



95-746 Cloud Security

Wednesdays, 6:30pm - 9:20pm, Location: Remote/Zoom

Semester: Spring, Mini 4, Year: 2021

Units: 6, Section: A4

Instructor information

Name	George Werbacher
Contact Info	gwerbach@andrew.cmu.edu or george.werbacher@blackbaud.com
Office location	Remote
Office hours	Wednesdays, 5:30 pm - 6:30 pm (email for availability)

TA Information

TA name	Rutvij Parthiv Trivedi
TA Contact Info	rtrivedi@andrew.cmu.edu
Office location	TBD
Office hours	TBD

Course Description

In the age of disruption, digitally transformed products and services have enabled more significant innovation, faster go-to-market, and reduced capital expenditure. A majority of these technological advancements rely on the cloud. As a 260 billion dollar industry, with growth expected to rise 14% by 2025, organizations adopt the public cloud at increasing rates. This increased adoption of cloud computing has adversely affected security practices that are not fully transferable from on-premise security programs.

This course will provide a foundational understanding of what is required to secure a cloud ecosystem, regardless of the vendor. The concepts and principles discussed will help bridge the gaps between traditional and cloud architectures while accounting for the shifting thought patterns involving enterprise risk management. Students who complete this course will enter into any organization utilizing the cloud and immediately bring value to the infrastructure and security teams.

Learning Objectives

- Understand core cloud computing concepts and fundamental principles, including standard delivery models and service designs.
- Understand the foundational security practices that are required to secure modern cloud computing infrastructures.
- Understand the differences between traditional data security practices and cloud-based data security methodologies.
- Understand the identity and access management practices of both cloud providers and consumers.

- Understand how to protect data-at-rest, data-in-transit, and data-in-use within a cloud environment.
- Understand standard cloud security network designs and architecture models.
- Understand the complexity of cloud threat actors and techniques used to attack a cloud computing infrastructure
- Understand the regulatory requirements needed to secure data in the cloud and the difficulties in meeting those requirements.

Learning Resources

- **Required** - Practical Cloud Security: A Guide for Security Design and Deployment, 1st Edition (ISBN: 978-1492037514)
- **Optional** - Cloud Computing Security: Foundations and Challenges, 2nd Edition (ISBN: 978-0367560331)
- **Additional Readings** - Provided via Canvas & Google Drive

Assessments

The final course grade will be calculated using the following categories:

Assessment	Percentage of Final Grade
Reading Quizzes	10%
Assignments	15%
Mid-Term Exam	25%
Final Exam	30%
Research Paper	20%

- **Reading Quizzes:** Quizzes will be given at the start of each lecture based on the required readings assigned for that lecture. Quizzes will consist of **5 multiple choice** questions and will be open book.
- **Assignments:** Assignments will be given periodically throughout the course to provide a more in-depth understanding of this course's topics. Assignments will be **3-4 questions** that require a specific # of paragraph responses.
- **Mid-Term Exam:** The Mid-Term Exam will be a multiple-choice exam that will test your knowledge up to that point of the course. This will be a **closed-book exam**.
- **Research Paper:** The Research Paper will be a **6-8 (individual) or 10-12 (partners) page** report based on a list of topics provided on the first day of class. If you wish to partner up, you must inform me before the beginning of Lecture 2.
- **Final Exam:** The Final Exam will be a multiple-choice exam that will test your knowledge of the course in its entirety. This will be a **closed-book exam**.
- **Optional Final Exam:** Students who wish not to take the final exam will have the opportunity to receive a passing grade (A) on their final exam if they **take and pass**, one of the following:
 - [AWS Certified Cloud Practitioner](#)
 - [AZ-900: Microsoft Azure Fundamentals](#)
 - [GCP Cloud Engineer](#)

Students will be assigned the following final letter grades, based on calculations from the course assessment section.

Grade	Percentage Interval
A	90-100%
B	80-89%
C	70-79%
D	60-69%
R (F)	< 60%

Grading Policies

- **Late-work policy:** Work will not be accepted more than **48 hours** after the assigned due date. Late work is subject to a point deduction. Any work that is submitted **after 48 hours** will not be reviewed and will automatically receive zero points.

Course Policies

- **Accommodations for students with disabilities:** If you have a disability and require accommodations, please contact Catherine Getchell, Director of Disability Resources, 412-268-6121, getchell@cmu.edu. If you have an accommodations letter from the Disability Resources office, I encourage you to discuss your accommodations and needs with me as early in the semester as possible. I will work with you to ensure that accommodations are provided as appropriate.
- **Statement on student wellness:** As a student, you may experience a range of challenges that can interfere with learning, such as strained relationships, increased anxiety, substance use, feeling down, difficulty concentrating and/or lack of motivation. These mental health concerns or stressful events may diminish your academic performance and/or reduce your ability to participate in daily activities. CMU services are available, and treatment does work. You can learn more about confidential mental health services available on campus at: <http://www.cmu.edu/counseling/>. Support is always available (24/7) from Counseling and Psychological Services: 412-268-2922.

Course Schedule

Date	Theme/Topic	Assignments Due
3/24/21	Cloud Computing Overview & Security Foundations	None
3/31/21	Cloud Infrastructure Design and Security	Reading Quiz 1
4/7/21	Guest Speaker: Jason Chan, VP Information Security - Netflix Cloud Asset Management and Data Protection	Reading Quiz 2
4/14/21	Cloud Identity and Access Management Case Study: Capital One Data Breach	Reading Quiz 3 Mid-Term Due 4-18
4/21/21	Guest Speaker: TBD Cloud Data Protection and Privacy	Reading Quiz 4

4/28/21	Guest Speaker: TBD Cloud Security Threat Management	Reading Quiz 5
5/5/21	Cloud Security Compliance & Regulations	Reading Quiz 6
5/12/21	Final Exam	--