CA20320A **(3L + 1 T hrs./week)**

VIRTUALIZATION AND CLOUD SECURITY

No. of questions to be set: Total 5 questions will be given from Unit I & Unit II.
No. of questions to be answered: All questions to be answered.

Objectives: This course gives an insight into virtualization techniques and security practices in computing.

Pre-requisites: Operating Systems and Computer Network.

Course Outcomes (CO):

CO1	Students will able to understand the importance and role of virtualization in cloud.
CO2	Students will be able to understand the concept of security related threats in virtual environment for cloud computing.
CO3	Students will be able to understand the technology and platform for cloud security.

UNIT I

Virtualized Data Centre Architecture [6 Hrs]
Cloud infrastructures; public, private, hybrid. Service provider interfaces; SaaS, PaaS, IaaS. VDC environments; concept, planning and design, business continuity and disaster recovery principles. Managing VDC and cloud environments and infrastructures.

Information Storage Security and Design [6 Hrs]
Storage strategy and governance; security and regulations. Designing secure solutions; the considerations and implementations involved. Securing storage in virtualized and cloud environments. Monitoring and management; security auditing and SIEM.

Storage Network Design [8 Hrs]
Architecture of storage, analysis and planning. Storage network design considerations; NAS and FC SANs, hybrid storage networking technologies (iSCSI, FCIP, FCoE), design for storage virtualization in cloud computing, host system design considerations.

UNIT II

Security Concepts [7 Hrs]
Confidentiality, privacy, integrity, authentication, non-repudiation, availability, access control, defence in depth, least privilege, how these concepts apply in the cloud, what these concepts mean and their importance in PaaS, IaaS and SaaS. e.g. User authentication in the cloud; Cryptographic Systems- Symmetric cryptography, stream ciphers, block ciphers, modes of operation, public-key cryptography, hashing, digital signatures, public-key infrastructures, key management, X.509 certificates, OpenSSL.

Secure Virtual Networking [7 Hrs]
Configuration and change management goals and guidelines, tools and technologies in virtualized environments; Virtual network security architecture, network segmentation and traffic isolation to secure a virtual network configuration.

Cloud Security and Privacy [6 Hrs.]

Infrastructure security, Data security, Security management in cloud, Privacy, Security in the cloud, Cloud Information security, Cloud security services, Design principles, Secure Cloud Software Requirements, Cloud Computing Security Challenges. Future of cloud computing.

Text Book

1. Greg Schulz, “Cloud and Virtual Data Storage Networking”, Auerbach Publications, 2011.
2. Tim Mather, SubraKumaraswamy, ShahedLatif, “Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance” O'Reilly Media; 1st edition, 2009

References

1. Marty Poniatowski, “Foundations of Green IT” Prentice Hall; 1 edition, 2009.
2. EMC, “Information Storage and Management” Wiley; 2 edition,2012.
3. Volker Herminghaus, Albrecht Scriba, “Storage Management in Data Centers” Springer, 2009.