AC –
Item No. –

As Per NEP 2020

University of Mumbai

Syllabus for Major

Vertical – 1, 4, 5

Name of the Programme – B.E (Computer Science and Engineering –Internet of Things and Cyber Security Including Blockchain)		
Faculty of Engineering		
Board of Studies in Information Technology		
U.G. Third Year Programme	**Exit Degree**	**B.Sc.Tech in Computer Science and Engineering – Internet of Things and Cyber Security Including Blockchain**
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:_____**	**B.E. (Computer Science and Engineering - Internet of Things and Cyber Security Including Blockchain)**
2	**Exit Degree**	**U.G. Diploma in Computer Science and Engineering -Internet of Things and Cyber Security Including Blockchain**
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. TEU-600C** **R. TEU-600D**	**Attached herewith**
6	**Semesters**	**Sem. V & VI**
7	**Program Academic Level**	**5.00**
8	**Pattern**	**Semester**
9	**Status**	**New**
10	**To be implemented from Academic Year**	**2026-27**

Sd/-	**Sd/-**	**Sd/-**
Dr. Vaishali Khairnar	**Dr. Deven Shah**	**Prof. Shivram S. Garje**
BoS Chairman, Computer Engineering	**Associate Dean**	**Dean**
Faculty of Science & Technology	**Faculty of Science & Technology**	**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 Information Technology 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 Information Technology in Engineering for open electives and multidisciplinary minor courses in semester 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 Information Technology 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 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.

Credit Structure (Sem. V & VI)

Level	Semester	Major		Minor	OE	VSC, SEC (VSEC)	AEC, VEC, IKS	OJT, FP, CEP, CC,RP	Cum. Cr. / Sem.	Degree/ Cum. Cr.
		Mandatory	Electives							
	R: _____C									
5.5	V	2345111:3 2345112:3 2345113:3 2345115: 1 2345116:1 2345117:1	2345114X:3 2345118X:1	MDC:3 MDL:1	OE:2	--	234551: 2	--	24	B.Sc. Tech Engineering 48
	R:_____D									
	VI	2346111:3 2346112:3 2346115:1 2346116:1	2346113X:3 2346114X:3 2346117X:1 2346118X:1	MDC: 3 MDL:1	--	2346411: 2	2346511: 2	--	24	
	Cum Cr.	20	12	8	2	2	*2+2*	--	48	

Exit option: Award of UG Diploma in Major and MDM with 90 credits and additional 4 credits core **one** theory subject with 3 credits and **one** lab with 1 credit from one third 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]

T.E.

Semester

V & VI

(Computer Science and Engineering- Internet of Things and Cyber Security Including Blockchain Scheme)

T.E. Computer Science and Engineering- Internet of Things and Cyber Security Including Blockchain Scheme Scheme

Program Structure for Third Year of Computer Science and Engineering
(Internet of Things and Cyber Security Including Blockchain)
UNIVERSITY OF MUMBAI (With Effect from 2026-2027)
SEMESTER V

Course Code	Course Description	Teaching Scheme (Contact Hours)				Credit Assigned			
		Theory	Practical	Tutorial	Total	Theory	Tutorial	Practical	Total Credits
PCC501	Computer Networks	3	--	--	03	3	--	--	3
PCC502	IoT Architecture and Protocols	3	–	--	03	3	--	--	3
PCC503	Network Security and Cryptography	3	--	--	03	3	--	--	3
PEC501	PEC-1	3	--	--	03	3	--	--	3
MDC501	Multidisciplinary minor	3	--	--	03	3	--	--	3
PCL501	Computer Networks Lab	--	2	--	02	--	--	1	1
PCL502	IoT Architecture and Protocols Lab	--	2	--	02	--	--	1	1
PCL503	Network Security and Cryptography Lab	--	2	--	02	--	--	1	1
PEL501	PEL-1	--	2	--	02	--	--	1	1
MDL501	Multidisciplinary minor	--	2	--	02	--	--	1	1
OECL501	To be taken from the bucket provided by the University from other Faculty	2	--	---	02	2	--	--	2
234551	IKS – As Per Program	--	2* + 2	--	04		2	--	02
Total		**17**	**14**	**00**	**31**	**17**	**00**	**07**	**24**

* Two hours of practical class to be conducted for full class as demo/discussion.
# 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	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)					
PCC501	Computer Networks	20	20	40	60	2	--	--	100
PCC502	IoT Architecture and Protocols	20	20	40	60	2	--	--	100
PCC503	Network Security and Cryptography	20	20	40	60	2	--	--	100
PEC501	PEC-1	20	20	40	60	2	--	--	100
MDC501	Multidisciplinary minor	20	20	40	60	2	--	--	100
PCL501	Computer Networks Lab	--	--	--	--	--	25	--	25
PCL502	IoT Architecture and Protocols Lab	--	--	--	--	--	25	25	50
PCL503	Network Security and Cryptography Lab	--	--	--	--	--	25	25	50
PEL501	PEL-1	--	--	--	--	--	25	25	50
MDL501	Multidisciplinary minor Lab	--	--	--	--	--	25	25	50
OECL501	To be taken from the bucket provided by the University from other Faculty	--	--	--	--	--	50	--	50
IKS501	IKS syllabus as per Groups						50	--	50
Total		**100**	**100**	**200**	**300**	**10**	**225**	**125**	**825**

Course Code	Course Description
PEC5011	AI for IoT
PEC5012	IoT applications in Smart infrastructure
PEC5013	Wireless sensor networks with secure protocols
PEC5014	Internet Programming

Lab Code	Lab Description
PEC5011	AI for IoT
PEC5012	IoT applications in Smart infrastructure
PEC5013	Wireless sensor networks with secure protocols
PEC5014	Internet Programming

UNIVERSITY OF MUMBAI (With Effect from 2026-2027)
SEMESTER VI

Course Code	Course Description	Teaching Scheme (Contact Hours)			Credit Assigned			
		Theory	Practical	Tutorial	Theory	Tutorial	Practical	Total Credits
PCC601	Blockchain Technology	3	--	--	3	--	--	3
PCC602	Ethical hacking and penetration testing	3	--	--	3	--	--	3
PEC601	PEC-1	3	--	--	3	--	--	3
PEC602	PEC-2	3	--	--	3	--	--	3
MDC601	Multi-disciplinary minor	3	--	--	3	--	--	3
AEC601	Professional Skill	--	2*+2	--	--	--	2	2
PCL601	Blockchain Technology Lab	--	2	--	--	--	1	1
PCL602	Ethical hacking and penetration testing Lab	--	2	--	--	--	1	1
PEL601	PEL-1	--	2	--	--	--	1	1
PEL602	PEL-2	--	2	--	--	--	1	1
MDL601	Multi-disciplinary minor Lab	--	2	--	--	--	1	1
2346411	Innovation Lab (Mini Project)	--	4	--	04	--	1	--
Total		**15**	**18**	**00**	**33**	**15**	**09**	**00**

* Two hours of practical class to be conducted for full class as demo/discussion.
@ Institute shall offer a course for MDM from other Engineering Boards Group.

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)					
PCC601	Blockchain Technology	20	20	40	60	2	--	--	100
PCC602	Ethical hacking and penetration testing	20	20	40	60	2	--	--	100
PEC601	PEC-1	20	20	40	60	2	--	--	100
PEC602	PEC-2	20	20	40	60	2	--	--	100
MDC601	multi-disciplinary minor	20	20	40	60	2	--	--	100
AEC601	Professional Skill	--	--	--	--	--	25	--	25
PCL601	Blockchain Technology Lab	--	--	--	--	--	25	25	50
PCL602	Ethical hacking and penetration testing Lab	--	--	--	--	--	25	25	50
2346411	Innovation Lab (Mini Project)	--	--	--		--	50	--	50
PEL601	PEL-1	--	--	--	--	--	25	25	50
PEL602	PEL-2	--	--	--	--	--	25	25	50
MDL601	multi-disciplinary minor	--	--	--	--	--	25	--	25
Total		**100**	**100**	**200**	**300**	**10**	**200**	**100**	**800**

Course Code	Course Description
PEC6011	AI in cyber threat intelligence management
PEC6012	Mobile and Wireless Security
PEC6013	Cyber Security and laws
PEC6014	Cloud and Web security
PEC6021	IoT Gateways and Middleware
PEC6022	Data Privacy and Protection Techniques
PEC6023	Information Security Management Systems (ISMS)
PEC6024	Web Application Security

Course Code	Lab Description
PEL6011	AI in cyber threat intelligence management Lab
PEL6012	Mobile and Wireless Security Lab
PEL6013	Cyber Security and laws Lab
PEL6014	Cloud and Web security Lab
PEL6021	IoT Gateways and Middleware Lab
PEL6022	Data Privacy and Protection Techniques Lab
PEL6023	Information Security Management Systems (ISMS)Lab
PEL6024	Web Application Security Lab

Vertical – 1
Major

PCC501 Computer Networks

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PCC501	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					
PCC501	Computer Networks	20	20	40	60	02	---	---	100

Course Objective: Students will be able to learn:

Sr. No.	Course Objectives
1	Fundamentals of computer networking and communication models.
2	Functions of different layers of the TCP/IP and OSI models.
3	Data link layer protocols and medium access techniques.
4	Network layer addressing and routing mechanisms.
5	Transport layer protocols and Internet application protocols.
6	Basics of IoT communication technologies and networking requirements.

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 fundamental concepts of computer networks and layered architecture.	L2
CO2	Analyze data link layer protocols and wireless communication technologies.	L4
CO3	Apply IP addressing and routing concepts in network communication.	L3
CO4	Explain transport layer protocols and Internet application protocols.	L2
CO5	Analyze network performance issues and congestion control mechanisms.	L4
CO6	Explain IoT communication technologies and networking challenges.	L2

Detailed Syllabus:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mappings
0	Prerequisite	Basics of computer systems, digital communication fundamentals, introduction to Internet technologies.	2	–
1	Introduction to Computer Networks	Data communication concepts, network components, types of networks (LAN, WAN, MAN), network topologies, network models: OSI model and TCP/IP model, protocol layering, network performance metrics (latency, throughput, bandwidth). **Self Study Topics** Software Defined Networking (SDN) ,Network Virtualization (NFV) ,Edge Computing and Fog Networking ,5G Network Architecture and Applications	6	CO1
2	Data Link Layer	Framing techniques, error detection and correction (Parity, CRC, Hamming Code), flow control mechanisms, ARQ protocols (Stop-and-Wait, Go-back-N, Selective Repeat), Medium Access Control protocols, Ethernet (IEEE 802.3), Wireless LAN basics (IEEE 802.11). **Self Study Topics** Forward Error Correction (FEC) techniques (Reed-	8	CO2

		Solomon, LDPC) Sliding Window protocol performance analysis Hidden and Exposed Terminal problems in wireless networks		
3	Network Layer	IPv4 addressing, subnetting, IPv6 addressing, packet forwarding, routing concepts, routing algorithms (Distance Vector and Link State), routing protocols overview (RIP, OSPF), introduction to NAT. **Self Study Topics** CIDR (Classless Inter-Domain Routing) and route aggregation BGP (Border Gateway Protocol) basics IPv6 transition mechanisms (Dual Stack, Tunneling) Software Defined Routing and Segment Routing	8	CO3
4	Transport Layer	Transport layer services, UDP and TCP protocols, TCP segment structure, three-way handshake, flow control, congestion control mechanisms, reliability mechanisms. **Self Study Topics** QUIC protocol and HTTP/3 TCP performance tuning and optimization Advanced congestion control algorithms (e.g., BBR) Multipath TCP (MPTCP)	6	CO4, CO5
5	Application Layer Protocols	DNS, HTTP/HTTPS, FTP, SMTP, DHCP, network socket concepts, client-server communication model. **Self Study Topics** Content Delivery Networks (CDN) and edge caching HTTP/2 and HTTP/3 optimizations DNS security extensions (DNSSEC) Microservices communication and REST vs gRPC	5	CO4
6	Networking for IoT (Overview)	Communication requirements for IoT devices, low power networks, IPv6 in IoT, 6LoWPAN concept, overview of IoT communication protocols (MQTT, CoAP), wireless technologies used in IoT (BLE, Zigbee, LoRa). **Self Study Topics** Edge AI in IoT communication systems LPWAN optimization techniques (NB-IoT, Sigfox) Security challenges in IoT communication (lightweight cryptography) Digital Twin communication architecture in IoT	3	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 and Reference Books:

Textbooks:	
1	Behrouz A. Forouzan – Data Communications and Networking, McGraw Hill.
2	Andrew S. Tanenbaum – Computer Networks, Pearson.
3	Kurose & Ross – Computer Networking: A Top-Down Approach.
Reference Books:	
1	William Stallings – Data and Computer Communications.
2	David Hanes – IoT Fundamentals: Networking Technologies.
3	Olivier Hersent – The Internet of Things: Key Applications and Protocols.
Access to software and virtual labs:	

1	Implementation of Different Network Topologies https://cn-iitr.vlabs.ac.in/exp/network-topologies/
2	Implementation of Packet Switching: Setup, Transmission, and Teardown. https://cn-iitr.vlabs.ac.in/exp/packet-switching/
3	Programming Fundamentals : Command Line Interface & Operating System Commands https://infyspringboard.onwingspan.com/web/en/viewer/html/lex_auth_013501574075670528103 89

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

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

End Semester Theory Examination:

- Question paper format
  - Question Paper will comprise a total **of six questions each carrying 20 marks**
  - **Q.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 Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
  - A total of **Three questions** need to be answered.

PCC502 IoT Architecture and Protocols

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PCC502	IoT Architecture and Protocols	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					
PCC502	IoT Architecture and Protocols	20	20	40	60	02	---	---	100

Course Objectives:

The course aims to

- To understand IoT Characteristics and Conceptual Framework.
- To comprehend network architecture and design of IoT
- To understand smart objects in IoT.
- To correlate the connection of smart objects and IoT access technologies while exploring network and application layer protocols for IoT.
- To explore the IoT security aspect.
- To study the design of IoT applications using standard methodologies and appropriate tools in order to develop efficient and reliable IoT solutions.

Course Outcomes:
Students will able to

1. Describe the IoT Characteristics and Conceptual Framework.
2. Differentiate between the levels of the IoT architectures.
3. Interpret sensor network and its components.
4. Examine IoT access technologies and network-layer and application-layer protocols for efficient communication in IoT applications.
5. Analyze security issues in IoT and risk analysis structure.
6. Study design of IoT applications using standard methodologies and appropriate tools to develop efficient and reliable IoT solutions.

DETAILED SYLLABUS:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Programming of controller , How to use IDE to write code of microcontroller, TCP-IP protocol stack		
I	Introduction to IoT	1.1 Introduction to IoT- Defining IoT, Characteristics of IoT, Conceptual Framework of IoT, Physical design of IoT, Logical design of IoT, Functional blocks of IoT, Communication models & APIs, Basics of networking Communication protocol, wireless sensor networks. 1.2 Convergence of IT and OT , IoT Challenges, IoT protocol vs Web Protocol stack	4	CO1

		Self-learning Topics: Hardware and software development tools for - Arduino, NodeMCU, ESP32, Raspberry Pi pico		
II	IoT Network Architecture and Design	2.1 **Drivers Behind New Network Architectures :** Scale,Security,Constrained Devices and Networks ,Data,Legacy Device Support 2.2 **Architecture :** The IoT World Forum (IoTWF) Standardized Architecture :Layer 1-7, IT and OT Responsibilities in the IoT Reference Model,Additional IoT Reference Models, A Simplified IoT Architecture, The Core IoT Functional Stack ::Layer 1-3 , Analytics Versus Control Applications , Data Versus Network Analytics Data Analytics Versus Business Benefits , Smart Services, 2.3 **IoT Data Management and Compute Stack :**Fog Computing , Edge Computing ,The Hierarchy of Edge, Fog, and Cloud Case study on distribution of computing requirements across the edge, fog and cloud.	07	CO2
III	Smart Objects IoT	3.1 **Sensors, Actuators, and Smart Objects**: Different types of Sensors. Basic sensors and it's specifications - DHT 11, Ultrasonic, PIR, IR. Different types actuators. Basic actuators and it's specifications - Relay , motors, Solenoid. 3.2 **Micro-Electro-Mechanical Systems (MEMS)** Smart Objects: A Definition , Trends in Smart Objects, (Examples: Smartwatch, Smart Fans, Smart traffic lights, Smart speakers, Smart Mobile, Robot) 3.3 Sensor Networks , Wireless Sensor Networks (WSNs) , Communication Protocols for WSN, RFID ,NFC, **Self-learning Topics:** RFID in Libraries	5	CO3
IV	IoT Network Layer and Application protocols	4.1 **Communications Criteria**: Range , Frequency Bands , Power Consumption , Topology , Constrained Devices , Constrained-Node Networks , Data Rate and Throughput , Latency and Determinism , Overhead and Payload 4.2 **IoT Access Technologies** : Standardization and Alliances , Physical Layer , MAC Layer , Topology ,Security and Conclusion of IEEE 802.15.4, LoRaWAN, NB-IoT, LTE Cat 0, LTE-M, 4.3 The Business Case for IP , The Key Advantages of Internet Protocol ,Adoption or Adaptation of the Internet Protocol ,The Need for Optimization ,Constrained Nodes , Constrained Networks IP Versions , Optimizing IP for IoT , From 6LoWPAN to 6Lo, Header Compression, Fragmentation , Mesh Addressing ,Mesh-Under Versus Mesh-Over Routing , 6Lo Working Group , RPL , Objective Function Rank, RPL Headers ,Metrics , Authentication and Encryption on Constrained Nodes ,	10	CO4

		4.4 **IoT Application Layer Protocols**:- CoAP, MQTT, AMQP, SOAP, Time Synchronized Mesh Protocol (TSMP) and HART protocol. **Self-learning Topics:** case studies		
V	Securing IoT	5.1 **A Brief History of OT Security Common Challenges in OT Security :** Erosion of Network Architecture,Pervasive Legacy Systems,Insecure Operational Protocols like Modbus, DNP3 ,ICCP ,OPC , (IEC) Protocols, Device Insecurity 5.2 **Security Knowledge:** IT and OT Security Practices and Systems Vary, The Purdue Model for Control Hierarchy, OT Network Characteristics Impacting Security, Security Priorities: CIA, Security Focus 5.3 **Formal Risk Analysis Structures:** OCTAVE and FAIR, FAIRThe Phased Application of Security in an Operational Environment Secured Network, Infrastructure and Assets, Deploying Dedicated Security Appliances,	8	CO5
VI	IOT application design using standard methodology	Cover various application domains under this: follow design methodologies steps 1. Purpose & Requirements Definition 2. Process Specification 3. Domain Model Specification 4. Information Model Specification 5. Service Specification 6. IoT Level Specification 7. Functional View Specification 8. Operational View Specification 9. Device & Component Integration 10. Application Development 11. Security & Privacy Implementation Few Applications are mentioned here (not limited to): 1. Smart Homes & Building Automation 2. Healthcare & Remote Patient Monitoring 3. Industrial IoT (IIoT) & Manufacturing 4. Agriculture & Precision Farming 5. Environmental Monitoring & Disaster Management 6. Energy Management & Smart Grids	4	CO6

Text Books:

1. Arsheep Bahga (Author), Vijay Madisetti, Internet Of Things: A Hands-On Approach Paperback, Universities Press, Reprint 2020
2. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry, IoT Fundamentals Networking Technologies, Protocols, and Use Cases for the Internet of Things CISCO.

References:

1. Pethuru Raj, Anupama C. Raman, The Internet of Things: Enabling Technologies, Platforms, and Use Cases by , CRC Press.
2. Raj Kamal, Internet of Things, Architecture and Design Principles, McGraw Hill Education, Reprint 2018.
3. Perry Lea, Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security, Packt Publications, Reprint 2018.
4. Amita Kapoor, "Hands on Artificial intelligence for IoT", 1st Edition, Packt Publishing, 2019.
5. Sheng-Lung Peng, Souvik Pal, Lianfen Huang Editors: Principles of Internet of Things (IoT)Ecosystem:Insight Paradigm, Springer

Online References:

Sr. No.	Website Name
1	https://owasp.org/www-project-internet-of-things/
2	NPTEL: Sudip Misra, IIT Khargpur, Introduction to IoT: Part-1, https://nptel.ac.in/courses/106/105/106105166/
3	NPTEL: Prof. Prabhakar, IISc Bangalore, Design for Internet of Things, https://onlinecourses.nptel.ac.in/noc21_ee85/preview

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

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

End Semester Theory Examination:

- Question paper format
  - Question Paper will comprise a total **of six questions each carrying 20 marks**
  - **Q.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 Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
  - A total of **Three questions** need to be answered.

PCC503 Network Security and Cryptography

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PCC503	Network Security and Cryptography	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					
PCC503	Network Security and Cryptography	20	20	40	60	02	---	---	100

Course Objectives: Students will be able to learn.

The course aims to

1. To understand the basic concepts of computer and Network Security.
2. To understand various cryptographic algorithms including secret key management and different authentication techniques.
3. To understand different types of malicious software and its effect on security.
4. To describe various secure communication standards including IPsec, SSL/TLS and Email.
5. To study Network Management Security and Network Access Control Techniques in Computer Security.
6. To discuss the concepts and use of IDS and Firewall systems in Security mechanisms.

Course Outcomes: Students will be able to achieve the outcome.

1. Explain the fundamentals of concepts of computer security and network security.
2. Apply classical and block cipher techniques to perform encryption and decryption of data.
3. Understand different types of malicious software and their impact on system security.
4. Describe the security mechanisms at Network, Transport, and Application layers.
5. Apply network management security principles and configure basic Network Access Control (NAC) mechanisms.
6. Understand and compare the working of IDS and Firewall in real-world scenarios.

DETAILED SYLLABUS:

Prerequisite: Basic concepts of Discrete Mathematics, Operating System, Computer Networks.

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	**Prerequisite**	Basic concepts of Discrete Mathematics, Operating System, Computer Networks.	01	
I	Introduction to Network Security & Cryptography	1.1 Fundamentals of Security ➢ Computer Security & Network Security – Definitions ➢ CIA Triad (Confidentiality, Integrity, Availability) ➢ Security Services & Mechanisms ➢ Security Attacks (Passive & Active) ➢ OSI Security Architecture ➢ Network Security Model 1.2 Classical Cryptography ● Monoalphabetic & Polyalphabetic Ciphers ● Substitution Techniques: o Vigenère Cipher o Playfair Cipher ● Transposition Techniques: o Keyed Transposition o Keyless Transposition 1.3 Introduction to Steganography **Self-Learning:** ● Additional Classical Encryption Techniques ● Homomorphic Encryption in Cloud Computing	06	CO1
II	Modern Cryptography, Key Management & Authentication	2.1 Symmetric Key Cryptography 1. Block Cipher Principles 2. Modes of Operation (ECB, CBC, CTR) 3. Data Encryption Standard (DES) 4. Advanced Encryption Standard (AES) 5. RC5 Algorithm 2.2 Public Key Cryptography 1. RSA Algorithm 2. Diffie–Hellman Key Exchange 3. ElGamal Cryptosystem 4. Elliptic Curve Cryptography (ECC) 2.3 Cryptographic Hash Functions **1** SHA-256 **2** SHA-512 **3** HMAC **4** CMAC 2.4 Digital Signatures & Authentication 1 RSA Digital Signature 2 Digital Signature Standard (DSS) 3 Remote User Authentication Protocols 4 Kerberos 2.5 Public Key Infrastructure 1. X.509 Certificates 2. Public Key Infrastructure (PKI) **Self-Learning:** ECDSA and advantages over RSA	10	CO2
III	Malicious Software and Emerging Threats	3.1 Malware & Threat Landscape 1. SPAM 2. Trojan Horse 3. Viruses & Worms	04	CO3

		4. Trapdoor & Backdoors 5. Rootkits 6. Keyloggers 7. Phishing 8. Attack Agents 9. Information Theft 10. System Corruption 11. Denial of Service (DoS) 12. Zombie Systems **Self-Learning:** 1 Recent Malware Case Studies 2 Impact of Quantum Computing on Current Security Algorithms		
IV	Network & Transport Layer Security Protocols	4.1 IP Layer Security 1 Introduction to IPsec 2 IPsec Architecture 3 Authentication Header (AH) 4 Encapsulating Security Payload (ESP) 4.2 Transport Layer Security 1. VPN – Need & Architecture 2. SSL Architecture 3. Transport Layer Security (TLS) 4. HTTPS 5. Secure Shell (SSH) Protocol Stack 4.3 Email Security 1. Secure Email – S/MIME 2. PGP **Self-Learning:** ● Gmail Security & Privacy Mechanisms	07	CO4
V	Network Management Security & Access Control	5.1 Network Management Security 1. SNMP Overview 2. SNMP Versions (v1, v2c, v3) 3. SNMPv3 Security Features 4. Remote Monitoring (RMON) 5.2 Network Access Control (NAC) ● Principles of NAC ● NAC Enforcement Methods ● Implementation of NAC Solutions ● NAC Use Cases **Self-Learning:** Open-source Network Management Security Tools	07	CO5
VI	System Security & Defensive Mechanisms	6.1 Intrusion Detection Systems (IDS) ● Types of IDS ● Signature-based & Anomaly-based Detection 6.2 Firewall Technologies ● Firewall Design Principles ● Characteristics of Firewalls ● Types of Firewalls (Packet Filtering, Stateful, Proxy, NGFW) **Self-Learning:** 1. Firewall Rule Tables & Practical Configurations	04	CO6

Text Books:

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, “”, Cengage Learning.

References:

1 Bruce Schneier, "Applied Cryptography, Protocols Algorithms and Source Code in C", Second Edition, Wiley.

2 Atul Kahate, "Cryptography and Network Security", Tata McGraw-Hill Education, 2003

3 www.rsa.com

Online Resources

Sr. No	Website Name
1	NIST Computer Security Resource Center (CSRC) - cryptographic standards and guidelines. https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines
2	IETF RFC Repository - security protocol standards (TLS, IPsec, SSH, DNSSEC). https://www.rfc-editor.org/
3	OWASP Foundation - web security best practices and Top 10. https://owasp.org/www-project-top-ten/
4	OpenSSL Documentation - tools for TLS and crypto operations.
5	Krebs on Security:- Provides real-world cybersecurity news, malware analysis, and case studies of cyber attacks. https://krebsonsecurity.com
6	https://nptel.ac.in/courses/106105162

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

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

End Semester Theory Examination:

➢ **Question paper format**

- Question Paper will comprise a total **of six questions each carrying 20 marks**
- **Q.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 Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
- A total of **Three questions** need to be answered.

PEC5011 AI for IoT

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEC5011	AI for IoT	3	--	-	3	-	-	3

Course Code	Course Name	Theory					Term work	Pract / Oral	Total
		Internal Assessment (IAT)			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT- II (Total)					
PEC5011	AI for IoT	20	20	40	60	2	--	--	100

Course Objectives:

The course aims to
1. Understand the fundamentals of IoT architectures and AI techniques used in intelligent systems.
2. Learn data acquisition, preprocessing, and analytics for IoT environments.
3. Apply machine learning and deep learning models on IoT-generated data.
4. Design intelligent, real-time, and scalable AI-enabled IoT applications.
5. Understand edge, fog, and cloud intelligence for IoT.
6. Address security, privacy, and ethical challenges in AI-powered IoT systems.

Course Outcomes:
Students will able to

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Explain IoT architectures and the role of AI in intelligent IoT systems.	L2
2	Pre-process and analyze IoT-generated data for intelligent decision-making.	L4
3	Apply machine learning algorithms to solve IoT-based problems.	L3
4	Design deep learning models for perception and prediction in IoT applications.	L5
5	Deploy AI models in edge, fog, and cloud-based IoT environments.	L5
6	Evaluate security, privacy, and ethical issues in AI-powered IoT systems.	L6

DETAILED SYLLABUS:

Prerequisite: Basic concepts of Python and data structures and computer Networks

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Basic programming proficiency (Python); Fundamentals of data structures and algorithms; Introductory knowledge of probability, statistics, and computer networks	**02**	-
I	Fundamentals of IoT and AI Integration	Introduction to IoT: Definition, Characteristics, and Applications; IoT Architecture: Device, Gateway, Network, Cloud layers; Sensors, Actuators, and Embedded Platforms (Arduino, Raspberry Pi - overview); Communication Protocols: MQTT, CoAP, HTTP, AMQP Introduction to Artificial Intelligence and Machine Learning; Role of AI in IoT (AIoT): Motivation and Use Cases; Data lifecycle in IoT systems **Self-Learning Topic**: Survey of real-world AIoT applications (Smart Home, Smart Grid, Smart Health); Study of popular IoT platforms (AWS IoT, Azure IoT, Google IoT)	**06**	CO1
II	Data Management and Analytics for IoT	IoT Data Characteristics: Volume, Velocity, Variety, Veracity; Data Acquisition from IoT Devices; Study IoT data formats and standards (JSON, SenML); Handling missing and noisy sensor data; Data Cleaning, Filtering, and Normalization; Time-Series Data Analytics; Feature Extraction and Feature Selection for Sensor Data; Streaming Data Analytics; Introduction to Big Data Platforms for IoT (Hadoop, Spark - overview) **Self-Learning Topic**: Introduction to edge analytics vs cloud analytics; Open datasets for IoT and sensor analytics	**07**	CO2
III	Machine Learning for IoT Applications	Supervised Learning Algorithms (Linear Regression, Decision Trees, SVM); Unsupervised Learning Algorithms (Clustering, PCA); Classification and Regression for Sensor Data; Anomaly and Fault Detection in IoT Systems; Model Training, Testing, and Evaluation Metrics; Lightweight ML Models for Resource-Constrained Devices; Case Studies: Smart Home, Smart Agriculture, Healthcare IoT **Self-Learning Topic**: Study comparison of ML algorithms for IoT use cases; Hyperparameter tuning for sensor data models; AutoML concepts for IoT analytics; Case study analysis of anomaly detection system	**08**	CO3
IV	Deep Learning and Intelligent Perception in IoT	Introduction to Deep Learning; Neural Networks and Backpropagation; CNNs for Image-based IoT Applications (Surveillance, Traffic); RNNs and LSTM for Time-Series IoT Data; Transfer Learning for IoT Applications; Edge AI and TinyML Concepts; Tools and Frameworks: TensorFlow Lite, PyTorch (overview) **Self-Learning Topic**: Study TinyML use cases and real-world deployments; Energy-efficient deep learning models; Vision-based IoT applications using CNNs	**07**	CO4
V	Edge, Fog, and Cloud Intelligence for IoT	Cloud Computing for IoT Analytics; Edge and Fog Computing Concepts; AI Model Deployment at Edge vs Cloud; Latency, Bandwidth, and Energy Considerations; Distributed Intelligence in IoT Systems; Real-Time Decision Making; Case Studies: Smart Cities, Industrial IoT	**6**	CO5

		Self-Learning Topic: Study comparison of edge, fog, and cloud architectures; Model compression and quantization techniques; Serverless computing for IoT analytics; AI orchestration and pipeline management		
VI	Security, Privacy, and Emerging Trends in AIoT	IDS, Security Threats in IoT Systems; AI-based Intrusion and Attack Detection; Privacy-Preserving Machine Learning; Ethical Issues in AI-enabled IoT; Explainable AI (XAI) for IoT Applications; Sustainable and Green AIoT; Emerging Trends: Autonomous IoT, Generative AI for IoT **Self-Learning Topic**: Study federated learning for IoT systems; Blockchain integration with IoT; Trust management in AIoT; Regulatory frameworks for IoT and AI	**03**	CO6

Text Books

1. Mayur Ramgir, Internet of Things- Architecture, Implementation, and Security, Pearson Education, 2019.
2. Raj Kamal, Internet of Things – Architecture and Design Principles, 2nd Edition, McGraw Hill, 2022.
3. Shalli Rani, R. Maheswar, G. R. Kanagachidambaresan, Sachin Ahuja, Deepali Gupta, Machine Learning Paradigm for Internet of Things Applications, Wiley, 2022
4. Stuart Russell & Peter Norvig, Artificial Intelligence: A Modern Approach, Prentice Hall / Pearson, 2009.
5. Tom M. Mitchell, Machine Learning, McGraw-Hill, 2017.

References:

1. Ian Goodfellow, Yoshua Bengio, Aaron Courville, Deep Learning, MIT Press, 2016.
2. Mohammad G. Khosrow-Pour (Ed.), Artificial Intelligence Applications for Smart Cities and IoT, IGI Global, 2021.
3. Shancang Li, Li Da Xu, Securing the Internet of Things, Syngress, Elsevier, 2017.
4. Pethuru Raj, Anupama C. Raman, The Internet of Things: Enabling Technologies, Platforms, and Use Cases, CRC Press, 2017.
5. Daniel Situnayake, Jenny Plunkett, AI at the Edge, O'Reilly Media, 2021.
6. David Minoli, Edge Computing: A Primer, Wiley, 2019.

Online Resources

Sr. No.	Website Name
1	NPTEL: Introduction to Internet of Things – IIT Kharagpur / IIT Madras
2	NPTEL: Machine Learning – IIT Madras
3	Coursera / edX courses on AI, ML, and IoT (for self-learning and MOOC credits)
4	**Google Machine Learning – Data Preparation:** https://developers.google.com/machine-learning/data-prep **UCI Machine Learning Repository (sensor datasets):** https://archive.ics.uci.edu **Apache Spark documentation:** https://spark.apache.org/docs/latest/ **Time-series analysis (Towards Data Science):** https://towardsdatascience.com/tagged/time-series
5	https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

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

End Semester Theory Examination:

- Question paper format
  - Question Paper will comprise a total **of six questions each carrying 20 marks**
  - **Q.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 Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
  - A total of **Three questions** need to be answered.

PEC5012 IoT Applications in Smart Infrastructure

Course Code	Course Name IAT	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEC5012	IoT Applications in Smart Infrastructure	3	--	-	3	-	-	3

Course Code	Course Name	Theory					Term work	Pract / Oral	Total
		Internal Assessment (IAT)			End Sem Exam	Exam Duration (in Hrs)			
		-I	IAT - II	IAT-I + IAT-II (Total)					
PEC5012	IoT Applications in Smart Infrastructure	20	20	40	60	2	--	--	100

Course Objectives:

The course aims to

1. Understand IoT architecture, system design workflow, and its integration in smart infrastructure systems. –
2. Analyze IoT communication protocols, embedded platforms, and edgefog–cloud computing models used in smart infrastructure environments.
3. Understand cybersecurity principles, IoT threat landscape, and security-by-design approaches for protecting smart infrastructure systems.
4. Study IoT applications in smart cities, smart buildings, healthcare systems, smart grids, and intelligent transportation systems.
5. Examine IoT-enabled energy management, renewable integration, and predictive maintenance in smart grid infrastructure.
6. Analyse performance, scalability, sustainability, and ethical considerations in IoT-based smart infrastructure deployments.

Course Outcomes:

Students will able to

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Summarize IoT layered architecture, system design workflow, and edge–fog–cloud integration in smart infrastructure	L2
2	Analyze IoT communication technologies, protocols, and embedded platforms suitable for real-world infrastructure applications	L4
3	Identify IoT security threats and implement authentication, encryption, key management, and access control mechanisms.	L3
4	Evaluate IoT applications in smart cities, smart buildings, healthcare, and intelligent transportation systems.	L5
5	Analyze IoT-enabled smart grid architecture, energy monitoring, renewable integration, and predictive maintenance techniques.	L4

6	Apply IoT technologies to build an end-to-end solution for smart infrastructure applications with consideration for performance, scalability, and security.	L3

DETAILED SYLLABUS:

Prerequisite: IoT Architecture and Protocols

Sr. No.	Name of Module	Detailed Content	Hours	CO Mapping
I	Introduction to Smart Infrastructure	1.1 Introduction to concept of Smart infrastructure, IoT layered architecture (Middleware, Design) 1.2 IoT system Design workflow 1.3 Edge, Fog, and Cloud computing for smart infrastructure: introduction, features, need , application & challenges, Edge-to-cloud integration **Self Learning:** edge orchestration platforms,real-time streaming analytics & hybrid cloud deployment.	06	CO1, CO2
II	Security for IoT Systems Infrastructure	2.1 Threat landscape:threats, types of attackers, vulnerabilities, and risks. 2.2 Security-by-Design in IoT: Integrating security measures from the initial design phase of devices, networks, and applications. 2.3 IoT specific attacks, Security requirements for smart infrastructure 2.4 Authentication, authorization, Key management challenges in constraint devices , Secure data transmission and device management 2.5 Introduction to Industrial IoT (IIoT) ,OT and IT security , challenges **Self Learning:** Phased Application Security in Operational Environment,	08	CO3
III	Structural Health Monitoring (SHM) & Smart Buildings	3.1 Smart Water Management: IoT-Enabled Water Network Monitoring for Leak Detection and pH Regulation 3.2 Solid Waste Management: IoT-Enabled Solid Waste Management Using Sensor and RFID Integration 3.3Urban Air Quality: Urban Air Quality Grid Modeling Using PM2.5, PM10, and NO_2 Measurements. 3.4 Hospital management:Intelligent Hospital Environmental and Asset Monitoring	06	CO4

		Self Learning: Security and Privacy in Smart Hospitals		
IV	IoT Applications in Smart Cities	4.1 Architecture of a smart city,IoT integration across urban services 4.2 Transport: Intelligent transportation systems 4.3 Smart city use cases: traffic, waste, environment monitoring 4.4 Data analytics and Introduction of digital twin and real-world deployments 4.5 5G in smart cities ,Autonomous buildings . **Self Learning:** AI-driven building management systems	06	CO4
V	Smart Grids and Energy Infrastructure	5.1 Overview of smart grid architecture, 5.2 IoT- enabled energy monitoring and demand response, 5.3 Renewable energy & its integration , 5.4 Energy sources with IoT, 5.5 Smart metering, fault detection, and predictive maintenance 5.6 Role of IoT with AI for analytics in energy management **Self Learning:** Vehicle-to-grid (V2G) systems	07	CO5
VI	Emerging Infrastructure Technologies	6.1Role of IoT in Construction Safety 6.2 Impact of High Wind Speeds on Crane Operations 6.3 Micro-Weather Analytics for Aviation and Drone Safety 6.4 Smart Sensor-Based Early Warning Systems for Floods and Earthquakes 6.5 Renewable Energy Forecasting for Smart Grid Energy Balancing **Self Learning:** Quantum-Safe Security Technologies , Robotics and Automation in Infrastructure	06	CO6

Text Books:

1. T1: "Introduction to IoT" – S. Misra, A. Mukherjee, A. Roy, Cambridge University Press.
2. T2: Industrial Internet of Things: Cybermanufacturing Systems"
3. T3: "Internet of Things: Principles and Paradigms",Rajkumar Buyya & Amir Vahid Dastjerdi

References:

1. **"Internet of Things: A Hands-on-Approach"**, Arshdeep Bahga & Vijay Madisetti.
2. **"Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations."**
3. **"IoT Fundamentals:Networking Technologies,Protocols, and Use Cases for the Internet of Things**",David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry

Online References:

Sr. No.	Website Name
1	Introduction to Industry 4.0 and Industrial Internet of Things:- https://onlinecourses.nptel.ac.in/noc26_cs38/preview
2	Smart Grid: Basics to Advanced Technologies **https://onlinecourses.nptel.ac.in/noc26_ee84/preview**
3	Smart Cities https://onlinecourses.nptel.ac.in/noc26_ce11/preview
4	IEEE Xplore / Google Scholar: Use for case studies and research papers on smart city IoT applications.

Assessment:

Internal Assessment Test (IAT) for 20 marks each:

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

End Semester Theory Examination:

- Question paper format
  - Question Paper will comprise a total **of six questions each carrying 20 marks**
  - **Q.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 Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
  - A total of **Three questions** need to be answered.

PEC5013 Wireless Sensor Networks with Secure Protocols

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEC5013	**Wireless Sensor Networks with Secure Protocols**	**3**	**--**	**-**	**3**	**-**	**-**	**3**

Course Code	Course Name	Theory					Term work	Pract/ Oral	Total
		Internal Assessment (IAT)			End Sem Exam	Exam Duration (in Hrs)			
		IAT-I	IAT-II	IAT-I + IAT-II (Total)					
PEC5013	**Wireless Sensor Networks with Secure Protocols**	**20**	**20**	**40**	**60**	**2**	**--**	**--**	**100**

Course Objectives:

1. To introduce the fundamental concepts, architecture, and components of Wireless Sensor Networks.
2. To study wireless communication technologies and MAC protocols used in resource-constrained sensor networks.
3. To analyze routing, data aggregation, and energy-efficient mechanisms for reliable WSN operation.
4. To understand security requirements, threats, and vulnerabilities specific to wireless sens networks.
5. To design and evaluate secure protocols for authentication, confidentiality, integrity, and key management in WSNs.
6. To explore emerging trends such as IoT-enabled WSNs, LPWAN technologies, edge intelligence, and blockchain-based ecurity solutions.

The course aims to

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Explain the fundamentals and architecture of wireless sensor networks.	L2
2	Analyze MAC and routing protocols for efficient WSN communication.	L4
3	Evaluate energy management and power-aware techniques in WSNs	L5
4	Identify security threats and vulnerabilities in wireless sensor networks.	L1
5	Design and analyze secure protocols for authentication, confidentiality, and data integrity.	L6
6	Apply emerging technologies and research trends in secure WSN applications.	L3

DETAILED SYLLABUS:

Prerequisite: Basic concepts of Computer Networks & Network Design, Operating System

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Basic knowledge of **Computer Networks**, **Wireless Communication**, and **Fundamentals of Cryptography**.	**02**	-
I	Introduction to Wireless Sensor Networks	Overview of Wireless Sensor Networks, Sensor node architecture: hardware and software components, Network architectures and deployment models, Applications of WSNs: environmental monitoring, healthcare, smart cities, industrial IoT, military systems, WSN standards and protocols: IEEE 802.15.4, ZigBee, 6LoWPAN, Challenges in WSN design: scalability, fault tolerance, energy constraints **Self-Learning Topic**: Recent case studies of WSN deployments in smart cities and healthcare, Comparison of WSN with MANET and IoT architectures	**06**	CO1
II	Wireless Communication and MAC Protocols	Wireless transmission technologies for WSNs, Radio propagation and energy models, MAC layer design issues in WSNs, Contention-based MAC protocols: S-MAC, T-MAC, B-MAC, TDMA-based and hybrid MAC protocols, IEEE 802.15.4 MAC operation, Performance comparison of MAC protocols **Self-Learning Topic**: IEEE 802.15.4 PHY layer operation, Performance comparison of contention-based and schedule-based MAC protocols	**06**	CO2
III	Routing, Data Aggregation, and Energy Management	Routing challenges in WSNs, Data-centric routing: Directed Diffusion, SPIN, Hierarchical routing: LEACH, PEGASIS, Location-based routing protocols, Data aggregation and data fusion techniques, Energy-efficient routing strategies, Power management and energy harvesting concepts **Self-Learning Topic**: Simulation study of energy-efficient routing protocols, Data aggregation techniques for reducing communication overhead	**07**	CO3
IV	Security Issues and Threats in WSNs	Security requirements in WSNs: confidentiality, integrity, authentication, availability, Constraints affecting security design in WSNs, Common attacks: Denial of Service (DoS), Sybil attack, Wormhole and sinkhole attacks, Node capture and replay attacks. Trust management and intrusion detection in WSNs, Security comparison with traditional wireless networks **Self-Learning Topic**: Case studies of real-world attacks on sensor networks, Comparative study of security challenges in WSNs and IoT networks	**06**	CO4
V	Secure Protocols and Key Management in WSNs	Cryptographic primitives for sensor networks, Symmetric vs asymmetric cryptography in WSNs, Key management schemes: Pre-distributed key schemes, Pairwise key establishment. Secure routing protocols, Authentication and secure data aggregation, Security protocol suites: SPINS (SNEP, μTESLA), Lightweight security protocols for IoT-	**7**	CO5

		based WSNs **Self-Learning Topic**: Study of SPINS (SNEP and µTESLA) security protocols, Lightweight cryptographic algorithms for resource-constrained devices		
VI	Emerging Trends and Advanced Applications of Secure WSNs	WSN integration with Internet of Things (IoT), LPWAN technologies: LoRaWAN, NB-IoT, Sigfox, Edge and fog computing for secure WSNs, Blockchain-based security frameworks for WSNs, AI/ML-assisted intrusion detection in sensor networks, Applications in smart grids, smart healthcare, and Industry 4.0, Open research challenges and future directions **Self-Learning Topic**: Blockchain-based security solutions for WSNs, AI/ML-based intrusion detection in wireless sensor networks	**04**	CO6

Text Books

1 Kazem Sohraby, Daniel Minoli, Taieb Znati, *Wireless Sensor Networks: Technology, Protocols, and Applications*, Wiley.

2 Holger Karl, Andreas Willig, *Protocols and Architectures for Wireless Sensor Networks*, Wiley.

3 Ian F. Akyildiz, Mehmet Can Vuran, *Wireless Sensor Networks*, Wiley.

4 C. Siva Ram Murthy, B. S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*, Pearson.

References:

- Feng Zhao, Leonidas Guibas, *Wireless Sensor Networks: An Information Processing Approach*, Elsevier.
- William Stallings, *Cryptography and Network Security*, Pearson.
- Vijay Madisetti, Arshdeep Bahga, *Internet of Things: A Hands-On Approach*, Universities Press.
- Carlos de Morais Cordeiro, Dharma Prakash Agrawal, *Ad Hoc and Sensor Networks*, World Scientific.
- Research papers on SPINS, µTESLA, blockchain-based WSN security (IEEE / Springer).

Online Resources

Sr. No.	Website Name
1	https://www.arduino.cc
2	https://www.iotforall.com
3	https://www.netacad.com
4	https://ocw.mit.edu/
5	https://onlinecourses.nptel.ac.in/noc26_cs51/preview

Assessment:

Internal Assessment Test (IAT) for 20 marks each: IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I and the remaining 40% to 50% of the syllabus content must be covered in the IAT-II.

End Semester Theory Examination:
Question paper format

- Question Paper will comprise a total **of six questions each carrying 20 marks**
- **Q.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 Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
- A total of **Three questions** need to be answered.

PEC5014 Internet Programming

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEC5014	Internet Programming	3	--	-	3	-	-	3

Course Code	Course Name	Theory							
		Internal Assessment (IAT)			End Sem Exam	Exam Duration (in Hrs)	Term work	Pract / Oral	Total
		IAT-I	IAT-II	IAT-I + IAT-II (Total)					
PEC5014	Internet Programming	20	20	40	60	2	--	--	100

Course Objectives:

The course aims:

1. To get familiar with the basics of Internet Programming.
2. To acquire knowledge and skills for creation of web site considering both client and server side programming.
3. To gain ability to develop responsive web applications and explore different web extensions and web services standards.
4. To learn characteristics of RIA and React Js.

Course Outcomes:

Students will able to

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Implement interactive web page(s) using HTML and CSS.	L3
2	Design a responsive web site using JavaScript and demonstrate database connectivity using JDBC.	L6
3	Demonstrate Rich Internet Application using Ajax and demonstrate and differentiate various Web Extensions.	L3
4	Demonstrate web application using Reactive Js.	L3

DETAILED SYLLABUS:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mapping
1	**Introduction to Web Technology**	**1.1 Web Essentials:** Clients, Servers, HTTP Request/Response, URL, DNS. Accessibility-first design (industry expectation). **1.2 HTML5:** Semantic Elements (header, footer, nav, section, article), WCAG accessibility basics (ARIA roles, semantic HTML), Forms & Input Attributes, Audio & Video tags, Canvas. **1.3 CSS3:** Selectors, Box Model, Modern CSS Practices: CSS Variables, Responsive units (rem, vw, clamp()), Flexbox & CSS Grid (Layouts), Media Queries (Responsive Design), Transitions, Transforms, and Animations. **1.4 Frameworks:** Introduction to Bootstrap (Grid system, Components), Utility-first concepts (Tailwind CSS – introductory mention).	10	CO1
2	**Front End Development**	**2.1 Modern JavaScript (ES6+):** let vs const, Arrow Functions, Template Literals, Destructuring, Spread/Rest operators. **2.2 DOM Manipulation:** Selecting elements (querySelector), Modifying HTML/CSS via JS, Event Listeners (Click, Submit, Input). **2.3 Core Concepts:** Array Methods (map, filter, reduce), Objects, JSON (Syntax, Parsing, Stringifying), Form Validation.	07	CO2
3	**Back End Development**	**Introduction to Traditional Server-Side Rendering (Overview of Servlet Architecture and JSP Basics).** **3.1 Modern Backend Awareness:** RESTful backend architecture (conceptual). JSON-based client–server communication. **3.2 Database Connectivity:** JDBC Architecture, Drivers, Establishing Connection, CRUD Operations using PreparedStatement. **3.3 Security Fundamentals:** Input validation & sanitization. Secure session management. Password hashing concepts.	07	CO2
4	**Rich Internet Application (RIA)**	**4.1 Asynchronous Programming:** Callbacks, Promises, Async / Await syntax. **4.2 AJAX & APIs:** Introduction to REST APIs, HTTP Verbs (GET, POST), Consuming APIs using the Fetch API (Modern replacement for XMLHttp), Error Handling. **4.3 Libraries:** Brief introduction to Axios (vs Fetch).	04	CO3

5	**Web Extension: PHP and XML**	**Introduction to XML (Tree structure, Tags) vs. JSON for data exchange.** **5.1 PHP Basics:** Introduction to PHP Syntax, Variables, Control Structures. **5.2 PHP Application:** Handling simple HTML Form Submissions using PHP (GET/POST). Overview of connecting PHP to a database	05	CO3
6	**React js**	**6.1 Introduction: SPA (Single Page Applications), Virtual DOM, JSX Syntax, Setup (Vite/CRA).** **6.2 Modern React Practices:** Component-driven UI design (Breaking down UIs into reusable pieces), Components: Functional Components, Props (passing data). **6.3 Hooks:** Managing State with useState, Lifting state up (Sharing state between sibling components), Controlled components (Managing form inputs with React state), Side Effects with useEffect, API Integration: Fetching data from REST APIs in React (Using useEffect and fetch/Axios), Managing Loading & error states (Ensuring good UX during asynchronous data fetches). **6.4 Routing:** Basic introduction to React Router (Navigating between views).	06	CO4

Text Books:

a. Ralph Moseley, M.T. Savliya, "Developing Web Applications", Wiley India, Second Edition, 2011
b. "Web Technologies Black Book", Kogent Learning Solutions Inc., Dreamtech Press, Second Edition, 2018
c. Robin Nixon, "Learning PHP, MySQL & JavaScript: A Step-by-Step Guide to Creating Dynamic Websites", O'Reilly Media, Seventh Edition, 2025
d. Nicholas C. Zakas, "Professional JavaScript for Web Developers", Wrox (Wiley), Fourth Edition, 2019
e. Alex Banks and Eve Porcello, "Learning React: Modern Patterns for Developing React Apps", O'Reilly Media, Second Edition, 2020

References:

- Harvey & Paul Deitel, "Internet and World Wide Web How To Program", Pearson Education, Fifth Edition, 2012
- Achyut S Godbole and Atul Kahate, "Web Technologies", Tata McGraw Hill, Third Edition, 2013
- Thomas A. Powell and Fritz Schneider, "JavaScript: The Complete Reference", McGraw Hill, Third Edition, 2012
- David Flanagan, "JavaScript: The Definitive Guide", O'Reilly Media, Seventh Edition, 2020
- Steven Holzner, "PHP: The Complete Reference", McGraw Hill, First Edition (Latest Reprint), 2008
- Mike McGrath, "PHP & MySQL in easy steps", In Easy Steps Limited, Second Edition, 2023

Online References:

Sr. No.	Website Name
1	https://react.dev
2	https://www.guru99.com/reactjs-tutorial.html
3	https://nptel.ac.in/courses (Official NPTEL Portal)
4	https://www.w3schools.com
5	https://spoken-tutorial.org
6	https://www.coursera.org

Assessment:

Internal Assessment Test (IAT) for 20 marks each: IA will consist of Two Compulsory Internal Assessment Tests. Approximately 40% to 50% of the syllabus content must be covered in the IAT-I and the remaining 40% to 50% of the syllabus content must be covered in the IAT-II.

End Semester Theory Examination:
Question paper format

- Question Paper will comprise a total **of six questions each carrying 20 marks**
- **Q.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 Q.2 has part (a) from Module 3 then part (b) must be from any other Module randomly selected from all the modules)
- A total of **Three questions** need to be answered.

PCL501 Computer Networks Lab

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PCL501	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					
PCL501	Computer Networks Lab	---	---	---	---	---	25	25	50

Lab Objectives: The course aims to

Sr. No.	Lab Objectives
1	To understand basic networking tools and packet analysis.
2	To implement socket programming for client-server communication.
3	To analyze network protocols and packet structures.
4	To study routing, addressing, and subnetting concepts through simulation.
5	To use network diagnostic tools for troubleshooting.
6	To understand IoT communication protocols and networking basics.

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
LO1	Use networking tools for packet analysis and troubleshooting.	L2, L3
LO2	Implement client-server communication using socket programming.	L3
LO3	Analyze packet structures of TCP/IP protocols.	L3, L4
LO4	Configure IP addressing and subnetting for network communication.	L3
LO5	Demonstrate routing and network simulation using networking tools.	L3
LO6	Demonstrate IoT communication protocols such as MQTT or CoAP.	L2, L3

Hardware & Software Requirements:

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

DETAILED SYLLABUS:

Sr. No	Module	Detailed Content (Experiments)	Hours	LO Mapping	Bloom's Level
1	Basics & Networking Tools	Installation of Wireshark, Packet Tracer, Python setup. Study networking commands: ping, traceroute, ipconfig/ifconfig, netstat.	4	LO1	L2, L3
2	Packet Analysis & Application Layer	Analyze TCP/IP packets using Wireshark. Study HTTP, FTP, DNS protocols using packet capture.	4	LO3	L3, L4
3	Transport Layer Programming	Implement TCP client-server communication using sockets. Implement UDP communication using sockets.	4	LO2	L3
4	Data Link Layer Protocols	Simulate Stop-and-Wait ARQ protocol. Simulate Go-Back-N protocol. Analyze performance differences.	4	LO3	L3, L4
5	Network Layer & Routing	Perform subnetting and IP addressing using Packet Tracer. Configure LAN using switches/routers. Implement static routing / RIP.	6	LO4, LO5	L3, L4
6	IoT Networking & Integration	Study MQTT/CoAP protocol (demo/simulation). Integrated experiment combining routing + socket + protocol analysis. Mini Project/Viva based on IoT networking use-case.	4	LO2–LO6	L3, L4, L5

Text Books:

1. Behrouz A. Forouzan – Data Communications and Networking, McGraw Hill.
2. Andrew S. Tanenbaum – Computer Networks, Pearson.
3. Kurose & Ross – Computer Networking: A Top Down Approach

References:

1. William Stallings – Data and Computer Communications.
2. David Hanes – IoT Fundamentals: Networking Technologies.
3. Olivier Hersent – Internet of Things: Key Applications and Protocols.

Online References:

Sr. No.	Website Name
1	**Computer Networks, IIT Madras** Prof. Hema A Murthy https://nptel.ac.in/courses/106106091
2	Introduction to IoT and Digital Transformation https://www.netacad.com/courses/introduction-iot?courseLang=en-US&utm_campaign=writ&utm_content=Introduction-to-iot-get-started-button&utm_source=cisco.com&utm_medium=referral
3	Networking Basics https://www.netacad.com/courses/networking-basics?courseLang=en-US

List of Experiments.

Sr. No.	Experiment List	Hours	LO Mappings
0	Lab Prerequisite: Installation of Wireshark, Packet Tracer, Python environment setup	2	–
1	Study basic networking commands: ping, traceroute, ipconfig/ifconfig, netstat	2	LO1
2	Study packet analysis using Wireshark and analyze TCP/IP packets	2	LO3
3	Implement client-server communication using TCP sockets	2	LO2
4	Implement client-server communication using UDP sockets	2	LO2
5	Write a program to simulate Stop-and-Wait ARQ protocol	2	LO3
6	Write a program to simulate Go-Back-N protocol	2	LO3
7	Perform subnetting and IP address configuration using Packet Tracer	2	LO4
8	Configure simple LAN network using switches and routers in Packet Tracer	2	LO5
9	Configure routing protocols (Static Routing / RIP) using Packet Tracer	2	LO5
10	Study application layer protocols: HTTP, FTP and DNS using packet capture	2	LO3

Assessment:

Term Work: Term Work shall consist of 8 practicals based on the above list and one miniproject (group of 3-4 students)

Internal Practical Exam: Conduct an internal practical exam after completing the first three modules of the course to assess and ensure the learner's understanding.

Term Work Marks: 25 Marks (Total marks) =10 Marks (Experiment) + 10 Marks (miniproject) + 5 Marks (Attendance)

Practical& Oral Exam: An Oral / Practical exam will be held based on the above Experiments & miniproject.

PCL502 IoT Architecture and Protocols Lab

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PCL502	IoT Architecture and Protocols Lab	-	2	-	-	1	-	1

		Theory					Term work	Pract / Oral	Total
		Internal Assessment			End Sem Exam	Exam Duration (in Hrs)			
		Test 1	Test 2	Avg.					
PCL502	IoT Architecture and Protocols Lab	---	---	---	---	---	25	25	50

Lab Objectives: Students will be able to learn.

1. To Understand the definition and significance of the Internet of Things.
2. To Discuss the architecture, operation, and business benefits of an IoT solution.
3. To Examine the potential business opportunities that IoT can uncover.
4. To Explore the relationship between IoT, cloud computing, and Data Analytics.
5. To Identify how IoT differs from traditional data collection systems.
6. To Explore the interconnection and integration of the physical world and be able to design & develop IOT applications.

Lab Outcomes: Students will be able to achieve the outcome.

1. Adapt different techniques for data acquisition using various IoT sensors for different applications. (LO1)
2. Demonstrate the working of actuators based on the collected data. (LO2)
3. Use different IoT simulators and correlate working of IoT protocols. (LO3)
4. Adapt different techniques for Integrating IoT services to other third-party Clouds. (LO4)
5. Execute data analysis and encryption methodologies for deployment of IoT applications. (LO5)
6. Implement IoT protocols for communication to realize the revolution of internet in mobile devices, cloud and sensor networks. (LO6)

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hrs	LO Mapping
0	**Prerequisite**	Experimentation with Microprocessor and Microcontroller , Experimentation with python and c s.	02	--
1	Arduino	Introduction to Arduino, Hardware requirements, Software requirements, Arduino Programming Language, Arduino Uno Wired & Wireless connectivity, LCD commands, Serial Communication commands. Program for blinking LED using Arduino. Traffic Light pattern using Arduino. ESP8266 WiFi Module	05	LO1
2	Raspberry Pi	Introduction to Raspberry Pi, Installation of NOOBS and Raspbian on SD card, Libraries on Raspberry Pi, getting static IP address of Raspberry Pi, Interfacing of Relay, DHT11, DC Motor and LCD with Raspberry Pi.	05	LO2
3	Contiki OS	Contiki OS : History of Contiki OS,Applications, Features, ,Communication Components in Contiki OS, Cooja simulator ,Running Cooja Simulator	05	LO3
4	Cooja Simulator	Using the Contiki OS with the Cooja simulator to program the IoT for broadcasting data from sensors	03	LO3
5	Protocols and Security with Cooja	Understanding of 6LowPAN , COAP and protocol implementation in Cooja . Encryption Decryption techniques for IoT .	03	LO4
6	IoT data to Cloud	Installing the Remote desktop server. Installation of Pi camera, Face recognition, serial peripheral interface using Raspberry Pi. . DHT11 data logger with ThingSpeak/ thingsboard/ AWS/ Azure server .	03	LO4

List of Experiments.

Week No	List of Experiments	Hrs
1	IoT study and implement interfacing of different IoT sensors with Raspberry Pi pico/Arduino/NodeMCU. Exploring the Arduino for DI/DO, AI/AO and PWM i. Blink LED ii Connecting LED externally -DO iii. Reading the voltage from the voltage divider circuit - AI iv. RGB LED Color Control using PWM	02
2	To study and implement interfacing of actuators based on the data collected using IoT sensors. (like led switch ON/OFF, stepper motor) Controlling a device remotely using Relay (as an actuator), Blynk/thingspeak/thingsboard and ESP8266	02
3	Write a program for ESP8266 DHT11/DHT22 Temperature and Humidity Web Server with Arduino IDE	02
4	WAP for interfacing ESP32/ESP8266 with Proximity sensor and analyze the data on serial plotter or web dashboard (Thingspeak/Blynk/AWS/Azure).	02
5	Write a program on Arduino / Raspberry Pi/ESP32 subscribe to MQTT broker for temperature data and print it	02
6	Write a program on Raspberry Pi to push and retrieve the data from cloud like thingspeak/thingsboard/AWS/ Azure etc	02
7	To study and implement IoT Data processing using Pandas.	02
8	Write a program to collect data from sensor encrypt data send it to receiver (server) and decrypt is at receiving end Ardino/Raspberry Pi/ Contiki OS (simulator)	02
9	To study and demonstrate Contiki OS for RPL (like Create 2 border router and 10 REST clients, Access border router from other network (Simulator)	02
10	To study and demonstrate working of 6LoWPAN in Contiki OS (simulator)	02
11	Write a program to create TCP Server on Arduino/Raspberry Pi and respond with humidity data to TCP client when Requested	02
12	Mini Project: based on one real life applications using minimum 2 /3 sensors and 1 actuators with cloud connectivity	02

Assessment:

Term Work: Term Work shall consist of 8 practicals based on the above list and one miniproject (group of 3-4 students)

Internal Practical Exam: Conduct an internal practical exam after completing the first three modules of the course to assess and ensure the learner's understanding.

Term Work Marks: 25 Marks (Total marks) =10 Marks (Experiment) + 10 Marks (miniproject) + 5 Marks (Attendance)

Practical& Oral Exam: An Oral / Practical exam will be held based on the above Experiments & miniproject.

PCL503L Network Security and Cryptography Lab

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PCL503	Network Security and Cryptography 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					
PCL503	Network Security and Cryptography Lab	---	---	---	---	---	25	25	50

Lab Objectives: Students will be able to learn.

2. To implement classical and modern cryptographic algorithms.
3. To study malicious software behavior using practical tools.
4. To configure network security mechanisms such as IDS, Firewall and NAC.
5. To analyze real-world security scenarios using packet analysis tools.

Lab Outcomes: Students will be able to achieve the outcome.

1 Apply classical cryptographic techniques to perform encryption and decryption, and critically assess their security effectiveness and limitations.

2 Design and implement symmetric and asymmetric cryptographic algorithms, and examine their security features and computational performance.

3 Create and validate cryptographic hash values, digital signatures, and digital certificates to ensure data integrity and authentication.

4 Investigate the behavior of various malware types and demonstrate common network security attacks within a controlled laboratory environment.

5 Configure and evaluate network security protocols including IPsec, SSL/TLS, SSH, and secure email mechanisms to ensure secure communication.

6 Implement and assess network management and defense mechanisms such as SNMPv3, Intrusion Detection Systems (IDS), Firewalls, and Network Access Control (NAC).

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hours	CO Mapping
0	Prerequisite	Basic concepts of Computer Networks & Network Design, Operating System.	01	
I	Introduction to Network Security & Cryptography	Implementation of classical encryption techniques: Caesar Cipher, Vigenère Cipher, Playfair Cipher, Transposition Cipher, Basic Steganography	02	LO1

II	Modern Cryptography, Key Management & Authentication	Implementation of: DES and AES (CBC/CTR Modes), RSA Encryption–Decryption, Diffie–Hellman Key Exchange, SHA-256 and HMAC, Digital Signature Generation & Verification.	02	LO2, LO3
III	Malicious Software and Emerging Threats	Malware behavior study (Trojan, Worm, Rootkit, Phishing), DoS attack simulation in controlled lab, Packet capture and traffic analysis.	02	LO4
IV	Network & Transport Layer Security Protocols	SSL/TLS Configuration, HTTPS traffic analysis using Wireshark, SSH key-based authentication, Basic IPsec configuration, Secure Email (S/MIME) demonstration.	02	LO5
V	Network Management Security & Access Control	SNMPv3 configuration and monitoring, Network Access Control (NAC) simulation, RMON monitoring.	02	LO6
VI	System Security & Defensive Mechanisms	Firewall configuration and rule design, IDS setup and alert monitoring, Security log analysis.	02	LO6

List of Experiments

Sr. No.	List of Experiments	Hrs	LO
01	Implementation and cryptanalysis of any one classical cryptographic technique.	02	LO1
02	Implementation and analysis of any one modern cryptographic algorithm or secure key exchange mechanism.	02	LO2
03	Implementation and evaluation of any one cryptographic hash function, digital signature, authentication protocol, or public key infrastructure (PKI) mechanism.	02	LO3
04	Implementation and analysis of any one malware detection or threat investigation technique in a controlled laboratory environment.	02	LO4
05	Implementation and demonstration of any one network-based security attack simulation and its traffic analysis using appropriate tools in a controlled environment.	02	LO5
06	Implementation and configuration of any one network management and monitoring protocol using appropriate tools.	02	LO5
07	Implementation and simulation of any one network access control (NAC) mechanism for enforcing security policies.	02	LO6
08	Installation, configuration, and analysis of any one Intrusion Detection System (IDS) for monitoring and detecting network threats.	02	LO6
09	Implementation and configuration of any one firewall mechanism for traffic filtering, rule design, and security log analysis.	02	LO5
10	Implementation of SNMPv3 for Network Management.	02	LO6
11	Generation of Message Digest using SHA-256 or SHA-512	02	LO3
12	Study of malicious software using different tools: a) Keylogger attack using a keylogger tool. b) Simulate DOS attack using any tools c) Use the NESSUS/ISO Kali Linux tool to scan the network for vulnerabilities	02	LO4

13	Performance port scanning on a target system using Network Scanning Tools.	02	LO6
14	Implementation of RSA Algorithm for Public Key Encryption/Decryption.	02	LO2
15	Implementation of Diffie-Hellman Key Exchange algorithm to securely share a secret key.	02	LO2

Text Books:

1 Build your own Security Lab, Michael Gregg, Wiley India.
2 CCNA Security, Study Guide, TIm Boyles, Sybex.
3 Hands-On Information Security Lab Manual, 4th edition, Andrew Green, Michael Whitman, Herbert Mattord.
4 The Network Security Test Lab: A Step-by-Step Guide Kindle Edition, Michael Gregg.

References:

1 Network Security Bible, Eric Cole, Wiley India.
2 Network Defense and Countermeasures, William (Chuck) Easttom.
3 Principles of Information Security + Hands-on Information Security Lab Manual, 4th Ed. , Michael E. Whitman , Herbert J. Mattord.

Online Resource:

1. http://cse29-iiith.vlabs.ac.in/
2. https://www.dcode.fr/en

Assessment:

Term Work: Term Work shall consist of 10 practicals based on the above list

Internal Practical Exam: Conduct an internal practical exam after completing the first three modules of the course to assess and ensure the learner's understanding.

Term Work Marks: 25 Marks (Total marks) =10 Marks (Experiment) + 10 Marks (mini project) + 5 Marks (Attendance)

Practical& Oral Exam: An Oral / Practical exam will be held based on the above Syllabus

PEL5011 AI for IoT Lab

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEL5011	AI for IoT Lab	-	2	-	-	1	-	1

Course Code	Course Name	Examination Scheme		Term Work	Practical/ Oral	Total
		Theory Marks				
PEL503L	AI for IoT Lab	--	--	25	25	50

Lab Objectives: Students will be able to.

1. Gain hands-on experience with IoT sensors, devices, and data acquisition.
2. Develop skills in data preprocessing, visualization, and feature engineering for IoT datasets.
3. Implement machine learning and deep learning models for IoT-based applications.
4. Apply edge and cloud-based AI deployment techniques for real-time IoT systems.
5. Understand and implement security, privacy, and ethical considerations in AIoT systems.
6. Encourage problem-solving, experimentation, and system-level thinking for real-world AIoT use cases.

Lab Outcomes: Students will be able to achieve the outcome.

1. Interface IoT sensors and devices, acquire real-time data, and perform basic data logging using microcontrollers and IoT platforms. (LO1)
2. Perform data preprocessing, visualization, and exploratory analysis on IoT datasets using Python-based tools. (LO2)
3. Design, implement, and evaluate machine learning models for prediction and classification in IoT applications. (LO3)
4. Develop deep learning models for image, signal, or time-series data generated from IoT systems. (LO4)
5. Deploy AI models on edge or cloud platforms and analyze performance in terms of latency, accuracy, and resource utilization. (LO5)
6. Implement secure and ethical AIoT solutions considering data privacy, security threats, and responsible AI practices. (LO6)

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hrs	LO Mapping
0	Prerequisite	Basic programming in Python; Fundamentals of data structures and algorithms; Introductory knowledge of probability, statistics, and computer networks	01	--
1	IoT and AI Integration	Implementation of IoT system architecture using sensors and cloud platform.	02	LO1
2	Data collection and Pre-processing of IoT data	Data Acquisition from IoT Devices; Data Cleaning, Filtering, and Normalization	02	LO2
3	Analytics for IoT	Time-Series Data Analytics; Feature Extraction and Feature Selection for Sensor Data;	02	LO2

		Streaming Data Analytics		
4	Machine Learning for IoT Applications	Generate Supervised Learning Algorithms (Linear Regression, Decision Trees, SVM); Unsupervised Learning Algorithms (Clustering, PCA); Classification and Regression for Sensor Data	02	LO3
5	Machine Learning for IoT Applications	Anomaly and Fault Detection in IoT Systems; Model Training, Testing, and Evaluation Metrics; Lightweight ML Models for Resource-Constrained Devices	02	LO3
6	Deep Learning and Intelligent Perception in IoT	Introduction to Deep Learning; Neural Networks and Backpropagation; CNNs for Image-based IoT Applications (Surveillance, Traffic); RNNs and LSTM for Time-Series IoT Data; Transfer Learning for IoT Applications; Edge AI and TinyML Concepts; Tools and Frameworks: TensorFlow Lite, PyTorch (overview).	02	LO4
7	Edge, Fog, and Cloud Intelligence for IoT	Cloud Computing for IoT Analytics; Edge and Fog Computing Concepts; AI Model Deployment at Edge vs Cloud; Latency, Bandwidth, and Energy Considerations; Distributed Intelligence in IoT Systems; Real-Time Decision Making	02	LO5
8	Smart applications	Smart application case study (Smart Agriculture / Smart Home / Healthcare IoT).	02	LO1, LO2, LO3, LO4, LO5
9	AI based Intrusion Detection Alerts	IDS, Security Threats in IoT Systems; AI-based Intrusion and Attack Detection; Privacy-Preserving Machine Learning; Ethical Issues in AI-enabled IoT; Explainable AI (XAI) for IoT Applications; Sustainable and Green AIoT; Emerging Trends: Autonomous IoT, Generative AI for Io	02	LO6

List of Experiments.

Week No	List of Experiments	Hrs
01	Study and implementation of IoT system architecture using sensors and cloud platform.	02
02	Data collection from IoT sensors and preprocessing using Python.	02
03	Time-series analysis and visualization of IoT sensor data.	02
04	Implementation of supervised ML algorithms for IoT data classification.	02
05	Anomaly detection in IoT sensor data using unsupervised learning.	02
06	Prediction of sensor values using regression and LSTM models.	02
07	Deployment of a lightweight ML model on edge devices (TinyML concept).	02
08	Smart application case study (Smart Agriculture / Smart Home / Healthcare IoT).	02
09	AI-based intrusion or anomaly detection in IoT networks.	02
10	Capstone Project	06

Assessment:

Term Work: Term Work shall consist of 8 practicals based on the above list.
Internal Practical Exam: Conduct an internal practical exam after completing the first three modules of the course to assess and ensure the learner's understanding.

Term Work Marks: 25 Marks (Total marks) = 10 Marks (Experiment) + 10 Marks (Internal Practical Exam) + 5 Marks (Attendance)
Practical & Oral Exam: An Oral & Practical exam will be held based on the above syllabus.

PEL5012 IoT applications in Smart infrastructure Lab

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEL5012	IoT applications in Smart infrastructure Lab	**-**	**2**	**-**	**-**	**1**	**-**	**1**

Course Code	Course Name	Examination Scheme						
		Theory Marks						
		ernal assessment (IAT)			End Sem. Exam	Term Work	Practical/ Oral	Total
		IAT- I	IAT-II	IAT-I + IAT-II (Total)				
PEL5012	IoT applications in Smart infrastructure Lab	--	--	--	--	25	25	50

Lab Objectives :

Students will be able to learn.

1. Provide hands-on experience in designing and simulating IoT systems using edge and fog computing tools.
2. Enable students to interface sensors and development boards for real-time data acquisition and cloud integration.
3. Develop practical understanding of IoT cybersecurity analysis using vulnerability assessment tools.
4. Implement IoT-based smart infrastructure applications such as waste management, air quality monitoring, traffic control, and smart grids.
5. Exhibit real-time data transmission, analytics, and visualization using IoT simulation and middleware platforms.
6. Demonstrate real-time data transmission, analytics, and visualization using IoT simulation and middleware platforms.

Lab Course Outcomes:

Students will be able to achieve the outcome.

LO1: Design and simulate IoT systems using edge/fog computing platforms such as iFogSim.
LO2: Interface sensors with development boards and implement cloud-based data transmission and visualization.
LO3: Perform security analysis of IoT devices using network scanning and vulnerability assessment tools.
LO4: Develop and simulate smart infrastructure applications including smart waste management, air quality monitoring, and healthcare systems.
LO5: Implement IoT-based smart energy monitoring and traffic management systems using suitable simulators/ sensors.
LO6: Demonstrate real-time IoT data acquisition and processing using simulation tools (eg:digital twin case studies).

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hrs	LO Mapping
0	**Prerequisite**	Experimentation with IoT Architecture and Protocols	-	--
1	Edge & Fog Computing for Smart Infrastructure	Edge Computing Architecture, iFogSim, Edge-Based Data Analytics,edge simulator Comparison of cloud-only vs edge-based architecture (latency, bandwidth).	04	LO1
2	Sensor Interfacing & Cloud Integration	IoT Sensor Interfacing, Serial Communication Basics, Serial peripheral Interface (SPI) Interfacing Basics, Cloud integration	02	LO2

3	IoT Security & Industrial IoT (IIoT)	IoT architecture & networking, Network Scanning and Enumeration, Open Port Analysis & Vulnerability Identification, OT vs IT Security in Industrial IoT	04	LO3
4	Smart Infrastructure Applications	IoT-Based Smart City Applications, Sensor-Based Fill-Level Detection , System Architecture & Concepts	04	LO4
5	Smart Energy & Traffic Systems	Fundamentals of Energy Monitoring, Smart Grid Architecture, IoT-based automatic street light control system, Traffic density detection.	06	LO5
6	Real-Time IoT & Digital Twin	Real-time data acquisition , Node-RED, MQTT-based real-time data transmission. simulation	04	LO6

List of Experiments.

Week No	List of Experiments	Hrs	
01	1a) Design and deploy an edge computing architecture using edge / fog simulators such as Edge and Fog Simulators /ifogsim	2	LO1
02	1b) Develop and evaluate edge-based data analytics algorithms in an edge simulator.	2	LO1
03	2a) Interfacing basic sensor to any development board ,gathering sensor value and pushing on to cloud (Thinkspeak/ AWS)	2	LO2
04	3a) Analysis of exposed network ports and evaluate potential security risks (security weaknesses) in IoT devices using Nmap or relevant tools.	2	LO3
05	3b) Study of industrial IoT(IIoT) with application of OT (operational technology) security.	2	LO3
06	4a) Application design of Healthcare in IoT using ifogsim	2	LO4
07	4b) Design / Simulation (Edge and Fog Simulators /ifogsim/ other) of an IoT-enabled smart waste bin system for real-time monitoring and automated alert generation based on fill-level detection	2	LO4
08	4c) Measure air quality index using sensors like MQ135 /MQ2	2	LO4
09	5a) Case Study / design an IoT-based automatic street light control system.	2	LO5
10	5b) Simulation IoT-based traffic density detection.	2	LO5
11	5c) Design of an IoT-based energy monitoring system.	2	LO5
12	5d) Case Study: Smart Grid Architecture with industry application	2	LO5
13	6a) Real time data acquisition and transmission using NodeRed simulator	2	LO6
14	6b) MQTT using HiveMQ Cloud and Ri-Pi	2	LO6
15	6c) Case study of digital Twin for aviation	2	LO6

Assessment:

Term Work: Term Work shall consist of minimum 8 Practicals which shall cover all Lab Course Outcomes and 2 Assignments based on the above list.

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

Practical/ oral Exam: An Oral exam will be held based on the above experiments.

PEL5012 IoT applications in Smart infrastructure Lab

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEL5012	IoT applications in Smart infrastructure Lab	-	2	-	-	1	-	1

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Practical/ Oral	Total
		Internal assessment (IAT)			End Sem. Exam			
		IAT- I	IAT-II	IAT-I + IAT-II (Total)				
PEL5012	IoT applications in Smart infrastructure Lab	--	--	--	--	25	25	50

Lab Objectives(Lobj): Students will be able to learn.

1. Provide hands-on experience in designing and simulating IoT systems using edge and fog computing tools.
2. Enable students to interface sensors and development boards for real-time data acquisition and cloud integration.
3. Develop practical understanding of IoT cybersecurity analysis using vulnerability assessment tools.
4. Implement IoT-based smart infrastructure applications such as waste management, air quality monitoring, traffic control, and smart grids.
5. Exhibit real-time data transmission, analytics, and visualization using IoT simulation and middleware platforms.
6. Demonstrate real-time data transmission, analytics, and visualization using IoT simulation and middleware platforms.

Lab Course Outcomes: Students will be able to achieve the outcome.

LO1: Design and simulate IoT systems using edge/fog computing platforms such as iFogSim.
LO2: Interface sensors with development boards and implement cloud-based data transmission and visualization.
LO3: Perform security analysis of IoT devices using network scanning and vulnerability assessment tools.
LO4: Develop and simulate smart infrastructure applications including smart waste management, air quality monitoring, and healthcare systems.
LO5: Implement IoT-based smart energy monitoring and traffic management systems using suitable simulators/ sensors.
LO6: Demonstrate real-time IoT data acquisition and processing using simulation tools (eg:digital twin case studies).

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hrs	LO Mapping
0	**Prerequisite**	Experimentation with IoT Architecture and Protocols	-	--
1	Edge & Fog Computing for Smart Infrastructure	Edge Computing Architecture, iFogSim, Edge-Based Data Analytics,edge simulator	04	LO1

		Comparison of cloud-only vs edge-based architecture (latency, bandwidth).		
2	Sensor Interfacing & Cloud Integration	IoT Sensor Interfacing, Serial Communication Basics, Serial peripheral Interface (SPI) Interfacing Basics, Cloud integration	02	LO2
3	IoT Security & Industrial IoT (IIoT)	IoT architecture & networking, Network Scanning and Enumeration, Open Port Analysis & Vulnerability Identification, OT vs IT Security in Industrial IoT	04	LO3
4	Smart Infrastructure Applications	IoT-Based Smart City Applications, Sensor-Based Fill-Level Detection , System Architecture & Concepts	04	LO4
5	Smart Energy & Traffic Systems	Fundamentals of Energy Monitoring, Smart Grid Architecture, IoT-based automatic street light control system, Traffic density detection simulation.	06	LO5
6	Real-Time IoT & Digital Twin	Real-time data acquisition , Node-RED, MQTT-based real-time data transmission.	04	LO6

List of Experiments.

Week No	List of Experiments	Hrs	
01	1a) Design and deploy an edge computing architecture using edge / fog simulators such as Edge and Fog Simulators /ifogsim	2	LO1
02	1b) Develop and evaluate edge-based data analytics algorithms in an edge simulator.	2	LO1
03	2a) Interfacing basic sensor to any development board ,gathering sensor value and pushing on to cloud (Thinkspeak/ AWS)	2	LO2
04	3a) Analysis of exposed network ports and evaluate potential security risks (security weaknesses) in IoT devices using Nmap or relevant tools.	2	LO3
05	3b) Study of industrial IoT(IIoT) with application of OT (operational technology) security.	2	LO3
06	4a) Application design of Healthcare in IoT using ifogsim	2	LO4
07	4b) Design / Simulation (Edge and Fog Simulators /ifogsim/ other) of an IoT-enabled smart waste bin system for real-time monitoring and automated alert generation based on fill-level detection	2	LO4
08	4c) Measure air quality index using sensors like MQ135 /MQ2	2	LO4
09	5a) Case Study / design an IoT-based automatic street light control system.	2	LO5
10	5b) Simulation IoT-based traffic density detection.	2	LO5
11	5c) Design of an IoT-based energy monitoring system.	2	LO5
12	5d) Case Study: Smart Grid Architecture with industry application	2	LO5
13	6a) Real time data acquisition and transmission using NodeRed simulator	2	LO6

14	6b) MQTT using HiveMQ Cloud and Ri-Pi	2	LO6
15	6c) Case study of digital Twin for aviation	2	LO6

Assessment:

Term Work: Term Work shall consist of minimum 8 Practicals which shall cover all Lab Course Outcomes and 2 Assignments based on the above list.

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

Practical/ oral Exam: An Oral exam will be held based on the above experiments.

PEL5013 Wireless sensor networks with secure protocols

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEL5013	Wireless sensor networks with secure protocols	-	2	-	-	1	-	1

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Practical/ Oral	Total
		Internal assessment (IAT)			End Sem. Exam			
		IAT- I	IAT-II	IAT-I + IAT-II (Total)				
PEL5012	IoT applications in Smart infrastructure Lab	--	--	--	--	25	25	50

Lab Objectives: Students will be able to learn.

1. Learn sensor interfacing and wireless communication technologies used in WSNs.
2. Design and implement secure wireless sensor network solutions.
3. Study simulation, emulation, and deployment tools for WSNs.
4. Analyze energy efficiency and performance of WSN protocols.
5. Implement security mechanisms for data transmission in sensor networks.
6. Develop a hardware/software-based mini project incorporating emerging WSN trends.

Lab Outcomes: Students will be able to achieve the outcome.

1. Configure and interface sensors and wireless modules.
2. Simulate WSN protocols using standard tools.
3. Implement secure communication in sensor networks.
4. Analyze performance, energy, and security trade-offs.
5. Design an IoT-enabled secure WSN mini project.
6. Demonstrate and document the implemented WSN system.

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hrs	LO Mapping
1	Sensor Nodes and WSN Environment Setup	Study of sensor node architecture and WSN components Interfacing basic sensors (DHT11/22, PIR, Ultrasonic, Gas sensor) with Arduino / Raspberry Pi Data acquisition and visualization	03	LO1
2	Wireless Communication and MAC Protocols	Study of IEEE 802.15.4, Bluetooth, Zigbee communication Interfacing wireless modules (HC-05, XBee, ESP32) Simulation of MAC protocols using Contiki/Cooja or CupCarbon	04	LO2

		Analysis of energy consumption under different MAC schemes		
3	Routing, Data Aggregation, and Energy Efficiency	Simulation of routing protocols (LEACH, Directed Diffusion) Data aggregation techniques to reduce network traffic Measurement of energy utilization in routing Introduction to energy harvesting concepts (theoretical/demo-based)	04	LO3
4	Security Threats and Attacks in WSN	Implementation of basic encryption (AES) for sensor data Simulation of attacks such as sinkhole, replay, and DoS Analysis of attack impact on network performance Study of trust and intrusion detection concepts	04	LO4
5	Secure Protocols and Key Management	Implementation of secure data transmission Study and simulation of SPINS (SNEP, µTESLA) Key distribution and authentication mechanisms Secure routing protocol demonstration Secure IoT communication using MQTT/CoAP (basic)	03	LO5
6	Emerging Trends in Secure WSNs	Design and implementation of a hardware-based mini project Secure WSN integrated with IoT cloud / mobile interface Performance, security, and energy analysis Project report and presentation	05	LO6

List of Experiments

Week No	List of Experiments	Hrs	LO
01	Study and interfacing of sensors (DHT11/22, PIR, Ultrasonic, Gas sensor) using *Arduino / Raspberry Pi / SenseNut platform* and observation of sensor data.	02	LO1
02	Interfacing and configuration of wireless communication modules (Bluetooth, Zigbee, ESP8266/ESP32 or SenseNut nodes) for sensor data transmission.	02	LO1
03	Simulation of a basic Wireless Sensor Network using *Contiki/Cooja / CupCarbon / SenseNut simulation or dashboard tools*.	02	LO2
04	Simulation and performance analysis of MAC protocols (IEEE 802.15.4, CSMA/TDMA) using *Cooja / NS-3 / SenseNut network setup*.	02	LO2
05	Implementation of secure data transmission using encryption techniques (AES / lightweight cryptography) on *Arduino / ESP / SenseNut firmware*.	02	LO3
06	Implementation of authentication and secure communication between sensor nodes and gateway using *MQTT/HTTP with security features or SenseNut security framework*.	02	LO3

07	Performance and energy consumption analysis of routing protocols (LEACH / data-centric routing) using *Cooja / NS-3 / SenseNut analytics*.	02	LO4
08	Analysis of security attacks (replay / DoS) and their impact on WSN performance using *simulation tools or SenseNut test scenarios*.	02	LO4
09	Design and implementation of an IoT-enabled secure WSN application (smart agriculture / smart healthcare / smart lighting) using *Arduino/ESP or SenseNut IoT platform*.	02	LO5
10	Integration of WSN with cloud or mobile dashboard for real-time monitoring using *MQTT/HTTP / SenseNut cloud dashboard*.	02	LO5
11	Testing, validation, and documentation of the secure WSN mini project implemented using *simulation / hardware / SenseNut platform*.	02	LO6
12	Demonstration and oral presentation of the IoT-enabled secure WSN system with performance, energy, and security analysis.	02	LO6

Assessment:

Term Work: Term Work shall consist of 10 practicals based on the above list.
Internal Practical Exam: Conduct an internal practical exam after completing the first three modules of the course to assess and ensure the learner's understanding.

Term Work Marks: 25 Marks (Total marks) = 10 Marks (Experiment) + 10 Marks (Internal Practical Exam) + 5 Marks (Attendance)

Practical & Oral Exam: An Oral & Practical exam will be held based on the above syllabus.

PEL5014 Internet Programming Lab

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEL5014	Internet Programming Lab	-	2	-	-	1	-	1

Course Code	Course Name	Examination Scheme						
		Theory Marks						
		Internal assessment (IAT)			End Sem. Exam	Term Work	Practical/ Oral	Total
		IAT- I	IAT- II	IAT-I + IAT-II (Total)				
PEL5014	Internet Programming Lab	--	--	--	--	25	25	50

Lab Objectives: Students will be able to learn.

1. To familiarize with the fundamental concepts of responsive Web design using HTML5, CSS3 (Flexbox/Grid), and Bootstrap.
2. To understand client-side scripting, DOM manipulation, and modern ES6+ JavaScript features.
3. To orient students for developing Java-based backend applications using Servlets, JSP, and JDBC.
4. To understand the concepts of Asynchronous JavaScript using Promises and the Fetch API to consume REST services.
5. To familiarize with server-side scripting using PHP, MySQL connectivity, and JSON data exchange.
6. To orient students for developing modern Single Page Applications (SPA) using React.js Components and Hooks.

Lab Outcomes:
Students will be able to achieve the outcome.

Sr. No.	Course Outcomes	Cognitive levels of attainment as per Bloom's Taxonomy
On successful completion, of course, learner/student will be able to:		
1	Design interactive and responsive web layouts using HTML5, CSS3, and the Bootstrap framework.	L6
2	Apply modern JavaScript (ES6+) for form validation, event handling, and dynamic DOM manipulation.	L3
3	Develop dynamic server-side applications using Java Servlets, JSP, and JDBC for database operations.	L3
4	Implement asynchronous data retrieval from APIs using the Fetch API an handle JSON responses effectively.	L3
5	Build data-driven web applications using PHP and MySQL, utilizing JSO for data interchange.	L6
6	Construct functional Single Page Applications (SPAs) using React.js components, Props, and State Management (Hooks).	L6

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hrs	LO Mapping
I	Introduction to Web Technology	Foundations of web architecture, accessibility-first semantic HTML5, modern CSS layouts (Grid/Flexbox), and responsive design using Bootstrap and utility-first frameworks.	4	LO1
II	Front End Development	Mastery of Modern JavaScript (ES6+), DOM manipulation, and core functional concepts like array methods and JSON handling for dynamic user interfaces.	4	LO2
III	Back End Development	Server-side fundamentals including Servlet architecture, JSP, secure database connectivity (JDBC/MySQL), and session management with authentication protocols.	6	LO3
IV	Async JS & APIs (Formerly RIA)	Advanced asynchronous programming using Promises and Async/Await, and integrating RESTful services via Fetch API and Axios for seamless data exchange.	2	LO4
V	Web Extension: PHP & JSON	Server-side scripting with PHP, focusing on form processing, secure MySQL database integration (CRUD), and structured data exchange using JSON.	6	LO5
VI	React.js	Building Single Page Applications (SPAs) using functional components, state management with Hooks (useState, useEffect), and client-side routing.	4	LO6

List of Experiments.

Week No	List of Experiments	Hrs	LO
01	Create a personal portfolio website using HTML5 semantic elements and CSS3 Flexbox/Grid for layout, incorporating audio/video controls and transitions.	02	LO1
02	Design a fully responsive web page (e.g., a Landing Page) using the Bootstrap grid system and components to ensure compatibility across mobile and desktop devices.	02	LO1
03	Write a Modern JavaScript (ES6) program to demonstrate Form Validation (email/password) using Arrow Functions and Event Listeners.	02	LO2
04	Implement a JavaScript function to parse and display data from a JSON object (e.g., a student list) onto an HTML page using map() and DOM manipulation.	02	LO2
05	Develop a Java Servlet application to demonstrate the Servlet Life Cycle and implement Session Tracking using Cookies or HttpSession (e.g., Login/Logout).	02	LO3
06	Create a Data-Driven Web Application using JSP and JDBC to implement a User Registration System that inserts and validates credentials against a MySQL database.	02	LO3
07	Build an application that uses the Fetch API and Async/Await to retrieve data from a public API (like JSONPlaceholder) and display it without reloading the page.	02	LO4

08	Write a PHP script that accepts user input from an HTML form, processes it, and returns the response in JSON format (demonstrating JSON data exchange).	02	LO5
09	Create a PHP application connected to a MySQL database to demonstrate CRUD operations (Create, Read, Update, Delete) on a user dataset.	02	LO5
10	Setup a React.js environment (Vite/CRA) and build a functional component-based application (like a "Counter" or "To-Do List") using JSX and the useState Hook.	02	LO6

Assessment:

Term Work: Term Work shall consist of 8 practicals based on the above list.
Internal Practical Exam: Conduct an internal practical exam after completing the first three modules of the course to assess and ensure the learner's understanding.

Term Work Marks: 25 Marks (Total marks) = 10 Marks (Experiment) + 10 Marks (Internal Practical Exam) + 5 Marks (Attendance)

Practical & Oral Exam: An Oral

Sem VI

PCC601 Blockchain Technology

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PCC601	Blockchain Technology	3	--	-	3	-	-	3

Course Code	Course Name	Theory							
		Internal Assessment (IAT)			End Sem Exam	Exam Duration (in Hrs)	Term work	Pract / Oral	Total
		IAT-I	IAT-II	IAT-I + IAT-II (Total)					
PCC601	Blockchain Technology	20	20	40	60	2	--	--	100

Course Objectives: The course aims to

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: Students will able to

1. CO1: Describe the basic concepts, components, and types of Blockchain.
2. CO2: Explain the working of Bitcoin, transactions, mining, and consensus mechanisms.
3. CO3: Apply the concepts of Ethereum to perform basic transactions and explore its architecture.
4. CO4: Develop simple Smart Contracts using Solidity programming.
5. CO5: Compare and evaluate Private Blockchain frameworks and consensus algorithms.
6. CO6: Design basic blockchain-based solutions for real-world applications.

DETAILED SYLLABUS:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mapping
	Prerequisites	Basics of Distributed Systems: Centralized vs Peer-to-Peer networks, concept of nodes. Basics of Cryptography: Public key and private key, digital signatures, cryptographic hash functions.	02	
I	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, Forking, Limitations and Challenges of blockchain	05	CO1
II	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	07	CO2
III	Public Blockchain	Introduction to Public Blockchain, Ethereum and its Components, Ethereum block structure, Architecture and Workflow, Comparison between Bitcoin and Ethereum	07	CO3

		Types of test-networks used in Ethereum, Transferring Ethers using Metamask, Ethereum frameworks, Exploring etherscan.io and ether block structure		
IV	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	07	CO4
V	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.	07	CO5
VI	Tools and Applications	Tools: Corda, Ripple, Quorum and DeFi Applications: Supply Chain Management, Blockchain with IoT, Blockchain with Cyber Security	05	CO6

Text Books:

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

References:

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

Online References:

Sr. No.	Website Name
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 (IA) for 20 marks each:

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

End Semester Theory Examination:

- **Question paper format**
- Question Paper will comprise a total of **six questions each carrying 15 marks**
- **Q.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 Q.2 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 answer

PCC602Ethical Hacking and Penetration Testing

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PCC602	Ethical Hacking and Penetration Testing	3	--	-	3	-	-	3

Course Code	Course Name	Theory							
		Internal Assessment (IAT)			End Sem Exam	Exam Duration (in Hrs)	Term work	Pract / Oral	Total
		IAT-I	IAT-II	IAT-I + IAT-II (Total)					
PCC602	Ethical Hacking and Penetration Testing	20	20	40	60	2	--	--	100

Course Objectives: The course aims to

1. To introduce the fundamental concepts of ethical hacking and penetration testing along with the role of cybersecurity in protecting digital systems.
2. To develop understanding of information gathering and reconnaissance techniques used to identify target system information.
3. To explain various network scanning and enumeration techniques used to discover vulnerabilities and open services.
4. To provide knowledge about system hacking techniques, password attacks, malware concepts, and privilege escalation methods.
5. To understand web application security, IoT security, blockchain security, and AI security risks in modern systems.
6. To familiarise students with penetration testing methodologies, risk assessment, and professional reporting practices.

Course Outcomes: Students will able to

1. CO1: Explain the fundamentals of ethical hacking, cybersecurity principles, and phases of penetration testing.
2. CO2: Apply reconnaissance and footprinting techniques using OSINT and security tools to gather target information.
3. CO3: Perform network scanning and enumeration to identify vulnerabilities and active services in a system.
4. CO4: Demonstrate system hacking techniques including password attacks, privilege escalation, and exploitation methods.
5. CO5: Analyze security vulnerabilities in web applications, IoT devices, and emerging technologies such as blockchain and AI systems.
6. CO6: Implement penetration testing methodologies and prepare professional technical and executive security reports.

DETAILED SYLLABUS:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mapping
0	Prerequisites	Computer Networks, cryptography and system security	01	
I	Introduction to Ethical Hacking	Definition and importance of Ethical Hacking Types of hackers: White hat, Black hat, Grey hat Cybersecurity fundamentals Phases of ethical hacking: Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks Self learning : Legal aspects: IT Act 2000, GDPR, compliance issues	06	CO1
II	Footprinting and	Footprinting concepts and objectives	06	CO2

	Reconnaissance	Types: Passive and Active reconnaissance WHOIS, DNS, IP scanning Social Engineering attacks Tools: Maltego, Recon-ng, theHarvester OWAPS Top 10 Self learning: OSINT (Open Source Intelligence)		
III	Scanning and Enumeration	Network scanning techniques: TCP, SYN, ACK scans, ARP Port scanning and service identification Vulnerability scanning: Nessus, OpenVAS Enumeration: Enumeration techniques and tools SNMP, SMB, NetBIOS enumeration Identifying live hosts and open services Self learning : Firewall and IDS Configuration	07	CO3
IV	System Hacking and Exploitation	Gaining access: Exploiting vulnerabilities Password attacks: Brute force, Dictionary attacks, Rainbow tables Privilege escalation Covering tracks Malware basics: Trojans, Viruses, Worms IoT device scanning and security considerations Penetration testing for IoT devices Self learning : Windows hash security	07	CO4
V	Web Application and IoT Security	Web application vulnerabilities: XSS, CSRF & SSRF Database vulnerabilities & Exploitation IoT Security: Threats, vulnerabilities, and countermeasures Blockchain security considerations: Smart contract vulnerabilities, 51% attacks AI Security Self learning : AI Case study of API security	07	CO5
VI	Penetration Testing Methodologies and Reporting	Types of penetration tests: Black box, White box, Grey box Penetration testing methodology Risk assessment and mitigation Reporting and documentation: Executive report, Technical report Real-time exercises using labs or CTF platforms Self learning : OT testing	05	CO6

Text Books:

1. Ethical Hacking and Penetration Testing Guide: The Case for Intuition-Based Decision Making by Rafay Baloch
2. Ethical Hacking Masterclass 2026: A hands-on guide to offensive security,web application exploitation, penetration testing & real world cyber security careers by Kline Thornton
3. The Web Application Hacker's Handbook – Dafydd Stuttard & Marcus Pinto.

References:

1. Ethical Hacking & Penetration Testing : The Complete Guide by Certified ethical hacker code academy - 2021 edition
2. Erickson, Jon. *Hacking: The Art of Exploitation*. 2nd Edition, No Starch Press, USA.
3. Weidman, Georgia. *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, USA.

Online References:

1. https://cybercx.com/solutions/security-testing-and-assurance/penetration-testing-services/ot-scada-iot-penetration-testing/
2. https://smarttecs.com/en/cyber-security/services/penetration-tests/iot-product-security/
3. https://nptel.ac.in/courses/106105217
4. https://ethicalhacking.eccouncil.org/?utm_source=ecc_paid&utm_medium=GooglePmax&utm_campaign=ecc_cehv13__googlepmax_apac-india&utm_content=&gad_source=1&gad_campaignid=23474176287&gbraid=0AAAAAD1MC3In9QFMdZ3jAHKJxDDeCPjk-&gclid=Cj0KCQiA2bTNBhDjARIsAK89wlF_KFMLrtWNMNZt849ugnex9VNxIQiNfm2OzXRFpCZnPDNkjC24gmwaAjavEALw_wcB

Internal Assessment (IA) for 20 marks each:

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

End Semester Theory Examination:

- **Question paper format**

- Question Paper will comprise a total of **six questions each carrying 15 marks**
- **Q.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 Q.2 has part (a) from Module 3 then part (b) must be from any other Module 0randomly 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
PEC6011	AI in Cyber Threat Intelligence Management	3	--	-	3	-	-	3

Course Code	Course Name	Theory							
		Internal Assessment (IAT)			End Sem Exam	Exam Duration (in Hrs)	Term work	Pract / Oral	Total
		IAT-I	IAT-II	IAT-I + IAT-II (Total)					
PEC6011	AI in Cyber Threat Intelligence Management	20	20	40	60	2	--	--	100

Course Objectives: The course aims to

1. To understand the fundamentals of Cyber Threat Intelligence
2. To understand the fundamental concepts of Artificial Intelligence and Machine Learning .
3. To apply AI methods for detecting malware, intrusions, and anomalies.
4. To understand normalization and scaling concept
5. To utilize AI-based tools for OSINT and social media threat analysis.
6. To design AI-driven CTI solutions for IoT and blockchain environments.

Course Outcomes: Students will able to

1. Explain the fundamentals of Cyber Threat Intelligence
2. Describe core concepts of Artificial Intelligence and Machine Learning used in cyber threat.
3. Apply AI and ML techniques to detect malware, intrusions, phishing, and anomalous behavior.
4. Perform data pre-processing, normalization, scaling, and feature engineering for CTI datasets.
5. Utilize AI-driven Threat Intelligence Platforms and OSINT tools for threat analysis and visualization.
6. Design AI-based CTI solutions for securing IoT and blockchain environments.

TAILED SYLLABUS:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mapping
I	Foundations of Cyber Threat Intelligence	Overview of cybersecurity threats and attack trends, Threat actors: APTs, cybercriminals, insiders, hacktivists, Types of Cyber Threat Intelligence, CTI lifecycle: Planning, Collection, Processing, Analysis, Dissemination, Intelligence pyramid, Role of CTI in organizational risk management, Introduction to MITRE ATT&CK framework.	06	CO1
II	Artificial Intelligence & Machine Learning Fundamentals	Overview of AI, ML, and Deep Learning, Supervised, Unsupervised, Semi-supervised Learning, Data Collection and Preprocessing, Feature Selection and Dimensionality Reduction, Model Training and Evaluation, Introduction to Neural Networks.	06	CO2
III	AI Techniques for Threat Detection	AI-based Intrusion Detection Systems, Malware Detection using ML, Phishing and Spam Classification, Behavioral Analysis and Anomaly Detection, Deep Learning for Cyber	08	CO3

		Security, Automated Incident Response.		
IV	Data Preprocessing & Feature Engineering for CTI	Importance of Data Preprocessing in CTI, Types of Data in CTI, Data cleaning and normalization, Handling noisy and adversarial data, Feature Engineering in CTI, , Feature extraction from logs, text, and binaries, Labeling and class imbalance issues, Data enrichment technique	06	CO4
V	AI-Driven Threat Intelligence Platforms & OSINT	Threat Intelligence Platforms (TIPs), OSINT Data Sources and Tools, NLP for Threat Report Analysis, Social Media and Dark Web Intelligence, Threat Correlation and Visualization.	06	CO5
VI	AI in IoT and Blockchain Security	IoT Threats and Vulnerabilities, AI-based IoT Intrusion Detection, Blockchain Security Issues, AI for Smart Contract Vulnerability Detection, Blockchain-based Threat Intelligence Sharing, Blockchain Security & AI Integration.	07	CO6

Text Books:

1. Clarence Chio & David Freeman – *Machine Learning and Security*
2. Mark Talabis et al. – *Information Security Analytics*
3. Stuart Russell & Peter Norvig – *Artificial Intelligence: A Modern Approach*

References:

1. Jason Brownlee – *Machine Learning Mastery with Python*
2. Kevin J. Houle & George M. Weaver – *Computer Security Incident Handling Guide*

Internal Assessment (IA) for 20 marks each:

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

End Semester Theory Examination:

- **Question paper format**

- Question Paper will comprise a total of **six questions each carrying 15 marks**
- **Q.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 Q.2 has part (a) from Module 3 then part (b) must be from any other Module 0randomly selected from all the modules)A total of **four questions** need to be answered

PEC6013 Cyber Security and laws

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEC6013	Cyber Security and laws	3	--	-	3	-	-	3

Course Code	Course Name	Theory							
		Internal Assessment (IAT)			End Sem Exam	Exam Duration (in Hrs)	Term work	Pract / Oral	Total
		IA T-I	IA T-II	IAT-I + IAT-II (Total)					
PEC6013	Cyber Security and laws	20	20	40	60	2	--	--	100

Course Objectives: The course aims to

1. To understand the foundational concepts of cyber security and classification of cybercrimes.
2. To analyze various cyber attack techniques and their real-world implications.
3. To familiarize students with commonly used cybercrime tools and defensive strategies.
4. To understand legal dimensions governing cyberspace and e-commerce.
5. To understand statutory provisions and regulatory frameworks governing cyber activities in India.
6. To understand various international security standards and compliance requirements.

Course Outcomes: Students will able to

1. Students will be able to explain and classify different types of cybercrimes and cyber security challenges.
2. Students will be able to analyze cyber attack techniques and evaluate mitigation mechanisms.
3. Students will be able to demonstrate understanding of common cyber attack tools and defensive practices.
4. Students will be able to interpret legal provisions related to cyber law and e-commerce.
5. Students will be able to apply provisions of IT Act and related regulations to real-life cyber legal issues.
6. Students will be able to evaluate and implement appropriate security standards in system design.

DETAILED SYLLABUS:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mapping
I	Introduction to Cybercrime	Introduction to Cybercrime: Cybercrime definition and origins of the world, Cybercrime and information security, Classifications of cybercrime, Cybercrime and the Indian ITA 2000, A global Perspective on cybercrimes.	04	CO1
II	Cyber offenses & Cybercrime	How criminal plan the attacks, Social Engg, Cyber stalking, Cyber café and Cybercrimes, Botnets, Attack vector, Cloud computing, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile, Devices-Related Security Issues, Organizational Security Policies and Measures in Mobile Computing Era, Laptops	09	CO2

III	Tools and Methods Used in Cyberline	Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Over Flow, Attacks on Wireless Networks, Phishing, Identity Theft (ID Theft)	06	CO3
IV	The Concept of E-Commerce and Cyberspace	Definition of E- Commerce, Main components of E-Commerce, Elements of E-Commerce security, E-Commerce threats, E-Commerce security best practices, Advantage of e-commerce, Survey of popular e-commerce sites. The Contract Aspects in Cyber Law ,The Security Aspect of Cyber Law ,The Intellectual Property Aspect in Cyber Law , The Evidence Aspect in Cyber Law , The Criminal Aspect in Cyber Law, Global Trends in Cyber Law , Legal Framework for Electronic Data Interchange Law Relating to Electronic Banking , The Need for an Indian Cyber Law	08	CO4
V	Indian IT Act and Regulatory Framework	Cyber Crime and Criminal Justice: Penalties, Adjudication and Appeals Under the IT Act, 2000, IT Act. 2008 and its Amendments. Introduction to digital payments, Components of digital payment and stake holders, Modes of digital payments- Banking Cards, Unified Payment Interface (UPI), e-Wallets, Unstructured Supplementary Service Data (USSD), Aadhar enabled payments, Digital payments related common frauds and preventive measures. RBI guidelines on digital payments and customer protection in unauthorized banking transactions. Relevant provisions of Payment Settlement Act,2007.	06	CO5
VI	Information Security Standard compliances	SOX, GLBA, HIPAA, ISO, FISMA, NERC, PCI.	06	CO6

Text Books:

1. Nina Godbole, SunitBelapure, Cyber Security, Wiley India, New Delhi
2. Cyber Crime Impact in the New Millennium, by R. C Mishra, Auther Press. Edition 2010
3. The Indian Cyber Law by Suresh T. Vishwanathan; Bharat Law House New Delhi
4. The Information technology Act, 2000; Bare Act- Professional Book Publishers, New Delhi.
5. Cyber Law & Cyber Crimes By Advocate Prashant Mali; Snow White Publications, Mumbai
6. Nina Godbole, Information Systems Security, Wiley India, New Delhi
7. Kennetch J. Knapp, Cyber Security &Global Information Assurance Information Science Publishing.
8. William Stallings, Cryptography and Network Security, Pearson Publication
9. Websites for more information is available on : The Information Technology ACT, 2008- TIFR : https://www.tifrh.res.in
10. Website for more information , A Compliance Primer for IT professional https://www.sans.org/reading-room/whitepapers/compliance/compliance-primer-professionals-33538

References:

1. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)
2. Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.
3. Fundamentals of Network Security by E. Maiwald, McGraw Hill.
4. Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.

Online Resources

Sr. No.	Website Name
1	https://onlinecourses.nptel.ac.in/noc26_lw01/preview
2	https://onlinecourses.nptel.ac.in/noc23_cs127/preview
3	https://www.meity.gov.in
4	https://onlinecourses.swayam2.ac.in/cec21_ge10/preview

5	https://www.classcentral.com/tag/cybercrime
6	https://www.coursera.org/learn/cybersecurity-for-everyone
7	https://www.coursera.org/specializations/intro-cyber-security

Internal Assessment (IA) for 20 marks each:

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

End Semester Theory Examination:

- **Question paper format**

- Question Paper will comprise a total of **six questions each carrying 15 marks**
- **Q.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 Q.2 has part (a) from Module 3 then part (b) must be from any other Module 0randomly selected from all the modules)

- A total of **four questions** need to be answered

PEC6014 Cloud and Web Security

PEC6014 Cloud and Web Security**Course Code**	**Course Name**	**Teaching Scheme (Contact Hours)**			**Credits Assigned**			
		Theory	**Pract.**	**Tut.**	**Theory**	**Pract.**	**Tut.**	**Total**
PEC6014	Cloud and Web Security	03	--	-	03	-	-	03

Course Code	**Course Name**	**Theory**							
		Internal Assessment (IAT)			**End Sem Exam**	**Exam Duration (in Hrs)**	**Term work**	**Pract / Oral**	**Total**
		IAT-I	**IAT-II**	**IAT-I + IAT- II (Total)**					
PEC6014	Cloud and Web Security	20	20	40	60	2	--	--	100

Course Objectives: The course aims

1. To understand the fundamentals of cloud computing and cloud-specific security challenges.
2. To analyze cloud infrastructure, identity, and data security mechanisms.
3. To study cloud security operations, compliance frameworks, and DevSecOps practices.
4. To understand fundamental web security concepts and client-side attack vectors.
5. To analyze advanced web attacks and secure web application development practices.
6. To apply cloud and web security concepts through real-world applications and case studies.

Course Outcomes: Students will able to

1. Explain cloud computing models, architectures, and shared responsibility security principles.
2. Apply identity, access, and data protection mechanisms in cloud environments.
3. Analyze cloud security operations, compliance standards, and DevSecOps workflows.
4. Explain browser security models and common client-side web attacks.
5. Analyze server-side web attacks and implement secure web application practices.
6. Design secure cloud and web solutions using real-world case studies and best practices.

Prerequisite: Basic knowledge of Computer Networks, Operating Systems, and Web Technologies

DETAILED SYLLABUS:

Sr. No.	**Name of Module**	**Detailed Content**	**Hours**	**CO Mapping**
	Prerequisites	Basic knowledge of Computer Networks, Operating Systems, and Web Technologies	02	
I.	Introduction to Cloud Computing and Cloud Security	Introduction to cloud computing, evolution of centralized to distributed systems, cloud characteristics, cloud service models (IaaS, PaaS, SaaS), deployment models (public, private, hybrid, multi-cloud). Cloud architecture components, shared responsibility model, trust boundaries, cloud threat landscape, common misconfigurations, overview of real-world cloud security breaches. Cloud-Native Security: Cloud native vs Traditional	06	CO1

		Security, Security by design in cloud. Self-Study: Comparison of cloud deployment models used by AWS, Azure, and GCP.		
II.	Cloud Infrastructure, Identity, and Data Security	Virtualization security, container and Kubernetes security fundamentals, cloud network security (VPC, subnets, firewalls, security groups). Identity and Access Management (IAM), authentication vs authorization, RBAC, least privilege, MFA, identity federation, SSO. Data protection mechanisms: encryption at rest and in transit, key management systems (KMS), data masking, backup, disaster recovery, and privacy considerations. Self-Study: Study IAM policies and encryption services in any one cloud platform.	07	CO2
III.	Cloud Security Operations, Compliance, and DevSecOps	Cloud security monitoring and logging, intrusion detection, cloud security posture management (CSPM), incident response lifecycle. Role of SOC in cloud environment, SIEM and SOAR basics. Compliance standards and frameworks: ISO/IEC, NIST, CSA, GDPR, HIPAA, SOC 2. DevOps vs DevSecOps, secure CI/CD pipelines, threat modeling (STRIDE/DREAD), vulnerability management and automation, Shift-left security concepts. Self-Study: Case study on a cloud compliance failure and its impact.	07	CO3
IV.	Web Security Fundamentals and Client-Side Attacks	Web architecture overview (DNS, HTTP/HTTPS), web security goals, browser security model, same-origin policy, cookies and sessions, secure cookie attributes, CSRF attacks and prevention. Cross-Site Scripting (XSS) types, content security policy (CSP), client-side defense mechanisms. Self-Study: Analyze OWASP Top 10 client-side vulnerabilities.	06	CO4
V.	Web Attacks and Secure Web Development	Server-side attacks: SQL injection, command injection, authentication and authorization flaws, denial-of-service attacks, phishing, clickjacking. Transport Layer Security (TLS), HTTPS deployment, certificates, common TLS attacks. API Security: OWASP API Top 10, OAuth 2.0 and token abuse, Rate limiting and API gateways. Secure web design principles, OWASP Top 10, modern authentication mechanisms, password-less authentication, MFA enforcement and session security, secure coding practices. Self-Study: Study recent web application breaches and map them to OWASP Top 10.	07	CO5
VI.	Applications and Case Studies	Cloud security applications: securing APIs, microservices, serverless security. Web security applications: vulnerability assessment, penetration testing basics, privacy protection. Case studies of major cloud and web security breaches, zero trust architecture, emerging trends in cloud and web security.	05	CO6

Text Books:

1. Practical Cloud Security: A Guide for Secure Design and Deployment, Second Edition by Chris Dotson (O'Reilly, 2023)
2. Security as Code: DevSecOps Patterns with AWS by BK Sarthak Das (O'Reilly, 2023)
3. Web Application Security, 2nd Edition by Hoffman Andrew (O'Reilly, 2024)
4. Alice and Bob Learn Application Security by Tanya Janca (Wiley, 2020)
5. The Ai Cybersecurity Handbook by Caroline Wong (Wiley, 2026)

References:

1. Web Security for Developers by Malcolm McDonald (2020)
2. Cloud Security for Dummies by Ted Coombs (O'Reilly, 2022)
3. Cloud Native Security Cookbook: Recipes for a Secure Cloud 1st Edition by Josh Armitage (O'Reilly, 2022)
4. Cloud computing security: foundation and challenges, John R Vecca (CRC Press, 2020)

Online References:

1. NPTEL: Web Browser Security: https://nptel.ac.in/courses/128106006
2. NPTEL: Cloud Computing: https://nptel.ac.in/courses/106105167
3. Udemy: Web Security for Web Developers: https://www.udemy.com/course/websec4webdev/
4. Cloud Security Basics: https://www.coursera.org/learn/cloud-security-basics

Internal Assessment (IA) for 20 marks each:

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

End Semester Theory Examination:

- **Question paper format**

- Question Paper will comprise a total of **six questions each carrying 15 marks**
- **Q.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 Q.2 has part (a) from Module 3 then part (b) must be from any other Module 0randomly selected from all the modules)

- A total of **four questions** need to be answered

PEC6021 IoT Gateways and Middleware

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEC6021	IoT Gateways and Middleware	03	--	-	03	-	-	03

Course Code	Course Name	Theory							
		Internal Assessment (IAT)			End Sem Exam	Exam Duration (in Hrs)	Term work	Pract / Oral	Total
		IAT-I	IAT-II	IAT-I + IAT- II (Total)					
PEC6021	IoT Gateways and Middleware	20	20	40	60	2	--	--	100

Course Objectives: The course aims to

1. Understand the fundamentals of Internet of Things (IoT), IoT ecosystem, and device–gateway–cloud architecture.
2. Learn communication models, protocols, and connectivity technologies used in IoT systems.
3. Understand IoT gateway architecture, middleware architecture, and their role in data management and integration.
4. Develop skills to design and implement IoT gateway functionalities such as protocol translation, data aggregation, and edge processing.
5. Analyze cybersecurity requirements, threats, and protection mechanisms for IoT gateways and middleware.
6. Explore integration of emerging technologies such as Blockchain, Edge/Fog computing, and Cloud with IoT systems.

Course Outcomes: Students will able to

1. Describe basic concepts of IoT, gateways, middleware, and IoT architectures.
2. Interpret communication protocols and connectivity technologies used in IoT systems.
3. Design and implement IoT gateway and middleware components for data acquisition and processing.
4. Apply security mechanisms such as authentication, authorization, and encryption in IoT environments.
5. Develop secure IoT applications using gateways and middleware platforms.
6. Analyze real-world IoT case studies integrating cybersecurity and blockchain technologies.

DETAILED SYLLABUS:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mapping
I	INTRODUCTION TO IoT GATEWAY & MIDDLEWARE	Internet of Things – Definition, Evolution, IoT Ecosystem Components, Device–Gateway–Cloud Architecture, Need for IoT Gateway, Introduction to Middleware Role of Gateway & Middleware in Data Flow Overview of Security & Trust in IoT, Application Domains of IoT	06	CO1
II	IOT COMMUNICATION & CONNECTIVITY	IoT Communication Models, Wireless Technologies (Wi-Fi, BLE, Zigbee, LoRaWAN, NB-IoT), Transport Protocols – TCP vs UDP,	07	CO1, CO2

		Application Protocols, MQTT, CoAP, HTTP/REST, AMQP, Secure Communication Concepts TLS / DTLS Basics, Message Exchange Patterns		
III	IoT GATEWAY ARCHITECTURE & DESIGN	Gateway Hardware Architecture, Gateway Software Stack, Types of Gateways, Functions of Gateway, Protocol Translation, Data Aggregation, Filtering, Local Processing Edge Intelligence in Gateway, Gateway Device Management, Basic Gateway Security Secure Boot & Firmware Update	07	CO2, CO5
IV	IoT MIDDLEWARE & CYBERSECURITY ARCHITECTURE	Middleware Architecture Layers, Middleware Services, Device Management, Messaging, Data Management, API Management & REST Services, Identity & Access Management (IAM), Authentication & Authorization Models, Secure Middleware Communication, Cyber Attacks in IoT, Spoofing, Man-in-the-Middle, DoS and DDOS operations, Middleware Communication Models, Service-Oriented Architecture (SOA) in IoT, Middleware Platforms & Brokers, MQTT Brokers, Message Queues, Edge Middleware vs Cloud Middleware, Development workflow: Remix/Hardhat/Truffle, testing, deployment, interacting via Web3/ethers	07	CO4
V	BLOCKCHAIN EDGE, CLOUD, SECURITY INTEGRATION , SCALABILITY & INTEROPERABILITY	Study and implementation of a secure blockchain-enabled IoT architecture covering Distributed Ledger Technology (DLT), smart contracts, device identity management, secure data sharing, and integrated Edge–Fog–Cloud communication with end-to-end encryption, secure data pipelines, interoperability, scalability, and fault tolerance.	06	CO5
VI	IOT GATEWAY & MIDDLEWARE APPLICATION (CASE STUDIES & MINI PROJECTS)	Smart Home Gateway Architecture, Industrial IoT Gateway System, Healthcare IoT Gateway Design, Smart Agriculture System, Cloud-based IoT Platform Integration, Mini Project Design Steps, Requirement Analysis, Architecture Diagram, Technology Selection, Implementation, Testing & Deployment	07	CO6

Text Books:

1. Pethuru Raj & Anupama C. Raman, The Internet of Things: Enabling Technologies, Platforms, and Use Cases
2. Raj Kamal, Internet of Things – Architecture and Design Principles,McGraw-Hill Education
3. Imran Bashir , Mastering Blockchain – Distributed Ledger Technology, Smart Contracts, and Cryptocurrencies,Packt Publishing

References:

1. Honbo Zhou, The internet of Things : Perception , Communication and computing CRC Press
2. Subhas Chandra Mukhopadhyay, Internet of things : challenges and opportunities Springer
3. Shancang Li, Li Da Xu , Shanshan Zhao , The internet of things : Survey of topics and Trends Elsevier
4. William Stallings : Cryptography and Network Security : Principles and Practice Pearson Education .

Online References:

Sr. No.	Website Name
1	MQTT Official Documentation (https://mqtt.org).
2	IETF IoT Protocol Standards (CoAP, DTLS, etc.)(https://www.ietf.org)
3	AWS IoT Core Documentation(https://docs.aws.amazon.com/iot)

4	Microsoft Azure IoT Hub Documentation(https://learn.microsoft.com/azure/iot-hub)
5	Ethereum Smart Contract Documentation (https://ethereum.org/developers)

Internal Assessment (IA) for 20 marks each:

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

End Semester Theory Examination:

- **Question paper format**

- Question Paper will comprise a total of **six questions each carrying 15 marks**
- **Q.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 Q.2 has part (a) from Module 3 then part (b) must be from any other Module 0randomly 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
PEC6022	Data Privacy and Protection Techniques	3	--	-	3	-	-	3

Course Code	Course Name	Theory							
		Internal Assessment (IAT)			End Sem Exam	Exam Duration (in Hrs)	Term work	Pract / Oral	Total
		IAT-I	IAT-II	IAT-I + IAT-II (Total)					
PEC6022	Data Privacy and Protection Techniques	20	20	40	60	2	--	--	100

Course Objectives: The course aims to

1. Understand the fundamentals of data privacy and protection mechanisms in modern computing environments including IoT systems.
2. Explain anonymization techniques used for protecting structured datasets and analyze their role in preserving privacy.
3. Study privacy preservation methods for complex data structures such as graph data, time-series data, and transactional datasets.
4. Analyze threats and attacks on anonymized datasets and understand the limitations of existing anonymization models.
5. Apply privacy preserving data mining techniques for secure analytics and responsible data usage.
6. Understand dynamic data protection mechanisms such as tokenization and their applications in cloud and IoT systems.

Course Outcomes: Students will able to

CO No.	Course Outcome	Bloom Level
CO1	Explain fundamental concepts of data privacy, data security, and privacy challenges in IoT environments.	Understand
CO2	Apply anonymization techniques such as k-anonymity, l-diversity, and t-closeness to protect multidimensional datasets.	Apply
CO3	Analyze privacy preservation methods for complex data structures including graph, time-series, and transactional datasets.	Analyze
CO4	Examine threats and attacks on anonymized datasets such as re-identification and linkage attacks.	Analyze
CO5	Apply privacy preserving data mining techniques to enable secure analytics while maintaining data utility.	Apply
CO6	Illustrate dynamic data protection techniques such as tokenization and their applications in cloud and IoT systems.	Understand

DETAILED SYLLABUS:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mapping
	Prerequisites	Fundamentals of computer systems and operating systems; Basics of programming (C/C++/Java/Python); Basic database concepts such as tables, records and queries; Fundamentals of computer networks and Internet technologies; Introduction to information security principles including Confidentiality, Integrity and Availability; Basic understanding of web applications and data usage; Awareness of ethical practices and privacy principles in computing.	01	
I	Introduction to Data Privacy	Concept of data privacy and data security; Need for privacy protection in IoT environments; IoT data lifecycle and sources of data generation; Privacy risks in connected devices and smart systems; Basic protection mechanisms including encryption, access control, masking and tokenization; Privacy–utility trade-off; Principles of privacy-by-design; Overview of data protection regulations and standards (e.g., GDPR). Self Study: Study privacy challenges in smart city and healthcare IoT systems. Review examples of privacy violations in real-world applications.	05	CO1
II	Static Data Anonymization – Multidimensional Data	Characteristics of structured datasets; Classification of attributes including identifiers, quasi-identifiers and sensitive attributes; Concepts of data anonymization; Group-based anonymization techniques such as k-anonymity, l-diversity and t-closeness; Data generalization and suppression methods; Applications of anonymization in healthcare, census and sensor datasets. Self Study: Explore anonymization examples using publicly available datasets. Study additional anonymization models used in secure data publishing.	08	CO2
III	Static Data Anonymization – Complex Data Structures	Privacy challenges in complex data formats including graph data and network datasets; Privacy preservation in time-series data generated by IoT sensors; Challenges in protecting temporal datasets; Methods for protecting time-series and streaming data; Privacy preservation of longitudinal datasets; Privacy issues in transactional data; Case studies involving smart meters and wearable devices. Self Study: Study privacy risks in social network datasets and mobility data. Review privacy issues in wearable health monitoring systems.	07	CO3

IV	Threats to Anonymized Data	Types of privacy attacks on anonymized datasets; Re-identification attacks; Linkage attacks and background knowledge attacks; Threats associated with multidimensional datasets, graph data, time-series datasets and transactional data; Limitations and weaknesses of anonymization models such as k-anonymity, l-diversity and t-closeness; Discussion of privacy risks in big data analytics environments. Self Study: Study real-world examples of privacy breaches in large data systems and IoT platforms. Review notable re-identification case studies	07	CO4
V	Privacy Preserving Data Mining	Introduction to Privacy Preserving Data Mining (PPDM); Need for privacy-aware analytics in modern data-driven systems; Techniques for privacy preserving analysis including data perturbation, masking and secure multiparty computation; Privacy preserving test data generation; Concepts of test data utility, coverage and quality; Trade-off between privacy protection and analytical usefulness of data. Self Study: Study basic privacy-preserving machine learning concepts and applications. Explore datasets used for secure analytics.	06	CO5
VI	Dynamic Data Protection – Tokenization	Need for dynamic data protection in operational information systems; Tokenization concepts and principles; Dependent and independent tokenization methods; Tokenization architecture and system components; Comparison of tokenization with encryption and masking techniques; Applications of tokenization in financial systems, cloud services and IoT data platforms. Self Study: Study practical applications of tokenization in payment processing systems and cloud platforms. Review industry tools used for dynamic data protection.	05	CO6

Text Book:

1. NatarajVenkataramanan, AshwinShriram, “Data Privacy: Principles and Practice”, Chapman & Hall/CRC.
2. A. C. Yao and V. Shmatikov, *Privacy-Preserving Data Mining: Models and Algorithms*. New York, NY, USA: Springer, 2008.
3. B. C. Fung, K. Wang, R. Chen and P. S. Yu, *Privacy-Preserving Data Publishing: Concepts and Techniques*. Boca Raton, FL, USA: CRC Press, 2010.
4. C. Dwork and A. Roth, *The Algorithmic Foundations of Differential Privacy*. Boston, MA, USA: Now Publishers Inc., 2014.

Reference Books:

1. Nishant Bhajaria, “Data Privacy: A Runbook for Engineers”, Manning Publications.
2. Katharine Jarmul, “Practical Data Privacy”, O'Reilly Media.
3. Ronald Leenes, Rosamunde van Brakel, and Serge Gutwirth: Data Protection and Privacy: The Age of Intelligent Machines, Hart Publishing, 2017.
4. Naavi: Personal Data Protection Act of India (PDPA 2020) : Be Aware, Be Ready and Be Compliant, 2020.
5. Ravinder Kumar Gaurav Goyal, The Right to Privacy in India: Concept and Evolution, Publisher: Lightning Source, 2016.

Online Resources

Sr. No.	Website Name
1	Coursera, "Data Privacy and Security Courses." [Online]. Available: https://www.coursera.org
2	OECD, "Privacy Guidelines and Data Protection Framework." [Online]. Available: https://www.oecd.org/privacy
3	Cloud Security Alliance, "Privacy and Data Protection Resources." [Online]. Available: https://cloudsecurityalliance.org
4	National Programme on Technology Enhanced Learning (NPTEL), "Cyber Security and Privacy." [Online]. Available: https://nptel.ac.in

Assessment:
Internal Assessment (IA) for 20 marks each:

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

End Semester Theory Examination:

Question paper format

- Question Paper will comprise a total of **six questions each carrying 15 marks**
- **Q.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 Q.2 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
PEC6023	Information Security Management Systems	3	--	-	3	-	-	3

Course Code	Course Name	Theory							
		Internal Assessment (IAT)			End Sem Exam	Exam Duration (in Hrs)	Term work	Pract / Oral	Total
		IA T-I	IAT-II	IAT-I + IAT-II (Total)					
PEC6023	Information Security Management Systems	20	20	40	60	2	--	--	100

Course Objectives:

1. Understand the fundamentals of information security including security goals, services, attacks.
2. Develop mathematical foundations of cryptography, such as modular arithmetic, congruence, and algebraic structures used in cryptography algorithms.
3. Analyze classical and modern symmetric key cryptography techniques and understand their working principles and modes of operation.
4. Explain public key cryptography systems including RSA, Rabin Cryptosystem, and secure key management techniques.
5. Understand message authentication, hash functions, and digital signatures for ensuring data integrity, authentication, and non-repudiation.
6. Gain knowledge of network and system security concepts and tools used to protect communication and computing systems.

Course Outcomes: Students will able to

1. **CO1:** Provide fundamental concepts of information security including security goals, attacks, services.
2. **CO2:** Apply mathematical concepts such as modular arithmetic, congruence, algebraic structures, and primality testing in cryptography algorithms.
3. **CO3:** Analyze public key cryptographic systems and authentication mechanisms
4. **CO4:** Demonstrate understanding of message authentication mechanisms, hash functions, and their security properties for ensuring data integrity and authentication.
5. **CO5:** Describe digital signature schemes and apply network and system security concepts to protect communication and computing environments.
6. **CO6:** Apply enterprise security solutions considering legal, ethical, and emerging technological aspects.

DETAILED SYLLABUS:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mapping
0	Prerequisites	Computer & network literacy, Programming ability, Mathematical foundation for cryptography, Basic OS and security awareness	01	--

I	Basics of Information Security and Cryptographic Mathematics	Basics of Information Security – Information Security understanding, Security goals, Security attacks, Security services, security mechanisms Cryptographic Mathematics- Modular arithmetic, linear congruence, Algebraic structure, checking of primeness, quadratic congruence	04	CO1 CO2
II	Classical Ciphers and Modern symmetric key ciphers	Classical Ciphers – Symmetric cipher model, substitution ciphers, transposition ciphers, steganography Modern symmetric key ciphers – Modern block ciphers, modern stream ciphers, Data Encryption standard, advanced encryption standard, electronic code book mode, CBC, cipher feedback mode, output feedback mode	10	CO3
III	Public key cryptography	Public key cryptography – RSA, RSA proof, RSA attacks, Rabin cryptosystem, Key management: Diffie Hellman	04	CO3
IV	Message Authentication and Hash functions	Message Authentication and Hash functions Authentication requirements, functions, Message authentication codes (MAC), Hash functions, security of Hash functions Hash algorithms, Digital Signatures SHA- 512, Basics, digital signature standards	08	CO4 CO5
V	Enterprises and Network Security	Network and System Security IP Security (IPSec), Firewalls, IDS, IPS, Web and Email security, System hardening techniques, Cloud security fundamentals, Zero Trust Architecture, IoT security considerations	06	CO6
VI	Legal, Ethical & Emerging Trends	Network and System Security ISMS lifecycle (Plan–Do–Check–Act), ISO 27001 clauses overview, Overview of IT Act 2000 (India), Data protection principles, Digital forensics basics, Security in AI and Blockchain, Case studies of major security breaches	06	CO6

Text Book:

1. William Stallings, “Cryptography and Network Security – Principles and Practice”, Pearson Education.
2. William Stallings, “Network Essentials: Security Applications and Standards”, 6th Edition, Pearson Education.

Reference Books:

1. Bruce Scheneir: “Applied Cryptography”, John Wiley.
2. Behrouz Forouzan: “Cryptography & Network Security”, TMH.

Online Resources

Sr. No.	Website Name
1	https://www.classcentral.com/course/swayam-information-security-91683?utm_source=chatgpt.com
2	https://www.classcentral.com/course/youtube-computer-cryptography-and-network-security-47628?utm_source=chatgpt.com

3	https://www.udemy.com/course/cryptography-security-protect-data-from-cyber-threats/?utm_source=chatgpt.com
4	https://wizape.com/English/Cryptography-and-Secure-Communications?utm_source=chatgpt.com
5	https://www.classcentral.com/course/swayam-information-security-91683
6	https://www.udemy.com/course/cryptography-security-protect-data-from-cyber-threats/

Assessment:

Internal Assessment (IA) for 20 marks each:

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

End Semester Theory Examination:

Question paper format

- Question Paper will comprise a total of **six questions each carrying 15 marks**
- **Q.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 Q.2 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 answer

C6024 Web Application Security

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEC6024	Web Application Security	3	--	-	3	-	-	3

Course Code	Course Name	Theory							
		Internal Assessment (IAT)			End Sem Exam	Exam Duration (in Hrs)	Term work	Pract / Oral	Total
		IAT-I	IAT-II	IAT-I + IAT-II (Total)					
PEC6024	Web Application Security	20	20	40	60	2	--	--	100

Course Objectives: The course aims to

1. Understand the fundamentals of web application architecture, web technologies, and core security principles.
2. Learn common web application vulnerabilities, attack methodologies, and defensive coding practices.
3. Understand authentication, authorization, session management, and access control mechanisms in web applications.
4. Develop skills to design and implement secure web applications, APIs, and databases using cryptographic techniques and security frameworks.
5. Analyze cybersecurity threats, risk assessment methods, and protection mechanisms for modern web-based systems including IoT web interfaces.
6. Explore integration of emerging technologies such as Cloud security, DevSecOps, Zero Trust Architecture, and Blockchain for securing web applications.

Course Outcomes: Students will able to

1. Describe basic concepts of web application architecture, web technologies, and web security principles.
2. Interpret common web application vulnerabilities, attack techniques, and threat models.
3. Design and implement secure authentication, authorization, and session management mechanisms in web applications.
4. Apply security mechanisms such as encryption, hashing, secure communication, and access control in web systems.
5. Develop secure web applications and APIs using secure coding practices and security testing tools.
6. Analyze real-world web security case studies integrating cloud security, DevSecOps, and emerging protection technologies.

DETAILED SYLLABUS:

Sr. No.	Name of Module	Detailed Content	Hours	CO Mapping
I	Foundations of Web Application Security	Evolution of Web Applications and Web Architecture, Client–Server and Three-Tier Architecture, HTTP/HTTPS Protocol and Request–Response Cycle, Cookies, Sessions and Local Storage, Information Security Fundamentals (CIA Triad, Threat, Vulnerability, Risk), Authentication vs Authorization and OWASP Top 10 Overview	06	CO1
II	Web Application Vulnerabilities and Attacks	Introduction to Web Application Vulnerabilities, Injection Attacks (SQL Injection, Command Injection), NoSQL Injection and Input Manipulation, Cross-Site Scripting (Stored and Reflected XSS), DOM-Based XSS and Cross-Site Request Forgery (CSRF), Broken Authentication and Session Attacks, File Upload Vulnerabilities and Path Traversal	07	CO1, CO2
III	Secure Authentication and Cryptography	Password Security (Hashing and Salting), Secure Session Management, Multi-Factor Authentication, Cryptography Fundamentals, Symmetric and Asymmetric Encryption, Hash Functions and Digital Signatures, TLS/SSL Secure Communication	07	CO2, CO3
IV	API Security and Secure Web Design	Introduction to Web APIs and REST Architecture, REST API Security Threats, Token-Based Authentication, JSON Web Tokens (JWT), OAuth 2.0 Authentication Framework, Secure Coding Practices, Input Validation, Output Encoding and Secure Database Interaction	07	CO3,CO4
V	IoT Architecture and Web Integration Security	Introduction to Internet of Things Architecture, IoT Communication Protocols (MQTT, CoAP, HTTP), IoT Security Challenges, Device Authentication and Secure Firmware, Secure IoT Data Transmission and Cloud IoT Platforms, Privacy Issues in IoT Systems	06	CO4, CO5
VI	Security Testing and Industrial Applications	Vulnerability Assessment Concepts, Penetration Testing Methodology, Web Application Firewall (WAF), DevSecOps, Zero Trust Architecture, and Blockchain for securing web applications.	06	CO5, CO6

Text Books:

1. Dafydd Stuttard and Marcus Pinto, The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws, Wiley Publishing.
2. Andrew Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications, O’Reilly Media.
3. Joel Scambray, Mike Shema, and Caleb Sima, Hacking Exposed Web Applications, McGraw-Hill Education.

References:

1. Dafydd Stuttard and Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, Wiley Publishing.
2. Andrew Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications, O'Reilly Media.
3. Joel Scambray, Mike Shema, and Caleb Sima, Hacking Exposed Web Applications, McGraw-Hill Education.
4. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson Education.
5. Michael Shema, Hacking Web Apps: Detecting and Preventing Web Application Security Problems, Syngress.

Online References:

Sr. No.	Website Name
1	OWASP Official Documentation (https://owasp.org)
2	OWASP Top 10 Web Application Security Risks (https://owasp.org/www-project-top-ten/)
3	Mozilla Web Security Guidelines (https://developer.mozilla.org/en-US/docs/Web/Security)
4	NIST Computer Security Resource Center (https://csrc.nist.gov)
5	PortSwigger Web Security Academy (https://portswigger.net/web-security)

Assessment:

Internal Assessment (IA) for 20 marks each:

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

End Semester Theory Examination:

➢ **Question paper format**

- Question Paper will comprise a total of **six questions each carrying 15 marks**
- **Q.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 Q.2 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 answer

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PCL601	Blockchain Technology Lab	-	2	-	-	1	-	1

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Practical/ Oral	Total
		Internal assessment (IAT)			End Sem. Exam			
		IAT- I	IAT-II	IAT-I + IAT-II (Total)				
PCL601	Blockchain Technology Lab	--	--	--	--	25	25	50

Lab Objectives: Students will be able to learn.

1. Understand blockchain architecture and cryptographic foundations.
2. Perform cryptocurrency transactions using public blockchain tools.
3. Explore Ethereum ecosystem and blockchain explorers.
4. Develop and deploy Smart Contracts using Solidity.
5. Implement advanced Solidity features like inheritance and error handling.
6. Study and compare private blockchain frameworks.
7. Analyze real-world blockchain applications.

Lab Outcomes: Students will be able to achieve the outcome.

1. LO1: Demonstrate blockchain structure and cryptographic hashing mechanisms.
2. LO2: Perform and analyze cryptocurrency transactions using wallets.
3. LO3: Explore Ethereum blockchain and interpret block/transaction details.
4. LO4: Develop, deploy, and test smart contracts using Solidity.
5. LO5: Implement advanced smart contract features like inheritance and error handling.
6. LO6: Compare public and private blockchain platforms and propose application-based solutions.

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hrs	LO Mapping
0	Prerequisite	Basic of C/Python/Java and basic web concepts.	02	--
1	Blockchain Fundamentals and Cryptography	Blockchain overview, block structure, hashing mechanisms, Merkle tree concept and generation, data integrity verification, types of blockchain (Public, Private, Consortium).	02	LO1
2	Bitcoin Blockchain and Cryptocurrency	Bitcoin transaction process, UTXO model, double spending problem, cryptocurrency wallets (hot and cold), mining process, mining difficulty, consensus mechanisms such as PoW, PoS, PoB and PoET	04	LO2

3	Public Blockchain and Ethereum	Ethereum architecture and workflow, Ethereum block structure, comparison of Bitcoin and Ethereum, Ethereum test networks, Ether transactions using MetaMask, blockchain explorers such as Etherscan.	04	LO4
4	Smart Contract Development using Solidity	Introduction to smart contracts, Solidity programming environment (Remix IDE), variables and data types, functions and visibility specifiers, control statements, error handling mechanisms (require, assert, revert), events, inheritance and modifiers, smart contract interaction and deployment.	10	LO5
5	Private Blockchain Platforms	Concepts of private blockchain, enterprise blockchain requirements, Hyperledger Fabric architecture, components such as MSP and Chaincode, comparison of Hyperledger Fabric and Ethereum, consensus mechanisms used in private blockchains (PAXOS, RAFT, BFT, PBFT).	04	LO6
6	Blockchain Tools and Applications	Overview of blockchain tools and frameworks, blockchain-based application design, use cases such as supply chain management, IoT integration, and cybersecurity applications	04	LO6

List of Experiments:

Week No	List of Experiments	Hrs
01	Study blockchain fundamentals including hashing, Merkle tree construction, block structure, and types of blockchain (Public, Private, Consortium).	02
02	Study and simulate cryptographic hashing and Merkle tree generation for a set of transactions and verify data integrity.	02
03	Perform cryptocurrency transactions using MetaMask on Ethereum test network and analyze transaction hash, gas fees, and block details using Etherscan.	02
04	Study Bitcoin blockchain concepts including UTXO model, double spending problem, and cryptocurrency wallets (hot and cold wallets).	02
05	Study and simulate Bitcoin mining concepts including mining difficulty and comparison of consensus mechanisms (PoW, PoS, PoB, PoET).	02
06	Explore Ethereum architecture and workflow; examine Ethereum block structure and compare Bitcoin and Ethereum features.	02
07	Study Ethereum test networks and perform Ether transfer using MetaMask; analyze transaction details using blockchain explorers.	02
08	Write and deploy a basic Smart Contract in Solidity using Remix IDE demonstrating variables and data types	02
09	Implement functions and visibility specifiers (public, private, internal, external) in Solidity and interact with deployed contracts.	02
10	Implement control statements and error handling mechanisms (require, assert, revert) in Smart Contracts.	02
11	Develop Smart Contracts using inheritance and modifiers and test contract execution	02
12	Study the concept of state machines in Smart Contracts and demonstrate contract interaction using events.	02
13	Study Private Blockchain concepts and explore Hyperledger Fabric architecture including MSP and Chaincode	02
14	Study consensus mechanisms used in private blockchains including PAXOS, RAFT, BFT, and PBFT.	02
15	Design and demonstrate a simple blockchain-based application such as Supply Chain Management, Blockchain with IoT, or Cybersecurity use case.	02

Assessment:

Term Work: Term Work shall consist of 10 practicals based on the above list.

Internal Practical Exam: Conduct an internal practical exam after completing the first three modules of the course to assess and ensure the learner's understanding.

Term Work Marks: 25 Marks (Total marks) = 10 Marks (Experiment) + 10 Marks (Internal Practical Exam) + 5 Marks (Attendance)

Practical& Oral Exam: An Oral & Practical exam will be held based on the above syllabus.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PCL602	Ethical hacking and penetration testing Lab	-	2	-	-	1	-	1

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Practical / Oral	Total
		Internal assessment (IAT)			End Sem. Exam			
		IAT- I	IAT-II	IAT-I + IAT-II (Total)				
PCL602	Ethical hacking and penetration testing Lab	--	--	--	--	25	25	50

Lab Objectives: Students will be able to learn.

1. To introduce students to penetration testing tools and environments used in cybersecurity labs.
2. To develop practical skills in reconnaissance and information gathering techniques using security tools.
3. To provide hands-on experience in network traffic analysis and vulnerability scanning.
4. To demonstrate system exploitation techniques using penetration testing frameworks.
5. To analyze web application vulnerabilities and emerging security threats through practical experiments.
6. To train students in performing complete penetration testing exercises and preparing security reports.

Lab Outcomes: Students will be able to achieve the outcome.

1. **LO1:** Use ethical hacking tools such as Nmap, Wireshark, and Metasploit to perform security assessments.
2. **LO2:** Perform reconnaissance and information gathering using WHOIS, DNS tools, Google Dorks, and OSINT techniques.
3. **LO3:** Conduct network traffic analysis, service enumeration, and vulnerability scanning in a controlled lab environment.
4. **LO4:** Demonstrate password attacks and exploitation techniques using penetration testing frameworks.
5. **LO5:** Identify and analyze web application vulnerabilities such as SQL injection and CSRF attacks.
6. **LO6:** Execute a complete penetration testing cycle from reconnaissance to reporting and document findings professionally.

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hrs	LO Mapping
0	Prerequisite	Computer Networks, cryptography and system security	01	--
1	Overview of Tools	Introduction of different tools required to ethical hacking and penetration testing, Tools overview: Nmap, Wireshark, Metasploit	04	LO1

2	Footprinting, Scanning, and Social Engineering Attacks	WHOIS, DNS, IP scanning Social Engineering attacks : Phishing attack ,baiting, smishing , Tailgating	04	LO2
3	Network scanning	Network scanning techniques: TCP, SYN, ACK scans, ARP Port scanning and service identification	04	LO3
4	Scanning & Exploitation	Password attacks: Brute force, Dictionary attacks, Rainbow tables Exploiting with Metasploit IoT device scanning and security considerations Penetration testing for IoT devices	05	LO4
5	Web application & Blockchain security	Web application vulnerabilities: CSRF Database Exploitation with SQLmap Blockchain security considerations: Smart contract vulnerabilities, 51% attacks	04	LO5
6	Penetration testing & Reporting	Penetration testing methodology Risk assessment and mitigation Reporting and documentation: Executive report, Technical report	04	LO6

List of Experiments:

Week No	List of Experiments	Hrs
1	Port scanning and OS fingerprinting using NMAP	2
2	Reconnaissance using the tool : Maltego.	2
3	Use WHOIS and DNS tools to collect domain information	2
4	Perform passive reconnaissance using Google Dorks.	2
5	To demonstrate / Study Social Engineering techniques to collect sensitive information from a target web application.	2
6	Study of packet sniffer tools like Wireshark and its capture filters	2
7	Enumerate services using NetBIOS, SNMP, and SMB enumeration tools.	2
8	Scan IoT devices in a lab setup (like Raspberry Pi sensors) for open ports.	2
9	Perform vulnerability scanning with Nessus/OpenVAS in a controlled environment.	2
10	Perform password attacks (brute force, dictionary) on lab accounts.	2
11	Use Metasploit to exploit known vulnerable lab machines (Metasploitable VM)	2
12	Perform basic IoT device exploitation using lab-configured devices (simulate weak credentials or open services).	2
13	Simulate CSRF attack in the web applications lab.	2

14	Analyze blockchain smart contract vulnerabilities using Remix IDE (simulate reentrancy or overflow).	2
15	Detect SQL injection vulnerabilities in a website database using SQLMap	2
16	Use Metasploit and other tools to exploit lab machines in stages: reconnaissance → scanning → exploitation → reporting.	2
17	Create technical and executive penetration testing reports.	2

ext Books:

1. Computer & Internet Security — A Hands-On Approach – Wenliang Du
2. The Web Application Hacker's Handbook – Dafydd Stuttard & Marcus Pinto
3. Stuart Russell & Peter Norvig – *Artificial Intelligence: A Modern Approach*

References:

1. Erickson, Jon. *Hacking: The Art of Exploitation*. 2nd Edition, No Starch Press, USA.
2. Weidman, Georgia. *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, USA.

Assessment:

Term Work: Term Work shall consist of 10 practicals based on the above list.

Internal Practical Exam: Conduct an internal practical exam after completing the first three modules of the course to assess and ensure the learner's understanding.

Term Work Marks: 25 Marks (Total marks) = 10 Marks (Experiment) + 10 Marks (Internal Practical Exam) + 5 Marks (Attendance)

Practical& Oral Exam: An Oral & Practical exam will be held based on the above syllabus.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEL6011	AI in Cyber Threat Intelligence Management Lab	-	2	-	-	1	-	1

Course Code	Course Name	Examination Scheme						
		Theory Marks						
		Internal assessment (IAT)			End Sem. Exam	Term Work	Practical/ Oral	Total
		IAT-I	IAT-II	IAT-I + IAT-II (Total)				
PEL6011	AI in Cyber Threat Intelligence Management Lab	--	--	--	--	25	25	50

Lab Objectives: Students will be able to learn.

1. To familiarize students with real-world cyber-attack scenarios and threat intelligence reports.
2. To design and understand the Cyber Threat Intelligence (CTI) lifecycle workflow.
3. To implement supervised and unsupervised machine learning algorithms for cyber threat detection.
4. To apply data preprocessing and feature extraction techniques on cybersecurity datasets.
5. To provide hands-on experience with Threat Intelligence Platforms and OSINT tools.
6. To introduce emerging technologies such as blockchain for secure threat intelligence sharing.

Lab Outcomes: Students will be able to achieve the outcome.

1. Analyze cyber-attack case studies and interpret threat intelligence reports.
2. Create a CTI lifecycle model for a given organizational environment.
3. Develop ML-based models for phishing detection, intrusion detection, and anomaly detection.
4. Perform data cleaning, normalization, and feature extraction on security datasets.
5. Use Threat Intelligence Platforms and OSINT tools to collect and correlate threat information.
6. Demonstrate blockchain-based approaches for secure threat intelligence sharing.

List of Experiments:

Week No	List of Experiments	Hrs
01	Study and analysis of recent cyber-attack case studies and threat reports.	02
02	Creation of CTI lifecycle workflow for a sample organization.	02
03	Implementation of Naïve Bayes classifier for phishing/spam detection.	02
04	Unsupervised learning using K-Means clustering for anomaly detection.	02
05	Intrusion detection using Random Forest / SVM.	02
06	Data cleaning and normalization on a cybersecurity dataset.	02
07	Feature extraction from log files	02

08	Hands-on with Threat Intelligence Platform (MISP / OpenCTI).	02
09	Collection of OSINT data using open-source tools.	02
10	Demonstration of blockchain-based threat intelligence sharing.	02

Assessment:

Term Work: Term Work shall consist of 10 practicals based on the above list.

Internal Practical Exam: Conduct an internal practical exam after completing the first three modules of the course to assess and ensure the learner's understanding.

Term Work Marks: 25 Marks (Total marks) = 10 Marks (Experiment) + 10 Marks (Internal Practical Exam) + 5 Marks (Attendance)

Practical& Oral Exam: An Oral & Practical exam will be held based on the above syllabus.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEL6012	Mobile and Wireless Security Lab	-	2	-	-	1	-	1

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Practical/ Oral	Total
		Internal assessment (IAT)			End Sem. Exam			
		IAT- I	IAT-II	IAT-I + IAT-II (Total)				
PEL6012	Mobile and Wireless Security Lab	--	--	--	--	25	25	50

Lab Objectives: Students will be able to learn.

1. Understand and configure wireless and mobile network architectures and analyze their communication behavior.
2. Identify vulnerabilities and security threats in wireless local area networks.
3. Apply appropriate security mechanisms to protect WLANs and mobile communication systems.
4. Examine and evaluate the security architecture of Android and iOS mobile platforms.
5. Investigate mobile malware, attacks, and security breaches using analysis tools.
6. Implement and test security mechanisms for IoT devices and 5G-based mobile networks.

Lab Outcomes: Students will be able to achieve the outcome.

1. Configure and analyze wireless and mobile networks using simulation and real-world tools. (LO1)
2. Identify and exploit vulnerabilities in WLANs to evaluate the security posture of wireless networks (LO2)
3. Apply WLAN and mobile security mechanisms such as authentication, encryption, and secure tunneling (LO3)
4. Analyze the security architecture and protection mechanisms of Android and iOS mobile operating systems (LO4)
5. Investigate mobile malware, phishing, and cyberattacks using security analysis tools. (LO5)
6. Implement and evaluate security solutions for IoT devices and 5G-based communication systems. (LO6)

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	LO Mapping
1	Study of Wireless & Mobile Network Architecture	To study and simulate the architecture of wireless and mobile networks including access points, mobile nodes, and communication links using network simulation tools.	LO1
2	Wi-Fi Network Setup and Analysis	To configure a Wi-Fi network and analyze wireless traffic to understand connectivity, bandwidth, and security behaviour.	LO1
3	OSI Layer Mapping in WLAN	To capture and analyze WLAN packets and map the data flow across different OSI layers using a packet analyzer.	LO1

4	Detecting WLAN Vulnerabilities	To identify security weaknesses in wireless networks such as open networks, weak encryption, and misconfigured access points.	LO2
5	Rogue Access Point & Evil Twin Attack	To demonstrate the creation of a rogue access point and analyze how evil twin attacks compromise wireless user security.	LO2
6	Packet Sniffing & Man-in-the-Middle (MITM) in Wi-Fi	To capture wireless packets and demonstrate man-in-the-middle attacks to study information leakage in Wi-Fi networks.	LO2
7	WPA2 / WPA3 Security Testing	To test the strength of WPA2 and WPA3 encryption mechanisms by capturing and analyzing authentication handshakes.	LO3
8	Implementing 802.1X & RADIUS Authentication	To configure and test enterprise-level authentication for wireless networks using 802.1X and RADIUS server.	LO3
9	VPN & VLAN Security on WLAN	To implement VPN and VLAN mechanisms in a wireless network to ensure secure communication and network segmentation.	LO3
10	Android Device Security Analysis	To analyze the security architecture of Android devices and evaluate system-level protections.	LO4
11	Mobile App Permission & Sandbox Analysis	To examine mobile application permissions and sandboxing mechanisms to evaluate application-level security.	LO4
12	Mobile Malware Detection	To analyze mobile applications for malware and security threats using automated security analysis tools.	LO5
13	Device Fingerprinting	To identify and analyze unique device characteristics used for fingerprinting and tracking mobile devices.	LO5
14	IoT Device Security Testing	To evaluate security vulnerabilities in IoT devices by analyzing wireless communication and data transmission.	LO6

List of Experiments:

Sr. No.	List of Experiments	LO Mapping
1	To study the architecture of wireless and mobile networks including access points, mobile nodes, and communication links.	**LO1**
2	Simulation of wireless network topology to observe communication between multiple wireless devices and an access point.	**LO1**
3	To configure a basic Wi-Fi network and analyze connectivity between wireless clients.	**LO1**
4	Monitoring and analysis of wireless network traffic and bandwidth usage using Wireshark.	**LO2**
5	Capturing WLAN packets and mapping data flow across different layers of the OSI model.	**LO2**
6	Detection of wireless network vulnerabilities such as open authentication, weak encryption, and misconfigured access points.	**LO2**
7	Identification and analysis of rogue access points in a wireless network environment.	**LO3**
8	Demonstration of an Evil Twin attack by creating a fake access point and observing user connections.	**LO3**
9	Packet sniffing in Wi-Fi networks to capture and analyze wireless communication.	**LO3**

10	Demonstration of a Man-in-the-Middle (MITM) attack in Wi-Fi networks to study information interception.	**LO4**
11	Capturing and analyzing WPA2/WPA3 authentication handshakes using Aircrack-ng and Wireshark.	**LO4**
12	To analyze mobile applications for malware and security threats using automated security analysis tools.	**LO5**
13	Implementation of VPN and VLAN mechanisms to secure wireless communication and enable network segmentation.	**LO5**
14	Analysis of Android device security architecture and system-level protections using MobSF.	**LO6**
15	Examination of mobile application permissions, sandboxing mechanisms, and malware detection using automated mobile security analysis tools.	**LO6**

Text Books:

1. William Stallings, Wireless Communications and Networks, 2nd ed. Upper Saddle River, NJ, USA: Pearson Prentice Hall, 2005.
2. James F. Kurose and Keith W. Ross, Computer Networking: A Top-Down Approach, 8th ed. Hoboken, NJ, USA: Pearson, 2022.
3. William Stallings, Network Security Essentials: Applications and Standards, 6th ed. Boston, MA, USA: Pearson, 2017.
4. Joshua J. Drake, Zach Lanier, Collin Mulliner, Pau Oliva Fora, and Stephen A. Ridley, Android Hacker's Handbook. Indianapolis, IN, USA: Wiley, 2014.

Reference Books:

1. Johnny Cache, Joshua Wright, and Vincent Liu, Hacking Exposed Wireless: Wireless Security Secrets and Solutions, 2nd ed. New York, NY, USA: McGraw-Hill, 2010.
2. Laura Chappell, Wireshark Network Analysis. Elmwood Park, CA, USA: Chappell University, 2012.
3. Chris Sanders, Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems, 3rd ed. San Francisco, CA, USA: No Starch Press, 2017.
4. Himanshu Dwivedi, Chris Clark, and David Thiel, Mobile Application Security. New York, NY, USA: McGraw-Hill, 2010.
5. Srinivasa Rao Kotapati, Security in 5G Networks. Hoboken, NJ, USA: Wiley, 2021.

Online References:

1. https://www.wireshark.org/docs/wsug_html_chunked/
2. https://www.aircrack-ng.org/doku.php?id=getting_started
3. https://www.aircrack-ng.org/doku.php?id=cracking_wpa
4. https://owasp.org/www-project-mobile-security-testing-guide/latest/
5. https://mobsf.github.io/docs/

Assessment:

Term Work: Term Work shall consist of 10 practicals based on the above list.

Internal Practical Exam: Conduct an internal practical exam after completing the first three modules of the course to assess and ensure the learner's understanding.

Term Work Marks: 25 Marks (Total marks) = 10 Marks (Experiment) + 10 Marks (Internal Practical Exam) + 5 Marks (Attendance)

Practical& Oral Exam: An Oral & Practical exam will be held based on the above syllabus.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEL6013	Cyber Security and laws Lab	3	--	-	3	-	-	3

Course Code	Course Name	Examination Scheme						
		Theory Marks						
		Internal assessment (IAT)			End Sem. Exam	Term Work	Practical/ Oral	Tot
		IAT- I	IAT-II	IAT-I + IAT-II (Total)				
PEL6013	Cyber Security and laws Lab	--	--	--	--	25	25	50

Lab Objectives: Students will be able to learn.

1. To study the Information Technology Act of India.
2. To understand the importance and need of Cyber Security.
3. To learn and implement Offensive Cyber Security tools.
4. To learn and implement Defensive Cyber Security tools.
5. To perform security testing of Web Applications using appropriate tools.

Lab Outcomes: Students will be able to achieve the outcome.

1. Describe the Information Technology Act of India.
2. Explain fundamental Cyber Security concepts.
3. Demonstrate the use of Offensive Cyber Security tools.
4. Demonstrate the use of Defensive Cyber Security tools.
5. Perform security testing of Web Applications using appropriate tools.

List of Experiments:

Week No	List of Experiments	Hrs
01	Study of the Information Technology Act of India, including cyber crimes, penalties, and legal provisions.	02
02	Study of the importance, scope, and need of Cyber Security with reference to recent cyber incidents and vulnerabilities.	02
03	Hands-on study of offensive cyber security tools used for reconnaissance, scanning, and vulnerability identification.	02
04	Practical implementation of vulnerability scanning tools to identify security loopholes in systems and networks.	02
05	Security testing of web applications using OWASP Top 10 vulnerabilities and open-source security testing tools.	02
06	Study and implementation of defensive cyber security tools such as firewalls and intrusion prevention mechanisms.	02
07	Hands-on with Security Information and Event Management (SIEM) tools for log monitoring and incident detection.	02
08	Study and use of Open Source Intelligence (OSINT) tools for information gathering and cyber threat analysis.	02

09	Password security analysis using password strength checking, management, recovery, and attack tools.	02
10	Study of cyber security frameworks, secure operating systems, and reporting procedures to government cyber security agencies.	02

eferences

1. Awesome Security – https://github.com/sbilly/awesome-security
2. Open Web Application Security Project (OWASP) – https://owasp.org/
3. Indian Computer Emergency Response Team (CERT-In) – https://www.cert-in.org.in/
4. Kali Linux Tools Listing – https://tools.kali.org/tools-listing
5. National Cyber Crime Reporting Portal – https://cybercrime.gov.in/

Assessment:

Term Work: Term Work shall consist of 10 practicals based on the above list.

Internal Practical Exam: Conduct an internal practical exam after completing the first three modules of the course to assess and ensure the learner's understanding.

Term Work Marks: 25 Marks (Total marks) = 10 Marks (Experiment) + 10 Marks (Internal Practical Exam) + 5 Marks (Attendance)

Practical& Oral Exam: An Oral & Practical exam will be held based on the above syllabus.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEL6014	Cloud and Web Security Lab	-	2	-	-	1	-	1

Course Code	Course Name	Examination Scheme						
		Theory Marks						
		Internal assessment (IAT)			End Sem. Exam	Term Work	Practical / Oral	Total
		IAT-I	IAT-II	IAT-I + IAT-II (Total)				
PEL6014	Cloud and Web Security Lab	--	--	--	--	25	25	50

Lab Objectives: Students will be able to learn.

1. To familiarize with cloud platforms and basic cloud security configurations.
2. To implement identity, access control, and data security mechanisms in cloud environments.
3. To perform monitoring, logging, and compliance checks in cloud systems.
4. To understand and demonstrate common web security vulnerabilities.
5. To analyze and mitigate advanced web application security attacks.
6. To apply cloud and web security concepts through hands-on experiments and case studies.

Lab Outcomes: Students will be able to achieve the outcome.

1. Configure basic cloud services and identify security risks in cloud environments.
2. Implement IAM policies and data protection techniques in cloud platforms.
3. Perform cloud security monitoring, logging, and compliance verification.
4. Understand common client-side web vulnerabilities and their mitigation.
5. Analyze server-side web attacks and apply secure coding practices.
6. Design and evaluate secure cloud and web application solutions.

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hrs	LO Mapping
I	Cloud Environment Setup and Basic Security	Introduction to cloud lab environment, creating and configuring a cloud account (AWS/Azure/GCP – free tier), understanding cloud console, setting up virtual machines, basic network security groups, introduction to shared responsibility model.	4	LO1
II	Identity, Access, and Data Security in Cloud	Implementation of IAM users, roles, and policies, enforcing least privilege, enabling MFA, configuring secure storage, encryption at rest and in transit, key management basics, backup and recovery demonstration.	4	LO2

III	Cloud Monitoring, Logging, and Compliance	Cloud monitoring tools, enabling logs and alerts, basic intrusion detection concepts, vulnerability scanning overview, compliance checklist mapping with NIST/CSA guidelines.	4	LO3
IV	Web Security Fundamentals and Client-Side Attacks	Understanding web application architecture, demonstration of client-side attacks such as XSS and CSRF using test applications, browser security controls, mitigation techniques.	4	LO4
V	Server-Side Web Attacks and Secure Development	SQL injection, authentication flaws, session hijacking, use of input validation, prepared statements, secure authentication mechanisms, overview of OWASP Top 10.	4	LO5
VI	Integrated Applications and Case Studies	Securing cloud-hosted web applications, API security basics, vulnerability assessment using tools, analysis of real-world cloud and web security incidents, mini case study.	4	LO6

List of Experiments:

Week No	List of Experiments	Hrs
01	Study of Cloud Computing Models and Shared Responsibility Model	02
02	Identity and Access Management (IAM): Managing users, groups, roles, and policies to control access. (Using Resource-Based Policies to Secure an S3 Bucket)	02
03	Data Protection: Encryption techniques, key management, and data protection at rest and in transit. (Encrypting Data at Rest by Using AWS KMS)	02
04	Monitoring and Logging: Using AWS tools to audit and monitor for threats. (Monitoring and Alerting with CloudTrail and CloudWatch)	02
05	Study of Web Application Architecture and Threat Surface: Analyze a sample web application architecture and identify potential security risks using OWASP Top 10.	02
06	API Security Analysis and Testing (Open-Source Tools): Analyze common API security vulnerabilities using safe and controlled tools.	02
07	Secure Coding Practices for Web Applications: Implement input validation, authentication checks, and session handling in a simple demo application.	02
08	Web Security Testing Tools: Study and Demonstration: Study of tools such as OWASP ZAP/Burp Suite (Community Edition) for passive scanning and report analysis.	02
09	Case Study: Analysis of a real-world cloud or web security incident and proposal of preventive security architecture.	02
10	Mini Project: Design and Implement a Secure Cloud-Hosted Web Application	02

Assessment:Term Work: Term Work shall consist of 10 practicals based on the above list.
Internal Practical Exam: Conduct an internal practical exam after completing the first three modules of the course to assess and ensure the learner's understanding.

Term Work Marks: 25 Marks (Total marks) = 10 Marks (Experiment) + 10 Marks (Internal Practical Exam) + 5 Marks (Attendance)

Practical& Oral Exam: An Oral & Practical exam will be held based on the above syllabus.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEL6021	IoT Gateways and Middleware Lab	3	--	-	3	-	-	3

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Practical / Oral	Total
		Internal assessment (IAT)			End Sem. Exam			
		IAT-I	IAT-II	IAT-I + IAT-II (Total)				
PEL6021	IoT Gateways and Middleware Lab	--	--	--	--	25	25	50

Lab Objectives: Students will be able to learn.

1. Understand IoT device–gateway–cloud architecture and data flow.
2. Configure IoT gateways and implement communication using standard IoT protocols.
3. Develop gateway-level services such as protocol translation, filtering, and aggregation.
4. Deploy and configure middleware services for device management and data handling.
5. Implement cybersecurity mechanisms for IoT gateways and middleware.
6. Integrate blockchain with IoT systems for secure data storage and device identity.
7. Design and implement application-oriented IoT gateway and middleware solutions.

Lab Outcomes: Students will be able to achieve the outcome.

1. **LO1:** Configure IoT devices and gateways and demonstrate end-to-end connectivity.
2. **LO2:** Implement IoT communication protocols and messaging models.
3. **LO3:** Develop gateway functionalities such as protocol translation and edge processing.
4. **LO4:** Deploy and configure middleware services for messaging and device management.
5. **LO5:** Apply cybersecurity techniques to secure IoT gateway and middleware systems.
6. **LO6:** Integrate blockchain with IoT systems and develop application-oriented solutions.

DETAILED SYLLABUS:

Sr. No.	Module	Detailed Content	Hrs	LO Mapping
0	Prerequisite	Basics of C/Python, networking fundamentals, basic Linux commands.	01	--
1	Introduction to IoT Gateway & Middleware	IoT ecosystem, device–gateway–cloud architecture, role of gateway and middleware	03	LO1

2	IoT Communication & Connectivity	MQTT, CoAP, HTTP/REST, TCP/UDP, message exchange patterns.	04	LO2
3	Gateway Architecture & Design	Hardware & software architecture, protocol translation, data aggregation, edge intelligence	05	LO3
4	IoT Middleware & Cybersecurity	Middleware services, device management, IAM, authentication, TLS/DTLS, cyber attacks	05	LO4, LO5
5	Blockchain, Edge–Cloud Integration & Security	Blockchain for IoT, secure data sharing, edge–cloud integration, encryption, interoperability	04	LO6
6	IoT Gateway & Middleware Applications	Smart home, industrial IoT, healthcare, agriculture, minI project	04	LO6

List of Experiments:

Week No	List of Experiments	Hrs
01	Install and configure IoT development environment: Raspberry Pi/ESP32, OS, Node-RED, MQTT broker.	02
02	Establish device–gateway–cloud connectivity and visualize sensor data.	02
03	Implement MQTT publish–subscribe communication between device and gateway.	02
04	Implement secure MQTT communication using TLS certificates.	02
05	Perform protocol translation at gateway (HTTP ↔ MQTT).	02
06	Implement edge data filtering and aggregation at gateway.	02
07	Configure middleware for device registration and management.	02
08	Implement authentication and authorization for IoT devices using tokens/keys.	02
09	Integrate blockchain to store IoT data hash or device identity.	02
10	Mini Project: Design and implement secure IoT gateway & middleware application (smart home / agriculture / industry).	02

Assessment:

Term Work: Term Work shall consist of 10 practicals based on the above list.

Internal Practical Exam: Conduct an internal practical exam after completing the first three modules of the course to assess and ensure the learner's understanding.

Term Work Marks: 25 Marks (Total marks) = 10 Marks (Experiment) + 10 Marks (Internal Practical Exam) + 5 Marks (Attendance)

Practical& Oral Exam: An Oral & Practical exam will be held based on the above syllabus.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEL6022	Data Privacy and Protection Techniques Lab	-	2	-	-	1	-	1

Course Code	Course Name	Examination Scheme						
		Theory Marks						
		Internal assessment (IAT)			End Sem. Exam	Term Work	Practical/ Oral	Total
		IAT-I	IAT -II	IAT-I + IAT-II (Total)				
PEL6022	Data Privacy and Protection Techniques Lab	--	--	--	--	25	25	50

Lab Objectives: Students will be able to learn.

1. To understand the fundamental concepts of data privacy and data protection.
2. To analyze privacy risks present in real-world systems and datasets.
3. To implement basic security and privacy-preserving techniques for protecting sensitive information.
4. To develop awareness of ethical, legal, and regulatory aspects related to data privacy and protection.
5. To apply data anonymization techniques such as k-Anonymity, l-Diversity, and t-Closeness for privacy-preserving data analysis.
6. To design privacy protection strategies for IoT-based systems such as smart home, smart healthcare, or smart city applications.

Lab Outcomes: Students will be able to achieve the outcome.

1. LO1: Identify and classify IoT data types and privacy-sensitive attributes, and analyze privacy risks in IoT sensor datasets.
2. LO2: Apply data anonymization techniques such as k-Anonymity, l-Diversity, and t-Closeness on real-world datasets.
3. LO3: Implement anonymization transformation methods including data generalization, suppression, and perturbation for privacy protection.
4. LO4: Evaluate anonymized datasets by comparing different anonymization models and simulating re-identification attacks.
5. LO5: Implement privacy-preserving techniques such as synthetic data generation, tokenization, encryption, and privacy-preserving data mining.
6. LO6: Design and develop a privacy protection strategy for an IoT-based system (e.g., Smart Home, Smart Healthcare, or Smart City).

Detailed Syllabus:

Sr. No.	Module	Detailed Content	Hrs	LO Mapping
0	Prerequisite	Fundamentals of computer systems and operating systems Basics of programming (C / C++ / Java / Python) Basic database concepts such as tables, records, and queries Fundamental concepts of computer networks and internet technologies Introduction to information security concepts including confidentiality, integrity, and availability Basic understanding of web applications and data usage Awareness of ethical practices and privacy principles in computing	01	--
1	Data Privacy Audit	Introduction to data privacy and personal data Types of sensitive and personal information Data lifecycle: collection, storage, processing, sharing Identifying privacy risks and vulnerabilities Audit tools and checklists Risk assessment techniques Preparing audit findings and recommendations	02	LO1, LO2
2	Privacy Impact Assessment	Concept of Privacy Impact Assessment Data flow diagrams Identifying stakeholders and data subjects Privacy risk identification methods Impact analysis on individuals Risk mitigation strategies Documentation of PIA report	03	LO1, LO2
3	Regulation Compliance	Overview of data protection laws (GDPR, DPDP Act) Rights of data subjects Roles of data controller and processor Lawful basis for data processing Consent management Data retention and deletion policies Compliance checklist and reporting	03	LO2, LO4
4	Cryptography	Introduction to cryptography Symmetric and asymmetric encryption Hashing algorithms (SHA, MD5) Digital signatures Key management concepts Hands-on implementation using programming tools Performance and security analysis	03	LO3

5	Anonymization Techniques	Need for data anonymization k-anonymity and l-diversity Differential privacy basics Data masking and pseudonymization Applying anonymization to datasets Measuring data utility vs privacy Result analysis	03	LO3
6	Privacy Policy Analysis:	Purpose of privacy policies Legal and ethical requirements Key elements of a privacy policy Policy comparison techniques Identifying gaps and ambiguities Recommendations for improvement Drafting a revised privacy policy	03	LO1, LO4
7	Privacy-Enhancing Technologies	Introduction to PETs Virtual Private Networks (VPNs) Tor network and anonymity Secure messaging applications Browser privacy tools Advantages and limitations of PETs Practical evaluation and comparison	03	LO2, LO3
8	Privacy Breach Response Plan	Types of data breaches Breach detection and identification Incident response lifecycle Roles and responsibilities Communication with stakeholders Legal and regulatory reporting Post-incident review	03	LO1,LO2,LO4
9	Ethical Considerations	Ethics in information security Privacy vs security trade-offs Consent and transparency Bias and discrimination in data use Impact on marginalized communities Responsible data handling practices Ethical decision-making frameworks	02	LO4
10	Case Studies	Case study methodology Famous privacy breaches Successful privacy protection models Root cause analysis Lessons learned	01	LO1,LO2,LO4

Text Books:

1. Nina Godbole, Sunit Belapure Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives Wiley India Pvt. Ltd.
1. Charles P. Pfleeger, Shari Lawrence Pfleeger Security in Computing Pearson Education.
2. William Stallings Cryptography and Network Security: Principles and Practice Pearson Education.
3. Deborah Russell, G.T. Gangemi Computer Security Basics O'Reilly Media.

References:

1. Ronald Leenes, Rosamunde van Brakel, and Serge Gutwirth: Data Protection and Privacy: The Age of Intelligent Machines, Hart Publishing, 2017.
2. Naavi: Personal Data Protection Act of India (PDPA 2020) : Be Aware, Be Ready and Be Compliant, 2020.

3. Ravinder Kumar Gaurav Goyal, The Right to Privacy in India: Concept and Evolution, Publisher: Lightning Source, 2016.

Online Resources:

Sr. No.	Website Name
1	https://wizape.com/English/Advanced-Data-Privacy-Techniques
2	https://onlinecourses.nptel.ac.in/noc25_cs116/preview
3	https://academy.riskpro.in/courses/privacy-impact-analysis
4	https://www.coursera.org/learn/northeastern-data-privacy/home/info

List of Experiments:

Week No.	List of Experiment	Hours
1	To understand and evaluate data privacy practices of an organization.	02
2	To assess privacy risks of a new system or technology.	02
3	To understand and implement data protection regulations.	02
4	To implement basic cryptographic techniques for data security.	02
5	To apply anonymization techniques to protect data privacy.	02
6	To analyze and evaluate privacy policies of organizations.	02
7	To study tools that enhance user privacy.	02
8	To design an effective data breach response strategy.	02
9	To understand ethical challenges in data privacy.	02
10	To analyze real-world data privacy cases.	02

Assessment:

Term Work: Term Work shall consist of 10 practicals based on the above list.

Internal Practical Exam: Conduct an internal practical exam after completing the first three modules of the course to assess and ensure the learner's understanding.

Term Work Marks: 25 Marks (Total marks) = 10 Marks (Experiment) + 10 Marks (Internal Practical Exam) + 5 Marks (Attendance)

Practical& Oral Exam: An Oral & Practical exam will be held based on the above syllabus.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEL6023	Information Security Management Systems Lab	-	2	-	-	1	-	1

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Practical/ Oral	Total
		Internal assessment (IAT)			End Sem. Exam			
		IAT- I	IAT-II	IAT-I + IAT-II (Total)				
PEL6023	Information Security Management Systems Lab	--	--	--	--	25	25	50

Lab Objectives: Students will be able to learn.

1. Familiarize students with security tools and techniques used in network, web, and system security.
2. Ability to implement symmetric and asymmetric key encryption techniques
3. Enable students to understand and analyze security goals
4. Provide hands-on experience in implementing classical and modern cryptographic algorithms.
5. Provide practical exposure to digital signature algorithms for authentication and non-repudiation.
6. Enable students to implement message authentication mechanisms such as Message Authentication Codes (MAC).

Lab Outcomes: Students will be able to achieve the outcome.

1. **LO1:** Demonstrate understanding of information security goals by analyzing common web security attacks.
2. **LO2:** Implement classical encryption techniques such as substitution and transposition ciphers.
3. **LO3:** Perform encryption and decryption using modern symmetric key algorithms and block cipher modes of operation.
4. **LO4:** Implement asymmetric key cryptographic techniques for secure data transmission.
5. **LO5:** Design and implement digital signature algorithms to ensure authentication, integrity, non-repudiation.
6. **LO6:** Implement message authentication mechanisms using MAC to verify data integrity and authenticity.

Detailed Syllabus:

Sr. No.	Module	Detailed Content	Hrs	LO Mapping
0	Prerequisite	Computer & network literacy, Programming ability, Mathematical foundation for cryptography, Basic OS and security awareness	01	--
1	Performing web security attacks	Implementation of security attacks (such as SQL injection, cross-site scripting, etc.) to understand and analyze security goals like confidentiality, integrity, and availability	04	LO2

2	Implementation of encryption and decryption techniques	Implement Caesar cipher and monoalphabetic cipher, to understand classical symmetric key cryptography.	04	LO1
3	Performing block cipher encryption and decryption	Demonstrating the working of modern symmetric key algorithms and their modes of operation.	04	LO3
4	Implementation of a Digital Signature Algorithm	To ensure authentication, integrity, and non-repudiation of messages.	04	LO4, LO6
5	Performing asymmetric key encryption and decryption	Using public key cryptographic techniques.	05	LO4
6	Implementation of Message Authentication Codes (MAC)	To verify message integrity and authenticity.	05	LO5

Textbooks

1. William Stallings, "Cryptography and Network Security: Principles and Practice", 8th Edition, Pearson
2. William Stallings, "Network Security Essentials: Applications and Standards", 6th Edition, Pearson
3. Behrouz A. Forouzan, "Cryptography and Network Security", 2nd Edition, McGraw Hill
4. Wade Trappe & Lawrence C. Washington, "Introduction to Cryptography with Coding Theory", 2nd Edition, Pearson

References:

1. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press
2. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 20th Anniversary Edition, Wiley
3. Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, "Cryptography Engineering: Design Principles and Practical Applications", Wiley
4. Andrew Hoffman, "Web Application Security: Exploitation and Countermeasures for Modern Web Applications", CRC Press
5. Charlie Kaufman, Radia Perlman, Mike Speciner, "Network Security: Private Communication in a Public World", 2nd Edition, Pearson

Online Resources

Sr. No.	Website Name
1	https://www.classcentral.com/course/swayam-information-security-91683?utm_source=chatgpt.com
2	https://www.classcentral.com/course/youtube-computer-cryptography-and-network-security-47628?utm_source=chatgpt.com
3	https://www.udemy.com/course/cryptography-security-protect-data-from-cyber-threats/?utm_source=chatgpt.com
4	https://wizape.com/English/Cryptography-and-Secure-Communications?utm_source=chatgpt.com

List of Experiments:

Week No.	List of Experiment	Hours
1	Study of information security tools and security concepts	02
2	Performing web security attacks to understand security goals.	02
3	Implementation of Caesar cipher	02
4	Implementation of monoalphabetic substitution Implementation of monoalphabetic cipher	02
5	Implementation of transposition cipher	02
6	Implementation of block cipher encryption (DES/AES)	02
7	Implementation of block cipher modes (ECB, CBC)	02
8	Implementation of asymmetric key encryption (RSA)	02
9	Implementation of digital signature algorithm	02
10	Implementation of Message Authentication Code (MAC)	02

Assessment:

Term Work: Term Work shall consist of 10 practicals based on the above list.

Term Work Marks: 25 Marks (Total marks) = 10 Marks (Experiment) + 10 Marks (Internal Practical Exam) + 5 Marks (Attendance)

Practical& Oral Exam: An Oral & Practical exam will be held based on the above syllabus.

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
PEL6024	Web Application Security Lab	3	--	-	3	-	-	3

Course Code	Course Name	Examination Scheme						
		Theory Marks				Term Work	Practical/ Oral	Total
		Internal assessment (IAT)			End Sem. Exam			
		IAT- I	IAT-II	IAT-I + IAT-II (Total)				
PEL6024	Web Application Security Lab	--	--	--	--	25	25	50

Lab Objectives: Students will be able to learn.

1. Understand web application architecture, request–response flow, and security attack surfaces.
2. Configure development environments and implement basic secure web application functionalities.
3. Develop secure authentication, authorization, and session management mechanisms.
4. Implement secure database interactions and input validation techniques to prevent common vulnerabilities.
5. Perform vulnerability assessment and penetration testing using standard web security tools.
6. Apply cryptographic techniques and secure communication protocols in web applications and APIs.
7. Design and implement application-oriented secure web solutions incorporating industry security practices.

Lab Outcomes: Students will be able to achieve the outcome.

1. LO1: Configure web application environments and demonstrate client–server communication.
2. LO2: Implement secure authentication, authorization, and session management mechanisms.
3. LO3: Develop secure database interactions and input validation to prevent common web vulnerabilities.
4. LO4: Perform vulnerability assessment and penetration testing using web security tools.
5. LO5: Apply cryptographic techniques and secure communication for protecting web applications and APIs.
6. LO6: Develop application-oriented secure web solutions using industry security practices.

List of Experiments:

Week No	List of Experiments	Hrs
01	Study of Web Application Architecture and HTTP Request–Response Communication using browser developer tools and packet analysis.	02
02	Implementation of secure user authentication using password hashing and role-based authorization.	02
03	Demonstration of SQL Injection vulnerability and its prevention using prepared statements.	02
04	Demonstration and mitigation of Cross-Site Scripting (XSS) using input validation and output encoding.	02
05	Implementation of secure session management and protection against Cross-Site Request Forgery (CSRF).	02
06	Design and implementation of a secure REST API with token-based	02

	authentication using JSON Web Tokens (JWT).	
07	Vulnerability assessment of a web application using automated security testing tools.	02
08	Analysis of secure communication mechanisms using hashing and encryption techniques for protecting data transmission.	02
09	Implementation of secure IoT device communication with a web interface using MQTT/HTTP protocols.	02
10	Case study analysis of a real-world web or IoT security incident and identification of vulnerabilities and defense mechanisms.	02

Assessment:

Term Work: Term Work shall consist of 10 practicals based on the above list.

Internal Practical Exam: Conduct an internal practical exam after completing the first three modules of the course to assess and ensure the learner's understanding.

Term Work Marks: 25 Marks (Total marks) = 10 Marks (Experiment) + 10 Marks (Internal Practical Exam) + 5 Marks (Attendance)

Practical& Oral Exam: An Oral & Practical exam will be held based on the above syllabus.

Vertical - 4

VSEC

Innovation Lab (Mini Project)

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Practical	Tutorial	Total
2346411	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					
2346411	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/41c6fec2122dd47fdfaca31924647499
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

Indian Knowledge System

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Practical	Tutorial	Total
2346511	Indian Knowledge System	--	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	--	--	--	--	--	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 • 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.	10	CO1
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	10	CO2

		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 • 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	10	CO3

		• Measurement for Time Distance and Weight • Measurement of Time- An Illustration from Purana		
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, 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	10	CO4
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.	10	CO5

		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. • 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.	10	CO6

		• Exploration of Sanskrit digital dictionaries and Sanskrit reader tools. • Comparison of grammar rules and computer program rules.		

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 Temperament.	04
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 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.	04
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	01

	problem being addressed, the IKS principle used, and how the proposed solution can be useful in present-day society.	
08	Study the basic Sanskrit grammar concepts of sounds, words, roots, suffixes, 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.	01

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)

AEC

Course Code	Course Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Practical	Tutorial	Total
2346511	Professional Skill	--	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	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** • 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	8	CO1
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	4	CO2

		• **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		
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 • 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)	8	CO3

		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 • 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	4	CO6

		• 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 (Examinational 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)

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
Faculty of Science & Technology