Item 03:08 – Annexure VII

ROHINI
COLLEGE OF ENGINEERING & TECHNOLOGY
(AUTONOMOUS)
Approved By AICTE & Affiliated to Anna University
NBA Accredited for All Eligible B.E/B.Tech Programs | NAAC Accredited with A+ Grade
Near Anjugramam - Kanyakumari Main Road, Palkulam, Variyoor P.O.-629401, Kanyakumari Dist, Tamil Nadu.

Minor Degree Course

CYBER SECURITY

Curriculum & Syllabus

(2024-2025 Admitted Students Onwards)

CREDIT INFO		
Sl.No	**Category**	**Credits**
1	Minor Courses	18

CREDIT DISTRIBUTION

Course Category	Credit/Semester								No. of Credits
	I	II	III	IV	V	VI	VII	VIII	
Minor Courses	-	-	-	-	6	6	6	-	18

MINOR COURSES						
CYBER SECURITY						
Sl.No	**Course Code**	**Course Title**	**L**	**T**	**P**	**C**
1	24CY501	Foundations of Cyber Security and Ethical Hacking	3	0	0	3
2	24CY502	Network Security and Secure Communication	3	0	0	3
3	24CY601	Cyber Security for IoT, Industrial Control Systems and Smart Infrastructure	3	0	0	3
4	24CY602	Cloud Security, Digital Forensics and Incident Response	3	0	0	3
5	24CY701	AI for Cyber Security and Threat Intelligence	3	0	0	3
6	24CY702	Cyber Security Applications in Smart Engineering Systems	3	0	0	3

Course Code:	**24CY501**	**Course Title:**	**Foundations of Cyber Security and Ethical Hacking**
Credits:	**3**	**L – T – P**	**3-0-0**
Prerequisite	Basic Computer Fundamentals		

Course objectives:

The course enables the students to:

- Understand the fundamental concepts of cyber security, information security, cyber threats, and security principles applicable to engineering systems.
- Apply security mechanisms, cryptographic techniques, authentication methods, and access control to protect digital assets.
- Identify system and network vulnerabilities using ethical hacking methodologies and security assessment tools.
- Perform basic vulnerability assessment and penetration testing (VAPT) in a controlled environment while adhering to legal and ethical standards.
- Design security-aware solutions to protect industrial systems, smart infrastructure, healthcare devices, and IoT-enabled engineering applications

Teaching-Learning Process:

Suggested strategies that teachers may use to effectively achieve the course outcomes:

1. Interactive Lectures with Real-World Cyber Attack Case Studies
2. Demonstration of Cyber Security and Ethical Hacking Tools
3. Hands-on Laboratory Sessions using Kali Linux
4. Problem-Based Learning
5. Project-Based Learning
6. Flipped Classroom
7. Capture-the-Flag (CTF) Exercises
8. Group Discussions on Cyber Laws and Ethics
9. Industry Expert Sessions
10. Mini Projects on Security Assessment

UNIT I – FUNDAMENTALS OF CYBER SECURITY	**[9 hours]**

Introduction to Cyber Security – Information Security Concepts – Confidentiality, Integrity and Availability (CIA Triad) – Cyber Security Goals – Types of Cyber Threats – Malware, Ransomware, Spyware, Viruses, Worms and Trojans – Social Engineering Attacks – Phishing and Spear Phishing –

Insider Threats – Cyber Security Frameworks – Security Policies – Risk Management – Cyber Security in Smart Manufacturing, Healthcare, Power Systems and Smart Cities.

UNIT II – SECURITY MECHANISMS AND CRYPTOGRAPHY	**[9 hours]**
Fundamentals of Cryptography – Symmetric and Asymmetric Encryption – Hash Functions – Digital Signatures – Public Key Infrastructure (PKI) – Authentication Methods – Multi-Factor Authentication – Authorization – Access Control Models – Password Security – Identity and Access Management – Secure Communication Protocols (SSL/TLS, HTTPS, SSH) – Data Protection Techniques – Secure File Storage and Backup.	

UNIT III – ETHICAL HACKING AND VULNERABILITY ASSESSMENT	**[9 hours]**
Introduction to Ethical Hacking – Hacking Methodology – Footprinting and Reconnaissance – Scanning Networks – Enumeration – Vulnerability Assessment – Common Security Vulnerabilities – Penetration Testing Concepts – Web Application Security Basics – OWASP Top 10 Overview – Password Cracking Concepts – Wireless Security Basics – Security Assessment Reports – Responsible Disclosure – Legal and Ethical Issues in Ethical Hacking.	

UNIT IV – CYBER ATTACKS, DEFENCE AND SYSTEM SECURITY	**[9 hours]**
Network Attacks – Denial-of-Service (DoS) and Distributed DoS Attacks – Man-in-the-Middle Attacks – SQL Injection and Cross-Site Scripting (Concepts) – Malware Analysis Basics – Firewalls – Intrusion Detection and Prevention Systems – Endpoint Security – Antivirus and Anti-malware Solutions – Email Security – Secure System Configuration – Patch Management – Backup and Recovery – Security Monitoring and Incident Reporting.	

UNIT V – CYBER SECURITY FOR SMART ENGINEERING SYSTEMS	**[9 hours]**
Cyber Security in Industrial Control Systems (ICS) – Operational Technology (OT) Security – Industrial Internet of Things (IIoT) Security – Smart Grid Security – Medical Device Security – Smart Building Security – Connected Vehicle Security – Cloud Security Fundamentals – AI in Cyber Security – Cyber Security Governance – Cyber Laws in India – IT Act 2000 (with amendments) – Privacy and Data Protection – Engineering Case Studies and Best Practices.	

Course outcomes:

On completion of the course, the student will have the ability to:

CO1	Explain cyber security principles, cyber threats, attack vectors, and security controls applicable to engineering systems.
CO2	Apply cryptographic techniques, authentication mechanisms, and access control methods to secure digital information.
CO3	Perform vulnerability assessment using ethical hacking tools to identify security weaknesses in computer systems and networks
CO4	Analyze cyber attacks and recommend appropriate preventive and mitigation strategies for engineering applications.
CO5	Develop secure engineering solutions by incorporating cyber security best practices, legal requirements, and ethical hacking principles.

COs and POs Mapping:

CO's	**PO's**										
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
1	2	2	1	1	1	3		-	-	1	2
2	1	1	1	1	2	3	-	-	-	1	2
3	1	1	1	2	2	3	-	-	-	1	2
4	1	1	1	2	2	2	-	-	-	2	2
5	1	1	1	2	2	2	-	-	-	2	2

Level 3- Highly Mapped, Level 2- Moderately Mapped, Level 1- Low Mapped, Level 0- Not Mapped

Scheme of Evaluation:

Component	**Typeof assessment**	**Max Marks**	**Reduced Marks**	**Total**	**Final marks**
Continuous Internal Examination (CIE)	CIE – I	100	50	100	40
	CIE – II	100			
	MCQ	20	10		
	Skill Assessment - I	40	40		
	Skill Assessment - II	40			
End Semester Examination (ESE)	Theory Exam	100	60	60	60
				Total	100

End semester Examination: (QP PATTERN)

- Each unit consists of two 2 marks questions and one 16 marks question (either or).
- All the fifteen questions have to be answered.

Assessment Pattern

Bloom's Category	Continuous Assessment Tests		Terminal Examination
	1	2	
Remember	60	50	60
Understand	40	50	40
Apply	0	0	0
Analyze	0	0	0
Evaluate	0	0	0
Create	0	0	0

TEXT BOOKS:

1. Charles J. Brooks, Christopher Grow, Philip Craig and Donald Short, Cyber Security Essentials, Wiley, 2024.
2. William Stallings, Cryptography and Network Security: Principles and Practice, 9th Edition, Pearson, 2024.
3. Michael T. Simpson, Kent Backman and James Corley, Hands-On Ethical Hacking and Network Defense, Cengage Learning, Latest Edition.

REFERENCE BOOKS:

1. EC-Council, Ethical Hacking Essentials (EHE), EC-Council Press, 2024.
2. Matt Walker, CEH Certified Ethical Hacker All-in-One Exam Guide, McGraw-Hill, Latest Edition.
3. Nina Godbole and Sunit Belapure, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India.
4. Michael E. Whitman and Herbert J. Mattord, Principles of Information Security, Cengage Learning.
5. Bruce Schneier, Applied Cryptography, Wiley.

SUGGESTED SKILL ACTIVITIES

Students shall complete the following laboratory and skill-oriented activities.

1. Install and configure Kali Linux in a virtual machine.
2. Perform basic network reconnaissance using Nmap.
3. Capture and analyze network packets using Wireshark.

4. Conduct vulnerability scanning using OpenVAS/Greenbone or Nessus Essentials.
5. Demonstrate password security and multi-factor authentication.
6. Configure firewall rules and secure system settings.
7. Analyze phishing emails and identify social engineering attacks.
8. Perform a basic web application security assessment using OWASP ZAP.
9. Prepare a cyber security risk assessment report for an engineering organization.
10. Complete a mini project on securing an Industrial IoT or smart engineering application

Course Code:	**24CY502**	**Course Title:**	**Network Security and Secure Communication**
Credits:	**3**	**L – T – P**	**3-0-0**
Prerequisite	**24CY501 - Foundations of Cyber Security and Ethical Hacking**		

Course objectives:

The course enables the students to:

- Understand the fundamentals of computer networks, communication protocols, and network security principles for protecting engineering systems.
- Apply cryptographic protocols, authentication mechanisms, firewalls, and intrusion detection techniques to secure wired and wireless communication networks.
- Analyze network vulnerabilities and cyber threats affecting enterprise, Industrial IoT (IIoT), Operational Technology (OT), and smart engineering systems.
- Configure secure communication services using VPNs, secure routing, wireless security protocols, and network monitoring tools.
- Design secure communication solutions for industrial automation, smart grids, healthcare, transportation, and other engineering applications

Teaching-Learning Process:

1. Interactive Lectures with Industry Case Studies
2. Network Simulation using Cisco Packet Tracer
3. Hands-on Laboratory Sessions
4. Demonstration of Network Security Tools
5. Problem-Based Learning
6. Project-Based Learning
7. Flipped Classroom
8. Collaborative Learning
9. Cyber Security Workshops
10. Mini Projects and Technical Seminars

UNIT I – COMPUTER NETWORKS AND NETWORK SECURITY FUNDAMENTALS	**[9 hours]**

Introduction to Computer Networks – OSI and TCP/IP Reference Models – IP Addressing – Routing and Switching Fundamentals – Network Devices – Network Services – Network Security Concepts – Security Goals – Network Threat Landscape – Attack Surface – Common Network Attacks – Security

Policies – Risk Assessment – Network Security Architecture – Applications in Industrial and Enterprise Networks.

UNIT II – SECURE COMMUNICATION PROTOCOLS AND CRYPTOGRAPHY	**[9 hours]**
Secure Communication Principles – Cryptographic Protocols – Secure Socket Layer (SSL) and Transport Layer Security (TLS) – HTTPS – Secure Shell (SSH) – Virtual Private Networks (VPN) – IP Security (IPSec) Concepts – Public Key Infrastructure (PKI) – Digital Certificates – Authentication Protocols – Multi-Factor Authentication – Secure Email – Secure File Transfer – Data Integrity and Digital Signatures.	

UNIT III – NETWORK DEFENCE AND INTRUSION DETECTION	**[9 hours]**
Firewalls – Packet Filtering – Stateful Inspection – Proxy Firewalls – Network Address Translation (NAT) – Intrusion Detection Systems (IDS) – Intrusion Prevention Systems (IPS) – Network Access Control (NAC) – Malware Detection – Security Information and Event Management (SIEM) Concepts – Network Traffic Monitoring – Packet Analysis using Wireshark – Security Logging – Incident Detection and Response.	

UNIT IV – WIRELESS, IoT AND INDUSTRIAL NETWORK SECURITY	**[9 hours]**
Wireless Network Fundamentals – Wi-Fi Security (WPA2, WPA3) – Bluetooth Security – ZigBee and LoRaWAN Security Concepts – Internet of Things (IoT) Security – Industrial Internet of Things (IIoT) – Operational Technology (OT) Networks – SCADA Security Fundamentals – Industrial Communication Protocols (Modbus, DNP3, OPC UA – Concepts) – Smart Grid Communication Security – Secure Sensor Networks – Zero Trust Networking Principles	

UNIT V – NETWORK SECURITY APPLICATIONS IN SMART ENGINEERING SYSTEMS	**[9 hours]**
Network Security for Smart Manufacturing – Secure Communication in Industrial Automation – Smart Grid Network Protection – Intelligent Transportation Networks – Healthcare Network Security – Cloud Network Security Fundamentals – Remote Monitoring and Secure Access – Network Security Policies and Compliance – Business Continuity and Disaster Recovery – AI-Assisted Network Security Monitoring – Engineering Case Studies on Critical Infrastructure Protection.	

Course outcomes:

On completion of the course, the student will have the ability to:

CO1	Explain network architectures, communication protocols, and security mechanisms for protecting enterprise and industrial networks.
CO2	Configure secure communication protocols, firewalls, VPNs, and wireless security solutions to safeguard network infrastructure.
CO3	Analyze network traffic and detect cyber threats using network monitoring and intrusion detection tools.
CO4	Assess network vulnerabilities and recommend appropriate security controls for Industrial IoT and smart engineering systems.
CO5	Design secure communication architectures for smart manufacturing, healthcare, power systems, transportation, and critical infrastructure.

COs and POs Mapping:

CO's	**PO's**										
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
1	2	2	1	1	1	3		-	-	1	2
2	1	1	1	1	2	3	-	-	-	1	2
3	1	1	1	2	2	3	-	-	-	1	2
4	1	1	1	2	2	2	-	-	-	2	2
5	1	1	1	2	2	2	-	-	-	2	2

Level 3- Highly Mapped, Level 2- Moderately Mapped, Level 1- Low Mapped, Level 0- Not Mapped

Scheme of Evaluation:

Component	**Typeof assessment**	**Max Marks**	**Reduced Marks**	**Total**	**Final marks**
Continuous Internal Examination (CIE)	CIE – I	100	50	100	40
	CIE – II	100			
	MCQ	20	10		
	Skill Assessment - I	40	40		
	Skill Assessment - II	40			
End Semester Examination (ESE)	Theory Exam	100	60	60	60
				Total	100

End semester Examination: (QP PATTERN)

- Each unit consists of two 2 marks questions and one 16 marks question (either or).
- All the fifteen questions have to be answered.

Assessment Pattern

Bloom's Category	Continuous Assessment Tests		Terminal Examination
	1	2	
Remember	60	50	60
Understand	40	50	40
Apply	0	0	0
Analyze	0	0	0
Evaluate	0	0	0
Create	0	0	0

TEXT BOOKS:

1. William Stallings, Network Security Essentials: Applications and Standards, 7th Edition, Pearson, 2024.
2. William Stallings, Cryptography and Network Security: Principles and Practice, 9th Edition, Pearson, 2024.
3. Behrouz A. Forouzan, Data Communications and Networking, 6th Edition, McGraw-Hill Education.

REFERENCE BOOKS:

1. Charlie Kaufman, Radia Perlman, and Mike Speciner, Network Security: Private Communication in a Public World, 3rd Edition, Pearson.
2. Eric Maiwald, Network Security: A Beginner's Guide, McGraw-Hill.
3. Nina Godbole and Sunit Belapure, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India.
4. Douglas E. Comer, Computer Networks and Internets, 7th Edition, Pearson.
5. Joseph Migga Kizza, Guide to Computer Network Security, Springer.

SUGGESTED SKILL ACTIVITIES

Students shall complete the following laboratory and skill-oriented activities.

1. Configure IP addressing and secure network topology using Cisco Packet Tracer.
2. Analyze network packets using Wireshark.
3. Configure firewall rules for enterprise network protection.
4. Establish secure remote communication using SSH.

5. Configure a Virtual Private Network (VPN) for secure communication.
6. Perform wireless network security analysis and secure Wi-Fi configuration.
7. Monitor network traffic and identify suspicious activities.
8. Simulate intrusion detection using open-source IDS tools.
9. Design a secure Industrial IoT communication architecture.
10. Develop a mini project on secure communication for a smart engineering application.

Course Code:	**24CY601**	**Course Title:**	**Cyber Security for IoT, Industrial Control Systems and Smart Infrastructure**
Credits:	**3**	**L – T – P**	**3-0-0**
Prerequisite	**24CY501 - Foundations of Cyber Security and Ethical Hacking** **24CY502 - Network Security and Secure Communication**		

Course objectives:

The course enables the students to:

- Understand the security architecture, vulnerabilities, and cyber threats associated with IoT, Industrial Control Systems (ICS), Operational Technology (OT), and smart infrastructure.
- Apply cyber security principles to secure Industrial IoT (IIoT) devices, sensors, communication networks, and industrial automation systems.
- Analyze cyber attacks on SCADA, PLCs, smart grids, smart buildings, transportation systems, and connected healthcare devices.
- Implement risk assessment, security monitoring, access control, and incident response strategies for critical engineering infrastructure.
- Design resilient cyber security solutions for Industry 5.0 applications involving manufacturing, energy, civil infrastructure, healthcare, and agriculture.

Teaching-Learning Process:

1. Interactive Lectures with Industrial Cyber Security Case Studies
2. Demonstration of Industrial IoT Security Tools
3. Simulation-Based Learning
4. Hands-on Laboratory Sessions
5. Problem-Based Learning
6. Project-Based Learning
7. Flipped Classroom
8. Collaborative Learning
9. Industry Expert Talks
10. Team-Based Mini Projects

UNIT I – IoT AND INDUSTRIAL CYBER SECURITY FUNDAMENTALS	**[9 hours]**

Introduction to Internet of Things (IoT) – Industrial Internet of Things (IIoT) – Cyber-Physical Systems (CPS) – Smart Sensors and Embedded Devices – IoT Architecture – Edge Computing – Fog Computing – IoT Communication Protocols (MQTT, CoAP, AMQP – Concepts) – Security

Challenges in IoT – Device Identity – Secure Boot – Firmware Security – Applications in Smart Manufacturing, Healthcare, Agriculture, Energy, and Smart Cities.

UNIT II – INDUSTRIAL CONTROL SYSTEMS (ICS) AND OPERATIONAL TECHNOLOGY (OT) SECURITY	**[9 hours]**
Industrial Control Systems Architecture – Supervisory Control and Data Acquisition (SCADA) – Programmable Logic Controllers (PLCs) – Distributed Control Systems (DCS) – Human Machine Interface (HMI) – Industrial Communication Protocols (Modbus, DNP3, OPC UA – Concepts) – Operational Technology (OT) Networks – Industrial Network Segmentation – Asset Inventory – Secure Remote Access – Zero Trust Architecture for Industrial Systems	

UNIT III – CYBER THREATS AND RISK MANAGEMENT FOR CRITICAL INFRASTRUCTURE	**[9 hours]**
Cyber Threat Landscape for Critical Infrastructure – Malware Targeting Industrial Systems – Ransomware Attacks – Supply Chain Attacks – Insider Threats – Vulnerability Assessment – Risk Assessment Methodologies – Security Monitoring – Intrusion Detection Systems (IDS) – Security Information and Event Management (SIEM) Concepts – Incident Response – Business Continuity – Disaster Recovery – Industrial Cyber Security Standards (IEC 62443, NIST CSF – Overview).	

UNIT IV – SECURITY OF SMART ENGINEERING SYSTEMS	**[9 hours]**
Cyber Security for Smart Manufacturing – Secure Robotics and Automation – Smart Grid Cyber Security – Renewable Energy System Security – Smart Building Security – Intelligent Transportation Systems – Connected Vehicles – Biomedical Device Security – Telemedicine Security – Precision Agriculture Security – Drone Security – Cloud and Edge Security for Smart Engineering Applications.	

UNIT V – AI-ENABLED CYBER SECURITY FOR INDUSTRY 5.0	**[9 hours]**
Artificial Intelligence for Threat Detection – Machine Learning for Anomaly Detection – AI-Based Predictive Security – Security Analytics – Digital Twin Security Concepts – Cyber Security for Autonomous Systems – Security Operations Centre (SOC) Fundamentals – Threat Intelligence – Explainable AI in Cyber Security – Responsible AI – Engineering Case Studies – Cyber Security Governance and Best Practices for Smart Infrastructure.	

Course outcomes:

On completion of the course, the student will have the ability to:

CO1	Explain the architecture, communication protocols, and security requirements of IoT, ICS, OT, and smart infrastructure systems.
CO2	Apply appropriate security mechanisms to protect Industrial IoT devices, industrial communication networks, and cyber-physical systems.
CO3	Analyze cyber threats, vulnerabilities, and attacks on SCADA systems, PLCs, smart grids, and connected engineering assets.
CO4	Develop risk mitigation, monitoring, and incident response strategies for securing critical engineering infrastructure.
CO5	Design secure cyber-physical systems for smart manufacturing, healthcare, transportation, energy, agriculture, and smart cities.

COs and POs Mapping:

CO's	PO's										
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
1	2	2	1	1	1	3		-	-	1	2
2	1	1	1	1	2	3	-	-	-	1	2
3	1	1	1	2	2	3	-	-	-	1	2
4	1	1	1	2	2	2	-	-	-	2	2
5	1	1	1	2	2	2	-	-	-	2	2

Level 3- Highly Mapped, Level 2- Moderately Mapped, Level 1- Low Mapped, Level 0- Not Mapped

Scheme of Evaluation:

Component	**Typeof assessment**	**Max Marks**	**Reduced Marks**	**Total**	**Final marks**
Continuous Internal Examination (CIE)	CIE – I	100	50	100	40
	CIE – II	100			
	MCQ	20	10		
	Skill Assessment - I	40	40		
	Skill Assessment - II	40			
End Semester Examination (ESE)	Theory Exam	100	60	60	60
				Total	100

End semester Examination: (QP PATTERN)

- Each unit consists of two 2 marks questions and one 16 marks question (either or).
- All the fifteen questions have to be answered.

Assessment Pattern

Bloom's Category	Continuous Assessment Tests		Terminal Examination
	1	2	
Remember	60	50	60
Understand	40	50	40
Apply	0	0	0
Analyze	0	0	0
Evaluate	0	0	0
Create	0	0	0

TEXT BOOKS:

1. Eric D. Knapp and Joel Thomas Langill, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA and Other Industrial Control Systems, 3rd Edition, Syngress, 2024.
2. Andrew Minteer, Analytics for the Internet of Things (IoT): Intelligent Analytics for Your Intelligent Devices, Packt Publishing.
3. Alasdair Gilchrist, Industry 4.0: The Industrial Internet of Things, 2nd Edition, Apress, 2024.

REFERENCE BOOKS:

1. Tyson Macaulay and Bryan Singer, Cybersecurity for Industrial Control Systems, CRC Press.
2. William Stallings, Network Security Essentials: Applications and Standards, 7th Edition, Pearson.
3. Nina Godbole and Sunit Belapure, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India.
4. Joseph Migga Kizza, Guide to Computer Network Security, Springer.
5. Sravani Bhattacharjee, IoT Security: Advances in Authentication, Wiley.

SUGGESTED SKILL ACTIVITIES

Students shall complete the following laboratory and skill-oriented activities.

1. Configure and secure an IoT device communication network using MQTT.
2. Perform vulnerability assessment of Industrial IoT devices.

3. Simulate a SCADA/PLC communication environment using open-source tools.
4. Analyze industrial network traffic using Wireshark.
5. Design a secure network architecture for a smart manufacturing plant.
6. Perform cyber risk assessment for a smart building or industrial facility.
7. Configure secure remote access for Industrial Control Systems.
8. Develop a security monitoring dashboard using industrial sensor data.
9. Build a machine learning model for anomaly detection in IoT network traffic.
10. Complete a mini project on cyber security for a smart engineering application.

Course Code:	**24CY602**	**Course Title:**	**Cloud Security, Digital Forensics and Incident Response**
Credits:	**3**	**L – T – P**	**3-0-0**
Prerequisite	**24CY501 - Foundations of Cyber Security and Ethical Hacking, 24CY502 - Network Security and Secure Communication**		

Course objectives:

The course enables the students to:

- Understand cloud computing security models, shared responsibility, and security controls for protecting cloud-based engineering applications and critical infrastructure.
- Apply cloud security mechanisms, identity and access management, data protection, and virtualization security to secure cloud environments.
- Perform digital forensic investigations by acquiring, preserving, analyzing, and documenting digital evidence using standard forensic procedures.
- Develop incident response strategies for identifying, containing, investigating, recovering, and reporting cyber security incidents.
- Design resilient cloud security and incident response solutions for industrial systems, healthcare, smart infrastructure, and Industry 5.0 applications.

Teaching-Learning Process:

1. Interactive Lectures with Real-World Incident Case Studies
2. Demonstration of Cloud Security Platforms
3. Hands-on Laboratory Sessions
4. Digital Forensics Practical Exercises
5. Project-Based Learning
6. Problem-Based Learning
7. Flipped Classroom
8. Simulation of Cyber Security Incidents
9. Collaborative Learning
10. Mini Projects and Technical Presentations

UNIT I – CLOUD COMPUTING AND CLOUD SECURITY FUNDAMENTALS	**[9 hours]**

Cloud Computing Concepts – Cloud Service Models (IaaS, PaaS, SaaS) – Cloud Deployment Models (Public, Private, Hybrid, Community) – Virtualization and Containerization Concepts – Shared Responsibility Model – Cloud Threat Landscape – Cloud Security Principles – Data Security in Cloud

– Identity and Access Management (IAM) – Multi-Factor Authentication – Cloud Security Architecture – Applications of Cloud Computing in Industry 5.0, Smart Manufacturing, Healthcare, Smart Cities, and Engineering Systems.

UNIT II – CLOUD DATA PROTECTION AND SECURITY MANAGEMENT	**[9 hours]**
Cloud Data Encryption – Key Management Concepts – Secure Storage and Backup – Secure APIs – Cloud Network Security – Secure Virtual Machines – Container Security – Security Monitoring and Logging – Cloud Security Posture Management (Concepts) – Compliance and Governance – Privacy Protection – Business Continuity – Disaster Recovery – Cloud Risk Assessment – Cloud Security Best Practices.	

UNIT III – DIGITAL FORENSICS AND DIGITAL EVIDENCE	**[9 hours]**
Introduction to Digital Forensics – Digital Forensic Process – Evidence Identification – Evidence Acquisition – Preservation of Digital Evidence – Chain of Custody – Disk Forensics – Memory Forensics – File System Analysis – Log Analysis – Mobile Device Forensics – Email and Network Forensics – Cloud Forensics – Digital Forensic Reporting – Legal and Ethical Considerations.	

UNIT IV – CYBER INCIDENT RESPONSE AND RECOVERY	**[9 hours]**
Cyber Security Incident Lifecycle – Incident Detection – Security Monitoring – Incident Classification – Containment Strategies – Malware Investigation – Root Cause Analysis – Incident Eradication – System Recovery – Vulnerability Remediation – Threat Hunting Concepts – Security Operations Centre (SOC) Fundamentals – Incident Documentation – Business Continuity Planning – Disaster Recovery Planning – Lessons Learned and Continuous Improvement.	

UNIT V – CLOUD SECURITY AND DIGITAL FORENSICS FOR SMART ENGINEERING SYSTEMS	**[9 hours]**
Cloud Security for Industrial IoT – Secure Smart Manufacturing Platforms – Cloud Security for Smart Grid Systems – Healthcare Cloud Security – Secure Smart Building Management Systems – Digital Forensics for Industrial Control Systems – AI-Assisted Threat Detection – Security Automation – Zero Trust Architecture – Cloud Security Governance – ISO/IEC 27017 and ISO/IEC 27018 Concepts – Engineering Case Studies on Cloud Security and Incident Response.	

Course outcomes:

On completion of the course, the student will have the ability to:

CO1	Explain cloud security architectures, deployment models, and security controls applicable to engineering and enterprise environments
CO2	Apply cloud security techniques including identity management, encryption, virtualization security, and data protection to secure cloud services
CO3	Perform digital forensic investigations by collecting, preserving, analyzing, and documenting digital evidence following accepted forensic practices
CO4	Develop incident response plans to detect, contain, eradicate, recover, and report cyber security incidents.
CO5	Design cloud-enabled cyber resilience solutions for smart manufacturing, healthcare, smart grids, Industrial IoT, and critical infrastructure.

COs and POs Mapping:

CO's	**PO's**										
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
1	2	2	1	1	1	3		-	-	1	2
2	1	1	1	1	2	3	-	-	-	1	2
3	1	1	1	2	2	3	-	-	-	1	2
4	1	1	1	2	2	2	-	-	-	2	2
5	1	1	1	2	2	2	-	-	-	2	2

Level 3- Highly Mapped, Level 2- Moderately Mapped, Level 1- Low Mapped, Level 0- Not Mapped

Scheme of Evaluation:

Component	**Typeof assessment**	**Max Marks**	**Reduced Marks**	**Total**	**Final marks**
Continuous Internal Examination (CIE)	CIE – I	100	50	100	40
	CIE – II	100			
	MCQ	20	10		
	Skill Assessment - I	40	40		
	Skill Assessment - II	40			
End Semester Examination (ESE)	Theory Exam	100	60	60	60
				Total	100

End semester Examination: (QP PATTERN)

- Each unit consists of two 2 marks questions and one 16 marks question (either or).
- All the fifteen questions have to be answered.

Assessment Pattern

Bloom's Category	Continuous Assessment Tests		Terminal Examination
	1	2	
Remember	60	50	60
Understand	40	50	40
Apply	0	0	0
Analyze	0	0	0
Evaluate	0	0	0
Create	0	0	0

TEXT BOOKS:

1. Ronald L. Krutz and Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley.
2. Jason T. Luttgens, Matthew Pepe, and Kevin Mandia, Incident Response and Computer Forensics, 3rd Edition, McGraw-Hill.
3. Bill Nelson, Amelia Phillips, and Christopher Steuart, Guide to Computer Forensics and Investigations, 7th Edition, Cengage Learning.

REFERENCE BOOKS:

1. Ben Clark, Cyber Security Incident Response, Apress.
2. EC-Council, Computer Hacking Forensic Investigator (CHFI) Official Courseware, Latest Edition.
3. William Stallings, Network Security Essentials, Pearson.
4. NIST Special Publication 800-61 Rev.2, Computer Security Incident Handling Guide.
5. Shon Harris and Fernando Maymí, CISSP All-in-One Exam Guide, McGraw-Hill

SUGGESTED SKILL ACTIVITIES

Students shall complete the following laboratory and skill-oriented activities.

1. Configure Identity and Access Management (IAM) policies in a cloud environment.
2. Secure cloud storage using encryption and access control mechanisms.
3. Monitor cloud security logs and identify suspicious activities.
4. Perform forensic imaging and verify evidence integrity using hashing techniques.
5. Analyze system and network logs for digital forensic investigation.

6. Conduct memory and disk forensic analysis using open-source forensic tools.
7. Develop an incident response plan for an Industrial IoT environment.
8. Simulate ransomware incident detection and recovery procedures.
9. Prepare a digital forensic investigation report following chain-of-custody principles.
10. Complete a mini project on cloud security or cyber incident response for a smart engineering application.

Course Code:	**24CY701**	**Course Title:**	**AI for Cyber Security and Threat Intelligence**
Credits:	**3**	**L – T – P**	**3-0-0**
Prerequisite	**24CY501 - Foundations of Cyber Security and Ethical Hacking** **24CY502 - Network Security and Secure Communication**		

Course objectives:

The course enables the students to:

- Understand the role of Artificial Intelligence, Machine Learning, and Threat Intelligence in modern cyber security operations and cyber defence.
- Apply AI and machine learning techniques to detect cyber threats, malware, phishing attacks, network anomalies, and insider threats.
- Analyze cyber threat intelligence from multiple sources to identify attack patterns, vulnerabilities, and emerging cyber risks.
- Develop AI-enabled security analytics and automated incident response solutions for enterprise, Industrial IoT, and critical infrastructure environments.
- Design intelligent cyber defence systems using AI, threat intelligence, and Security Operations Centre (SOC) technologies for Industry 5.0 applications.

Teaching-Learning Process:

1. Interactive Lectures with Recent Cyber Attack Case Studies
2. AI-Based Security Demonstrations
3. Hands-on Laboratory Sessions using Python
4. Threat Intelligence Analysis Workshops
5. Problem-Based Learning
6. Project-Based Learning
7. Flipped Classroom
8. Collaborative Learning
9. Industry Expert Sessions
10. Mini Projects and Technical Presentations

UNIT I – FUNDAMENTALS OF AI IN CYBER SECURITY	**[9 hours]**

Introduction to Artificial Intelligence in Cyber Security – Evolution of Intelligent Cyber Defence – Machine Learning Fundamentals – Supervised, Unsupervised and Reinforcement Learning Concepts – AI-Driven Security Operations – Cyber Threat Landscape – Attack Lifecycle – Security Analytics

– Security Operations Centre (SOC) Fundamentals – Applications of AI in Enterprise Security, Industrial IoT, Healthcare, Smart Manufacturing, and Smart Cities.

UNIT II – MACHINE LEARNING FOR CYBER THREAT DETECTION	**[9 hours]**
Cyber Security Data Sources – Security Logs – Network Traffic Data – Feature Engineering for Security Data – Classification Techniques – Anomaly Detection – Malware Detection – Phishing Detection – Spam Filtering – Intrusion Detection Systems using Machine Learning – Behavioural Analytics – User and Entity Behaviour Analytics (UEBA) – Model Evaluation Metrics for Cyber Security Applications	

UNIT III – CYBER THREAT INTELLIGENCE AND SECURITY ANALYTICS	**[9 hours]**
Introduction to Cyber Threat Intelligence (CTI) – Threat Intelligence Lifecycle – Threat Actors – Indicators of Compromise (IoCs) – Indicators of Attack (IoAs) – MITRE ATT&CK Framework (Overview) – Threat Hunting Concepts – Security Information and Event Management (SIEM) – Log Correlation – Threat Intelligence Platforms – Open-Source Intelligence (OSINT) – Cyber Risk Assessment – Security Analytics Dashboards.	

UNIT IV – AI-ENABLED INCIDENT RESPONSE AND SECURITY AUTOMATION	**[9 hours]**
AI-Based Incident Detection – Automated Threat Classification – Security Orchestration, Automation and Response (SOAR) Concepts – AI-Assisted Incident Response – Intelligent Malware Analysis – Endpoint Detection and Response (EDR) – Extended Detection and Response (XDR) Concepts – Cloud Security Analytics – AI for Industrial Cyber Security – Generative AI for Security Operations – Explainable AI in Cyber Security – Responsible AI and Ethical Considerations.	

UNIT V – AI APPLICATIONS IN CYBER SECURITY FOR SMART ENGINEERING	**[9 hours]**
AI-Based Security for Industrial IoT – Smart Manufacturing Security Analytics – Smart Grid Threat Detection – Healthcare Cyber Security Analytics – Connected Vehicle Security – Smart Building Security – AI-Based Fraud Detection – Digital Twin Security Concepts – Cyber Resilience – Zero Trust Security – Future Trends in AI for Cyber Security – Engineering Case Studies and Industry Applications	

Course outcomes:

On completion of the course, the student will have the ability to:

CO1	Explain AI, machine learning, and cyber threat intelligence concepts for intelligent cyber defence and security monitoring.
CO2	Apply machine learning algorithms to detect cyber attacks, malicious activities, and abnormal network behaviour.
CO3	Analyze cyber threat intelligence to identify vulnerabilities, assess risks, and support proactive cyber security operations.
CO4	Develop AI-enabled security analytics and automated incident response solutions for enterprise and industrial environments.
CO5	Design intelligent cyber security frameworks for Industrial IoT, cloud platforms, smart infrastructure, healthcare, and critical engineering systems.

COs and POs Mapping:

CO's	PO's										
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
1	2	2	1	1	1	3		-	-	1	2
2	1	1	1	1	2	3	-	-	-	1	2
3	1	1	1	2	2	3	-	-	-	1	2
4	1	1	1	2	2	2	-	-	-	2	2
5	1	1	1	2	2	2	-	-	-	2	2

Level 3- Highly Mapped, Level 2- Moderately Mapped, Level 1- Low Mapped, Level 0- Not Mapped

Scheme of Evaluation:

Component	**Typeof assessment**	**Max Marks**	**Reduced Marks**	**Total**	**Final marks**
Continuous Internal Examination (CIE)	CIE – I	100	50	100	40
	CIE – II	100			
	MCQ	20	10		
	Skill Assessment - I	40	40		
	Skill Assessment - II	40			
End Semester Examination (ESE)	Theory Exam	100	60	60	60
				Total	100

End semester Examination: (QP PATTERN)

- Each unit consists of two 2 marks questions and one 16 marks question (either or).
- All the fifteen questions have to be answered.

Assessment Pattern

Bloom's Category	Continuous Assessment Tests		Terminal Examination
	1	2	
Remember	60	50	60
Understand	40	50	40
Apply	0	0	0
Analyze	0	0	0
Evaluate	0	0	0
Create	0	0	0

TEXT BOOKS:

1. Clarence Chio and David Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms, O'Reilly Media, 2018.
2. Mark Stamp, Introduction to Machine Learning with Applications in Information Security, CRC Press, 2021.
3. Sushil Jajodia, Peng Liu, Vipin Swarup and Cliff Wang (Eds.), Cyber Situational Awareness: Issues and Research, Springer.

REFERENCE BOOKS:

1. Nina Godbole and Sunit Belapure, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India.
2. Jason Andress, The Basics of Information Security, 3rd Edition, Elsevier.
3. William Stallings, Network Security Essentials: Applications and Standards, 7th Edition, Pearson.
4. Palo Alto Networks, The AI Revolution in Cybersecurity (Industry Reference).
5. MITRE, ATT&CK® Framework Documentation (Reference Resource)

SUGGESTED SKILL ACTIVITIES

Students shall complete the following laboratory and skill-oriented activities.

1. Analyze cyber security datasets using Python and machine learning libraries.
2. Develop a phishing email detection model using supervised learning.
3. Perform anomaly detection on network traffic data.

4. Build a machine learning-based intrusion detection model.
5. Analyze security logs and identify Indicators of Compromise (IoCs).
6. Create a cyber threat intelligence dashboard using open-source datasets.
7. Develop an AI-assisted malware classification model.
8. Implement automated threat prioritization using machine learning techniques.
9. Prepare a cyber threat intelligence report for an engineering organization.
10. Complete a mini project on AI-enabled cyber defence for Industrial IoT or smart infrastructure.

Course Code:	**24CY702**	**Course Title:**	**Cyber Security Applications in Smart Engineering Systems**
Credits:	**3**	**L – T – P**	**3-0-0**
Prerequisite	**24CY501 - Foundations of Cyber Security and Ethical Hacking** **24CY502 - Network Security and Secure Communication**		

Course objectives:

The course enables the students to:

- Apply cyber security principles, tools, and best practices to design secure smart engineering systems across multidisciplinary domains.
- Develop cyber-resilient solutions for Industrial IoT (IIoT), Operational Technology (OT), cloud platforms, and critical infrastructure using modern security technologies.
- Integrate ethical hacking, digital forensics, AI-driven cyber security, and threat intelligence into engineering applications for proactive cyber defence.
- Build and evaluate secure engineering prototypes through vulnerability assessment, risk analysis, incident response, and security monitoring.
- Demonstrate professional competency through industry-oriented cyber security projects addressing real-world engineering and societal challenges.

Teaching-Learning Process:

1. Project-Based Learning
2. Challenge-Based Learning
3. Design Thinking Methodology
4. Hands-on Cyber Security Laboratory Sessions
5. Industry Case Studies
6. Capture-the-Flag (CTF) Exercises
7. Security Simulation and Demonstration
8. Collaborative Team Projects
9. Industry Expert Lectures
10. Technical Presentation and Project Review

UNIT I – CYBER SECURITY FOR SMART MANUFACTURING AND INDUSTRIAL AUTOMATION	**[9 hours]**

Industry 5.0 and Smart Manufacturing Security – Cyber-Physical Systems (CPS) Security – Industrial Internet of Things (IIoT) Security – Operational Technology (OT) Security – Industrial Control Systems (ICS) – SCADA and PLC Security – Industrial Network Segmentation – Secure Robotics –

AI-Based Predictive Maintenance Security – Supply Chain Security – Industrial Risk Assessment – Cyber Resilience in Manufacturing.

UNIT II – CYBER SECURITY FOR SMART ENERGY, TRANSPORTATION AND CIVIL INFRASTRUCTURE	**[9 hours]**
Smart Grid Cyber Security – Renewable Energy System Security – Intelligent Transportation System Security – Connected Vehicle Security – Smart Building Security – Building Management System (BMS) Security – Structural Health Monitoring Security – Water Distribution System Security – Smart City Security – Critical Infrastructure Protection – Disaster Recovery Planning – Infrastructure Cyber Resilience.	

UNIT III – CYBER SECURITY FOR HEALTHCARE, AGRICULTURE AND EMERGING ENGINEERING SYSTEMS	**[9 hours]**
Healthcare Information Security – Medical Device Security – Connected Healthcare Systems – Telemedicine Security – Precision Agriculture Security – Smart Irrigation Security – Agricultural Drone Security – Smart Warehouse Security – Supply Chain Cyber Security – Environmental Monitoring Systems – AI-Based Risk Assessment – Engineering Security Compliance	

UNIT IV – AI-DRIVEN CYBER DEFENCE, DIGITAL FORENSICS AND SECURITY OPERATIONS	**[9 hours]**
Artificial Intelligence for Cyber Defence – Security Analytics – Threat Intelligence – Security Operations Centre (SOC) – Security Information and Event Management (SIEM) – Security Orchestration, Automation and Response (SOAR) Concepts – Digital Forensics – Incident Response – Cloud Security Operations – Zero Trust Architecture – Cyber Security Governance – Business Continuity and Disaster Recovery	

UNIT V – CAPSTONE PROJECT: CYBER SECURITY SOLUTIONS FOR SMART ENGINEERING SYSTEMS	**[9 hours]**
Problem Identification – Cyber Risk Assessment – Requirement Analysis – Secure System Design – Security Architecture Development – Vulnerability Assessment – Threat Modelling – Security Testing – Prototype Development – Performance Evaluation – Security Compliance Assessment – Technical Documentation – Project Demonstration – Viva Voce – Industry Case Presentation.	

Course outcomes:

On completion of the course, the student will have the ability to:

CO1	Analyze cyber security risks and vulnerabilities in smart engineering systems and recommend appropriate security controls

CO2	Develop secure Industrial IoT, cloud, and communication architectures for multidisciplinary engineering applications
CO3	Apply ethical hacking, digital forensics, AI-based threat detection, and incident response techniques to engineering systems.
CO4	Implement cyber security monitoring, risk management, and compliance strategies for critical infrastructure and industrial environments.
CO5	Design, develop, and demonstrate an industry-oriented cyber security solution that addresses real-world engineering problems.

COs and POs Mapping:

CO's	PO's										
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
1	2	2	1	1	1	3		-	-	1	2
2	1	1	1	1	2	3	-	-	-	1	2
3	1	1	1	2	2	3	-	-	-	1	2
4	1	1	1	2	2	2	-	-	-	2	2
5	1	1	1	2	2	2	-	-	-	2	2

Level 3- Highly Mapped, Level 2- Moderately Mapped, Level 1- Low Mapped, Level 0- Not Mapped

Scheme of Evaluation:

Component	Typeof assessment	Max Marks	Reduced Marks	Total	Final marks
Continuous Internal Examination (CIE)	CIE – I	100	50	100	40
	CIE – II	100			
	MCQ	20	10		
	Skill Assessment - I	40	40		
	Skill Assessment - II	40			
End Semester Examination (ESE)	Theory Exam	100	60	60	60
				Total	100

End semester Examination: (QP PATTERN)

- Each unit consists of two 2 marks questions and one 16 marks question (either or).

- All the fifteen questions have to be answered.

Assessment Pattern

Bloom's Category	Continuous Assessment Tests		Terminal Examination
	1	2	
Remember	60	50	60
Understand	40	50	40
Apply	0	0	0
Analyze	0	0	0
Evaluate	0	0	0
Create	0	0	0

TEXT BOOKS:

1. Eric D. Knapp and Joel Thomas Langill, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA and Other Industrial Control Systems, 3rd Edition, Syngress, 2024.
2. William Stallings, Network Security Essentials: Applications and Standards, 7th Edition, Pearson, 2024.
3. Jason Andress, The Basics of Information Security, 3rd Edition, Elsevier, 2023.

REFERENCE BOOKS:

1. Nina Godbole and Sunit Belapure, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India.
2. Jason T. Luttgens, Matthew Pepe, and Kevin Mandia, Incident Response and Computer Forensics, McGraw-Hill.
3. Clarence Chio and David Freeman, Machine Learning and Security, O'Reilly Media.
4. Tyson Macaulay and Bryan Singer, Cybersecurity for Industrial Control Systems, CRC Press.
5. EC-Council, Certified Ethical Hacker (CEH) Official Courseware, Latest Edition

SUGGESTED SKILL ACTIVITIES

Students shall complete the following laboratory and skill-oriented activities.

Mini Skill Activities

1. Perform a cyber security audit for an Industrial IoT system.
2. Design a secure network architecture for a smart manufacturing plant.
3. Configure a firewall and intrusion detection system for a laboratory network.

4. Develop a vulnerability assessment report using open-source security tools.
5. Create a Security Operations Centre (SOC) dashboard for network monitoring.
6. Perform digital forensic analysis on simulated security incidents.
7. Develop an AI-based anomaly detection model for industrial sensor data.
8. Prepare an incident response and disaster recovery plan for a smart engineering system.
9. Conduct cyber risk assessment for healthcare, smart grid, or smart building applications.
10. Present findings through technical reports and project demonstrations.

CAPSTONE PROJECT DOMAINS

Students shall undertake projects in any one of the following domains.

Mechanical Engineering

- Secure Smart Manufacturing System
- Cyber Security for CNC Machines
- Industrial Robot Security
- Predictive Maintenance Security

Civil Engineering

- Smart Building Security
- Structural Health Monitoring Security
- Smart Water Distribution Security
- Intelligent Traffic Management Security

Electrical and Electronics Engineering

- Smart Grid Security
- Substation Cyber Security
- Renewable Energy System Protection
- Industrial Automation Security

Biomedical Engineering

- Connected Medical Device Security
- Hospital Information System Security
- Telemedicine Security
- Wearable Healthcare Device Protection

Agricultural Engineering

- Precision Agriculture Security
- Smart Irrigation Protection
- Agricultural Drone Security
- Smart Greenhouse Cyber Security

Multidisciplinary Projects

- Smart Campus Cyber Security
- AI-Based Threat Detection for Critical Infrastructure
- Secure Cloud Platform for Engineering Applications
- Cyber Security Framework for Industry 5.0
- Digital Twin Security Assessment
- Secure Smart City Monitoring System