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

COURSE CONTENT

DISTRIBUTED SYSTEMS AND SECURITY								
VII Semester: CSE(DS)								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
ACDD20	**Core**	3	0	0	3	40	60	100
Contact Classes: 48	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 48**		
Prerequisites: **Basic understanding of operating systems, computer networks, and programming fundamentals.**								

I. COURSE OVERVIEW:

This course introduces the fundamental principles and practical aspects of distributed systems and security. It explores the architecture, communication models, coordination algorithms, and fault-tolerant techniques required for building distributed applications. Students will gain an understanding of how independent systems cooperate, share resources, and ensure consistency in a networked environment. The course also covers essential security aspects such as cryptographic techniques, authentication, access control, and secure communication protocols. Through case studies and hands-on exercises, students will learn to develop reliable and secure distributed systems suitable for cloud, peer-to-peer, and enterprise environments.

II. COURSE OBJECTIVES:

The students will try to learn:

I. The core principles of distributed systems, including architecture, communication, coordination, and fault tolerance across multiple nodes in a networked environment.
II. The models, algorithms, and mechanisms used in implementing key distributed system functionalities such as time synchronization, consensus, replication, and resource sharing.
III. The fundamentals of cybersecurity in distributed environments, including authentication, access control, secure communication, and encryption techniques.
IV. The practical challenges of designing secure distributed applications, focusing on threats, vulnerabilities, and defense strategies in cloud, peer-to-peer, and decentralized systems.

III. COURSE OUTCOMES:

CO1 **Explain** the fundamental concepts and architectural models of distributed systems, including transparency, scalability, and fault tolerance.
CO2 **Analyze** communication mechanisms such as Remote Procedure Call (RPC), Remote Method Invocation (RMI), and message-passing used in distributed environments.
CO3 **Apply** algorithms for synchronization, mutual exclusion, and election in distributed computing environments.
CO4 **Evaluate** consistency and replication models and their role in achieving data reliability and availability in distributed systems.
CO5 **Implement** security mechanisms including encryption, authentication, access control, and secure communication protocols in distributed systems.
CO6 **Assess** threats, vulnerabilities, and appropriate countermeasures in the design and deployment of secure distributed applications.

IV. COURSE CONTENT:

MODULE – I: INTRODUCTION TO DISTRIBUTED SYSTEMS (09)
Introduction to Distributed Systems, Characteristics of Distributed Systems: Transparency, Openness, Scalability, Fault Tolerance, System Architectures: Client-Server, Peer-to-Peer, Middleware, Communication in Distributed Systems: Message Passing, RPC, RMI, Case Study: Distributed File Systems

MODULE – II: TIME, SYNCHRONIZATION, AND COORDINATION (10)
Clock Synchronization: Cristian's Algorithm, Berkeley Algorithm, Logical Clocks: Lamport Timestamps, Vector Clocks, Coordination and Agreement: Mutual Exclusion Algorithms (Centralized, Ricart-Agrawala), Election Algorithms: Bully and Ring Algorithms, Distributed Deadlock Detection and Recovery

MODULE – III: CONSISTENCY, REPLICATION, AND FAULT TOLERANCE (10)
Data-Centric Consistency Models: Strict, Sequential, Causal, Client-Centric Consistency: Monotonic Reads, Writes, Read-Your-Writes.

Replication Techniques: Active vs Passive Replication, Fault Tolerance Mechanisms: Byzantine Fault Tolerance, Recovery Models, Case Study: Google File System, Hadoop Distributed File System (HDFS)

MODULE – IV: FUNDAMENTALS OF SECURITY IN DISTRIBUTED SYSTEMS (09)
Overview of Information Security: CIA Triad, Cryptographic Techniques: Symmetric and Asymmetric Encryption, Hashing, Authentication: Passwords, Digital Certificates, Kerberos, Access Control: DAC, MAC, Role-Based Access Control (RBAC), Secure Communication: SSL/TLS Protocols

MODULE – V: SECURITY CHALLENGES AND APPLICATIONS (10)
Security in Cloud and Grid Environments, Web Services Security: XML Encryption, XML Signature, Threats and Vulnerabilities: DOS, Man-in-the-Middle, Malware, Intrusion Detection and Prevention Systems, Secure Software Development Practices, Case Studies: Blockchain Security, Secure File Transfer Protocols

V. TEXTBOOKS:

1. Andrew S. Tanenbaum and Maarten Van Steen, Distributed Systems: Principles and Paradigms, 2nd Edition, Pearson Education, 2007
2. George Coulouris, Jean Dollimore, Tim Kindberg, and Gordon Blair, Distributed Systems: Concepts and Design, 5th Edition, Pearson Education, 2012
3. William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson, 2017
4. Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill Education, 2007

VI. REFERENCE BOOKS:

1. **Dieter Gollmann**, *Computer Security*, 3rd Edition, Wiley India, **2011**

VII. WEB REFERENCES

1. NPTEL - Distributed Systems – by IIT Madras
2. NPTEL - Cryptography and Network Security – by IIT Kharagpur
3. GeeksforGeeks – Distributed Systems Tutorials
4. IBM Developer – Introduction to Distributed Systems

VIII. MATERIALS ONLINE

1. Course template
2. Tutorial question bank
3. Tech talk topics
4. Open-ended experiments
5. Definitions and terminology
6. Assignments
7. Model question paper – I
8. Model question paper – II
9. Lecture notes
10. PowerPoint presentation
11. E-Learning Readiness Videos (ELRV)