Title	Cloud Security
Duration	40 hours
Tuition	USD 2,500

Course Syllabus: Cloud Security

Objectives:

Cloud computing infrastructure have become a mainstay of the IT industry, opening the possibility for on demand, highly elastic and infinite compute power with scalability and supporting the delivery of mission critical secure enterprise applications and services. This course provides the ground-up coverage on the high level concepts of cloud landscape, architectural principles, techniques, design patterns and real-world best practices applied to Cloud service providers and consumers and delivering secure Cloud based services. The course will describe the Cloud security architecture and explore the guiding security design principles, design patterns, industry standards, applied technologies and addressing regulatory compliance requirements critical to design, implement, deliver and manage secure cloud based services. The course delves deep into the secure cloud architectural aspects with regards to identifying and mitigating risks, protection and isolation of physical & logical infrastructures including compute, network and storage, comprehensive data protection at all OSI layers, end-to-end identity management & access control, monitoring and auditing processes and meeting compliance with industry and regulatory mandates. The course will leverage cloud computing security guidelines set forth by ISO, NIST, ENISA and Cloud Security Alliance (CSA). Students will learn and develop understanding of the following:

Fundamentals of cloud computing architectures based on current standards, protocols, and best practices intended for delivering Cloud based enterprise IT services and business applications.

Identify the known threats, risks, vulnerabilities and privacy issues associated with Cloud based IT services.

Understand the concepts and guiding principles for designing and implementing appropriate

safeguards and countermeasures for Cloud based IT services

Approaches to designing cloud services that meets essential Cloud infrastructure characteristics – on demand computing, shared resources, elasticity and measuring usage.

Design security architectures that assures secure isolation of physical and logical infrastructures including compute, network and storage, comprehensive data protection at all layers, end-to-end

Identity and access management, monitoring and auditing processes and compliance with industry and regulatory mandates.

- Understand the industry security standards, regulatory mandates, audit policies and compliance

requirements for Cloud based infrastructures.

Prerequisites:

Some web application development and/or systems administration experience is helpful.

Materials of Instruction:

This class covers a great deal of information about Cloud security technologies, so no single textbook can cover it all. Class notes will be provided for all topics covered.

The course material will follow the Cloud security guidelines prescribed by NIST, Cloud Security Alliance and ENISA.

To begin participating in the course, review the Weekly Checklist found in the course web site.

Topics & Assignments:

Week 1 Fundamentals of Cloud Computing and Architectural Characteristics

Understand what is Cloud computing

Architectural and Technological Influences of Cloud Computing

Understand the Cloud deployment models

Public, Private, Community and Hybrid models

Scope of Control

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

Cloud Computing Roles

Risks and Security Concerns

Week 2 Security Design and Architecture for Cloud Computing

Guiding Security design principles for Cloud Computing

Secure Isolation

Comprehensive data protection

End-to-end access control

Monitoring and auditing

Quick look at CSA, NIST and ENISA guidelines for Cloud Security

Common attack vectors and threats

Week 3 Secure Isolation of Physical & Logical Infrastructure

Compute, Network and Storage

Common attack vectors and threats

Secure Isolation Strategies

Multitenancy, Virtualization strategies

Inter-tenant network segmentation strategies

Storage isolation strategies

Week 4 Data Protection for Cloud Infrastructure and Services

- 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

Week 5 Enforcing Access Control for Cloud Infrastructure based Services

- 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

Week 6 Monitoring, Auditing and Management

- 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
- Security Information and Event Management

Week 7 Introduction to Cloud Design Patterns

Introduction to Design Patterns

Understanding Design Patterns Template

Architectural patterns for Cloud Computing

Platform-to-Virtualization & Virtualization-to-Cloud

Cloud bursting

Week 8 Introduction to Identity Management in Cloud Computing

- User Identification, Authentication, and Authorization in Cloud Infrastructure
- Be able to understand the concepts of Identity & Access Management
- Single Sign-on
- Identity Federation
- Identity providers and service consumers
- The role of Identity provisioning

Week 9 Cloud Computing Security Design Patterns - I

- Security Patterns for Cloud Computing
- 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

Week 10 Cloud Computing Security Design Patterns - II

Security Patterns for Cloud Computing – Network Security, Identity &

Access Management & Trust

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

Week 11 Policy, Compliance & Risk Management in Cloud Computing

- Be able to understand the legal, security, forensics, personal & data privacy issues within Cloud environment
- Cloud security assessment & audit reports

- Laws & regulatory mandates
- Personal Identifiable Information & Data Privacy
- Privacy requirements for Cloud computing (ISO 27018)
- Metrics for Service Level Agreements (SLA)
- Metrics for Risk Management

Week 12 Cloud Compliance Assessment & Reporting - Case Study

- PCI DSS 3.0 Compliant Cloud Tenant - Case Study
- HIPAA compliance Case Study - Protecting PHI in Cloud
- Discussions (for DL) Discussion topics will be posted on LATTE.

Week 13 Cloud Service Providers – Technology Review

OpenStack Platform

Docker

Amazon Web Services

Week 14 Wrap Up & Final Projects Review

- Course outcomes review
- Real-world Compliance Case Study Review
- Final projects presentation & review

Expectations:

- All assignments must be student's original work, with sources properly cited.
- All assignment/work submissions must be made in Microsoft DOC or Adobe PDF formats.
- Students are allowed to work as small teams (2 -3 members) on the final project and submit their
- project together as teamwork.