INSTITUTE OF AERONAUTICAL ENGINEERING
(Autonomous)
Dundigal - 500 043, Hyderabad, Telangana

COURSE CONTENT

SECURITY ARCHITECTURE AND PROTOCOLS								
VII Semester: CSE (CS)								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
ACCD19	Core	3	0	0	3	40	60	100
Contact Classes: 48	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 48**		
Prerequisites: There are no prerequisites to take this course								

I. COURSE OVERVIEW:
Security Architecture and Protocols focus on designing secure network infrastructures, cryptographic mechanisms, and security protocols. The course covers authentication, access control, and emerging technologies like SDN and NFV. Students will analyze threats, implement mitigation strategies, and configure security frameworks. Hands-on labs provide practical experience in securing networks and defending against cyber threats.

II. COURSE OBJECTIVES:
The students will try to learn:

I	The implementation of cryptographic techniques and network security protocols.
II	The security mechanisms in networked and distributed systems
III	The deployment of secure architectures using SDN and NFV.
VI	The analysis of network vulnerabilities and threat mitigation techniques.

III. COURSE OUTCOMES:
After successful completion of the course, students should be able to:

CO1	Implement cryptographic techniques and secure communication protocols.
CO2	Configure and analyze security measures in SDN and NFV environments
CO3	Evaluate security vulnerabilities in various network architectures.
CO4	Design secure network frameworks using contemporary security technologies.
CO5	Use security tools for penetration testing, monitoring, and threat analysis.
CO6	Demonstrate best practices in network security and cyber defense strategies.

IV. COURSE CONTENT:

MODULE -I: FUNDAMENTALS OF SECURITY ARCHITECTURE (10)

Introduction to security architecture and cryptographic protocols; Secure networking environment setup; Authentication mechanisms and access control models; Secure socket implementation and VPN configurations; Cryptographic algorithms: AES, RSA, SHA; Key exchange and management techniques; Intrusion detection and prevention systems (IDS/IPS); Network traffic analysis using packet sniffers; Case study on security failures in network architectures.

MODULE –II: NETWORK SECURITY PROTOCOLS (10)

Implementation of SSL/TLS for secure communication; IPsec and secure data transmission techniques; Email security protocols: PGP, S/MIME; Firewall configuration and access control list (ACL) rules; Wireless security: WPA3, network authentication; Securing DNS and mitigating DNS-based attacks; Application-layer security: HTTPS, OAuth, JWT; Multi-factor authentication (MFA) implementation; Case study on protocol vulnerabilities and real-world attacks.

MODULE-III: NETWORK FUNCTION VIRTUALIZATION AND NETWORK TOPOLOGY(09)

Introduction to NFV and its security challenges; Implementation of virtualized network functions; Secure cloud-based network architectures; Network segmentation and micro-segmentation techniques; Virtual network traffic monitoring and analysis; Security automation and orchestration in NFV; DDoS mitigation strategies in NFV environments; Case study on NFV security concerns; Hands-on lab for secure NFV deployment.

MODULE-IV: BUILDING AN SDN FRAMEWORK (10)

Introduction to SDN and its security implications; SDN controller setup and secure API configuration; Secure communication between SDN components; Role-based access control in SDN environments; Threat modeling and attack prevention in SDN; Secure data plane and control plane communication; Case study on SDN security breaches and mitigation; Anomaly detection techniques in SDN; Hands-on lab for securing SDN-enabled networks.

MODULE-V: ADVANCED SECURITY IN NETWORK FUNCTION VIRTUALIZATION (NFV) (09)

Security challenges in NFV-based network infrastructures; Deploying security mechanisms in NFV environments; Secure service function chaining in NFV; AI/ML applications in NFV security; Performance analysis of NFV security solutions; Orchestration tools for NFV security management; Mitigation of side-channel attacks in NFV; Case study on NFV security implementation strategies; Hands-on lab for NFV security deployment.

V. TEXTBOOKS:

1. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson Education, 8th Edition, 2022.
2. Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security: Private Communication in a Public World, Pearson, 3rd Edition, 2022.
3. Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill, 2nd Edition, 2010.

VI. REFERENCE BOOKS:

1. Bruce Schneier, Applied Cryptography, Wiley, 2nd Edition, 1995.
2. Douglas R. Stinson, Cryptography: Theory and Practice, CRC Press, 3rd Edition, 2005.
3. Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, Cryptography Engineering: Design Principles and Practical Applications, Wiley, 1st Edition, 2010.

VII. ELECTRONIC RESOURCES:

1. https://www.nist.gov
2. https://ieeexplore.ieee.org
3. https://www.sans.org
4. https://owasp.org
5. https://www.coursera.org

VIII. MATERIAL ONLINE:

1. Course template
2. Tech-talk topics
3. Assignments
4. Definition and terminology
5. Tutorial question bank
6. Model question paper – I
7. Model question paper – II
8. Lecture notes
9. Early lecture readiness videos (ELRV)
10. Power point presentations