National Forensic Sciences University
Knowledge | Wisdom | Fulfilment
An Institution of National Importance
(Ministry of Home Affairs, Government of India)

Subject Name: Cloud Security and Forensics

Subject Code: CTMSCS SIII P3

Teaching and Evaluation Scheme:

Teaching Scheme					Evaluation Scheme								
Th	Tu	Pr	C	TCH	Theory						Practical		Total
					Internal Exams				University Exams		University Exams (LPW)		
					TA-1/TA-2		MSE						
					Marks	Hrs	Marks	Hrs	Marks	Hrs	Marks	Hrs	
3	0	0	3	3	25	45 min	50	1.5	100	3	-	-	200

*Note: TA-2 will be in the form of assignments or workshops.

Objectives:

1. Understand key terms and concepts in cloud security and forensics.
2. Understand the underlying principles in how a cloud is built and operated.
3. Ability to understand the available cloud infrastructure.
4. Ability to identify, analyze and remediate cloud security breaches by learning and implementing real-world scenarios.
5. Develop policies to strengthen the security of the cloud and carry out forensic analysis.

UNIT – I
Introduction to cloud computing

Introduction to cloud computing, characteristic of cloud computing, Evolution of Cloud Computing, Feature, characteristic and components of cloud computing, cloud computing reference architecture of NIST, Layer and Types of Cloud, Risk and Approaches of Migration into Cloud, Research challenges. Cloud Computing Security Baseline: Overview of computer security, vulnerabilities and attacks, privacy and security in cloud storage services, privacy and security in multi clouds, Understanding the Threats, Classification and countermeasures: Infrastructure and host threats, service provider threats, generic threats, threat assessment.

UNIT - II
Cloud Computing Architecture

Different storage types,: Object storage, Block storage, File storage, Securing the Hypervisor :Various types of virtualization, Full virtualization, Paravirtualization, Partial virtualization, Comparison of virtualization levels, Hypervisors: Kernel based Virtual Machine, Xen, VMware ESXi, Hyper-V, BareMetal, Containers, Docker, Linux Containers, Criteria for choosing a hypervisor : Team expertise, Product or project maturity, Certifications and attestations, Features and performance, Hardware concerns, Hypervisor memory optimization, Additional security features, Hardening the hardware management: Physical hardware - PCI passthrough,Virtual hardware with Quick Emulator, virtualization, Hardening the host operating

UNIT - III
Cloud Service Models

Cloud computing models: Service model and deployment model : PaaS -Working Principle, Example, SaaS -Working Principle, Example, laas -Working Principle, Example, Recent Service Models : BMaas, XaaS, cloud services and technologies, Service Management in Cloud, Service Level Agreements (SLAS). Billing & Accounting, Comparing scaling, Datacenter Design and Interconnection Network, Cloud Logging Services, Log Collection and Analysis

UNIT-IV
Securing Cloud Communications and API

Encryption security, Symmetric encryption, Stream cipher, Block cipher, Asymmetric encryption, Difie-Hellman, RSA algorithm, Elliptic Curve Cryptography, Symmetric/asymmetric comparison and synergies, Hashing, MD5, SHA, Public key, infrastructure, signed certificates versus self-signed certificates, cipher security, Designing a redundant environment for your APls. Identification and Authentication System and Its Dashboard dentification versus authentication versus authorization, Identification, Authentication: Something you know, something you have, something you are, The multifactor authentication, Authorization: Mandatory Access Control, Discretionary Access Control, Role-based Access Control, Lattice-based Access Control, Session management, Federated identity.

UNIT-V
Emerging Cloud Environments and Cloud Forensics

Case Study on Open Source and Commercial Clouds: Emerging Cloud Environment, Eucalyptus Architecture, Open Nebula, Nimbus. Google App Engine (GAE), IBM Cloud, VM Ware cloud, Cloud Forensics, Cloud Forensic Frameworks, Digital Forensic Investigation and Cloud Computing, Dimensions of cloud forensics, cloud crime, challenges in cloud forensics, usages of cloud forensics, Cloud forensics tools.

Reference Books

1. Practical Cloud Security: A Guide for Secure Design and Deployment by Chris Doston
2. CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide by Brian T O'Hara
3. OpenStack Cloud Security Paperback by Alessandro Locati Fabio, PacktPub
4. Cloud Computing Security: Foundations and Challenges edited by John R. Vacca, CRC Press
5. Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Ronald L. Krutz, Russell Dean Vines, John Wiley & Sons