राष्ट्रीय प्रौद्योगिकी संस्थान पटना / NATIONAL INSTITUE OF TECHNOLOGY PATNA
संगणक विज्ञान एंव अभियांत्रिकी विभाग / DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
अशोक राजपथ, पटना-८००००५, बिहार / ASHOK RAJPATH, PATNA-800005, BIHAR
Phone No.: 0612-2372715, 2370419, 2370843, 2371929 Ext- 200, 202 Fax-0612-2670631 Website: www.nitp.ac.in

No:- Date:

CSXX2825: Cloud Computing Security

L-T-P-Cr: 3-0-0-3

Pre-requisites: Prior knowledge ofComputer Network, Cryptography

Course Objectives:

1. To understand the fundamental of cloud computing architectures.
2. To identify the threats, risks, and privacy issues of cloud computing.
3. To design cloud security architecture
4. To monitor, auditing and managing cloud infrastructure
5. To understand the industry security standards, regulatory mandates, audit policies and compliance requirements.

CO-PO Mapping:

No	**Course Outcomes**	**Mapping to POs**
1	Recall basic concepts of cloud computing.	PO1, PO5, PO6
2	Understand the concepts of NIST cloud computing architecture and its design challenges.	PO1, PO4, PO6
3	Analyze the issues in resource provisioning and security governance in the cloud.	PO1, PO3, PO6
4	Apply access control and monitor a cloud computing environment efficiently.	PO1,PO3,PO5
5	Understanding policy, compliance and risk management in cloud computing.	PO1, PO6, PO8
6.	Design cloud security models and apply them to solve real life problems.	PO1, PO3, PO5, PO6, PO9, PO11

Syllabus

UNIT I: Fundamentals of Cloud Computing **Lectures: 2**

Introduction to cloud computing, Characteristics, Advantages, Disadvantages, Architectural and technological influences of cloud computing, Deployment models (Public, Private, Community, and Hybrid models), Service delivery models (SaaS, PaaS, and IaaS), Risks and security concerns

UNIT II: Security Design and Architecture for Cloud Computing **Lectures: 3**

Security design principles for cloud computing: secure isolation, comprehensive data protection, end-to-end access control, and monitoring and auditing

CSA, NIST, and ENISA guidelines for cloud security, Common attack vectors and threats

UNIT III: Secure Isolation of Physical and Logical Infrastructure **Lectures: 3**

Isolation: compute, network and storage, Common attack vectors and threats,

Secure isolation strategies: multitenancy, virtualization strategies, inter-tenant network segmentation strategies, and storage isolation strategies

UNIT IV: Data Protection for Cloud Infrastructure and Services **Lectures: 4**

Understand the cloud based information life cycle, Data protection for confidentiality and integrity, Common attack vectors and threats, Encryption, data redaction, tokenization, obfuscation, PKI and key management, assuring data deletion, Data retention, deletion and archiving procedures for tenant data, Data protection strategies

UNIT V: Enforcing Access Control for Cloud Infrastructure based Services **Lectures: 6**

Understand the access control requirements for cloud infrastructure, Common attack vectors and threats, Enforcing access control strategies: Compute, network and storage: Authentication and authorization, roles-based access control, multi-factor authentication, host, storage and network access control options, OS hardening and minimization, securing remote access, verified and measured boot, firewalls, IDS, IPS and honeypots

UNIT VI: Monitoring, Auditing and Management **Lectures: 6**

Proactive activity monitoring, Incident response, Monitoring for unauthorized access, malicious traffic, abuse of system privileges, intrusion detection, events, and alerts, Auditing: record generation, reporting and management, Tamper-proofing audit logs, Quality of services, Secure management: user management, identity management, and security information and event management

Introduction to design patterns: understanding design patterns template, Architectural patterns for cloud computing: platform-to-virtualization and virtualization-to-cloud, and cloud bursting

UNIT VII: Cloud Computing Security Design **Lectures: 8**

Design pattern I: trusted Platform, geo-tagging, cloud VM platform encryption, trusted cloud resource pools, secure cloud interfaces, cloud resource access control, cloud data breach protection, permanent data loss protection, in-transit cloud data encryption

Design pattern II: secure on-premise internet access, secure external cloud connection, cloud denial-of-service protection, cloud traffic hijacking protection, automatically defined perimeter, cloud authentication gateway, federated cloud authentication, cloud key management, trust attestation service, collaborative monitoring and logging, independent cloud auditing

UNIT VIII: Policy, Compliance and Risk Management in Cloud Computing **Lectures: 4**

Legal, security, forensics, personal and data privacy issues within Cloud environment, Cloud security assessment and audit reports, Laws and regulatory mandates, Personal identifiable information and

data privacy, Privacy requirements for cloud computing (ISO 27018), Metrics for service level agreements
Metrics for risk management: ENISA, NIST SP 800, PCI DSS, and SAS 70
CSA Security, Trust, and Assurance Registry (STAR)

UNIT IX: Cloud Service Providers and Cloud Compliance Assessment Lectures: 4

OpenStack platform, Docker, Amazon web services
PCI DSS 3.0 compliant cloud tenant - case study
HIPAA compliance case study - protecting PHI in cloud

Text Book:

1. P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom, “Spectre attacks: Exploiting speculative execution”, 2018
2. M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, and M. Hamburg, M., “Meltdown: Reading kernel memory from user space”, 2018.
3. W. Jansen and T. Grance, “Guidelines on security and privacy in public cloud computing”, 2011 (NIST Special Publication 800-144).
4. Joint Task Force, “Risk management framework for information systems and organizations: A system life cycle approach for security and privacy”, 2018 (NIST Special Publication 800-37, Revision 2).

Reference Books:

1. T. Mather, S. Kumaraswamy, and S. Latif, “Cloud security and privacy: An enterprise perspective on risks and compliance”, 2009.
2. R. L. Krutz and R. D. Vines, “Cloud security”, 2010.
3. J. Rittinghouse and J. Ransome, “Cloud computing”, 2009.
4. J. R. ("Vic") Winkler, “Securing the cloud”, 2011.