Bansilal Ramnath Agarwal Charitable Trust's
VISHWAKARMA INSTITUTE OF TECHNOLOGY, PUNE – 37
(An Autonomous Institute Affiliated to Savitribai Phule Pune University)
Department of Computer Engineering (Software Engineering)

Structure & Syllabus of

Double Minor Courses in Network Security

Offered by

Computer Engineering (Software Engineering)

With Effect from Academic Year 2025-26

College Vision and Mission

Vision:

To be a globally acclaimed Institute in Technical Education and Research for holistic socio-economic development

Mission:

- To ensure that 100% of students are employable and employed in industry, higher studies, entrepreneurship, civil or defence services, government jobs, and other areas like sports and arts.
- To strengthen Academic Practices in Curriculum, Pedagogy, Assessment and Faculty Competence.
- To Promote Research Culture among Students and Faculty through Projects and Consultancy
- To make students Socially Responsible Citizens

Department Vision and Mission

Vision:

- Empowering Industry through Comprehensive Software Engineering Services to Achieve Excellence.

Mission:

- To produce industry-ready software engineering graduate with a blend of technical expertise and ethical responsibility
- To provide software engineering students with the utmost quality in developing technical, social, innovative, and entrepreneurial skills

Knowledge and Attitude Profile (WK)

- WK1: A systematic, theory-based understanding of the natural sciences applicable to the discipline and awareness of relevant social sciences.
- WK2: Conceptually-based mathematics, numerical analysis, data analysis, statistics and formal aspects of computer and information science to support detailed analysis and modelling applicable to the discipline.
- WK3: A systematic, theory-based formulation of engineering fundamentals required in the engineering discipline.
- WK4: Engineering specialist knowledge that provides theoretical frameworks and bodies of knowledge for the accepted practice areas in the engineering discipline; much is at the forefront of the discipline.
- WK5: Knowledge, including efficient resource use, environmental impacts, whole-life cost, reuse of resources, net zero carbon, and similar concepts, that supports engineering design and operations in a practice area.
- WK6: Knowledge of engineering practice (technology) in the practice areas in the engineering discipline.
- WK7: Knowledge of the role of engineering in society and identified issues in engineering practice in the discipline, such as the professional responsibility of an engineer to public safety and sustainable development.
- WK8: Engagement with selected knowledge in the current research literature of the discipline, awareness of the power of critical thinking and creative approaches to evaluate emerging issues.
- WK9: Ethics, inclusive behavior and conduct. Knowledge of professional ethics, responsibilities, and norms of engineering practice. Awareness of the need for diversity by reason of ethnicity, gender, age, physical ability etc. with mutual understanding and respect, and of inclusive attitudes.

Program Outcomes (POs)

- PO1: Engineering Knowledge: Apply knowledge of mathematics, natural science, computing, engineering fundamentals and an engineering specialization as specified in WK1 to WK4 respectively to develop to the solution of complex engineering problems.
- PO2: Problem Analysis: Identify, formulate, review research literature and analyze complex engineering problems reaching substantiated conclusions with consideration for sustainable development. (WK1 to WK4)
- PO3: Design/Development of Solutions: Design creative solutions for complex engineering problems and design/develop systems/components/processes to meet identified needs with consideration for the public health and safety, whole-life cost, net zero carbon, culture, society and environment as required. (WK5)
- PO4: Conduct Investigations of Complex Problems: Conduct investigations of complex engineering problems using research-based knowledge including design of experiments, modelling, analysis & interpretation of data to provide valid conclusions. (WK8).
- PO5: Engineering Tool Usage: Create, select and apply appropriate techniques, resources and modern engineering & IT tools, including prediction and modelling recognizing their limitations to solve complex engineering problems. (WK2 and WK6)
- PO6: The Engineer and The World: Analyze and evaluate societal and environmental aspects while solving complex engineering problems for its impact on sustainability with reference to economy, health, safety, legal framework, culture and environment. (WK1, WK5, and WK7).
- PO7: Ethics: Apply ethical principles and commit to professional ethics, human values, diversity and inclusion; adhere to national & international laws. (WK9)
- PO8: Individual and Collaborative Team work: Function effectively as an individual, and as a member or leader in diverse/multi-disciplinary teams.
- PO9: Communication: Communicate effectively and inclusively within the engineering community and society at large, such as being able to comprehend and write effective reports and design documentation, make effective presentations considering cultural, language, and learning differences
- PO10: Project Management and Finance: Apply knowledge and understanding of engineering management principles and economic decision-making and apply these to one's own work, as a member and leader in a team, and to manage projects and in multidisciplinary environments.
- PO11: Life-Long Learning: Recognize the need for, and have the preparation and ability for i) independent and life-long learning ii) adaptability to new and emerging technologies and iii) critical thinking in the broadest context of technological change. (WK8)

Program Specific Outcomes (PSO)

- PSO 1 – Software Design & Development

  Analyze, design, and implement reliable, efficient, and scalable software solutions by applying software engineering principles, modern programming tools, and innovative methodologies to solve real-world problems.

- PSO 2 – Professional Growth & Innovation

  Demonstrate professionalism, ethics, effective communication, and teamwork, while engaging in lifelong learning, research, Industry and entrepreneurial activities to contribute to emerging areas.

CESEXXX: Double Minor in Network Security

Semester	Course Name	Teaching Scheme			Examination Scheme					Total	Credit
		Theory	Lab	Tut	CVV	CP	LAB CA	GD/ PPT/ HA	ESE		
III	Data Communication	2	2	-							3
IV	Information Security	2	2	-							3
V	Wireless & Mobile Networks	2	2	-							3
VI	Network Security	2	2	-							3
VII	Named Data Networking	2	4	-							4
VIII	Cyber Defense and Threat Intelligence	2	4	-							4

Course Code: Data Communication

Teaching Scheme	**Examination Scheme**
Credits: 3	CP: Marks
Lectures: 2 Hrs/week	GD/PPT/HA: Marks
Practical: 2 Hrs/week	MSE (W/O): Marks
Tutorial: - Hrs/week	ESE (W/O): Marks

Prerequisites:	
•	Basic knowledge of Engineering Mathematics, Computer Fundamentals.
Course Objectives:	
•	Understand fundamentals of analog and digital data, signals, transmission impairments, and data rate limits.
•	Learn modulation, multiplexing, and spread spectrum techniques used in data communication systems.
•	Study transmission media, switching techniques, and basic access technologies such as DSL.
•	Analyze error detection, correction methods, and data link layer protocols for reliable data communication.
Course Outcomes:	
	After completion of the course, student will be able to
1.	Analyze analog and digital signals, transmission impairments, and performance parameters.
2.	Apply modulation, multiplexing, and spread spectrum techniques in communication systems.
3.	Compare guided and unguided transmission media and switching techniques.
4.	Implement and evaluate error control techniques and data link layer protocols.

Section1:	**Topics/Contents**
Fundamentals of Signals: Analog and Digital: Analog and Digital Data, Analog and Digital Signals, Periodic and Non-periodic Signal Periodic Analog Signals: Sine Wave, Phase, Wavelength, Time and Frequency Domains, Composite Signals Bandwidth Digital Signals: Bit Rate, bit Length, Digital Signal as a Composite Analog Signal, Transmission of Digital Signals Transmission Impairment: Attenuation, Distortion, Noise Data Rate Limits: Noiseless Channel: Nyquist Bit Rate, Noisy Channel: Shannon Capacity	

Performance: Bandwidth, Throughput, Latency (delay)

Modulation and Multiplexing Technique:

Digital-to-digital Conversion: Line Coding, Line Coding Schemes, Block Coding, Scrambling, Analog to
digital Conversion: Pulse Code Modulation (PCM), Delta Modulation (DM), ADM Transmission modes:
parallel transmission, serial transmission, Analog-to-analog Conversion: Amplitude Modulation, Frequency
Modulation, Phase Modulation, Multiplexing: Frequency-Division Multiplexing (FDM), WavelengthDivision Multiplexing Synchronous Time-Division Multiplexing, Statistical Time-Division Multiplexing
Spread Spectrum: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum.

Section2:	**Topics/Contents**

Transmission Media and Switching:

Guided Media: Twisted-Pair, Coaxial and Fiber-Optic Cable. Unguided Media: Radio Waves, Microwaves, Infrared. (RJ45, RJ11, BNC, SC/ST etc.) Circuit-switched Networks: Three Phases, Packet switching: Datagram networks, Virtual circuit networks Brief introduction of Digital Subscriber Line: ADSL, HDSL, SDSL, VDSL (DMT).

Error Control and Data Link Control:

Types of errors: Redundancy, detection versus correction, forward error correction versus retransmission,
Block coding: error detection, error correction, CRC, polynomial, checksum, hamming code, hamming distance DLC Services: Framing, Flow and error control DLL Protocols: Simple protocol, Stop n wait, Go back to N, Selective repeat HDLC Protocol: configurations and transfer modes, frames, control field.
Point to-point Protocol (PPP): Framing, Transition Phases, Multiplexing, Multilink PPP

Text Books: ***(As per IEEE format)***

1	**Behrouz A. Forouzan**, *Data Communications and Networking*, 5th Edition, McGraw-Hill Education.
2	**William Stallings**, *Data and Computer Communications*, 10th Edition, Pearson Education.

Reference Books: ***(As per IEEE format)***

1	**Andrew S. Tanenbaum**, *Computer Networks*, 5th Edition, Pearson Education.
2	**Leon-Garcia & Widjaja**, *Communication Networks*, McGraw-Hill.
3	**John G. Proakis**, *Digital Communications*, McGraw-Hill.

List of Practical's:

1. Study of analog and digital signals using simulation tools.

2. Generation and analysis of sine wave, frequency, phase, and bandwidth.
3. Implementation of line coding schemes (NRZ, RZ, Manchester, Differential Manchester).
4. Study of block coding and scrambling techniques.
5. Simulation of PCM, DM, and ADM techniques.
6. Performance analysis of parallel vs serial transmission.
7. Simulation of AM, FM, and PM modulation techniques.
8. Study and simulation of FDM and TDM multiplexing.
9. Implementation of FHSS and DSSS spread spectrum techniques.
10. Study of guided transmission media (UTP, coaxial, optical fiber) and connectors (RJ45, BNC, SC/ST).
11. Simulation of circuit switching and packet switching techniques.
12. Implementation of CRC and checksum for error detection.

CO-PO Mapping

CO	Program Outcomes (PO)											PSO	
CO/PO	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PSO1**	**PSO2**
CO1	3	3		2							2	2	
CO2	3	2	3		3						2	3	
CO3	3	3				1					2	2	
CO4	2	2	3	2	3			2	1	1	2	3	2
Average	2.75	2.5	3	2	3	1		2	1	1	2	2.5	2

Course Code: Information Security

Teaching Scheme	**Examination Scheme**
Credits: 3	CP: Marks
Lectures: 2 Hrs/week	GD/PPT/HA: Marks
Practical: 2 Hrs/week	MSE (W/O): Marks
Tutorial: - Hrs/week	ESE (W/O): Marks

Prerequisites:	
•	Computer Network, Data Communication
Course Objectives:	
•	To introduce fundamental concepts of information security and security goals for stored and transit data.
•	To understand authentication, authorization, access control, and secure data storage mechanisms.
•	To study cryptographic techniques and protocols used to secure data in transit.
•	To analyze and apply encryption, integrity, and authentication algorithms in real-world systems.
Course Outcomes:	
	After completion of the course, student will be able to
1.	Explain information security concepts, security goals, policies, standards, and risk scenario
2.	Apply authentication, authorization, and secure storage techniques to protect stored data.
3.	Analyze mechanisms and protocols used to secure data during transmission.
4.	Analyze information security governance, risk management practices, legal and ethical requirements, and emerging security challenges to support organizational security decision-making.

Section1:	**Topics/Contents**
Introduction: Definition and importance, securing two types of data 1. Stored data 2. Transit data, Security Goals: Confidentiality, Integrity, Availability, Security Policies and Standards: ISO 27001, risk scenarios **Securing Stored data:** User Authentication: Passwords, biometrics, third party, MFA, Authorization Models: Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Permission Management: File system permissions, access control lists (ACLs) in	

firewalls, Audit Logs and Monitoring, data backup recovery techniques, RAID, Data Sharding, encrypted File System	
Section2:	**Topics/Contents**
Securing Transit Data: Encryption, SSL, TLS, HTTPS, VPN, IPSec, Digital Signature, data integrity verification, wireless security protocols **Information Security Management and Emerging Trends** Information Security Governance and Management, Security policies, standards, procedures, and guidelines, Information Security Management System (ISMS) overview, Risk management process: asset identification, risk assessment, and risk treatment, Security audits and compliance requirements, Incident reporting and basic incident handling procedures, Insider threats and social engineering attacks, Data privacy concepts and regulations (overview of IT Act, GDPR), Security awareness and training programs, Emerging challenges in information security: Cloud data security (overview), IoT security issues, Mobile device security basics	

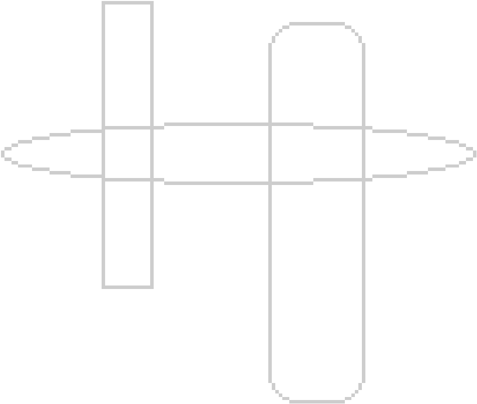
Text Books: ***(As per IEEE format)***	
1	W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th ed. Boston, MA, USA: Pearson Education, 2020. ISBN: 978-0135764039.
2	N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering*, Indianapolis, IN, USA: Wiley Publishing, 2010. ISBN: 978-0470474242.
Reference Books: ***(As per IEEE format)***	
1	D. Gollmann, *Computer Security*, 3rd ed. Hoboken, NJ, USA: Wiley, 2011. ISBN: 978-0470741153.
2	M. Bishop, *Computer Security: Art and Science*, 2nd ed. Boston, MA, USA: Addison-Wesley, 2018. ISBN: 978-0321712332.
3	J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed. Boca Raton, FL, USA: CRC Press, 2014. ISBN: 978-1466570269.

List of Practical's:

1. Study of CIA triad, ISO 27001, and security policies
2. Implementation of password hashing and MFA simulation
3. RBAC and ABAC implementation using sample applications
4. File system permissions, ACLs, and audit logging
5. Secure data storage using encryption and RAID concepts
6. SSL/TLS and HTTPS communication analysis using tools
7. VPN and IPSec configuration
8. Implementation of AES and RSA encryption algorithms
9. Diffie-Hellman key exchange implementations
10. Hashing and integrity verification using SHA-256 / SHA-3
11. Message Authentication Code (HMAC) implementation
12. Mini-project: Secure file transfer or secure storage system

CO-PO Mapping

CO	**Program Outcomes (PO)**											**PSO**	
CO/PO	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PSO1**	**PSO2**
CO1	3	2				2	1				2		2
CO2	3	2	3		3		1				2	3	
CO3	3	3		2	3						2	2	
CO4	2	2	3		3						2	3	
Average	2.5	2.25	3	2	3	2	1				2	2.75	2



Course Code: Network Security

Teaching Scheme	**Examination Scheme**
Credits: 3	CP: Marks
Lectures: 2 Hrs/week	GD/PPT/HA: Marks
Practical: 2 Hrs/week	MSE (W/O): Marks
Tutorial: - Hrs/week	ESE (W/O): Marks

Prerequisites:	
•	Data Communication, Computer Networks, Information Security
Course Objectives:	
•	To understand network-level security threats, vulnerabilities, and attack models in modern communication systems.
•	To study security mechanisms, protocols, and architectures for protecting network infrastructure and data in transit.
•	To analyze and apply cryptographic, authentication, and access control mechanisms in network environments.
•	To design and evaluate secure network solutions considering performance, scalability, and ethical issues.
Course Outcomes:	
	After completion of the course, student will be able to
1.	Explain network security concepts, threats, protocols, and architectures.
2.	Apply cryptographic and authentication mechanisms to secure network communication.
3.	Analyze secure network protocols and mechanisms such as TLS, IPSec, VPN, and wireless security.
4.	Design and evaluate secure network solutions using firewalls, IDS/IPS, and access control mechanisms.

Section1:	**Topics/Contents**

Introduction to Network Security

Network security fundamentals and objectives, Relationship between Data Communication, Information Security, and Network Security, Security threats, vulnerabilities, and attacks, Network security models and architectures, CIA triad in network context, Security policies, risk assessment, and compliance (ISO 27001 overview)

Cryptography for Network Security:

Review of cryptography for networks, Symmetric encryption: AES, DES (use in networks), Asymmetric encryption: RSA, ECC, Key management and distribution

Diffie–Hellman key exchange, Hash functions: SHA-256, SHA-3, MD5 (limitations) Message Authentication Codes (HMAC)	
Section2:	**Topics/Contents**
Secure Network Protocols: Transport-layer security: SSL, TLS, HTTPS, IP security: IPSec architecture, AH, ESP, modes, Virtual Private Networks (VPN): Site-to-site, Remote access, Digital signatures and certificates, Wireless security protocols: WEP, WPA, WPA2, WPA3 **Network Défense Mechanisms:** Firewalls: Packet filtering, stateful, application-level gateways, Access control lists (ACLs) and rule design, Intrusion Detection and Prevention Systems (IDS/IPS), Network monitoring, logging, and audit trails, Secure routing and switching concepts, Network security case studies	

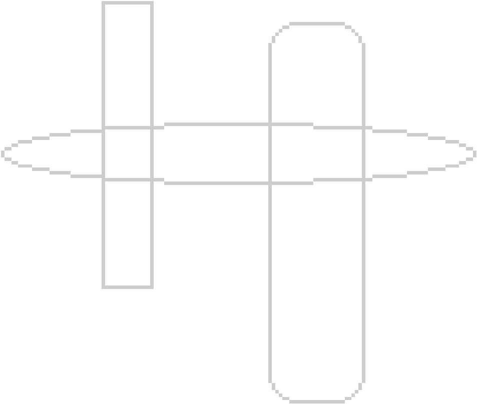
Text Books: ***(As per IEEE format)***	
1	W. Stallings, *Cryptography and Network Security: Principles and Practice,* 8th ed. Boston, MA, USA: Pearson Education, 2020. ISBN: 978-0135764039.
2	J. M. Kizza, *Guide to Computer Network Security*, 4th ed. Cham, Switzerland: Springer, 2020.
Reference Books: ***(As per IEEE format)***	
1	C. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World*, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2002.
2	D. Gollmann, *Computer Security*, 3rd ed. Hoboken, NJ, USA: Wiley, 2011.
3	B. Schneier, *Applied Cryptography*, 2nd ed. New York, NY, USA: Wiley, 2015.

List of Practical's:

1. Study basic network security concepts, threats, and the CIA triad.
2. Analyze security policies, risk scenarios, and ISO 27001 controls.
3. Implement symmetric encryption using AES for secure data transmission.
4. Implement asymmetric encryption and digital signature using RSA or ECC.
5. Simulate Diffie–Hellman key exchange for secure key generation.
6. Analyze secure communication using SSL/TLS and HTTPS.
7. Configure and evaluate VPN and IPSec for secure network communication.
8. Configure and analyze wireless security protocols (WPA2/WPA3).
9. Design and implement firewall rules and access control lists (ACLs).
10. Configure and analyze an Intrusion Detection System (IDS).
11. Perform network monitoring and security log analysis.
12. Develop a mini-project on secure network design or application.

CO-PO Mapping

CO	Program Outcomes (PO)											PSO	
CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	3	2				2	1				2		2
CO2	3	2	3		3						2	3	
CO3	3	3		2	3						2	2	
CO4	2	2	3	2	3		1	2	1	1	2	3	2
Average	2.75	2.5	3	2	3	2	1	2	1	1	2	2.75	2



Course Code: Wireless and Mobile Networks

Teaching Scheme	Examination Scheme
Credits: 3	CP: Marks
Lectures: 2 Hrs/week	GD/PPT/HA: Marks
Practical: 2 Hrs/week	MSE (W/O): Marks
Tutorial: - Hrs/week	ESE (W/O): Marks

Prerequisites:	
•	Data Communication, Computer Networks, Information Security
Course Objectives:	
•	To understand fundamentals of wireless communication and mobile networking technologies.
•	To study wireless transmission media, multiple access techniques, and wireless LAN standards.
•	To analyze mobility management, routing, and transport issues in mobile networks.
•	To understand security challenges and solutions in wireless and mobile networks.
Course Outcomes:	
	After completion of the course, student will be able to
1.	Explain wireless communication principles, transmission issues, and access techniques.
2.	Analyze WLAN, PAN, and cellular network architectures and protocols.
3.	Apply mobility management and routing mechanisms in mobile networks.
4.	Evaluate security challenges and solutions in wireless and mobile networks.

Section1:	**Topics/Contents**
Wireless Communication Fundamentals Wireless communication overview and challenges, Review of signals for wireless systems, Wireless transmission impairments: path loss, fading, interference, noise, Performance metrics: bandwidth, throughput, latency, jitter, Multiple access techniques: FDMA, TDMA, CDMA, OFDMA, Spread spectrum techniques: FHSS, DSSS **Wireless LANs and PANs:** IEEE 802.11 architecture and components, MAC layer in WLAN: CSMA/CA, RTS/CTS, WLAN standards: 802.11a/b/g/n/ac/ax, Bluetooth architecture and protocol stack, ZigBee and IoT wireless networks, Wireless LAN performance issues	
Section2:	**Topics/Contents**

Mobile and Cellular Networks: Cellular concept and frequency reuse, GSM architecture and channels, CDMA and LTE overview, 4G LTE architecture and services, Introduction to 5G networks and features Mobility management: location management, handoff techniques **Mobile Networking Protocols and Security:** Mobile IP: entities, operations, tunneling, Routing in mobile ad hoc networks (MANETs), Transport layer issues in wireless networks, Wireless and mobile network security threats, WLAN security: WEP, WPA, WPA2, WPA3, Security in cellular and mobile IP networks	
Text Books: ***(As per IEEE format)***	
1	T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Upper Saddle River, NJ, USA: Pearson Education, 2010.
2	J. Schiller, *Mobile Communications*, 2nd ed. Boston, MA, USA: Pearson Education, 2003.
Reference Books: ***(As per IEEE format)***	
1	W. Stallings, *Wireless Communications and Networks*, 2nd ed. Upper Saddle River, NJ, USA: Pearson Education, 2005.
2	A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 5th ed. Boston, MA, USA: Pearson Education, 2011.
3	C. Siva Ram Murthy and B. S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*, Upper Saddle River, NJ, USA: Pearson Education, 2004.

List of Practical’s:

1. Simulate path loss, noise, and fading effects in a wireless channel.
2. Implement and compare FDMA, TDMA, and CDMA multiple access techniques.
3. Analyze IEEE 802.11 WLAN architecture and frame structure.
4. Configure and analyze WLAN performance parameters such as throughput and delay.
5. Analyze cellular network concepts such as frequency reuse and cell splitting.
6. Analyze LTE / 4G network architecture and services.
7. Simulate handoff techniques in mobile cellular networks.
8. Study Mobile IP architecture and packet routing mechanism.
9. Analyze routing protocols used in Mobile Ad Hoc Networks (MANETs).
10. Configure and analyze WLAN security protocols: WEP, WPA, WPA2, and WPA3.
11. Identify and analyze security threats in wireless and mobile networks.
12. Case study on recent wireless or mobile network security attacks and mitigation techniques.

CO-PO Mapping

CO	Program Outcomes (PO)											PSO	
CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	3	2									2	2	
CO2	3	3									2	2	
CO3	2	2	3		3						2	3	
CO4	2	2		2	3		1	2	1		2	2	2
Average	2.5	2.25	3	2	3	2	1	2	1	1	2	2.25	2

Course Code: Named Data Networking (NDN)

Teaching Scheme	**Examination Scheme**
Credits: 3	CP: Marks
Lectures: 2 Hrs/week	GD/PPT/HA: Marks
Practical: 4 Hrs/week	MSE (W/O): Marks
Tutorial: 0 Hrs/week	ESE (W/O): Marks

Prerequisites:	
•	Computer Networks
•	Data Communication
•	Operating Systems
•	Basic knowledge of Linux and Python
•	Fundamentals of TCP/IP Networking
Course Objectives:	
•	To understand the limitations of IP-based networking and the need for Information-Centric Networking.
•	To study the architecture, components, and packet formats of Named Data Networking.
•	To implement NDN communication using real simulators and tools.
•	To analyze NDN performance for next-generation Internet applications such as IoT, multimedia, and security
Course Outcomes:	
	After completion of the course, student will be able to
1.	Describe the limitations of IP-based networking and the principles and architecture of Named Data Networking.
2.	Analyze NDN packet formats, forwarding mechanisms, and in-network caching strategies.
3.	Implement basic NDN applications using ndnSIM and NDN-CXX tools.
4.	Evaluate NDN security mechanisms and assess its suitability for next-generation networking applications such as IoT and multimedia systems.

Section1:	**Topics/Contents**
INTRODUCTION TO INFORMATION-CENTRIC NETWORKING & NAMED DATA NETWORKING (NDN) Evolution of Internet architecture, Limitations of IP networking, Information-Centric Networking (ICN) overview, NDN architecture, Naming conventions and hierarchical naming, NDN packet types: Interest, Data, NACK, Comparison between IP and NDN **NDN FORWARDING AND CACHING MECHANISMS**	

NDN forwarding plane, Content Store (CS), Pending Interest Table (PIT), Forwarding Information Base (FIB), Interest forwarding strategies, In-network caching, Cache replacement policies, Multicast and mobility support	
Section2:	**Topics/Contents**
NDN SECURITY AND TRUST MODELS Data-centric security, Packet signing and verification, Trust schema and certificate management, Key distribution mechanisms, Privacy and access control, Secure content dissemination, DoS attacks and mitigation in NDN **NDN SIMULATION, IMPLEMENTATION & APPLICATIONS** ndnSIM architecture, NDN Forwarding Daemon (NFD), NDN-CXX library, Implementing producer–consumer applications, NDN for IoT, Smart Cities, Multimedia streaming, Performance evaluation metrics	
Text Books: ***(As per IEEE format)***	
1	Named Data Networking: The Ultimate Step-By-Step, 1st ed. New Delhi, India: 5starcooks, Sep. 2018, pp. 1–286. ISBN: 978-0655406822 link: https://www.amazon.in/Named-Networking-Ultimate-Step-Step/dp/0655406824
2	L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, K. C. Claffy, P. Crowley, C. Papadopoulos, L. Wang and B. Zhang, Named Data Networking, ACM SIGCOMM Computer Communication Review, vol. 44, no. 3, pp. 66–73, Jul. 2014. Available: https://doi.org/10.1145/2656877.2656887
Reference Books: ***(As per IEEE format)***	
1	K. Pentikousis, G. Xylomenos, and A. F. Harris (Eds.), Information-Centric Networking: Techniques and Applications, Springer, 2022. Available: https://link.springer.com/book/10.1007/978-3-030-46736-4
2	B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, A Survey of Information-Centric Networking, Springer, 2018. (Reference book covering architectures, challenges, and implementation issues). — (Publisher link: https://www.springer.com/gp/book/9783319925555)

List of Practical's:

1. Install and configure the ndnSIM simulator and NDN-CXX libraries on a Linux platform. Verify the installation by compiling and running a sample NDN application to ensure the environment is ready for development and simulation.
2. Design and implement a basic NDN producer and consumer application using ndnSIM. The consumer should send Interest packets for a named data prefix, and the producer should respond with Data packets. Analyze Interest–Data communication flow.
3. Simulate an NDN network topology and capture Interest and Data packets. Analyze packet flow, name prefixes, hop count, and latency using ndnSIM trace tools.
4. Demonstrate the working of Pending Interest Table (PIT), Forwarding Information Base (FIB), and Content Store (CS) by generating multiple Interests and observing packet forwarding, aggregation, and caching behavior.

5. Implement and compare different caching policies (LRU, FIFO, Random) in ndnSIM. Evaluate their effect on cache hit ratio, latency, and bandwidth utilization.
6. Implement data packet signing using NDN security mechanisms. Enable consumers to verify digital signatures and evaluate trust management effectiveness.
7. Simulate NDN traffic under varying Interest generation rates and node densities. Measure throughput, delay, and packet loss to analyze NDN performance.
8. Design a small-scale NDN-based IoT or Smart City communication model (e.g., smart traffic or sensor network). Implement producer-consumer nodes and evaluate secure, efficient data retrieval using NDN

CO-PO Mapping

CO	**Program Outcomes (PO)**											**PSO**	
CO/ PO	**PO 1**	**PO 2**	**PO 3**	**PO 4**	**PO 5**	**PO 6**	**PO 7**	**PO 8**	**PO 9**	**PO 10**	**PO 11**	**PSO 1**	**PSO2**
CO1	3	2	1	-	–	1	–	-	1	–	1	**1**	-
CO2	2	3	2	1	2	–	–	-	1	–	1	**2**	**-**
CO3	2	2	3	2	3	-	–	2	2	1	1	**3**	**1**
CO4	1	2	2	3	2	3	3	1	1	–	2	**2**	**3**
Average	2.00	2.25	2.00	2.00	2.33	2.00	3.00	1.50	1.25	1.00	1.25	2.00	2.00

Course Code: Cyber Defense and Threat Intelligence

Teaching Scheme	Examination Scheme
Credits: 3	CP: Marks
Lectures: 2 Hrs/week	GD/PPT/HA: Marks
Practical: 4 Hrs/week	MSE (W/O): Marks
Tutorial: - Hrs/week	ESE (W/O): Marks

Prerequisites:	
•	Data Communication, Computer Networks, Information Security
Course Objectives:	
•	To understand real-world cyber threats, attack methodologies, and adversary behavior.
•	To analyze cyber incidents using threat intelligence and security analytics.
•	To apply cyber defense mechanisms, incident response, and forensics techniques.
•	To understand cyber security governance, laws, ethics, and organizational security.
Course Outcomes:	
	After completion of the course, student will be able to
1.	Identify and classify cyber threats, attack vectors, and adversary techniques.
2.	Analyze cyber attacks using threat intelligence frameworks and security logs.
3.	Apply incident response and digital forensics techniques.
4.	Evaluate organizational cyber security posture, compliance, and risk.

Section1:	Topics/Contents
Cyber Threat Landscape and Adversary Models Cyber kill chain and attack lifecycle, Threat actors: nation-state, hacktivists, cyber criminals, insiders, Tactics, Techniques, and Procedures (TTPs), MITRE ATT&CK framework, Advanced Persistent Threats (APT), Supply chain attacks, Zero-day vulnerabilities (concept) **Vulnerability Assessment and Penetration Testing Concepts:** Vulnerability vs threat vs risk, Vulnerability discovery methods, Common vulnerabilities: OWASP Top 10, Penetration testing phases and methodology, Ethical hacking overview (reconnaissance, exploitation, post-exploitation), Security misconfigurations and human errors, Responsible disclosure	
Section2:	**Topics/Contents**

Security Operations and Incident Response:
Security Operations Center (SOC), Log analysis and security monitoring, SIEM concepts and correlation rules, Incident response lifecycle (Preparation, Detection, Containment, Eradication, Recovery), Malware analysis fundamentals (static vs dynamic – overview), Ransomware response strategies, Business continuity and disaster recovery planning

Digital Forensics, Governance, and Compliance:
Digital forensics process and chain of custody, Evidence acquisition and analysis (disk, memory, logs), Cyber crime investigation overview, Cyber laws and regulations (IT Act, GDPR overview), Security governance and risk management, Cyber ethics and professional responsibility

Text Books: ***(As per IEEE format)***	
1	E. Cole, S. Northcutt, and J. Harris, *Hacking Exposed: Network Security Secrets and Solutions*, 7th ed., McGraw-Hill, 2012.
2	M. Sikorski and A. Honig, *Practical Malware Analysis*, No Starch Press, 2012
Reference Books: ***(As per IEEE format)***	
1	K. Scarfone and P. Mell, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, NIST Special Publication 800-94.
2	J. Andress, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Syngress.
3	R. Bejtlich, *The Practice of Network Security Monitoring*, No Starch Press.

List of Practical's:

1. Study cyber threat landscape and classification of threat actors.
2. Analyze real-world cyber attacks using Cyber Kill Chain model.
3. Map attack techniques using MITRE ATT&CK framework.
4. Identify vulnerabilities using OWASP Top-10 case studies.
5. Perform basic vulnerability assessment using open-source tools.
6. Analyze system and network logs for suspicious activities.
7. Case study on ransomware attack and incident response strategy.
8. Simulate incident response lifecycle for a cyber breach scenario.
9. Analyze digital evidence and chain of custody process.
10. Study cyber laws, IT Act, and compliance requirements.
11. Case study on supply-chain or APT attack.
12. Prepare cyber risk assessment and mitigation report for an organization.

CO-PO Mapping

CO	Program Outcomes (PO)											PSO	
CO/PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PSO1	PSO2
CO1	2	3	–	–	–	2	–	–	–	–	2	2	2
CO2	2	3	2	2	2	–	–	–	–	–	2	3	2
CO3	–	2	2	3	2	2	–	2	2	–	2	2	3
CO4	–	2	–	–	–	3	3	2	2	2	2	–	3
Average	2	2	2	2.5	2	2.25	3	2	2	2	2	2.25	2.5