

20CS017 CLOUD SECURITY

Hours Per Week :

L	T	P	C
3	-	-	3

Total Hours :

L	T	P	WA/RA	SSH/HSB	CS	SA	S	BS
45	-	-	15	30	-	5	5	-

Course Description and Objectives:

The course on cloud security introduces the basic concepts of security systems and cryptographic protocols, which are widely used in the design of cloud security. The issues related multi tenancy operation, virtualized infrastructure security and methods to improve virtualization security are also dealt with in this course.

Course Outcomes:

Upon the Completion of the course, students will be able to:

- ✓ Articulate the main concepts of cloud security.
- ✓ Analyze the architecture design of cloud storage.
- ✓ Understand the core issues of cloud management and security.
- ✓ Design & Development current cloud Technologies.
- ✓ Apply secure design for cloud Models.

SKILLS:

- ✓ MVC standard development of applications.
- ✓ Working with Integrated Development Environment.
- ✓ Internationalization concepts.
- ✓ Web services concepts.

UNIT I

Cloud Computing Fundamentals: Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vs private clouds, role of virtualization in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture.

UNIT II

Cloud Applications: Technologies and the processes required when deploying web services Deploying a web service from inside and outside a cloud architecture, advantages, and disadvantages- Development environments for service development; Amazon, Azure, Google App.

UNIT III

Securing the Cloud: Security Concepts - Confidentiality, privacy, integrity, authentication, nonrepudiation, availability, access control, defence in depth, least privilege- how these concepts apply in the cloud and their importance in PaaS, IaaS and SaaS. e.g. User authentication in the cloud

UNIT IV

Virtualization Security: Multi-tenancy Issues: Isolation of users/VMs from each other- How the cloud provider can provide this- Virtualization System Security Issues: e.g. ESX and ESXi Security, ESX file system security- storage considerations, backup and recovery- Virtualization System Vulnerabilities.

UNIT V

Cloud Security Management: Security management in the cloud – security management standards SaaS, PaaS, IaaS availability management- access control- Data security and storage in cloud.

TEXT BOOKS:

1. Gautam Shroff, "Enterprise Cloud Computing Technology Architecture Applications", Cambridge University Press; 1 edition [ISBN: 978- 0521137355], 2010.
2. Toby Velte, Anthony Velte, Robert Eisenpeter, "Cloud Computing, A Practical Approach", Tata McGraw-Hill Osborne Media; 1 edition 22, [ISBN: 0071626948], 2009.

REFERENCE BOOKS:

1. Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", O'Reilly Media; 1 edition, [ISBN: 0596802765], 2009.
2. Ronald L. Krutz, Russell Dean Vines, "Cloud Security", Wiley [ISBN: 0470589876], 2010.
3. Kai Hwang, Geoffrey C Fox, Jack G Dongarra, "Distributed and Cloud Computing, From Parallel Processing to the Internet of Things", Morgan Kaufmann Publishers, 2012.