecycle case studies. • Research CMMI levels and industry examples. • Explore emerging trends like AI in software engineering. •	04	CO1

2	Process Models	Prescriptive Process Models including Waterfall and Incremental models; Evolutionary Process Models such as RAD and Spiral; Agile process models including Extreme Programming (XP), Scrum and Kanban; comparison of models with advantages and limitations. Self-Learning Topics: • Compare Waterfall vs Agile using case studies. Study Scrum roles and ceremonies in detail.	07	CO2
3	Introduction to DevOps	Concept of DevOps, DevOps lifecycle, collaboration between development and operations teams, tools used for coding, building, testing, configuration management and monitoring applications. Self-Learning Topics: • Study CI/CD pipeline architecture. • Analyze DevOps case studies from industry.	06	CO3
4	Version Control using GIT	Concept of Version Control Systems, GIT installation and configuration, working with local and remote repositories, GitHub operations, branching, merging, rebasing, Git workflow strategies, integration with IDE, and AWS CodeCommit. Self-Learning Topics: • Practice Git commands using GitHub repositories. • Study Git workflow strategies (GitFlow, Feature branching). • Explore pull requests and code reviews.	07	CO4

5	Working with Jenkins	Introduction to Jenkins architecture, installation and configuration, integration with Ant, managing Jenkins nodes, creating and managing pipelines, deployment using Tomcat server. Self-Learning Topics: • Create a simple CI/CD pipeline project. • Study Jenkins plugins and their uses. • Research real-time DevOps automation examples.	06	CO5
6	Introduction to Selenium and Testing	Introduction to software testing, types and levels of testing, testing strategies, automated vs manual testing, overview of testing tools, Selenium architecture, integration of Selenium with Jenkins, TestNG, GitLab, AWS CodePipeline. Self-Learning Topics: • Develop basic Selenium test scripts. • Study TestNG framework features. • Compare manual vs automated testing case studies.	06	CO6

Note: No questions will be asked in the end-semester exam from self-study topics. However, students are encouraged to explore these topics for a better understanding of the subject.

Text Books:	
1	<i>“The DevOps Handbook”</i> by Gene Kim, Jez Humble, Patrick Debois, John Willis
2	<i>“Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation”</i> by Jez Humble & David Farley

3	<i>“DevOps for Developers”</i> by Michael Hüttermann
Reference Books:	
1	<i>Mastering DevOps with GitLab CI/CD</i> by Tanay Pant (Packt)
2	<i>“Jenkins 2: Up and Running”</i> by Oleg Nenashev & others (O’Reilly)
3	<i>“Practical DevOps”</i> by Joakim Verona (Packt)
Industry articles and case studies :	
1	Tool-Specific Resources Version Control & CI ● Git & GitHub ○ <i>Pro Git (Free ebook)</i> — https://git-scm.com/book ○ Git tutorials on GitHub Learning Lab ● Jenkins ○ Jenkins official tutorials ○ YouTube practical labs by <i>Automation Step by Step</i> Docker & Containers ● Docker official docs + Docker-Labs GitHub ● <i>A Docker Tutorial for Beginners</i> by TutorialsPoint Kubernetes ● Kubernetes official docs ● <i>Kubernetes by Example</i>
Any other (Access to AI tools / Data driven insights (if applicable) or any other):	
1	● YouTube Channels ○ <i>Simplilearn DevOps Tutorials</i> ○ <i>Edureka DevOps Playlist</i> ○ <i>FreeCodeCamp DevOps intro videos</i> ○ <i>Automation Step by Step – Raghav Pal (excellent practical tutorials)</i> ● Official Docs & Guides ○ Jenkins User Documentation

	○ GitHub Actions Docs ○ GitLab CI/CD Docs ○ Docker & Kubernetes official docs ● Free Platforms ○ Codecademy Free DevOps Lessons ○ Kubernetes Basics – by Google Cloud Skills Boost ○ AWS Free Tier – DevOps Labs
--	---

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

- IAT will consist of two compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I the remaining syllabus content must be covered in the IAT-II.

End Semester Theory Examination:

- Question Paper will comprise a total of **six questions each carrying 15 marks. Question 1** will be **compulsory** and should **cover the maximum contents of the syllabus.**
- **Remaining questions** will be **mixed in nature.** (Part (a) and part (b) of each question must be from different modules. For example, if Q2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules).
- A total of **four questions** need to be answered.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24461141	Malware Analysis	3	---	---	3	---	---	3

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24461141	Malware Analysis	20	20	40	60	02	---	---	100

Course Objective: Students will be able to learn:

Sr. No.	Course Objectives
1	Possess the skills necessary to carry out independent analysis of modern malware samples using both static and dynamic analysis techniques.
2	Have an intimate understanding of executable formats, Windows internals and API, and analysis techniques.
3	Extract investigative leads from host and network-based indicators associated with a malicious program.
4	Apply techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples.
5	Apply malware analysis knowledge to investigate advanced threats and propose mitigation and response strategies in enterprise and cloud environments.
6	Achieve proficiency with industry standard tools including IDA Pro, OllyDbg, WinDBG, PE Explorer, ProcMon, etc.

Course Outcomes: On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Analyze modern malware samples independently using appropriate static and dynamic analysis techniques.	L2
2	Demonstrate a comprehensive understanding of executable file formats, Windows internals, APIs, and their role in malware behavior analysis.	L2
3	Extract and interpret host-based and network-based indicators to derive investigative leads from malicious programs.	L2
4	Apply advanced malware analysis techniques to unpack, decrypt, and bypass anti-analysis and obfuscation mechanisms used by modern malware	L2
5	Investigate advanced and emerging malware threats and propose effective mitigation and incident response strategies for enterprise and cloud environments.	L2
6	Utilize industry-standard malware analysis tools such as IDA Pro, OllyDbg, WinDBG, PE Explorer, ProcMon, and related utilities to perform in-depth malware analysis.	L2

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mappings
0	Prerequisites and Course Outline	Prerequisite Concepts and Course Introduction. Self-Learning Topics: • Review basic operating system concepts (process, memory, file system). • Study fundamentals of computer networks. • Explore cybersecurity basics and threat landscape. • Familiarize with virtual lab setup for malware analysis.	02	---
1	Malware Analysis	Types of Malware, Introduction to malware analysis. General rules for Malware Analysis. Basic Static Techniques including Antivirus Scanning, Hashing, Finding Strings, Packed and Obfuscated Malware, Portable Executable Malware, Portable Executable File Format, OS security concepts, malware threats and evolution, types such as viruses, worms, rootkits, Trojans, bots, spyware, adware, logic bombs. Concepts of static and dynamic malware analysis. Self-Learning Topics: • Analyze sample malware hashes using VirusTotal. • Study PE file structure in detail. • Research evolution of malware over decades. • Practice basic string and hash analysis tools.	06	CO1

2	Static and Dynamic Analysis	STATIC ANALYSIS: X86 Architecture including main memory and instructions, Antivirus scanning, malware fingerprinting, Portable Executable file format, Analyzing Windows programs, Anti-static analysis techniques, obfuscation, packing, metamorphism and polymorphism. DYNAMIC ANALYSIS: Live and dead malware analysis, analyzing traces such as system calls, API calls, registry changes and network activities. Self-Learning Topics: • Practice static analysis using tools like PEiD or Dependency Walker. • Explore sandbox environments (Any.Run, Cuckoo Sandbox). • Study API monitoring tools. • Compare static vs dynamic analysis approaches.	07	CO2
3	Dynamic Behaviour & Debugging	Use of Debuggers such as OllyDbg and WinDBG, setting breakpoints, stepping through code, tracking API calls at runtime, detecting anti-debug techniques, understanding execution flow and call stacks. Self-Learning Topics: • Practice debugging simple executable programs. • Study common anti-debugging tricks. • Analyze call stack behavior in sample programs. • Explore runtime monitoring tools.	06	CO3
4	Anti-Analysis & Obfuscation Techniques	Anti-debug and Anti-VM techniques, packed and encrypted malware, polymorphism and metamorphism, use of unpackers and custom tools, practical identification and evasion of anti-analysis mechanisms. Self-Learning Topics: • Study common packers (UPX) and unpacking methods. • Research anti-VM detection techniques. • Practice identifying encrypted payloads.	07	CO4

5	Advanced Malware & Emerging Threats	Fileless malware, Living-off-the-Land (LoL) attacks, Advanced Persistent Threats (APT), Ransomware ecosystems, malware targeting cloud and containerized environments, mobile and IoT malware overview, threat intelligence integration, incident response and mitigation strategies, future trends in malware development and defense. Self-Learning Topics: • Study recent APT case studies. • Research fileless malware techniques. • Explore cloud security attack scenarios. • Review threat intelligence platforms.	06	CO5
6	Case Studies & Reporting	Analysis of real-world malware cases, forensic documentation, writing analysis reports (Behaviour Summary, Indicators of Compromise, Suggested countermeasures), ethical considerations in malware analysis. Self-Learning Topics: • Prepare a sample malware analysis report. • Study professional forensic documentation standards. • Review ethical and legal considerations in malware research. • Analyze publicly available malware reports.	05	CO6

Note: No questions will be asked in the end-semester exam from self-study topics. However, students are encouraged to explore these topics for a better understanding of the subject.

Text Books:

1. Android Malware by Xuxian Jiang and Yajin Zhou, Springer ISBN 978-1-4614-7393-0
2. Windows Malware Analysis Essentials by Victor Marak, Packt Publishing, 2015

References:

1. Practical malware analysis The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig ISBN-10: 159327-290-1, ISBN-13: 978-1-59327-290-6
2. Computer viruses: from theory to applications by Filiol, Eric Springer Science & Business Media
3. Hacking exposed™ malware & rootkits: malware & rootkits security secrets & Solutions by Michael Davis, Sean Bodmer, Aaron Lemasters, McGraw-Hill, ISBN: 978-0-07-159119-5

Online References:

Sr. No.	Website Name
1	https://cuckoosandbox.org/community-sub/download
2	https://sourceforge.net/projects/ghidra.mirror/
3	virustotal.com/gui/
4	Office of Scientific and Technical Information (OSTI): Provides various reports on malware analysis, including Windows internals, behavior analysis, and specific case studies like SolarWinds
5	IEEE Xplore & ACM Digital Library: Repositories for conference papers regarding malware analysis, such as "Hardware-Assisted Malware Analysis" and "Graph Based Malware Analysis API"

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

- IAT will consist of two compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I the remaining syllabus content must be covered in the IAT-II.

End Semester Theory Examination:

- Question Paper will comprise a total of **six questions each carrying 15 marks. Question 1** will be **compulsory** and should **cover the maximum contents of the syllabus**.
- **Remaining questions** will be **mixed in nature**. (Part (a) and part (b) of each question must be from different modules. For example, if Q2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules).
- A total of **four questions** need to be answered.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24461142	Information Security Management Systems (ISMS)	3	---	---	3	---	---	3

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24461142	Information Security Management Systems (ISMS)	20	20	40	60	02	---	---	100

Course Objective: Students will be able to learn:

Sr. No.	Course Objectives
1	Fundamentals of information security and security management systems
2	Security threats, vulnerabilities, and organizational security challenges
3	Security policies, governance, and access control mechanisms
4	Legal aspects of cyber security and cyber crime
5	Data privacy and data protection laws in India
6	Standards, compliance, and best practices in information security management

Course Outcomes: On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Explain concepts of information security and management systems	L3
2	Analyze threats and vulnerabilities affecting information systems	L4
3	Design and apply security policies and governance frameworks	L6
4	Analyze access control and identity management mechanisms	L3
5	Apply cyber laws and data privacy regulations in information security	L6
6	Implement standards and compliance practices in information security management	L6

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mapping
0	Prerequisites	Prerequisite Concepts and Course Introduction.	02	
1	Introduction to Information Security	Concept and need of information security, information as an organizational asset, CIA triad, information security objectives, challenges in information management, overview of information management security systems Self Learning Topics: • Analyze real-world security incidents affecting organizations. • Study OWASP Top 10 vulnerabilities. • Review CIA triad practical examples	04	CO 1
2	Information Security Management, Threats and Vulnerabilities	Information security management concepts, ISMS, security governance, roles and responsibilities, asset identification and classification, internal and external threats, vulnerabilities, common attacks, insider threats, malware, phishing, social engineering, impact on CIA triad Self Learning Topics: • Research ISO 27001 framework basics. • Study real-world threat case studies.	06	CO 2
3	Security Policies and Governance	Purpose and types of security policies, policy development lifecycle, security governance framework, security awareness and training, policy enforcement and compliance monitoring, role of management Self Learning Topics: • Draft a sample organizational security policy. • Study governance frameworks used in Indian	07	CO 3

		organizations. • Explore compliance case examples.		
4	Access Control and Identity Management	Principles of access control, authentication, authorization and accountability, access control models (DAC, MAC, RBAC), identity and access management concepts, user provisioning and privilege management Self Learning Topics: • Compare DAC, MAC and RBAC models with examples. • Study IAM implementation in cloud platforms. • Explore Multi-Factor Authentication case studies.	07	CO 4
5	Cyber Laws and Legal Aspects	Overview of cyber laws, Information Technology Act 2000, cyber crimes and offences, penalties and adjudication, digital evidence and admissibility, cyber law enforcement agencies, ethical issues. Self Learning Topics: • Study important sections of IT Act 2000. • Analyze real cybercrime case judgments India. • Explore role of CERT-In and cyber cells.	06	CO 5
6	Data Standards Privacy, and Compliance	Data privacy concepts, Digital Personal Data Protection Act 2023, rights and obligations, consent and data breach reporting, ISO/IEC 27001 and 27002 standards, security controls, audits, compliance and cloud data protection issues Self Learning Topics: • Study Digital Personal Data Protection Act 2023 in detail. • Review ISO 27001 certification process. • Analyze cloud data breach case studies.	07	CO 6

Text Books:

- **Nina Godbole**, *Information Systems Security*, Wiley India
- **William Stallings**, *Computer Security: Principles and Practice*, Pearson India
- **Pavan Duggal**, *Cyber Law in India*, Saakshar Law Publications
- **Vivek Sood**, *Data Protection Law in India*, Oxford University Press India

References:

- **Michael E. Whitman & Herbert J. Mattord**, *Principles of Information Security*, Cengage\
- **ISO/IEC 27001:2022** – Information Security Management Standards
- **NIST Special Publications (SP 800 Series)**

Online References:

Sr. No.	Website Name
1	https://www.meity.gov.in
2	https://nvlpubs.nist.gov
3	https://www.cert-in.org.in

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

- IAT will consist of two compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I the remaining syllabus content must be covered in the IAT-II.

End Semester Theory Examination:

- Question Paper will comprise a total of **six questions each carrying 15 marks. Question 1** will be **compulsory** and should **cover the maximum contents of the syllabus**.
- **Remaining questions** will be **mixed in nature**. (Part (a) and part (b) of each question must be from different modules. For example, if Q2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules).
- A total of **four questions** need to be answered.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theor y	Pract.	Tut.	Theory	Pract.	Tut.	Total
24461143	Cloud Computing and Security	3	---	---	3	---	---	3

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24461143	Cloud Computing and Security	20	20	40	60	02	---	---	100

Course Objectives: Students will be able to learn:

Sr. No.	Course Objectives
1	To comprehend Characteristics and Concept of cloud techniques.
2	To understand levels of virtualization
3	To correlate the connection of cloud service providers
4	To understand cloud implementation
5	Analyze compliance requirements and risk assessment in cloud environments.
6	To explore security and risk involved with cloud computing

Course Outcomes: On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Differentiate between different cloud computing techniques.	L2
2	Understand virtualization and its key concepts	L2
3	Compare various cloud computing providers/software.	L4
4	Handle open source cloud implementation and administration.	L2
5	Understand risks involved in cloud computing.	L4
6	Apply course knowledge through projects, demonstrating the ability to secure and deploy cloud applications from design to implementation.	L3

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mappings
1	Introduction to Cloud Computing	Introduction– Components of Cloud Computing, comparison with Virtualization, Grids, Utility Computing, client-server model and P2P computing, impact of cloud computing on business, key drivers, service delivery models. Cloud Types – Private, Public and Hybrid, when to avoid public cloud, Cloud API. Self Learning Topics: Study real-world cloud case studies (AWS, Azure, GCP). • Compare public, private and hybrid cloud deployments. • Explore cloud service pricing models. • Review current cloud adoption trends in India.	07	CO1

2	Virtualization	Introduction and benefits of Virtualization, implementation levels, VMM design requirements and providers, OS level virtualization, middleware support, Hypervisor and Xen architecture, full and para virtualization, CPU, memory and I/O virtualization, hardware support in Intel x86 processors. Self Learning Topics: • Install and experiment with VirtualBox or VMware. • Study Xen and KVM hypervisors. • Analyze CPU and memory virtualization techniques.	06	CO2
3	Cloud Computing Services and Business Value	XaaS, IaaS, PaaS, DBaaS, SaaS, leveraging PaaS for productivity, comparison of various cloud providers and software platforms. Self Learning Topics: • Create trial accounts on AWS/Azure free tier. • Compare IaaS vs PaaS use cases. • Study SaaS applications used in enterprises.	08	CO3

4	Cloud Deployment Techniques	Factors for successful cloud deployment, network requirements, problem areas and mitigation, cloud network topologies, automation and self-service features, cloud performance, mobile cloud computing architecture, benefits and challenges. Self Learning Topics: • Design a sample cloud deployment architecture. • Study cloud networking basics (VPC, Subnets). • Explore mobile cloud computing examples. • Research cloud performance optimization techniques.	08	CO4
5	Architecture for Cloud Application	Cloud application requirements, traditional vs cloud architecture, multi-tier architecture, SOA for cloud applications, resource-oriented, method-oriented and event-driven SOA, parallelization, in-memory operations. Self Learning Topics: • Design a multi-tier cloud application architecture. • Study microservices vs monolithic architecture. • Explore serverless computing concepts. • Analyze real-world SOA implementations.	06	CO5

6	Security	Security for virtualization platforms, host security for SaaS, PaaS and IaaS, data security concerns, confidentiality, encryption, availability, integrity, cloud storage gateways, firewall, security as a service, identity management as a service. Self Learning Topics: • Study cloud security best practices (CSA guidelines). • Explore encryption techniques used in cloud. • Analyze recent cloud data breach incidents. • Review IAM implementation in AWS/Azure.	04	CO6
---	----------	---	----	-----

Note: No questions will be asked in the end-semester exam from self-study topics. However, students are encouraged to explore these topics for a better understanding of the subject.

Text Books:

- Cloud computing: concepts, Technology and architecture : The Pearson Service Technology Series from Thomas Erl) 1st Edition
- Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" by Tim Mather et al
- Cloud Computing: Concepts, Technology & Architecture" by Thomas Erl

References:

- Rajkumar Buya,' Cloud computing principles and Paradigms', Wiley
- Kai Hwang,' Distributed and cloud computing', MK Publications.
- Cloud computing, black book, Dreamtech publication.

Online References:

Sr. No.	Website Name
1	Coursera (e.g., AWS Security Specialty)
2	edX (Microsoft Azure courses)
3	Terraform Documentation: terraform.io
4	cloudflare.com/learning

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

- IAT will consist of two compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I the remaining syllabus content must be covered in the IAT-II.

End Semester Theory Examination:

- Question Paper will comprise a total of **six questions each carrying 15 marks. Question 1** will be **compulsory** and should **cover the maximum contents of the syllabus.**

- **Remaining questions** will be **mixed in nature**. (Part (a) and part (b) of each question must be from different modules. For example, if Q2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules).
- A total of **four questions** need to be answered.

DRAFT

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24461144	User Interface Design with Security	3	---	---	3	---	---	3

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24461144	User Interface Design with Security	20	20	40	60	02	---	---	100

Course Objective: Students will be able to learn:

Sr. No.	Course Objectives
1	Fundamentals of user interface (UI) and user experience (UX) design
2	Human-computer interaction principles and usability guidelines
3	Standard UI/UX design guidelines and best practices
4	Accessibility and inclusive design standards
5	Security risks arising from poor UI design
6	Secure, privacy-aware, and usable interface design techniques

Course Outcomes: On successful completion, of course, learner/student will be able to:

Sr. No.	Course Outcomes	Cognitive Levels of Attainment (Bloom's Taxonomy)
CO1	Explain UI/UX and HCI principles	L2

CO2	Analyze usability, accessibility, and user requirements	L4
CO3	Design secure and usable user interfaces	L6
CO4	Analyze UI-based security vulnerabilities	L4
CO5	Apply accessibility and privacy guidelines in UI design	L3
CO6	Evaluate UI designs for usability, security, and user experience	L3

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mapping
0	Introduction to UI/UX and Security	UI and UX concepts, importance of UI in software systems, UI vs UX, characteristics of good UI, usability and security relationship, overview of secure UI design. Self-Learning Topics: Case studies of good and bad UI designs and their impact on usability and security.	02	CO1
1	Human-Computer Interaction & Usability Guidelines	HCI concepts, human cognitive models, interaction styles, usability goals, Nielsen's usability heuristics, learnability, efficiency, memorability, error prevention, user-centered design. Self-Learning Topics: Identification of usability issues in real-world web and mobile applications.	06	CO1, CO2
2	User Interface Design Guidelines & Standards	UI design guidelines, consistency, feedback, visibility, affordance, simplicity, navigation design, layout principles, typography, color theory, icon design. Self-Learning Topics: Study of UI guidelines followed by popular applications and operating systems.	06	CO3

3	Accessibility & Inclusive Design Guidelines	Accessibility concepts, inclusive design principles, accessibility barriers, WCAG principles (Perceivable, Operable, Understandable, Robust), color contrast, keyboard navigation, screen-reader friendly UI, accessible forms. Self-Learning Topics: WCAG compliance levels and overview of accessibility testing tools.	07	CO5
4	Security Issues in UI Design	UI-based security threats, phishing attacks, clickjacking, UI redressing, insecure input forms, misleading error messages, information leakage through UI, dark patterns, social engineering through interface design. Self-Learning Topics: Analysis of phishing and deceptive UI examples.	04	CO4
5	Secure Authentication, Privacy & Data Protection UI	Secure login UI design, password usability vs security, CAPTCHA and multi-factor authentication interfaces, secure session handling, consent UI, privacy notices, data minimization, UI considerations for data protection laws. Self-Learning Topics: Study of privacy dashboards and authentication flows of real systems.	07	CO3, CO5
6	UI Evaluation, Testing & Emerging Secure UI Trends	Usability testing methods, heuristic evaluation, accessibility testing, UI security testing basics, secure UX metrics, UI design for mobile, cloud, and IoT applications. Self-Learning Topics: Emerging UI/UX trends and secure UI challenges in mobile and IoT systems.	07	CO6

Note: No questions will be asked in the end-semester exam from self-study topics. However, students are encouraged to explore these topics for a better understanding of the subject.

Text Books:

- Alan Dix et al., *Human-Computer Interaction*, Pearson India
- Wilbert O. Galitz, *The Essential Guide to User Interface Design*, Wiley India
- Nina Godbole, *Cyber Security*, Wiley India

References

- Ben Shneiderman, *Designing the User Interface*, Pearson
- Don Norman, *The Design of Everyday Things*
- ISO 9241 – Ergonomics of Human-System Interaction

Online References:

Sr. No.	Website Name
1	https://www.usability.gov
2	https://www.w3.org/WAI
3	https://owasp.org
4	https://material.io/design

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

- IAT will consist of two compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I the remaining syllabus content must be covered in the IAT-II.

End Semester Theory Examination:

- Question Paper will comprise a total of **six questions each carrying 15 marks. Question 1** will be **compulsory** and should **cover the maximum contents of the syllabus**.
- **Remaining questions** will be **mixed in nature**. (Part (a) and part (b) of each question must be from different modules. For example, if Q2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules).
- A total of **four questions** need to be answered.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
2446115	Blockchain Technology Lab	---	2	---	---	1	---	1

Course Code	Course Name	Theory					Term Work	Pract / Oral	To tal
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
2446115	Blockchain Technology Lab	---	---	---	---	---	25	25	50

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
1	To develop and deploy smart contracts on local Blockchain
2	To deploy the smart contract on test networks.
3	To deploy and publish smart contracts on Ethereum test network.
4	To design and develop crypto currency.
5	To deploy chain code on permissioned Blockchain
6	To design and develop a Full-fledged DApp using Ethereum/Hyperledger

Lab Outcomes: Upon completion of the course students will be able to:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
---------	--------------	--

1	Develop and test smart contract on local Blockchain	L5
2	Develop and test smart contracts on Ethereum test networks.	L6
3	Write and deploy smart contract using Remix IDE and Metamask	L5
4	Design and develop Cryptocurrency.	L3
5	Write and deploy chain code in Hyperledger Fabric.	L6
6	Develop and test a Full-fledged DApp using Ethereum/Hyperledger Fabric	L6

DRAFT

Hardware & Software Requirements:

Hardware Requirement: PC with following Configuration Intel Core i3/i5/i7, 8 GB RAM	Software Requirement: Google Chrome Browser (latest), Go/Java 8 or above, NodeJS, React, Python, Docker.
---	--

DETAILED SYLLABUS:

Sr. No	Title of Experiment	Ref Books	LO's	Bloom's levels
1	• <u>Cryptography in Blockchain, Create Merkle tree</u>	T1,T3, R1,R2	LO1, LO4	BL3, BL4
	• <u>Create a Blockchain using Python</u>			
2	Create a metamask wallet, mine test ethers, perform crypto transactions	T1,T3, R1,R2	LO1,2	BL1, BL2, BL3
3	study explorer etherscan.io and bitcoin explorer.	T1,T3, R1,R2	LO1,2	BL1, BL2, BL3
4	Implement peer-to-peer network and Create crypto currency (consensus algorithm).	T1,T3, R1,R2	LO1, LO4	BL3, BL4
5	• Create Smart Contract using Solidity and Remix IDE.	T2,T3	LO2	BL3, BL4
	• Create Transactions using Solidity and Remix IDE			
6	Develop private Blockchain platform ethereum using Geth.	T2,T3	LO3	BL2, BL3
7	Create ERC 20 Token	T2,T3	LO1	BL2, BL3
8	Case study on any one application using Permissioned Blockchain/Hyperledger Fabric	T2,T3	LO4	BL3, BL4
9&10	Creating a blockchain Application and demonstration (Mini – Project)	T1, T2, T3, R1,R2, R3	LO1- LO6	BL1, BL2, BL3, BL4, BL5, BL6

Software Tools: Remix IDE, Geth, Ganache, Metamask, Colab notebook, Java, Python, Solidity, Flask, Postman

Text Books:

- A. Antonopoulos, Mastering Bitcoin, Programming The Open Blockchain, O'Reilly.
- M. Andreas. G Wood, Mastering Ethereum, Building Smart Contract and DApps, O'Reilly.
- C. Subramanian, A George, K Abhillash, M Karthikeyan, Blockchain Technology, Universities Press.
- A. Kumar, Hyperledger Fabric In-Depth: Learn, Build and Deploy Blockchain Applications using Hyperledger Fabric, BPB.
- R. Modi, Solidity Programming Essentials: A beginner's Guide to Build Smart Contracts for Ethereum and Blockchain, Packt.

References:

- I. Bashir, Mastering Blockchain, Packt.

- M. Andreas. Antonopoulos, Mastering Bitcoin Unlocking Digital Cryptocurrencies, O'Reilly.
- K. Saurabh and A. Saxena, Blockchain Technology: Concepts and Applications, Wiley.
- R. Modi, A. Lewis, The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them for Ethereum and Blockchain, Packt.

Online References:

Sr. No.	Website Name
1	https://trufflesuite.com/
2	https://metamask.io/
3	https://remix.ethereum.org/
4	https://www.hyperledger.org/use/fabric

Assessment:

Term Work: Term work shall consist of at least 10-12 Practical based on above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiments) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above list of Practical.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
2446116	Cyber Forensics & Incident Response Lab`	---	2	---	---	1	---	1

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
2446116	Cyber Forensics & Incident Response Lab`	---	---	---	---	---	25	25	50

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
1	Understand the cyber security lab environment and forensic tools
2	Identify and analyze common cyber threats and incidents
3	Apply incident response lifecycle for handling cyber incidents
4	Perform log analysis and incident detection
5	Understand legal, ethical, and compliance aspects of cyber forensics
6	Develop hands-on skills using incident response and forensic tools

Lab Outcomes: Upon completion of the course students will be able to:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Explain cyber security concepts and threat landscape	L2
2	Analyze different types of cyber attacks	L4
3	Design and apply incident response strategies	L6
4	Analyze logs, alerts, and security incidents	L4
5	Apply cyber laws and ethical principles in investigations	L3
6	Use tools for incident response and digital forensics	L3

Hardware & Software Requirements:

Hardware Requirement: PC with following Configuration Intel Core i3/i5/i7, 8 GB RAM	Software Requirement: Python 3.x, Autopsy Digital Forensics Tool, Wireshark Network Protocol Analyzer, Volatility Framework (Memory Forensics), Splunk (Free Edition) / ELK Stack, VirtualBox / VMware Workstation, Kali Linux (Virtual Machine).
---	---

DETAILED SYLLABUS:

Sr. No.	Experiment List	Hours	LO Mappings
1	Introduction to Cyber Security Lab Environment and Tools	02	LO1
2	Identification and Analysis of Cyber Threats and Attacks	04	LO1,2
3	Case Study on Malware, Phishing, and Ransomware Attacks	04	LO2
4	Study of Incident Response Concepts and IR Team Structure	04	LO3
5	Implementation of Incident Response Lifecycle on Sample Incident	04	LO3
6	Log Collection and Analysis for Incident Detection	04	LO4
7	Identification of Indicators of Compromise (IOCs)	04	LO4
8	Digital Evidence Collection and Chain of Custody Documentation	04	LO5
9	Disk and Memory Forensics Using Forensic Tools	04	LO6
10	Mini Project / Case Study on Cyber Forensics & Incident Response	04	LO3,6

Text Books:

- Chris Prosise, Kevin Mandia, Incident Response & Computer Forensics, McGraw-Hill, ISBN: 0074041966
- John Sammons, The Basics of Digital Forensics, Syngress, ISBN: 0128006469

References:

- William Stallings, Lawrie Brown, Cyber Security Essentials, Pearson
- William Stallings, Computer Security: Principles and Practice, Pearson

Online References:

Sr. No.	Website Name
1	https://www.sans.org/white-papers
2	https://www.cisa.gov/incident-response
3	https://attack.mitre.org
4	https://www.nist.gov/cyberframework

Assessment:

Term Work: Term work shall consist of at least 10-12 Practical based on above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiments) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above list of Practical.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24461171	Cyber Threat Intelligence and Risk Management Lab	---	2	---	---	1	---	1

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24461171	Cyber Threat Intelligence and Risk Management Lab	---	---	---	---	---	25	25	50

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
1	To familiarize students with practical concepts of Cyber Threat Intelligence (CTI).
2	To enable collection and analysis of threat data using open-source intelligence tools.
3	To understand and apply threat intelligence lifecycle stages through hands-on exercises.
4	To map threat indicators to industry frameworks such as MITRE ATT&CK and Cyber Kill Chain.
5	To integrate CTI findings with risk assessment and mitigation strategies.
6	To develop intelligence-driven decision-making skills for real-world cybersecurity scenarios.

Lab Outcomes: Upon completion of the course students will be able to:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Identify and analyze cyber threats using threat intelligence sources and tools.	L4
2	Collect, normalize, and enrich Indicators of Compromise (IOCs).	L3
3	Apply CTI frameworks for adversary behavior analysis.	L3
4	Perform basic risk assessment using intelligence inputs.	L3
5	Support incident response and threat hunting activities using CTI techniques.	L3
6	Demonstrate practical understanding of intelligence-led cybersecurity operations.	L2

Hardware & Software Requirements:

Hardware Requirement: PC with configuration: Intel Core i3/i5/i7, 4 GB RAM	Software requirement: Angular IDE, Visual Studio Code, Notepad++, Python Editors (PyCharm / IDLE / VS Code Python), MySQL, XAMPP, JDK
--	---

DETAILED SYLLABUS:

Sr. No.	Experiment List	Hours	LO Mappings
1	Study of Cyber Threat Intelligence Concepts and Lifecycle Understand CTI fundamentals, intelligence lifecycle stages, and types of threat intelligence.	02	LO1
2	Collection of Open-Source Threat Intelligence (OSINT) Collect threat data from open sources such as public reports, blogs, and vulnerability databases.	04	LO1
3	IOC Identification and Classification Identify Indicators of Compromise (IP addresses, hashes, domains) from given datasets and classify them.	04	LO2
4	Threat Intelligence Data Processing and Normalization Use Python scripts to clean, normalize, and structure threat data for analysis.	04	LO3
5	Mapping Threats Using MITRE ATT&CK Framework Map observed adversary techniques to MITRE ATT&CK tactics and techniques.	04	LO4
6	Cyber Kill Chain Analysis of a Real-World Attack Case Analyze a ransomware or phishing attack using the Cyber Kill Chain model.	04	LO5
7	Threat Actor Profiling and Attribution Create a basic threat actor profile using available intelligence sources.	04	LO6
8	Integration of CTI with Risk Assessment Perform qualitative risk assessment by mapping threats, vulnerabilities, and assets using CTI inputs.	04	LO4
9	Threat Hunting Based on Intelligence Indicators Simulate threat hunting using sample logs and intelligence indicators.	04	LO5
10	Mini Project: Intelligence-Driven Incident Response Scenario Design an intelligence-led response strategy for a given organizational cyber incident.	04	LO6

Text Books:

- R. M. Lee, M. J. Assante, and T. Conway, *Applied Cyber Threat Intelligence*, O'Reilly Media.
- K. Scarfone and P. Mell, *Guide to Cyber Threat Information Sharing*, NIST Special Publication.
- S. Miller, *Practical Cyber Threat Intelligence*, Packt Publishing.
- J. Hebel, M. Fisher, R. Blace, A. Perez-Lopez, *Semantic Web Programming*, Wiley Publishing, Inc.

References:

- M. Ahmad, *Incident Response with Threat Intelligence*, Packt Publishing.

- S. Trim and M. Lee, Cyber Security Management and Strategic Intelligence, Routledge.
- A. Kott and B. McEwen, Cyber Defense and Situational Awareness, Springer.
- R. Behl and A. Behl, Cyber Risk Management, McGraw-Hill Education.

Online References:

Sr. No.	Website Name
1	Coursera – Cyber Threat Intelligence – https://www.coursera.org/learn/basics-of-cyber-threat-intelligence

Assessment:

Term Work: Term work shall consist of at least 10-12 Practical based on above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiments) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above list of Practical.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24461172	ML & DL for Security Analytics Lab	---	2	---	---	1	---	1

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24461172	ML & DL for Security Analytics Lab	---	---	---	---	---	25	25	50

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
1	To understand practical implementation of ML and DL techniques for cybersecurity applications.
2	To perform preprocessing and feature engineering on security datasets.
3	To implement supervised learning algorithms for intrusion and malware detection.
4	To apply unsupervised learning techniques for anomaly detection in network traffic.
5	To evaluate and optimize ML/DL models using standard performance metrics.
6	To design security analytics solutions using AI techniques for real-world cybersecurity problems.

Lab Outcomes: Upon completion of the course students will be able to:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Apply data preprocessing and exploratory analysis techniques on cybersecurity datasets.	L3
2	Implement machine learning algorithms for detecting cyber threats and anomalies.	L3
3	Develop deep learning models for security analytics applications.	L4
4	Evaluate ML/DL models using visualization and performance metrics for security analysis.	L4
5	Deploy AI models for real-time cyber threat detection systems.	L3
6	Interpret and communicate AI-driven security insights using explainable AI and dashboards.	L5

Hardware & Software Requirements:

Hardware Requirement:	Software requirement:
------------------------------	------------------------------

DETAILED SYLLABUS:

Sr. No.	Experiment List	Hours	LO Mappings
1	Perform data cleaning, normalization, and feature engineering on a cybersecurity dataset (e.g., KDD Cup or NSL-KDD) to prepare it for machine learning models.	02	LO1, LO2
2	Analyze network traffic data using statistical visualization techniques to identify suspicious patterns and anomalies.	02	LO1, LO3
3	Build and evaluate a Logistic Regression model to classify normal and malicious network traffic.	02	LO2, LO3
4	Develop a supervised ML model to detect malware activities based on system behavior features.	02	LO2, LO3
5	Implement unsupervised learning techniques to detect anomalous network traffic patterns.	02	LO2, LO4
6	Apply PCA or t-SNE to reduce high-dimensional cybersecurity datasets and visualize attack clusters.	02	LO2, LO4
7	Build a Deep Neural Network (DNN) model to classify cyber attacks using network traffic datasets.	02	LO3, LO4
8	Implement LSTM-based models to detect botnet activity from sequential network traffic logs.	02	LO3, LO5
9	Develop an Autoencoder model to detect anomalies in system logs and network behavior.	02	LO3, LO5
10	Use SHAP or LIME techniques to interpret machine learning model decisions in intrusion detection systems.	02	LO4, LO6
11	Deploy a trained ML/DL model as a REST API to perform real-time cyber threat detection.	02	LO5, LO6
12	Create an interactive dashboard showing attack trends, model predictions, and anomaly alerts.	02	LO4, LO6
	Mini Project: Design and implement an AI-based Security Analytics System that uses Machine Learning and Deep Learning techniques to detect, classify, and visualize cyber threats from network traffic and system logs.	06	

Note: Conduct any 10 Practical's from the above list of experiments. Mini Project is Compulsory.

Textbooks:

1	Brij B. Gupta, Quan Z. Sheng – Machine Learning for Computer and Cyber Security, CRC Press.
2	Tony Thomas, Athira Vijayaraghavan – Machine Learning Approaches in Cyber Security Analytics, Springer.

3	Aurélien Géron – Hands-On Machine Learning with Scikit-Learn, Keras and TensorFlow, O'Reilly
4	Ian Goodfellow, Yoshua Bengio, Aaron Courville – Deep Learning, MIT Press.
5	Pramod Gupta, Naresh Sehgal – Introduction to Machine Learning with Security, Springer

Reference Books:

1	Mark Stamp – Introduction to Machine Learning with Applications in Cybersecurity, Chapman & Hall.
2	Somdip Dey – Cybersecurity Data Science, CRC Press.
3	Clarence Chio, David Freeman – Machine Learning and Security, O'Reilly Media.
4	Nicolas Papernot – Machine Learning Security Principles, Cambridge University Press.
5	Aditya K. Sood, Richard Enbody – Targeted Cyber Attacks, Syngress.

Online References:

1	NIST Cybersecurity AI Resources- https://www.nist.gov/cybersecurity
2	MIT OpenCourseWare – Artificial Intelligence / Machine Learning, https://ocw.mit.edu
3	Google Machine Learning Crash Course-- https://developers.google.com/machine-learning/crash-course
4	Coursera – Machine Learning by Andrew Ng-- https://www.coursera.org/learn/machine-learning
5	Kaggle – Security & ML Datasets and Tutorials-- https://www.kaggle.com

Assessment:

Term Work: Term work shall consist of Practical based on above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiments) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above list of Practical.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24461173	IoT Device Security & Embedded Systems Lab	---	2	---	---	1	---	1

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24461173	IoT Device Security & Embedded Systems Lab	---	---	---	---	---	25	25	50

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
1	To understand the architectural components of IoT devices and embedded systems through hands-on experiments.
2	To identify and analyze security vulnerabilities and threats in IoT and embedded environments.
3	To apply secure provisioning, authentication, and firmware integrity techniques in IoT devices.
4	To evaluate IoT communication protocols and implement secure communication mechanisms.
5	To perform vulnerability assessment and penetration testing on IoT and embedded systems.
6	To design secure IoT device architectures using best practices and emerging security approaches.

Lab Outcomes: Upon completion of the course students will be able to:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Explain IoT and embedded system architectures and identify common security vulnerabilities.	L2
2	Analyze threats, attacks, and risks in IoT and embedded environments.	L3
3	Apply secure provisioning, authentication, and firmware protection mechanisms.	L3
4	Evaluate IoT communication protocols and implement secure communication solutions.	L3
5	Perform vulnerability assessment, penetration testing, and risk mitigation for IoT systems.	L2
6	Design secure IoT device architectures incorporating countermeasures and best practices.	L4

Hardware & Software Requirements:

Hardware Requirement: PC i3 Processor or above. Arduino / ESP8266 / ESP32 / Raspberry Pi, Sensors (Temperature, Motion, Light, etc.)	Software requirement: Open CV, Python. QGIS/ArcGIS, WebODM, Arduino IDE / PlatformIO, Visual Studio Code, Python Editors (PyCharm / IDLE / VS Code Python), Wireshark
--	---

DETAILED SYLLABUS:

Sr. No.	Experiment List	Hours	LO Mappings
1	Study of IoT Device and Embedded System Architecture Identify hardware components, firmware layers, sensors, and communication interfaces.	02	-
2	Analysis of IoT Threat Models and Security Vulnerabilities Study common IoT vulnerabilities using real-world case studies (e.g., Mirai botnet).	02	LO1
3	Secure Boot and Firmware Integrity Demonstration Implement or simulate secure boot and checksum/hash-based firmware integrity verification.	02	LO1
4	Device Identity and Authentication Mechanisms Implement certificate-based or token-based authentication for IoT devices.	02	LO2
5	Secure Communication Using MQTT / CoAP Configure MQTT or CoAP with TLS/DTLS and analyze encrypted traffic.	02	LO3
6	Wireless IoT Network Security Analysis Analyze Zigbee / BLE / Wi-Fi security using packet capture and protocol inspection tools	02	LO2
7	Static Analysis of Embedded Firmware Perform static analysis of embedded firmware to identify hardcoded credentials and vulnerabilities.	02	LO4
8	Dynamic Analysis and IoT Device Scanning Use network scanning and IoT-specific tools to detect exposed services and weaknesses.	02	LO5
9	IoT Penetration Testing and Risk Mitigation Conduct penetration testing on an IoT ecosystem and recommend mitigation strategies.	02	LO3
10	Mini Project: Secure IoT Architecture Design Design a secure IoT device architecture incorporating secure boot, encrypted communication, identity management, and monitoring.	02	LO5,LO6

Text Books:

- Sunil Cheruvu, Anil Kumar, Ned Smith, David M. Wheeler, *Demystifying Internet of Things Security*, Apress / Springer Nature.
- Raj Kamal, *Embedded Systems SoC, IoT, AI & Real Time Systems*, McGraw-Hill Education.
- Benjamin Aziz, Alvaro Arenas, Bruno Crispo (Eds.), *Engineering Secure Internet of Things Systems*, IET / CRC Press.

References:

- Kersten Heins, *Trusted Cellular IoT Devices: Design Ingredients and Concepts*, Springer.
- Olivier Markowitch, Jean-Michel Dricot (Eds.), *IoT Security: Threat Detection, Analysis and Defense*, MDPI Books.
- Adesh Kumar, Surajit Mondal, Gaurav Verma, Prashant Mani (Eds.), *Embedded Devices and Internet of Things: Technologies and Application*, CRC Press.
- Saad Motahhir & Yassine Maleh (Eds.), *Security Engineering for Embedded and Cyber-Physical Systems*, CRC Press.

Online References:

Sr. No.	Website Name
1	https://www.coursera.org/specializations/gis-mapping-spatial-analysis
2	https://onlinecourses.nptel.ac.in/noc25_ce108/preview
3	https://onlinecourses.nptel.ac.in/noc25_ae30/preview
4	https://www.udemy.com/course/spatial-data-analysis-introductory-gis-and-remote-sensing

Assessment:

Term Work: Term work shall consist of at least 10-12 Practical based on above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiments) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above list of Practical.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24461174	DevOps and CI/CD Automation Lab	---	2	---	---	1	---	1

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24461174	DevOps and CI/CD Automation Lab	---	---	---	---	---	25	25	50

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
1	Apply diverse software development methodologies, including traditional and Agile models.
2	Gain insight into DevOps principles and practices, along with the responsibilities of DevOps Engineers.
3	Implement version control using Git and GitHub to manage source code effectively.
4	Deploy and test applications on Jenkins, integrating automated testing into the CI/CD pipeline.
5	Implement Jenkins pipelines to automate software delivery workflows.
6	Configure Jenkins Master/Slave architecture for distributed build processing

Lab Outcomes: Upon completion of the course students will be able to:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Apply diverse software development methodologies, including traditional and Agile models.	L2
2	Gain insight into DevOps principles and practices, along with the responsibilities of DevOps Engineers.	L3
3	Implement version control using Git and GitHub to manage source code effectively.	L3
4	Deploy and test applications on Jenkins, integrating automated testing into the CI/CD pipeline.	L3
5	Implement Jenkins pipelines to automate software delivery workflows.	L2
6	Configure Jenkins Master/Slave architecture for distributed build processing	L4

Hardware & Software Requirements:

Hardware Requirement: PC i3 Processor or above. Arduino / ESP8266 / ESP32 / Raspberry Pi, Sensors (Temperature, Motion, Light, etc.)	Software requirement: Open CV, Python. QGIS/ArcGIS, WebODM, Arduino IDE / PlatformIO, Visual Studio Code, Python Editors (PyCharm / IDLE / VS Code Python), Wireshark
--	---

DETAILED SYLLABUS:

Sr. No.	Experiment List	Hours	LO Mappings
1	Application of at least two traditional process models.	02	-
2	Application of the Agile process models.		LO1
3	Case study to understand DevOps: Principles, Practices, and DevOps Philosophy Engineer Role and Responsibilities.	02	LO1
4	To implement Version control for different files/directories using GIT, install git, and create a GitHub account.	02	LO2
5	Advance git commands	02	LO3
6	To implement version control using GitHub to sync local GIT repositories and perform various related operations using a GIT	02	LO2

	Cheat-Sheet		
7	To deploy and test Java/web/Python applications on Jenkins server To implement Jenkins pipeline using scripted/declarative pipeline	02	LO4
8	To use Jenkins to deploy and run test cases for Java/Web applications using Selenium/TestNG	02	LO5
9	To Install Docker and basic docker commands	02	LO3
10	To perform basic container management operations.	02	LO5,LO6

Text Books:

- “The DevOps Handbook” by Gene Kim, Jez Humble, Patrick Debois, John Willis
- “Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation” by Jez Humble & David Farley
- “DevOps for Developers” by Michael Hüttermann

References:

- Mastering DevOps with GitLab CI/CD” by Tanay Pant (Packt)
- “Jenkins 2: Up and Running” by Oleg Nenashev & others (O’Reilly)
- “Practical DevOps” by Joakim Verona (Packt)

Online References:

Sr. No.	Website Name
1	Simplilearn DevOps Tutorials
2	Edureka DevOps Playlist
3	FreeCodeCamp DevOps intro videos
4	Automation Step by Step – Raghav Pal (excellent practical tutorials)

Assessment:

Term Work: Term work shall consist of at least 10-12 Practical based on above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiments) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above list of Practical.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24461181	Malware Analysis Lab	---	2	---	---	1	---	1

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24461181	Malware Analysis Lab	---	---	---	---	---	25	25	50

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
1	Perform static analysis of malware samples, including disassembly and signature identification.
2	Conduct dynamic analysis using sandboxes and virtual environments to observe runtime behavior.
3	Reverse engineer malware binaries to uncover payloads, persistence mechanisms, and command-and-control (C2) communications.
4	Identify and classify malware types, evasion techniques, and indicators of compromise (IoCs).
5	Apply ethical and legal considerations in malware handling, including reporting and containment.
6	Use tools for automated analysis and integrate findings into threat intelligence reports.

Lab Outcomes: Upon completion of the course students will be able to:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Perform detailed static analysis of malware samples, including file disassembly, signature identification.	L3
2	Perform hashing to extract initial insights without execution.	L4
3	Identify and classify various malware types, including indicators of compromise (IoCs) and propagation methods.	L3
4	Develop and apply scripts (e.g., in Python) for automated malware triage.	L3
5	Complete comprehensive malware analysis projects, synthesizing static, dynamic, and forensic techniques to produce actionable insights and presentations.	L3
6	Apply legal and ethical considerations in handling malware.	L6

Hardware & Software Requirements:

Hardware Requirement: PC i3 Processor or above.	Software requirement: MATLAB / Open CV, Python.
---	---

DETAILED SYLLABUS:

Sr. No.	Experiment List	Hours	LO Mappings
0	Set up a safe virtual environment to analyze malware.	02	-
1	Quickly extract network signatures and host-based indicators.	02	LO1
2	Use key analysis tools like IDA Pro, OllyDbg, and WinDbg.	02	LO2
3	Overcome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques.	02	LO3
4	Use your newfound knowledge of Windows internals for malware analysis.	02	LO3
5	Develop a methodology for unpacking malware and get practical experience with five of the most popular packers.	02	LO4
6	Analyze special cases of malware with shellcode, C++, and 64-bit code.	02	LO4
7	Using Sandboxing: Cuckoo Sandbox or Joe Sandbox for automated malware execution in a safe container.	02	LO5
8	Install Reanimator in your Windows machine and scan the system for Malware and prepare one report for the same.	04	LO6

Text Books:

- Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig
- Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code by Michael Hale Ligh, Steven Adair, Blake Hartstein, and Matthew Richard

References:

- The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory by Michael Hale Ligh, Andrew Case, Jamie Levy, and Aaron Walters
- Reverse Engineering for Beginners by Dennis Yurichev

Online References:

Sr. No.	Website Name
1	OpenSecurityTraining or Malwarebytes' blog

Assessment:

Term Work: Term work shall consist of at least 10-12 Practical based on above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiments) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above list of Practical.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24461182	Information Security Management Systems (ISMS) Lab	---	2	---	---	1	---	1

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24461182	Information Security Management Systems (ISMS) Lab	---	---	---	---	---	25	25	50

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
1	To understand information security tools and lab environment
2	To study ISMS concepts and security policies
3	To identify threats, vulnerabilities, and access control mechanisms
4	To understand cyber laws and legal aspects of information security
5	To study data privacy and compliance requirements
6	To apply information security management concepts through case studies

Lab Outcomes: Upon completion of the course students will be able to:

LO	Lab Outcome	Cognitive Levels of Attainment as per Bloom's Taxonomy
LO1	Study and understand ISMS concepts	L6
LO2	Analyze threats, vulnerabilities, and access control	L6
LO3	Configure authentication and user privileges	L3

LO4	Implement security policies	L6
LO5	Analyze cyber laws and digital evidence	L3
LO6	Apply data privacy and security compliance concepts	L6

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Explain the concepts, advantages, and tools used in automated software testing.	L2
2	Develop and execute automated test scripts for web-based applications.	L2
3	Apply automation techniques for data-driven, functional, and regression testing.	L3
4	Analyze and interpret automated test execution reports to identify defects and test coverage.	L4
5	Detect and resolve exceptions and dynamic element handling issues in automated tests.	L4
6	Design and implement a reusable automation testing framework following industry practices.	L6

Hardware & Software Requirements:

Hardware Requirement: PC i5 Processor or above, 8 GB RAM	Software requirement: Python/Java, DevOps Tools
--	---

Sr. No.	Experiment List	Hours	LO Mapping
0	Introduction to Information Security Lab Environment and Tools	2	–
1	Study of Information Security Policies and ISMS Framework	2	LO1
2	Identification and Classification of Information Assets	2	LO1
3	Study of Threats and Vulnerabilities in Information Systems	2	LO2
4	Access Control Configuration in Linux Environment	2	LO2
5	User Authentication and Privilege Management	2	LO3
6	Study and Implementation of Security Policies	2	LO4
7	Study of Cyber Laws and IT Act Case Studies	2	LO5
8	Study of Digital Evidence and Documentation Process	2	LO5
9	Study of Data Privacy and DPDP Act 2023 Compliance	2	LO6
10	Mini Project / Case Study on Information Security Management	4	LO6

Text Books:

1. Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, Cengage Learning
2. ISO/IEC 27001:2022, Information Security Management Systems – Requirements, ISO Standard Publication

References:

1. Stuart McClure, Joel Scambray, George Kurtz, Hacking Exposed: Network Security Secrets & Solutions, McGraw Hill
2. Nina Godbole, Sunit Belapure, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India

Online References:

Sr. No.	Website Name
1	https://www.udemy.com/share/10bh7u/
2	https://www.coursera.org/learn/automate-workflows-across-tools-seamlessly
3	https://www.coursera.org/specializations/packt-learn-automation-testing-with-java-and-selenium-webdriver

Assessment:

Term Work: Term work shall consist of at least 10-12 Practical based on above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiments) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above list of Practical.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24461183	Cloud Computing and Security Lab	---	2	---	---	1	---	1

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24461183	Cloud Computing and Security Lab	---	---	---	---	---	25	25	50

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
1	To make students familiar with key concepts of virtualization.
2	To make students familiar with various deployment models of cloud such as private, public, hybrid and community.
3	To understand the using and adopting appropriate type of cloud for their application.
4	To make students familiar with various service models such as IaaS, SaaS, PaaS, Security as a Service (SECaaS) and Database as a Service.
5	Apply the different service models for the application.
6	To make students familiar with security and privacy issues in cloud computing and how to address them.

Lab Outcomes: Upon completion of the course students will be able to:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Implement different types of virtualization techniques.	L3
2	Analyze various cloud computing service models and implement them to solve the given problems.	L4
3	Design and develop real world web applications and deploy them on commercial cloud(s).	L6
4	Explain major security issues in the cloud and mechanisms to address them.	L2
5	Explore various commercially available cloud services and recommend the appropriate one for the given application.	L4
6	Implement the concept of containerization.	L3

Hardware & Software Requirements:

Hardware Requirement:	Software requirement:
-----------------------	-----------------------

DETAILED SYLLABUS:

Sr. No.	Experiment List	Hours	LO Mappings
1	Lab Prerequisites.	02	-
2	To study and implement Hosted Virtualization & Implement Bare-metal Virtualization using Xen, HyperV or VMware Esxi.	02	LO1
3	To study and implement Infrastructure as a Service using AWS/Microsoft Azure/Google cloud platform.	02	LO2
4	Design and develop Web Application on AWS/GCP/Azure.	04	LO3
5	To study and implement Security as a Service on AWS/Azure.	04	LO4
6	To study and implement Identity and Access Management (IAM) practices on AWS/Azure cloud.	02	LO4
7	To study and implement Virtual Private Network using AWS/GCP/Azure.	02	LO4
8	To study and implement Storage as a Service using AWS/Azure Storage.	02	LO5
9	To study and launch AWS/GCP/Azure instance using terraform.	04	LO6
10	To study and monitor logs of AWS/GCP/Azure.	04	LO6

Text Books:

1. B. Sosinsky, Cloud computing Bible, Wiley.
2. K. Jayaswal, J. Kallalurchi, D. Houde, D. Shah, Cloud Computing Black Book, Dreamtech Press
3. R. Buyya, Mastering Cloud Computing, McGraw Hill.
4. J. Baron, AWS certified solution Architect, Cybex.
5. T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy, O'Reilly.
6. R. Krutz, R. Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley.

References:

1. K. Hwang, G. Fox, J. Dongarra, Distributed and Cloud Computing From Parallel Processing to the Internet of Things, Morgan Kaufmann.
2. J. Hurwitz, Cloud Computing for Dummies, Wiley.
3. G. Reese, Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, O'Reilly.
4. J. Vecca, Cloud computing security: foundation and challenges, CRC Press.

Online References:

Sr. No.	Website Name
1	https://phoenixnap.com/kb/ubuntu-install-kvm/
2	NIST Cloud Computing Security Reference Architecture
3	https://docs.citrix.com/en-us/xenserver/7-1/install.html
4	https://docs.aws.amazon.com

5	https://docs.microsoft.com/en-us/azure
6	https://docs.docker.com/get-started/
7	https://kubernetes.io/docs/home/

Assessment:

Term Work: Term work shall consist of at least 10-12 Practical based on above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiments) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above list of Practical

DRAFT

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
24461184	User Interface Design with Security Lab	---	2	---	---	1	---	1

Course Code	Course Name	Theory					Term Work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
24461184	User Interface Design with Security Lab	---	---	---	---	---	25	25	50

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
1	To understand UI/UX guidelines through hands-on design activities
2	To design user interfaces using standard usability principles
3	To implement accessibility and inclusive design features
4	To identify UI-based security vulnerabilities
5	To design secure authentication and data entry interfaces
6	To evaluate UI designs for usability, accessibility, and security

Lab Outcomes: Upon completion of the course students will be able to:

Sr. No.	Lab Outcomes	Cognitive Levels of Attainment as per Bloom's Taxonomy
1	Apply UI/UX guidelines in interface design	L3
2	Create wireframes and prototypes	L3
3	Design accessible user interfaces	L3
4	Identify UI-based security risks	L4
5	Design secure authentication and form interfaces	L6

DRAFT

Hardware & Software Requirements:

Hardware Requirement: PC i3 Processor or above.	Software requirement: TCL, NS2.35, Ubuntu Operating System, Protocol Analyzer(e.g. Wireshark).
---	--

DETAILED SYLLABUS:

Sr. No.	Experiment List	Hours	LO Mapping
0	Introduction to UI/UX tools and secure UI concepts	02	–
1	Designing basic UI screens using usability guidelines	02	LO1
2	Creating wireframes and low-fidelity prototypes	02	LO2
3	Designing accessible UI following WCAG guidelines	02	LO3
4	Usability evaluation using heuristic evaluation	02	LO4
5	Identification of UI-based security vulnerabilities	02	LO4
6	Designing secure login and authentication UI	02	LO5
7	Secure form design and error message guidelines	02	LO5
8	Designing privacy notice and consent UI	02	LO6
9	Mini Project: Secure UI/UX design for an application	02	LO6
10	Project demonstration along with security aspects	04	LO6

Text Books:

- Alan Dix et al., *Human–Computer Interaction*, Pearson India
- Wilbert O. Galitz, *The Essential Guide to User Interface Design*, Wiley India
- Nina Godbole, *Cyber Security*, Wiley India

References

- Ben Shneiderman, *Designing the User Interface*, Pearson
- Don Norman, *The Design of Everyday Things*
- ISO 9241 – Ergonomics of Human–System Interaction

Lab Resource Material / Online References

(User Interface Design with Security)

Online References:

Sr. No.	Website Name
1	https://www.usability.gov
2	https://www.w3.org/WAI
3	https://owasp.org
4	https://material.io/design

Assessment:

Term Work: Term work shall consist of Practical based on above list. Also, Term work Journal must include at least 2 assignments.

Term Work Marks: 25 Marks (Total marks) = 15 Marks (Experiments) + 5 Marks (Assignments) + 5 Marks (Attendance)

Oral Exam: An Oral exam will be held based on the above list of Practical.

Vertical - 4

VSEC

DRAFT

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Practical	Tutorial	Total
2446411	Innovation Lab (Mini Project)	---	04	---	---	02	---	02

Course Code	Course Name	Theory					Term Work	Practical / Oral	Total
		Internal Assessment			End Semester Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II					
2446411	Innovation Lab (Mini Project)	---	---	---	---	---	50	---	50

Course Objectives:

Sr. No.	Course Objectives
1	To enable students to identify real-world problems through need-based surveys, literature review, and structured requirement analysis.
2	To develop skills in formulating clear problem statements and project objectives based on feasibility, innovation, and societal relevance.
3	To train students in designing and planning project execution using tools such as Gantt charts, PERT/CPM, and structured methodologies.
4	To provide hands-on experience in developing and implementing functional prototypes or models using appropriate engineering tools and domain-specific technologies.
5	To enhance teamwork, leadership, and project management skills through collaborative group work, progress tracking, and review presentations.
6	To cultivate professional competencies in documentation, technical communication, validation, and evaluation of project outcomes with sustainability and continuous learning focus.

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

Sr. No.	Course Outcomes	Cognitive Levels of Attainment as per
---------	-----------------	---------------------------------------

		Bloom's Taxonomy
1	Formulate a real-world problem by conducting need-based surveys and demonstrating professional responsibility in problem selection.	L2, L3, L4
2	Implement appropriate engineering methods to develop a functional solution while collaboratively exhibiting ethical teamwork behaviour.	L2, L3, L4, L5, L6
3	Demonstrate effective leadership or collaboration by actively coordinating project tasks and responding constructively to group dynamics.	L2, L3, L4
4	Validate experimental results through analytical techniques and justify findings with disciplined technical documentation.	L2, L3, L4, L5, L6
5	Evaluate the societal and environmental impact of the developed solution while applying sustainable engineering practices.	L3, L4, L5
6	Execute project activities using standard engineering tools while exhibiting commitment towards continuous self-directed learning.	L2, L3, L4, L5, L6

Guidelines for Innovation Lab (Mini Project):

1	Students shall form a group of 3 to 4 students. While forming a group less than three or more than four students shall not be allowed, as it is a group activity.
2	Interdisciplinary project is also allowed.
3	Students should do survey and identify needs, which shall be converted into problem statement for project in consultation with faculty supervisor/head of department/internal committee of faculties.
4	Students shall submit implementation plan in the form of Gantt/PERT/CPM chart, which will cover weekly activity of project.
5	A logbook to be prepared by each group, wherein group can record weekly work progress, guide/supervisor can verify and record notes/comments.
6	Faculty supervisor may give inputs to students during project activity; however, focus shall be on self-learning.
7	Students in a group shall understand problem effectively, propose multiple solution and select best possible solution in consultation with guide/ supervisor.
8	Students shall convert the best solution into working model using various components of their domain areas and demonstrate.
9	The solution to be validated with proper justification and report to be compiled in standard format of University of Mumbai.
10	With the focus on the self-learning, innovation, addressing societal problems and entrepreneurship quality development within the students through the project.
11	The goal is to develop a product and create avenues for IP filing.

Term Work:

The review/ progress monitoring committee shall be constituted by head of departments of each institute. The progress of project to be evaluated on continuous basis, minimum two reviews in the semester.

In continuous assessment focus shall also be on each individual student, assessment based on individual's contribution in group activity, their understanding and response to questions.

Distribution of Term work marks shall be as below:		Marks
1	Marks awarded by guide/supervisor based on logbook	5
2	Marks awarded by review committee (Average of Review 1 & Review 2)	40

Project Review - 1		
1	Identification of Problem	4
2	Requirement analysis and Feasibility of the proposed work	4
3	Literature Review	4
4	Objectives of the proposed work	4
5	Methodology of the proposed work	4
	Total Marks	20

Project Review - 2			
	a	Planning of project work and team structure	4
	b	Design Methodology	4
	c	Conceptual and Technical Demonstration	4
	d	Presentation: Oral delivery, contact with audience, slides, timing	4
	e	Quality of answers	4

	Total Marks	20
	Quality of Project Report	5

Online References:

Sr. No.	URL
1	https://www.geeksforgeeks.org/project-idea-college-network/?ref=ml_lbp
2	https://www.simplilearn.com/tutorials/artificial-intelligence-tutorial/ai-project-ideas
3	https://roadmap.sh/backend/project-ideas
4	https://webflow.com/blog/website-ideas
5	https://gist.github.com/MWins/41c6fec2122dd47dfaca31924647499
6	https://www.projectpro.io/article/artificial-intelligence-project-ideas/461
7	https://github.com/The-Cool-Coders/Project-Ideas-And-Resources
8	https://nevonprojects.com/project-ideas/software-project-ideas/
9	https://roadmap.sh/projects

Vertical - 5

IKS

DRAFT

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Practical	Tutorial	Total
2346511	Indian Knowledge System – As Per Program common to all Program - Group A	--	2*+2	--	--	2	--	2

Course Code	Course Name	Theory					Term Work	Practical / Oral	Total
		Internal Assessment			End Semester Exam	Exam Duration (in Hrs)			
		IAT -I	IAT -II	IAT -I + IAT -II					
2346511	Indian Knowledge System – As Per Program common to all Program - Group A	--	--	--	--	--	50	--	50

* Two hours of practical class to be conducted for full class as demo/discussion.

Rationale:

The proposed IKS modules contextualize core engineering principles across Computer, IT, EXTC, Electronics, and Electrical engineering—within scientifically analyzable Indian knowledge

traditions. By mapping indigenous practices to modern technical frameworks, students critically examine foundational engineering concepts through interdisciplinary and systems-based perspectives. This approach strengthens conceptual understanding, promotes analytical reinterpretation of traditional knowledge using contemporary tools, and aligns engineering education with culturally rooted yet technically rigorous inquiry.

Prerequisite: --

Course Objectives:

1. Provide foundational knowledge of Indian acoustic practices.
2. To Understand Ancient Indian use of renewable energy.
3. Introduce Sanskrit grammar in simple language, with special attention to its rule-based structure.
4. Learners should be able to explain key contributions of ancient Indian mathematics in simple language.
5. Understand how Indian traditions of logic, language, knowledge organization, design thinking, governance, sustainability, and wellbeing can support modern IT solutions.
6. Understand the basic structure of Sanskrit grammar and relate selected grammatical ideas to computational modules used in information technology.

Course Outcomes:

On successful completion of the course learner will be able to:

1. Analyze traditional Indian acoustic practices and interpret their relevance to frequency analysis.
2. Apply the traditional knowledge to modern energy solutions and sustainable engineering.
3. Apply Indian Knowledge Systems in linguistics, Sanskrit-based NLP, traditional number systems, measurement practices, and ancient rainfall prediction techniques using calendars, nakshatras, and natural indicators.
4. Apply basic modular arithmetic, pattern recognition, and place-value ideas to simple IT examples such as coding, data representation, and checksums.
5. Apply basic concepts of Indian Knowledge Systems such as logic, language, knowledge organization, ethics, sustainability, and responsible decision-making to design simple technology-based solutions like apps, chatbots, databases, or awareness tools.
6. Apply basic Sanskrit grammar concepts and Pāṇinian rule-based principles to understand formal grammar, algorithms, and simple computational language processing applications in IT.

DETAILED SYLLABUS:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	-	-	-
I	Acoustic Science in Vedic Chanting and Indian Music	I.1 Concept of Nāda (Sound) and Shruti Physical interpretation: frequency, pitch, harmonic content	10	CO1

		• Shruti system (22 microtones) and frequency discrimination I.2 Resonance and Architectural Acoustics • Temple architecture and echo control • Natural acoustic amplification • Relation to reverberation time and standing waves I.3 Structured Sound Encoding in Vedic Recitation • Pada, Krama, Ghana patha recitation methods • Built-in redundancy → error detection and correction • Parallel to digital communication redundancy schemes Self-Study: Study of sounds and analysis in time and frequency domains.		
II	Tradition	1. Introduction to IKS in renewable energy 2. Ancient Indian use of renewable energy a) Solar Energy: Solar Architecture, Solar Heating Systems b) Wind Energy: Ancient Windmills, Wind-Powered Water Lifting c) Water (Hydro) Energy: Ancient Watermills, Irrigation Systems d) Bioenergy: Biomass Fuel, Bioenergy Production 3. Integration of ancient Traditional knowledge of renewable energy with Modern Technologies. Students shall study the following to understand the use of ancient technologies in Renewable Energy: • Gujarat Windmills • Watermills in the Indus Valley	10	CO2

		Konark Sun Temple		
III	Linguistics, Number Systems, and rainfall Prediction	Linguistics: - Components of language - Panini's work on Sanskrit grammar - Role of Sanskrit in Natural Language Processing Number System and Units of Measurement - Number system in India- Historical Evidence - Decimal System - Unique Approaches to represent Numbers- Katapayadi System - Pingala and the Binary System Ancient Indian techniques for predicting Rainfall - Introduction - Elements of the Indian Calendar - Panchang and Nakshtras - Non-bio indicators and Bio indicators Self-Learning: - An Ecosystem for Sanskrit Language Processing - Salient Features of the Indian Numeral System - Salient Features of the Indian Numeral System - Measurement for Time Distance and Weight - Measurement of Time- An Illustration from Purana	10	CO3
IV	Mathematics Foundations in Ancient India and Its Relevance to Information Technology	4.1 Historical context and number ideas: Indian knowledge systems, the development of numeration, zero as placeholder and number, decimal place value. 4.2 Major contributors and procedural mathematics: Aryabhata, Brahmagupta,	10	CO4

		Bhaskara II, and examples of rule-based or sutra-like calculation methods in plain language. 4.3 Algorithmic thinking and computation: Historical mathematical procedures connect to algorithms, flowcharts, decomposition, and computational logic. 4.4 Modular arithmetic, binary-style ideas, and data representation: Clock arithmetic, remainders, cyclic reasoning, two-state representation, bits, bytes, and simple binary conversion. 4.5 Relevance to IT and synthesis: Coding, checksums/parity, simple cryptography idea, data representation, and how ancient mathematical thinking supports modern IT problem-solving. Self-Learning Topics and Activities: • Zero and place value in daily life • Algorithmic thinking • Modular arithmetic • Binary representation		
V	Indian Logic and its applications in Information Technology	5.1 Introduction to IKS and its relevance to contemporary technology. 5.2 Indian logic, language, and computation with simple examples. 5.3 Knowledge organization, data, and decision-making. 5.4 Ethics, society, sustainability, and responsible digital systems. 5.5 Mini activity where students design a small app, chatbot, database, or awareness tool using one IKS principle. Self-Learning Topics and Activities: • Basic ideas of Nyaya logic: observation, inference, debate, and evidence. • Introduction to Paninian grammar and why structured language matters in NLP.	10	CO5

		- Traditional knowledge classification and its connection with databases and knowledge graphs. - Technology for Indian languages, heritage preservation, digital museums, and public services. - Design thinking activity: identify a local problem and propose an IKS-inspired IT solution.		
VI	Sanskrit Grammar and Computational Modules	6.1 Introduction to Indian Knowledge Systems, Sanskrit as structured language, and relevance to IT. 6.2 Basic Sanskrit grammar concepts: sounds, words, roots, suffixes, sandhi, and sentence structure. 6.3 Pāṇinian grammar as a rule-based system; relation with algorithms and formal grammar. 6.4 Computational modules: tokenization, morphology, parsing, language rules, and NLP examples. 6.5 Demonstration of Sanskrit digital tools, reflection activity, and discussion on interdisciplinary applications. Self-Learning Topics and Activities: - Basic Sanskrit alphabet and sound classification. - Simple sandhi examples and word joining rules. - Introduction to Pāṇini and the Aṣṭādhyāyī. - Dhātu, pratyaya, pada, and kāraka in simple terms. - Basics of natural language processing: tokenization, morphology, and parsing. - Exploration of Sanskrit digital dictionaries and Sanskrit reader tools. - Comparison of grammar rules and computer program rules.	10	CO6

Text and Reference Books or Articles:

1. Acoustics of Chants, Conch-Shells, Bells & Gongs in Worship Spaces. Available: https://www.academia.edu/38208102/Acoustics_of_Chants_pdf?utm_source=chatgpt.com
2. V. R. S. Nalluri, V. J. K. S. Sonti, and G. Sundari, "Analysis of frequency dependent Vedic chanting and its influence on neural activity of humans," *International Journal of Reconfigurable and Embedded Systems*, vol. 12, no. 2, pp. 230–239, Jul. 2023, doi: 10.11591/ijres.v12.i2.pp230-239.
3. The Garland Encyclopedia of World Music: South Asia. Available: https://api.pageplace.de/preview/DT0400.9781351544399_A30892028/preview-9781351544399_A30892028.pdf?utm_source=chatgpt.com
4. J. Pattanayak, Y. Belur, and J. Ilavarasu, "Acoustic and psychological effects of Omkar chanting in novice Indian adults: A quasi-experimental study," *Journal of Clinical and Diagnostic Research*, 2025, doi: 10.7860/JCDR/2025/77365.21111. Available: https://www.jcdr.net/articles/PDF/21111/77365_CE%5BRa1%5D_F%28IS%29_QC%28PS_SS%29_PF1%28AB_IS%29_redo_PFA%28IS%29_PB%28AB_IS%29_PN%28IS%29.pdf?utm_source=chatgpt.com
5. "Indian Knowledge System: Integrating Heritage with Engineering" by Gagan Bansa, Deep Science Publishing; ISBN: 978-93-49307-77-3 E-ISBN: 978-93-49307-29-2;
6. The textbook of Indian Knowledge Systems, University of Mumbai, ISBN: 978-93-5915-553-1
7. Introduction to Indian Knowledge System: Concepts and Applications, Mahadevan, B., Bhat, Vinayak Rajat, Nagendra Pavana R.N. by PHI Learning Pvt Ltd. Delhi, ISBN: 978-93-91818-20-3
8. Echoes of the Monsoon: Ancient Indian techniques for predicting Rainfall, Janak Joshi, Kandarp
9. Parmar, Lakhan Jain, Sharmistha Bhowmik and Bindu Bhatt, DOI: <https://www.doi.org/10.22271/27067483.2025.v7.i7a.386>.
10. Kim Plofker, *Mathematics in India: A clear historical overview of Indian mathematical developments, suitable for faculty use and advanced self-learners.*
11. George Gheverghese Joseph, *The Crest of the Peacock: An accessible introduction to non-European mathematical traditions, including India.*
12. Charles Petzold, *Code: The Hidden Language of Computer Hardware and Software: A beginner-friendly bridge from numbers and symbols to data representation and computing.*
13. Simon Singh, *The Code Book: Useful for simple explanations of ciphers, encryption, and the mathematics behind communication security.*
14. T. A. Sarasvati Amma, *Geometry in Ancient and Medieval India: A more specialized reference for deeper exploration of traditional mathematical methods.*

15. Mahadevan, B., Bhat, V. R., and Nagendra Pavana R. N. Introduction to Indian Knowledge System: Concepts and Applications. PHI Learning.
16. Kapur, K., and Singh, A. K. (Eds.). Indian Knowledge Systems, Vol. 1. Indian Institute of Advanced Study, Shimla.
17. Bora, M. C. Bharatiya Knowledge Systems. Khanna Publishing House.
18. Rao, S. S. Engineering and Technology in Ancient India. Indian National Science Academy / related academic editions.
19. Selected open articles or chapters from IKS Division / AICTE / Ministry of Education resources may be used as supplementary reading.
20. S. D. Joshi and J. A. F. Roodbergen, The Aṣṭādhyāyī of Pāṇini.
21. V. N. Jha, The Philosophy of Sanskrit Grammar.
22. Peter M. Scharf, Sanskrit Syntax and Discourse Structures.
23. Daniel Jurafsky and James H. Martin, Speech and Language Processing — for introductory NLP concepts.
24. Rajeev Sangal, Akshar Bharati, and Vineet Chaitanya, Natural Language Processing: A Paninian Perspective.

Other Online Resources:

Sr. No.	Website Name
1.	NPTEL course page: For a structured academic overview of mathematics in India. https://nptel.ac.in/courses/111101080
2.	NPTEL YouTube playlist: For lecture-based learning that can support flipped or self-paced study. https://www.youtube.com/playlist?list=PLbMVogVj5nJThf31TNSQzuN7zqxe7HdRN
3.	IKS India: For broader Indian Knowledge Systems context and additional learning resources. https://www.nist.gov/cryptography
4.	Responsible AI and India-context resources: https://indiaai.gov.in/
5.	IKS Division, Ministry of Education / AICTE: https://iksindia.org/
6.	NPTEL: Introduction to Pāṇinian Grammar URL: https://onlinecourses.nptel.ac.in/noc24_hs44/preview
7.	Sanskrit Heritage Reader URL: https://sanskrit.inria.fr/

List of Practical and List of Assignments:

Sr No	List of Experiments	Hrs
01	Record a temple bell sound, conch sound, or classical “Sa” note and analyze it by plotting its time-domain waveform and frequency spectrum, identifying the fundamental frequency and harmonics, and comparing the observed harmonic structure with theoretical frequency ratios of Just Intonation and Equal	04

	Temperament.	
02	Observe the movement of sunlight and shadow around a building, monument, or open courtyard at different times of the day, record the shadow directions and lengths, and analyze how solar position can guide orientation, time estimation, and passive architectural planning in the context of traditional Indian solar design.	04
03	Examine images, plans, or a simple model of the Konark Sun Temple or any sun-oriented structure, identify how geometry, orientation, and sunlight interaction are used in the design, and prepare a visual explanation of how ancient solar architecture supports modern sustainable building concepts.	04
04	Construct a small paper or cardboard windmill, test its rotation under natural wind or fan airflow at different speeds, and document how blade movement demonstrates the basic principle of converting wind energy into mechanical motion, linking it to traditional wind-powered systems and modern turbines.	04
05	Build a simple working model using cups, straws, thread, or cardboard to simulate water lifting or channel-based irrigation, observe how water can be moved with minimal energy input, and relate the model to ancient Indian irrigation systems and watermill-based practices.	04
06	Survey homes or nearby community spaces to identify traditional biomass fuels such as wood, agricultural residue, or cow-dung cakes, record their current use, benefits, and limitations, and compare the observed practices with modern ideas of bioenergy and sustainable fuel management..	04
07	Pronounce and classify selected Sanskrit sounds into vowels and consonants using a simple sound chart, group them according to articulation patterns, and analyze how this systematic sound organization supports pronunciation training, language learning, and speech-processing applications.	04
08	Create all possible combinations of short and long syllabic patterns of a fixed length, tabulate them systematically, and compare the resulting patterns with binary 0/1 combinations to understand how ancient combinatorial thinking connects with digital representation.	04
09	Solve real-life problems based on clocks, calendars, weekdays, or repeated events using modular arithmetic, record the remainder-based reasoning used in each case, and explain how cyclic patterns support time management, scheduling, and introductory cryptographic logic.	04
10	Convert selected decimal numbers into binary form, arrange them in bit patterns, append parity bits for even or odd parity, and interpret how binary representation and simple error-detection methods are used in digital systems for reliable data storage and transmission.	04
11	Use a basic Sanskrit dictionary, transliteration tool, or reader tool to input selected words, observe the output such as root, meaning, or grammatical analysis, and describe how such tools support language technology and digital preservation.	04
12	Select a real-life problem such as fake-news verification, waste segregation, or campus awareness, identify observation, evidence, inference, and conclusion using the basic framework of Indian logic, and represent the reasoning process as a decision tree, chatbot flow, or awareness tool concept.	04
13	Take a simple historical or rule-based calculation procedure associated with Indian	04

	mathematics, rewrite it as a sequence of input-process-output steps, and convert it into a flowchart to demonstrate the connection between procedural mathematics and modern algorithmic thinking.	
14	Represent selected large and small numbers using a place-value table, deliberately insert or remove zero in different positions, and analyze how zero functions both as a number and as a placeholder, showing its importance in arithmetic, accounting, and digital data representation.	04
Sr No	List of Assignments	Hrs
01	Study the concepts of Nāda and Shruti, temple acoustics, and Vedic recitation methods, and briefly explain their relation to modern concepts of frequency, resonance, reverberation, and redundancy/error correction in digital communication systems. Also write a short note on how Indian Knowledge Systems demonstrate scientific understanding of sound and communication.	01
02	Study the ideas of solar architecture in traditional Indian structures such as the Konark Sun Temple or courtyard-based houses, and explain how sunlight, orientation, shading, and ventilation were used for thermal comfort and energy efficiency. Also write a short note on how these traditional design ideas are relevant to modern sustainable architecture and climate-responsive planning..	01
03	Study one traditional Indian renewable energy practice such as wind-powered water lifting, watermills, solar heating, or biomass use, and compare it with one modern renewable energy technology. Explain how traditional knowledge systems supported sustainable living and discuss how these ideas can inspire present-day energy conservation and green technology.	01
04	Study the basic ideas of Pāṇinian grammar as a structured rule-based system, and explain how concepts such as sounds, roots, suffixes, and word formation relate to modern ideas in natural language processing, machine translation, and language analysis. Also write a short note on why Sanskrit grammar is often considered relevant to computational linguistics.	01
05	Study the historical development of zero as both a number and a placeholder, and explain how the decimal place-value system simplified arithmetic and record keeping. Also write a short note on how zero and place value continue to be essential in digital computation, data storage, and computer-based numerical processing.	01
06	Study the basic ideas of Indian logic, especially observation, inference, debate, and evidence in the Nyāya tradition, and explain how these ideas support careful reasoning and decision-making. Also write a short note on how such logical methods can be applied in present-day contexts such as data analysis, fake-news verification, ethical decision-making, and responsible digital systems.	01
07	Identify one idea from Indian Knowledge Systems in the syllabus, such as renewable energy, Indian numeration, Indian logic, or Sanskrit grammar, and propose a simple real-life solution such as an app, chatbot, awareness campaign, digital archive, poster, database, or educational tool based on that idea. Explain the problem being addressed, the IKS principle used, and how the proposed solution can be useful in present-day society.	01
08	Study the basic Sanskrit grammar concepts of sounds, words, roots, suffixes,	01

	sandhi, and sentence structure, and explain how grammar rules work like structured instructions. Also compare grammar rules with computer program rules, and briefly discuss how tokenization, morphology, and parsing in computational systems resemble traditional rule-based language analysis.	
--	--	--

Assessment:

- **Term Work:** Term work shall consist of at least 10-12 practical's based on above list. Also Term Work Journal must include at least 4 assignments
Term Work Marks: 50 Marks (Total marks) = 25 Marks (Experiment) + 20 Marks (Assignments) + 5 Marks (Attendance)

DRAFT

AEC

DRAFT

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Practical	Tutorial	Total
2996511	Professional Skill	--	2*+2	--	--	2	--	2

Cours e Code	Course Name	Theory				Term Wor k	Practical / Oral	Tota l	
		Internal Assessment			End Semeste r Exam				Exam Duratio n (in Hrs)
		IAT -I	IAT -II	IAT -I + IAT -II					
2996511	Professional Skill	--	--	--	--	--	25	--	25

Course Rationale:

This course equips engineering students with professional communication, ethical values and soft skills essential for global industry demands. It enhances technical writing, presentation and interpersonal abilities through practical sessions, fostering confidence, teamwork and social responsibility as competent engineering professionals.

Course Objectives:

Sr. No.	Course Objectives
1	Develop effective speaking, presentation, group discussion and interview skills required for employability and professional success.
2	Analyse and evaluate AI-generated content for accuracy, bias, credibility and ethical professional use.
3	Prepare clear, concise and professional technical/business documents such as resumes, reports, SOP and formal correspondence.
4	Demonstrate managerial and collaborative skills required for conducting meetings, preparing proposals and workplace communication.
5	Apply interpersonal, critical thinking, negotiations, time management, leadership, decision-making and adaptability skills for lifelong learning and career growth.
6	Exhibit ethical values, intellectual property awareness, digital responsibility and professionalism in workplace practices.

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

Sr. No.	Course Outcomes	Cognitive Levels of
---------	-----------------	---------------------

		Attainment as per Bloom's Taxonomy
1	Demonstrate effective speaking skills through participation in group discussions, interviews, presentations and collaborative activities.	L2
2	Analyse and evaluate AI-generated content in terms of quality, bias, reliability and ethical use for academic and professional purposes.	L4
3	Create professional documents such as resumes, cover letters, statements of purpose, reports and other technical/business correspondence using standard formats.	L6
4	Organise and execute professional meetings, proposals and technical papers using appropriate workplace communication strategies and digital tools.	L6
5	Apply and demonstrate interpersonal skills such as leadership, critical thinking, negotiation, decision-making, time management and adaptability to support career growth and lifelong learning.	L3
6	Exhibit ethical practices, digital responsibility and awareness of intellectual property rights in professional environments.	L4

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mapping
1	Employability Skills: Advanced Speaking	1.1. Group Discussions (GDs) - Purpose, Evaluation parameters, GD etiquette - Types: Factual (Regular & Controversial), Abstract, Case-based (Textual & Picture-based) and Role-plays (Textual & Cue-card-based) - Online GDs and digital collaboration etiquette (Zoom, Google-Meet, MS Teams etc.) 1.2. Personal Interviews - Planning and preparation for Technical and HR interviews - Interview types: Structured, Stress, Behavioural and Case-based - Virtual interviews, AI-assisted interview simulations and post-interview reflections (Google Interview Warmup, Yoodli, Pramp etc.) 1.3. Presentation Strategies	8	CO1

		• Purpose, Audience analysis, Content organisation • Slide design, Text, Infographics and AI-based presentation design (Canva, Beautiful.ai, Gamma AI etc.) • Division of roles, collaborative preparation and seamless transitions		
2	Critical AI Literacy	• Nature of AI Generated Language - Understanding AI-generated language as probabilistic output and distinguishing between Fluency and Accuracy while identifying risks such as AI Slop and Hallucination • Evaluating AI Content - Differentiating between Evidence and Assertion and applying verification strategies to assess Accuracy, Clarity and Depth • Bias, Framing and Information Silos - Understanding linguistic Bias, Framing, Information Silos and Selective Exposure that shape AI responses and limit perspective • Drafting, Editing and Prompt Engineering with AI - Using AI for Drafting and Editing through effective Prompt Engineering while maintaining originality, specificity and professional voice • Identifying Low-Quality AI Content - Identify markers of low-quality AI content, such as repetition, lack of depth, and absence of concrete detail, while applying ethical practices that distinguish Assistance from Substitution and ensure responsible AI use	4	CO2
3	Employability Skills: Advanced Technical Writing	3.1. Cover Letter & Resume • Difference between Bio-data, Resume and CV • Resume types: Chronological, Functional and Hybrid • Resume structure and content	8	CO3

- Digital resumes, Application Tracking System (ATS) friendly formatting and LinkedIn portfolio integration

3.2. Reports

- **Purpose:** Importance of reports in engineering and industry decision-making

Classification of Reports:

Subject Matter - Technical, R&D, Operations, Finance, Marketing etc.

Time Interval - Periodic, One-time, Special

Function - Informational, Examinational and Analytical

Reader Writer Relationship - Administrative, Professional and Independent

Format - Memo, Letter, Short, Long, E-Reports, Digital Dashboards

Digital and AI-aided reporting formats (Power BI, Google Data Studio, ChatGPT etc. for summaries)

Parts of a Long Formal Report

Prefatory Parts: Title Fly, Title Page, Letter of Transmittal, Table of Contents, List of Illustrations, Executive Summary

Report Proper (Main Body): Introduction, Intervening chapters with headings as per the topic, Result & Analysis, Summary (Informational) Or Summary & Conclusions (Examinational) **Or** Summary, Conclusions & Recommendations (Analytical)

Appended Parts: Appendix, List of References, Glossary, Index

- **Language and Style of Reports**

Tense, person and voice appropriate to reports

Numbering and labelling conventions for figures, tables, charts, equations etc.

Referencing formats (APA, MLA etc.)

		Plagiarism checks (Turnitin, Grammarly, other AI-detectors etc.) 3.3. Statement of Purpose (SOP) • Purpose: SOPs for international internships, funding for research programs and higher education • Structure: Paragraph 1 - Hook (introducing yourself in a unique manner and demonstrating your passion for the field) Paragraph 2 - Academic Background Paragraph 3 - Research-oriented Endeavours Paragraph 4 - All-round Development Paragraph 5 - Reasons for choosing the Program and Institution Paragraph 6 - Conclusion and Thank-you note		
4	Workplace Managerial Skills	4.1. Conducting Business Meetings • Types of Meetings: Executive Meetings - Decide Management Meetings - Implement Committee Meetings - Recommend Review Meetings - Evaluate Planning Meetings - Design the future Crisis Meetings - Resolve urgency • Roles and Responsibilities: Chair - Leads meeting, maintains order, ensures decisions Secretary - Records minutes, documents decisions, tracks actions Core Members - Discuss issues, contribute ideas, make decisions Specialists - Provide expertise, clarify issues, support decisions • Documentation: Notice, Agenda and Minutes • Meeting Platforms and AI Assistance: Virtual and hybrid meeting management, online etiquette, use of collaborative tools (Google Meet, Slack, Trello etc.)	6	CO4

		Digital documentation, e-Minutes and collaborative platforms like Notion or Microsoft OneNote 4.2. Writing Proposals • Types: Solicited vs. Unsolicited • Format: Memo, Short and Long • Parts of a Short Proposal: - Purpose of the proposal - Need for the proposal (SWOT analysis) - Description of the plan (budget, timeline etc.) - Evidence of ability to deliver - Benefits to both parties - Conclusion 4.3. Structuring and Formatting Technical Papers Components: Title, Author(s) & Affiliations, Abstract, Keywords/Index Terms, Introduction, Sections with different headings, Results, Discussion, Conclusion, Acknowledgement, References, Biography • Formatting and referencing (IEEE style) • Use of AI tools for grammar check, plagiarism validation and submission to international conferences		
5	21st Century Professional Skills	5. Interpersonal Skills Emotional Intelligence • Critical thinking, Reflection & Self Analysis • Leadership and Motivation Strategies • Conflict Management and Negotiation • Time Management • Anger and Stress Management • Decision Making and Adaptability	6	CO5
6	Digital Ecosystems and Ethics	6.1. Intellectual Property Rights (IPR) Categories: Copyrights, Trademarks, Patents, Industrial Designs, Geographical Indications, Integrated Circuits and Trade Secrets	4	CO6

		• AI-generated content ownership, open-source ethics, digital rights management • Social Media Content and Legal Responsibility 6.2. Case Studies on Corporate and Engineering Ethics Real-world ethical dilemmas • Corporate Social Responsibility (CSR) • Environmental Social Governance (ESG) • Sustainability and Green Engineering • AI Ethics in Design and Automation		
--	--	---	--	--

ASSESSMENTS

List of Compulsory Assignments for Term Work:

Module 1: GD documentation with Topic, Type and Highlights in 5 bullet points

Module 2: Assignment on Prompt Engineering

Module 3: A - Cover Letter, Resume and B - Statement of Purpose

Module 4: Meeting Documentation (Notice, Agenda & Minutes)

Module 5: Activities on Interpersonal Skills

Module 6: Case study on Ethical Dilemma

(To be conducted in the form of short notes, quizzes, role plays, case studies, presentations or MCQs)

SUGGESTED ASSIGNMENTS

Module No. & Title	Assignments and Activities
Module 1 Employability Skills: Advanced Speaking	• Conduct 4-5 types of Group Discussions and attach the summary and photographs as proof of activity • Prepare group presentation slides, based on the report topic (Examination or Analytical) using the latest presentation software (PowerPoint, Canva, Prezi etc.) and engage students in giving critical feedback • Present an 'Elevator Pitch' for either self-introduction or product or new business idea • Conduct mock interviews

Module 2 Critical AI Literacy	• Select an essay/article/video generated by AI (or give a general prompt) and analyse and detect AI bias (gender pronouns, gender-based occupational stereotypes, racial identifiers, historical bias etc.) • Differentiate between weak and strong prompts • Source verification task • AI versus human writing analysis
Module 3 Employability Skills: Advanced Technical Writing	• Draft a professional Cover Letter and Resume • Write a Statement of Purpose (SOP) for higher studies or internships • Develop or enhance a LinkedIn profile showcasing technical and project achievements • Prepare a book-format analytical/informational report using IEEE/APA/MLA referencing and plagiarism check tools (Grammarly/Turnitin). Main body should be minimum 20 pages excluding the Preparatory and Appended parts
Module 4 Workplace Managerial Skills	• Conduct a mock meeting with assigned roles (Chairperson, Secretary, Members) and generate documentation with the help of the latest software • Write a short proposal addressing an engineering or sustainability problem • A quiz on the formatting aspects of a Technical Paper
Module 5 21st Century Professional Skills	• Activities for developing team work, leadership, emotional intelligence etc.] • Problems and Puzzles on Critical thinking • Case-studies or Role-plays or Questionnaires on Conflict Resolution, Negotiation Skills and Decision Making • Application of SWOT analysis • Eisenhower Matrix to analyse a daily time log
Module 6 Digital Ecosystems and Ethics	• Conduct an awareness quiz on IPR laws and ethical business practices. • Analyse a corporate ethics case study • Digital footprint audit of Self Profile • Fake News and Deep Fake verification task

IMPORTANT NOTE

1. The main project/book report should contain a minimum of 20 pages, excluding prefatory and appended matter.
2. Each project group must consist of a minimum of 4 and a maximum of 6 students.
3. End-semester presentation will be based on the book/project report.

GUIDELINES FOR TERM WORK MARKS DISTRIBUTION

Components	Marks 25	Description
6 Compulsory Assignments	5	Based on completion and quality of module-wise tasks.
Attendance & Participation	5	Class engagement, teamwork, and professionalism.
GD	5	Based on group and individual performance
Report Hardcopy	5	Quality, structure and originality of the report
Oral Report Presentation	5	Based on group and individual performance

RECOMMENDED RESOURCES:

1. Raman, M., & Sharma, S. (2022). Technical communication: Principles and practice (4th ed.). Oxford University Press.
2. Anderson, P. V. (2018). Technical communication: A reader-centred approach (9th ed.). Cengage Learning.
3. Lesikar, R. V., Flatley, M. E., & Rentz, K. (2008). Basic business communication (11th ed.). McGraw-Hill.
4. Institute of Electrical and Electronics Engineers. (2020). IEEE code of ethics. IEEE.
5. American Society of Mechanical Engineers. (2021). ASME code of ethics of engineers. ASME.
6. Guffey, M. E., & Loewy, D. (2018). Essentials of business communication (11th ed.). Cengage Learning.
7. Sharma, R. C., & Mohan, K. (2017). Business correspondence and report writing (4th ed.). Tata McGraw-Hill Education.
8. Ram, A. (2018). Place mentor: Tests of aptitude for placement readiness. Oxford University Press.
9. Kumar, S., & Lata, P. (2018). Communication skills: A workbook. Oxford University Press.
10. Butterfield, J. (2017). Verbal communication: Soft skills for a digital workplace. Cengage Learning.
11. Crawford, K. (2021). Atlas of AI: Power, politics, and the planetary costs of artificial intelligence. Yale University Press.
12. Kearns, M., & Roth, A. (2019). The ethical algorithm: The science of socially aware algorithm design. Oxford University Press.

ONLINE RESOIRCES:

1. Ravichandran, T. (n.d.). Enhancing soft skills and personality [NPTEL course]. National Programme on Technology Enhanced Learning. <https://nptel.ac.in>
2. Ravichandran, T. (n.d.). Developing soft skills and personality [SWAYAM MOOC]. SWAYAM. <https://swayam.gov.in>
3. Coursera. (n.d.). Business communication for success [Online course]. <https://www.coursera.org>
4. edX. (n.d.). Business communication for success [Online course]. <https://www.edx.org>
5. All India Council for Technical Education. (n.d.). Employability enhancement and life skills modules. AICTE NEAT. <https://neat.aicte-india.org>
6. Indian Institute of Technology Guwahati. (n.d.). Virtual English and communication virtual lab. Virtual Labs. <https://ve-iitg.vlabs.ac.in/>
7. Indian Institute of Technology Bombay. (n.d.). Professional communication virtual lab. Virtual Labs. <http://vlabs.iitb.ac.in/vlabs-dev/labs/communication/>
8. TCS iON. (n.d.). Communication skills [Online course]. <https://www.tcsion.com/courses/tcs-ion/communication-skills/>
9. TCS iON. (n.d.). Introduction to soft skills [Online course]. <https://www.tcsion.com/courses/interview-and-job-prep/introduction-to-soft-skills/>
10. TCS iON. (n.d.). Presentation skills [Online course]. <https://www.tcsion.com/courses/tcs-ion/presentation-skills/>

QUESTION PAPER PATTERN
(External and Internal)

DRAFT

Letter Grades and Grade Points:

Semester GPA/ Programme CGPA Semester/ Programme	% of Marks	Alpha-Sign/ Letter Grade Result	Grading Point
9.00 - 10.00	90.0 – 100	O (Outstanding)	10
8.00 - < 9.00	80.0 - < 90.0	A+ (Excellent)	9
7.00 - < 8.00	70.0 - < 80.0	A (Very Good)	8
6.00 - < 7.00	60.0 - < 70.0	B+ (Good)	7
5.50 - < 6.00	55.0 - < 60.0	B (Above Average)	6
5.00 - < 5.50	50.0 - < 55.0	C (Average)	5
4.00 - < 5.00	40.0 - < 50.0	P (Pass)	4
Below 4.00	Below 40.0	F (Fail)	0
Ab (Absent)	-	Ab (Absent)	0

Sd/-

Dr. Vaishali D. Khairnar
BoS-Chairman-Information Technology
Faculty of Technology

Sd/-

Dr. Deven Shah
Associate Dean
Faculty of Science & Technology

Sd/-

Prof. Shivram S. Garje
Dean
Faculty of Science & Technology