Cummins College of Engineering for Women

(An autonomous institute affiliated to Savitribai Phule pune university)

Karve Nagar, Pune - 411 052.

Vision

To be globally renowned engineering institute for imparting holistic education and developing professional women leaders in engineering and technology

Syllabus Structure and Syllabus

of

Honors Degree Programme in
CYBER SECURITY
(Electronics and Telecommunication Engineering)

2023 Pattern [R0]

Autonomous Program Structure
B.Tech. in Electronics and Telecommunication

Honors Degree Programme in
CYBER SECURITY
Academic Year: 2025-2026 Onwards

TY Semester-V

Course Code	Course Title	Teaching Scheme Hours /Week			Examination Scheme			Marks	Credit
		Lecture	Tutorial	Practical	In Semester	End Semester	Pr/Or		
23HCS501	Data Security	3	1	0	50	50	0	100	4
23HCS502	Cloud Security	3	0	0	50	50	0	100	3
23HCS501L	Data and Cloud Security Lab	0	0	2	25	0	25	50	1
	Total	**6**	**1**	**2**	**125**	**100**	**25**	**250**	**8**

TY Semester-VI

Course Code	Course Title	Teaching Scheme Hours /Week			Examination Scheme			Marks	Credit
		Lecture	Tutorial	Practical	In Semester	End Semester	Pr/Or		
23HCS601	Web and Application Security	3	0	0	50	50	0	100	3
23HCS602	Network Security	2	0	0	50	0	0	50	2
23HCS601L	Web and Application Security Lab	0	0	2	25	0	25	50	1
	Total	**5**	**0**	**2**	**125**	**50**	**25**	**200**	**6**

APPROVED BY
Secretary Academic Council
MKSSS's Cummins College of Engineering
For Women, Pune-411052

APPROVED BY
Chairman Academic Council
MKSSS's Cummins College of Engineering
For Women, Pune-411052

MKSSS CUMMINS COLLEGE OF ENGG. FOR WOMEN ★ KARVENAGAR PUNE-52.

23HCS501 DATA SECURITY

Teaching Scheme
Lectures: 3 Hours / Week
Tutorial: 1 Hour/Week

Examination Scheme
ISE: 50 Marks
ESE: 50 Marks
Credits: 3

Prerequisite:

Course Objectives:

1 To understand cybersecurity fundamentals
2 To learn different encryption and authentication algorithms
3 To learn various types of network attacks and techniques to mitigate them
4 To understand wireless security

Course Outcomes:
After completion of the course, students will be able to

CO1 Explain the concepts of data security
CO2 Apply the cryptographic algorithms to secure the data
CO3 Explain the concept of digital signature and its schemes
CO4 Explain key managements and authentication protocols

Unit I: Basics of Data Security
Fundamental concepts data and its security, encryption, cryptography, authentication, and authorization, common cyber threats like phishing, malware, and ransomware

Unit II: Cryptography Fundamentals & Symmetric Key Cryptography
Basic Components, Security goals, Threats, Policy and Mechanism, Classical encryption techniques, Block and Chain ciphers, Symmetric Ciphers, Data Encryption Standard, Advanced Encryption Standard, RC5

Unit III: Asymmetric Key Cryptography
Asymmetric (Public) Key Cryptographic Systems: Concept of PKCS, RSA Cryptosystem-Variants of RSA – Primality testing – Security of RSA – Merkle – Hellman – Security of Merkle – Hellaman, ElGamal. Elliptical Curve Cryptography. Stream ciphers and block ciphers: The one time pad – Synchronous stream ciphers – Self-synchronizing stream ciphers – Feedback shift registers – Linear Complexity – Non-linear feedback shift registers – Stream ciphers based LFSRs

Unit IV: Digital Security
Message Integrity, Message Authentication, Secure Hash Algorithm (SHA) , Digital Signatures: Properties, Generic signature schemes,

Unit V: Key Management and Authentication Protocols
Symmetric Key Distribution, Distribution of public key, public key infrastructure, one-way authentication, Mutual Authentication. Kerberos

Text Books:

1. William Stallings, "Cryptography and Network Security: Principles and Practice", 6th Edition, Pearson Education,
ISBN 13: 9781292158587
2. Forouzan, B.A., "Cryptography & Network Security" Tata McGraw-Hill Education, ISBN-13: 978-0070702080
Kahate, A.,"Cryptography and Network Security". McGraw-Hill Higher Ed, ISBN-13: 9789353163303

Reference Books:

1. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C", 20th Anniversary Edition, Wiley, ISBN: 978-1-119-09672-6.
2 W. Stallings, Network Security Essentials: Applications and Standards,6th Edition, Pearson Prentice Hall, 2016.

Online Resources:

1. _ NPTEL course on Cryptography and Network Security
https://onlinecourses.nptel.ac.in/noc25_cs16/preview

23HCS502 CLOUD SECURITY

Teaching Scheme
Lectures: 3 Hours / Week

Examination Scheme
ISE: 50 Marks
ESE: 50 Marks
Credits: 3

Prerequisite:

Course Objectives:

1 Understand the fundamentals of cloud computing models and virtualization technologies.
2 Analyze security challenges in cloud environments and virtualization platforms.
3 Implement basic security practices in virtualized systems and cloud services.
4 Evaluate cloud access control, identity management, encryption, and compliance.
5 Demonstrate the ability to secure and monitor workloads in cloud infrastructures

Course Outcomes:
After completion of the course, students will be able to

CO1 Explain cloud architecture, service models, and virtualization technologies
CO2 Identify and assess potential security risks in cloud and virtual environments
CO3 Describe identity management and security mechanisms on cloud platforms
CO4 Apply security best practices and compliance policies in simulated cloud scenarios

Unit I: Introduction to Cloud and Virtualization
Cloud Computing Overview: Public, Private, Hybrid, Multi-cloud, Cloud Service Models: IaaS, PaaS, SaaS, Virtualization Basics: Hypervisors (Type 1 and 2), Virtual Machines, Containers, Virtualization Tools: VMware, VirtualBox, Docker, Benefits and Risks of Cloud Adoption

Unit II: Cloud Security Architecture
Cloud Security Concepts: Shared Responsibility Model, Attack Surfaces, Cloud Threats: Data breaches, insecure APIs, misconfiguration, DoS, Zero Trust Architecture in the Cloud, Virtualization Vulnerabilities and Mitigations, Cloud Security Alliance (CSA) Guidelines.

Unit III: Identity, Access, and Data Protection
Cloud IAM: Role-based Access Control (RBAC), Attribute-based Access Control (ABAC), Authentication and Authorization in Cloud, Identity Federation and SSO (e.g., SAML, OAuth2, OpenID Connect), Cloud Key Management Services (KMS), Encryption of Data at Rest/Transit, Audit Trails and Logging

Unit IV: Cloud Monitoring, Compliance, and Secure DevOps
Cloud Monitoring Tools (AWS CloudWatch, Azure Monitor), Incident Response in Cloud Environments, Cloud Compliance Frameworks (GDPR, HIPAA, SOC 2, ISO 27017), Container Security: Docker, Kubernetes Security Best Practices, Basics of DevSecOps: CI/CD Pipeline Security, Infrastructure as Code (IaC) Risks

Text Books:

1. **Tim Mather, Subra Kumaraswamy, Shahed Latif,** *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance,* Publisher: O'Reilly Media, **1st Edition, 2009**
2. **Thomas Erl,** *Cloud Computing: Concepts, Technology & Architecture,* Publisher: Pearson Education, **1st Edition, 2013**

Reference Books:

1. **Ronald L. Krutz & Russell Dean Vines,** *Cloud Security: A Comprehensive Guide to Secure Cloud Computing,* Publisher: Wiley, **1st Edition, 2010**
2. **Kris Jamsa,** *Cloud Computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security, and More* Publisher: Jones & Bartlett Learning, **1st Edition, 2013**
3. **Cloud Security Alliance (CSA),** *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0,* Published by CSA, **2017**
4. **OWASP Cloud-Native Application Security Top 10**
   OWASP Foundation, **Latest Version: 2022**

Online Resources:

1. NPTEL course on Cyber Security and Privacy. By Prof. Saji K Mathew | IIT Madras
   https://onlinecourses.nptel.ac.in/noc23_cs127/preview?utm_source=chatgpt.com
2. NPTEL course on Cloud Computing and Distributed Systems. By Prof. Rajiv Misra | IIT Patna
   https://onlinecourses.nptel.ac.in/noc22_cs18/preview?utm_source=chatgpt.com

23HCS501L DATA AND CLOUD SECURITY LAB

Teaching Scheme
Lectures: 2 Hours / Week

Examination Scheme
ISE: 25 Marks
ESE: 25 Marks
Credits: 1

Course Objective

1. Understand and apply fundamental concepts of cloud computing and virtualization tools
2. Analyze and implement various cloud service models
3. Explore and implement cloud security mechanisms
4. Utilize monitoring, compliance, and DevSecOps practices

Course Outcome

After completion of the course, students will be able to

CO1 Implement Symmetric and asymmetric Cryptographic algorithms
CO2 Implement message integrity and authentication protocols
CO3 Identify common cloud security threats
CO4 Apply encryption techniques for securing data using cloud-based key management services

List of Experiments:

1. Implement DES algorithm
2. Implement RSAalgorithm
3. Implement Message Digest Algorithm
4. Implementation of Diffie Hellman Key exchange
5. Installation and Comparison of Virtualization Tools: VirtualBox, VMware, and Docker
6. Deploying a Web Application Using IaaS, PaaS, and SaaS Models
7. Creating and Securing Docker Containers
8. Simulating Common Cloud Security Threats and Applying Mitigations
9. Implementing IAM with RBAC and ABAC Policies on a Cloud Platform
10. Encrypting Data at Rest and in Transit Using Cloud KMS
11. Monitoring Cloud Resources and Configuring Alerts
12. Implementing Security Policies and Compliance Controls
13. Building a Secure CI/CD Pipeline with Security Scanning Tools
14. Installation and Comparison of Virtualization Tools: VirtualBox, VMware, and Docker

20HCS601 WEB AND APPLICATION SECURITY

Teaching Scheme
Lectures: 3 Hours / Week

Examination Scheme
ISE: 50 Marks
ESE: 50 Marks
Credits: 3

Course Objectives:

1 Understand the fundamentals of web applications and security
2 To learn how to build secure APIs
3 To learn about Web services vulnerabilities, their tools and testing
4 To understand Secure API Development

Course Outcomes:

After completion of the course, students will be able to

CO1 Explain Web application fundamentals and web security fundamentals
CO2 Identify common web application security threats
CO3 Compare vulnerability assessment tools and penetration testing
CO4 Analyze Hacking techniques and Tools

Unit I: Web Application Fundamentals

Web Application Fundamentals Client-side scripting, Server-side scripting; Web server architecture - Windows & Linux, IIS and LAMP servers, Network protocols, Introduction to web applications, Web application hacking, Overview of browsers, extensions, and platforms, common web authentication mechanisms and online authentication services.

Unit II: Fundamentals of Web Application Security

The history of Software Security- Recognizing Web Application Security Threats, Web Application Security, Authentication and Authorization, Secure Socket layer, Transport layer Security, Session Management, Input Validation.

Unit III: Web services vulnerabilities, Assessment Tools and Penetration test

WSDL disclosure, input injection, external entity injection, and XPath injection. Web application management attacks against remote server management, web content management/authoring, admin misconfigurations, and developer-driven mistakes. Web browser exploits, Vulnerability Assessment Lifecycle, Vulnerability Assessment Tools, Types of Penetration Tests.

Unit IV: Secure API Development

API Security- Session Cookies, Token-Based Authentication, Securing Natter APIs: Addressing threats with Security Controls, Rate Limiting for Availability, Encryption, Audit logging, Securing

service-to-service APIs: API Keys, OAuth2, Securing Microservice APIs: Service Mesh, Locking Down Network Connections, Securing Incoming Requests.

Unit V: Network Security

Transport and Network Layer Security, Protocols IPsec, SSL, HTTPS, Types of Network attacks, LAN attacks, Network sniffing, DDoS attack, DNS Flood attack, Firewall, Virtual Private Networks (VPN). Wi-Fi Security, WEP, WPA, WPA-2, Mobile Device Security- Security Threats, Device Security, GSM and UMTS Security, IEEE 802.11/802.11i Wireless LAN Security, VPN Security.

Text Books:

1. Andrew Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications, First Edition, 2020, O'Reilly Media, Inc.
2. Bryan Sullivan, Vincent Liu, Web Application Security: A Beginners Guide, 2012, The McGraw-Hill Companies.
3. Neil Madden, API Security in Action, 2020, Manning Publications Co., NY, USA.
4 Forouzan, B.A., "Cryptography & Network Security" Tata McGraw-Hill Education, ISBN-13: 978-0070702080

Reference Books:

1. Michael Cross, Developer's Guide to Web Application Security, 2007, Syngress Publishing, Inc.
2. Ravi Das and Greg Johnson, Testing and Securing Web Applications, 2021, Taylor & Francis Group, LLC.
3. Prabath Siriwardena, Advanced API Security, 2020, Apress Media LLC, USA.
4. Malcom McDonald, Web Security for Developers, 2020, No Starch Press, Inc.
5. Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, and Terron Williams
6. Grey Hat Hacking: The Ethical Hacker's Handbook, Third Edition, 2011, The McGraw-Hill companies.

Online Resources:

1. NPTEL Information Security and Forensics, 2018 - Bangalore, IIT Madras
   https://nptel.ac.in/courses/128106006
2. NPTEL INTRODUCTION TO CYBER SECURITY
   https://onlinecourses.swayam2.ac.in/nou19_cs08/preview

20HCS602 NETWORK SECURITY

Teaching Scheme
Lectures: 2 Hours / Week

Examination Scheme
ISE: 50 Marks
Credits: 2

Prerequisite:

Course Objectives:

1 Understand the Network Attack Surface and underlying Technologies
2 Understand how Network Security is implemented
3 Explain Network Vulnerability Types and Exploitation
4 Explain Secure Implementation of Network Layer Devices and Tools

Course Outcomes:

After completion of the course, students will be able to

CO1 Explain key concepts, tools, and standards used in network security.
CO2 Apply security techniques to protect networks from breaches
CO3 Analyze security controls in public, private, and hybrid cloud networks
CO4 Evaluate network vulnerabilities and implement prevention and detection measures

Unit I: Basics of Network Security

Introduction to different types of Networks, Types of Protocols, Communication between various protocols, security techniques that makes overall communication secure, Concepts like Authentication/Authorization in Networks, SSL, VPN, TLS Protocols, Phases of Network Security Assessment, Foot printing and Reconnaissance Techniques, Network Scanning and Enumeration, Tools: Nmap, Nessus, whois, Shodan, TOR, Interceptor Proxy

Unit II: Network Security Tools and Technologies

Identify working of various Network Security tools, devices and underlying technologies, how to implement them, how to configure them, Usage of each tool as a safeguard against vulnerabilities, how the network later attacks are identified and prevented/detected by these tools, IDS/IPS, WAF, Firewalls, Anti-Virus, Endpoint Security, SIEM/SOAR, MDR, XDR Technologies

Unit III: Network Security in Cloud

Understand Public, Private and Hybrid Clouds, How the on-premises and Cloud platforms are different in terms of Networks, what is there to protect in Cloud, Underlying Cloud Network Technologies, Cloud Workload Protection, Cloud Native Application Protection, Secure communication in Virtual Private Cloud, Interfaces Security, Concepts like CWPP, CNAPP, CSPM, Explain the terminologies and demo of various Security Services on Azure Cloud Platform, Introduction to Amazon AWS and Google Cloud Platform

Unit IV: Network Vulnerabilities Exploitation and Prevention/Detection

Explain Network Vulnerabilities Exploitation and Prevention/Detection, understand different security vulnerabilities, explain how they impact the networks, how to identify the vulnerabilities, Secure logging, auditing Techniques, Packet based security analysis, Security at various levels of Network Implementation, Usage of Nessus, Nmap, Traceroute, Ping utilities, basic Linux commands for Network Security Analysis

Text Books:

1. William Stallings, "**Network Security Essentials: Applications and Standards**", *Pearson India Publications* (6th Edition), 2016
2. Robert Wilson, Michael T. Simpson, Nicholas Antill, "**Hands-on Ethical Hacking and Network Defense**", *Cengage India* (4th Edition), 2022

Reference Books:

1. Michael E. Whitman, Mattord, Herbert J, Mackey, David, "**Guide to Network Security**", *Cengage India* (7th Edition), 2021
2. Gordon Fyodor Lyon, "**Nmap Network Scanning: The Official Nmap Project Guide**", *Random House*, (3rd Edition), 2024

Online Resources:

1. **NPTEL Course:** Network Security: https://onlinecourses.nptel.ac.in/noc25_ee54/preview
2. https://tryhackme.com/module/network-security?

23HCS601L WEB AND APPLICATION SECURITY LAB

Teaching Scheme
Lectures: 2 Hours / Week

Examination Scheme
ISE 25 Marks
ESE: 25 Marks
Credits: 1

Course Objective

1. Understanding of web applications.
2. Understanding web application attacks and techniques.
3. Learn vulnerability assessments using various foot printing and enumeration techniques in web applications.

Course Outcome

After completion of the course, students will be able to

CO1 Apply the process for secure development and deployment of web applications
CO2 Acquire the skill to design and develop Secure Web Applications that use Secure APIs
CO3 Implement the vulnerability assessment and penetration testing,/Systematic vulnerability detection

List of Experiments:

1. Install Wireshark and explore the various protocols
2. Analyze the difference between HTTP vs HTTPS
3. Analyze the various security mechanisms embedded in different protocols.
4. Identify the vulnerabilities using OWASP ZAP tool
5. Create REST API for operations like GET, PUSH, POST, DELETE
6. Install Burp Suite to do SQL injection vulnerabilities
7. Perform cross-site scripting (XSS) vulnerabilities
8. Attack the website using Social Engineering method