CSCI E-49

CLOUD SECURITY

Course Syllabus

Class Meeting Times:

This course is offered via both on-campus and distance learning.

On-campus: Mondays, 7:40-9:40 PM EST, 1 Story Street, #302

Bi-weekly Online sections: Friday 8:00 PM EST

Class 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.

Class Prerequisites:

CSCI E-45a, CSCI E-45b, or the equivalent. Some web application development and/or systems administration experience is helpful.

Materials of Instruction:

Class Notes

- 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.

Recommended Texts

- Securing The Cloud: Cloud Computing Security Techniques and Tactics by Vic (J.R.) Winkler (Syngress/Elsevier) - 978-1-59749-592-9
- Cloud Computing Design Patterns by Thomas Erl (Prentice Hall) - 978-0133858563

Weekly Topics & Assignments:

Week 1	Fundamentals of Cloud Computing and Architectural Characteristics
Objectives	• Understand what is Cloud computing • Architectural and Technological Influences of Cloud Computing • Understand the Cloud deployment models a. Public, Private, Community and Hybrid models • Scope of Control a. Software as a Service (SaaS) b. Platform as a Service (PaaS) c. Infrastructure as a Service (IaaS) • Cloud Computing Roles • Risks and Security Concerns
Readings	• Refer to Instructor slides & course notes

Week 2	Security Design and Architecture for Cloud Computing
Objectives	• Guiding Security design principles for Cloud Computing

	o Secure Isolation o Comprehensive data protection o End-to-end access control o Monitoring and auditing • Quick look at CSA, NIST and ENISA guidelines for Cloud Security • Common attack vectors and threats
Readings	• Refer to Instructor slides & course notes
Assignments	• Assignment 1 posted

Week 3	**Secure Isolation of Physical & Logical Infrastructure**
Objectives	• Isolation o Compute, Network and Storage • Common attack vectors and threats • Secure Isolation Strategies o Multitenancy, Virtualization strategies o Inter-tenant network segmentation strategies o Storage isolation strategies
Readings	• Refer to Instructor slides & course notes

Week 4	**Data Protection for Cloud Infrastructure and Services**
Outcomes	• 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
Readings	• Refer to Instructor slides and course notes
Assignments	• Assignment 1 Due • Assignment 2 Posted

Week5	**Enforcing Access Control for Cloud Infrastructure based Services**

Objectives	• Understand the access control requirements for Cloud infrastructure • Common attack vectors and threats • Enforcing Access Control Strategies o 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
Readings	• Refer to Instructor slides and course notes

Week 6	**Monitoring, Auditing and Management**
Objectives	• 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 o User management o Identity management o Security Information and Event Management
Mid-Term Review	• Quick Review for Mid-Term
Readings	• Refer to instructor slides and course notes
Assignments	• Assignment 2 Due • Assignment 3 Posted

Week 7	**Introduction to Cloud Design Patterns**
Objectives	• Introduction to Design Patterns

	o Understanding Design Patterns Template • Architectural patterns for Cloud Computing o Platform-to-Virtualization & Virtualization-to-Cloud o Cloud bursting
Mid-Term Quiz - 30 Questions (1 Hour)	
Readings	• Refer to Instructor slides & course notes

Week 8	**Introduction to Identity Management in Cloud Computing**
Objectives	• User Identification, Authentication, and Authorization in Cloud Infrastructure • Be able to understand the concepts of Identity & Access Management o Single Sign-on o Identity Federation o Identity providers and service consumers • The role of Identity provisioning
Readings	• Refer to Instructor slides & course notes
Assignments	• Assignment 3 Due • Assignment 4 Posted

Week 9	**Cloud Computing Security Design Patterns - I**
Objectives	• Security Patterns for Cloud Computing o Trusted Platform o Geo-tagging o Cloud VM Platform Encryption o Trusted Cloud Resource Pools o Secure Cloud Interfaces o Cloud Resource Access Control o Cloud Data Breach Protection o Permanent Data Loss Protection o In-Transit Cloud Data Encryption
Readings	• Refer to Instructor Slides

Week 10	**Cloud Computing Security Design Patterns - II**
Objectives	• Security Patterns for Cloud Computing – Network Security, Identity &

	Access Management & Trust o Secure On-Premise Internet Access o Secure External Cloud Connection o Cloud Denial-of-Service Protection o Cloud Traffic Hijacking Protection o Automatically Defined Perimeter o Cloud Authentication Gateway o Federated Cloud Authentication o Cloud Key Management o Trust Attestation Service o Collaborative Monitoring and Logging o Independent Cloud Auditing
Readings	• Refer to Instructor Slides
Assignment	• Final Project Guidelines Posted

Week 11	**Policy, Compliance & Risk Management in Cloud Computing**
Objectives	• 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 o ENISA o NIST SP 800 o PCI DSS o SAS 70 • CSA Security, Trust, and Assurance Registry (STAR)
Readings	• Refer to Instructor slides and course notes
Assignments	• Assignment 4 Due

Week 12	**Cloud Compliance Assessment & Reporting - Case Study**
Objectives	• 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.
Readings	• Refer to Instructor slides & course notes
Assignments	• Final Project Abstracts due

Week 13	Cloud Service Providers – Technology Review
Outcomes	• OpenStack Platform • Docker • Amazon Web Services • Final Project Q & A
Readings	• Refer to Instructor slides & course notes

Week 14	Wrap Up & Final Projects Review
Outcomes	• Course outcomes review ○ Real-world Compliance Case Study Review ○ Final projects presentation & review
Final Quiz (30 Questions) – 1 Hour	
Assignments	• Final Project Due

Course Grading Criteria:

Percent	Component
60 %	4 Assignments
10%	Mid Term Quiz (Online)
10%	Final Quiz (Online)
20%	Final Project

Work 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.

Academic Integrity Requirements:

Students are responsible for understanding Harvard Extension School policies on academic integrity (www.extension.harvard.edu/resources-policies/student-conduct/academic-integrity) and how to use sources responsibly. Not knowing the rules, misunderstanding the rules, running out of time, submitting the wrong draft, or being overwhelmed with multiple demands are not acceptable excuses. There are no excuses for failure to uphold academic integrity.

To support student learning about academic citation rules, please visit the Harvard Extension School Tips to Avoid Plagiarism (www.extension.harvard.edu/resources-policies/resources/tips-avoid-plagiarism), where you'll find links to the Harvard Guide to Using Sources and two free online 15-minute tutorials to test your knowledge of academic citation policy. The tutorials are anonymous open-learning tools.

Accessibility:

The Extension School is committed to providing an accessible academic community. The Accessibility Office offers a variety of accommodations and services to students with documented disabilities.

Please visit www.extension.harvard.edu/resources-policies/resources/disability-services-accessibility for more information.

Faculty information:

Ramesh Nagappan
nramesh@post.harvard.edu
Hours by appointment (Monday 6 PM EST or Friday 6 PM EST)