USC Viterbi
School of Engineering

CSCI 699: Confidential Computing: Protecting Your Data on Cloud GPUs and CPUs

Units: 4.0

Spring 2025 — Thursdays — 4:00-7:20PM

Location: TBD

Instructor: Mengyuan Li
Office: GCS 502A
Office Hours: TBD
Contact Info: mli49061@usc.edu. Please include "CSCI 699" in your email subject. Replies can be expected within 48 hours during weekdays.

Catalogue Description

Explores confidential computing with emphasis on Trusted Execution Environments (TEEs), secure enclaves, confidential GPUs/VMs, side-channel defenses, and privacy-preserving techniques like FL, MPC, and FHE.

Course Description

This course offers an in-depth study of confidential computing and privacy-preserving computational techniques, focusing on protecting data in cloud environments using both CPUs and GPUs. Students will explore the design and implementation of Trusted Execution Environments (TEEs) and examine various cloud services that support confidential computing, including secure enclaves, Confidential Virtual Machines (CVMs), and confidential GPUs. Additionally, the course covers common threats to TEEs, such as hardware-based and side-channel attacks, alongside defenses against these threats. It also covers an overview of other popular privacy-preserving technologies, including Federated Learning (FL), Multi-Party Computation (MPC), and Fully Homomorphic Encryption (FHE).

Intended audience: This course is suitable for advanced undergraduate and graduate students in computer science or related fields who are interested in security, privacy, cloud computing, and hardware/software co-design. Students will develop an appreciation for the challenges of securing data in modern computing environments and the importance of privacy-preserving technologies in safeguarding sensitive information. By the end of the course, students will be equipped with the foundational knowledge to pursue further research or careers in the field of confidential cloud computing.

Learning Objectives

- A comprehensive understanding of confidential computing and TEE.
- Gain experience in reading, analyzing, and critically evaluating research papers from leading conferences in the fields of security, privacy, and cloud computing.
- Understand and experiment with state-of-the-art systems related to TEEs and CVMs.
- A better understanding of other common privacy-preserving computation techniques such as FL, MPC, and FHE.
- Improve academic writing and presentation skills through assignments and the final project.

Recommended Preparation

Students are encouraged to familiarize themselves with the fundamentals of computer architecture, operating systems, cryptography, computer security, and cloud computing concepts. Proficiency in programming languages such as C/C++ and Python will be beneficial.

Course Notes

Grading type: Letter or Credit/No Credit. The final grade is based on attendance, two assignments, reviewing, and presenting research papers, as well as a substantial final project. The standard week will involve reading 2-3 academic research papers in security and privacy. Lecture notes and slides will be posted online after each lecture. The lectures will not be recorded.

Technological Proficiency and Hardware/Software Required

Ability to understand research papers in security and privacy and to implement code (Usually using C/C++) as needed. Course projects require standard computing software (Virtual Machine, C++).

Required Readings and Supplementary Materials

There are no required textbooks. The following writeups are excellent supplemental readings and may be used as references:

- Remzi H. Arpaci-Dusseau and Andrea C. Arpaci-Dusseau, Operating Systems: Three Easy Pieces, free online version can be found at https://pages.cs.wisc.edu/~remzi/OSTEP/#book-chapters
- Costan, Victor. "Intel SGX explained." IACR Cryptol, EPrint Arch (2016). https://eprint.iacr.org/2016/086.pdf

- Li, M., Yang, Y., Chen, G., Yan, M. and Zhang, Y., 2024, July. SoK: Understanding Design Choices and Pitfalls of Trusted Execution Environments. https://dl.acm.org/doi/pdf/10.1145/3634737.3644993

Description of Assignments and How They Will Be Assessed

- Assignments (30%): Two assignments in total. Collaboration is permitted but must be explicitly acknowledged.
- Course Presentation (20%): You will present a recent research paper in the field of confidential computing. Papers will be assigned based on your interests, and each presentation should be 30 minutes long.
- Final Project (40%): A 4-page report on a topic related to confidential computing. This project can be a small extension of the paper you presented, an original idea, or an implementation of a topic related to confidential computing. Pursuing your own research topic is highly encouraged.
- Participation and Discussions (10%): Actively engage in discussions by reviewing, commenting, and providing feedback on each other's presentations and projects.

Participation

Students are expected to actively participate in class discussions, group activities, and online forums. Full credit for participation requires consistent engagement and collaboration with peers.

Grading Breakdown

Assessment Tool (assignments)	% of Grade
Assignment 1	15
Assignment 2	15
Course Presentation	20
Final Project	40
Participation and Discussion	10
TOTAL	100

Assignment Submission Policy

Written reports for paper seminar roles are due at the start of class on the day of the scheduled presentation. All assignments and project-related reports are due at 11:59pm on the day of the deadline. For submission information, see the course website.

Course-Specific Policies

There are no late days for the assignments. In addition, there are opportunities for extra credit by doing additional paper reviews and/or class presentations.

Attendance

Attendance is required unless you have notified the instructor in advance (e.g., due to conference travel).

Academic Integrity for this Class

Unless otherwise noted, this course will follow the expectations for academic integrity as stated in the USC Student Handbook. The general USC guidelines on Academic Integrity and Course Content Distribution are provided later in this syllabus.

Class Recordings and Course Content Distribution: You may not record this class without the express permission of the instructor and all other students in the class. Distribution of any notes, recordings, exams, or other materials from a university class or lectures — other than for individual or class group study — is prohibited without the express permission of the instructor; violations will be considered an intentional act to facilitate or enable academic dishonesty and reported to the university.

Use of Generative AI in this Course

Generative AI is encouraged: You are expected to use AI (e.g., ChatGPT and image generation tools) in this class. Learning to use AI is an emerging skill, and I welcome the opportunity to meet with you to provide guidance with these tools during office hours or after class. Keep in mind the following:

- AI tools are permitted to help you brainstorm topics or revise work you have already written.
- If you provide minimum-effort prompts, you will get low-quality results. You will need to refine your prompts to get good outcomes. This will take work.
- Proceed with caution when using AI tools and do not assume the information provided is accurate or trustworthy. If it gives you a number or fact, assume it is incorrect unless you either know the correct answer or can verify its accuracy with another source. You will be responsible for any errors or omissions provided by the tool. It works best for topics you understand.
- AI is a tool, but one that you need to acknowledge using. Please include a paragraph at the end of any assignment that uses AI explaining how (and why) you used AI and indicate/specify the prompts you used to obtain the results and what prompts you used to get the results. Failure to do so is a violation of academic integrity policies.
- Be thoughtful about when AI is useful. Consider its appropriateness for each assignment or circumstance. The use of AI tools requires attribution. You are expected to clearly attribute any material generated by the tool used.]

Course Evaluations

Course evaluation occurs at the end of the semester university wide. In addition, we will use continuous anonymous feedback to help shape the course to your best interests. Remember, this is an advanced level course and will be what you make of it.

Course Schedule

	Topics/Daily Activities	Readings/Preparation	Deliverables
Week 1	Introduction to Confidential Computing	- Course syllabus - Introductory articles on cloud security	
Week 2	Trusted Execution Environments - Principles and Architectures	- Relevant research papers* about SGX, AMD SEV, and Nvidia CC	
Week 3	Confidential Virtual Machines - Concepts and Implementations	- Articles on CVMs and cloud implementations	
Week 4	Programming with TEEs - Hands-on Lab with QEMU and VM	- Tutorial on VMs and QEMU	Assignment 1 Assigned
Week 5	Confidential Computing and Practical TEE Systems	- 2-3 relevant research papers	
Week 6	Hardware Attacks and Defenses - Side-Channel Attacks	- 2-3 relevant research papers	Assignment 1 Due
Week 7	Hardware Attacks and Defenses - Meltdown and Spectre Vulnerabilities	- 2-3 relevant research papers	Assignment 2 Assigned
Week 8	Confidential GPUs - GPU-Specific Attacks and Defenses	- 2-3 relevant research papers about GPU vulnerabilities	
Week 9	Introduction to Privacy-Preserving Techniques: Overview of FL, MPC, FHE		Assignment 2 Due
Week 10	Final Project Midterm Presentations		Project Midterm Report Due
Week 11	Secure Software Development Practices - software vulnerability in TEE-based system	- 2-3 relevant research papers about TEE side-channel Attacks	
Week 12	Balancing Security and Performance in Confidential Computing – CPU scenario	- 2-3 relevant research papers about TEE-based system optimization	
Week 13	Balancing Security and Performance in Confidential Computing – GPU scenario	- 2-3 relevant research papers about GPU-TEE-based Systems	
Week 14	Final Project Presentations		In class presentations.
Week 15	Final Project Presentations		In class presentations.
FINAL	Final Project Report		Due on the university-scheduled date of the final exam.

***All relevant research paper will be available in the course website.**

Academic Integrity

The University of Southern California is foremost a learning community committed to fostering successful scholars and researchers dedicated to the pursuit of knowledge and the transmission of ideas. Academic misconduct — which includes any act of dishonesty in the production or submission of academic work (either in draft or final form) — is in contrast to the university's mission to educate students through a broad array of academic, professional, and extracurricular programs.

This course will follow the expectations for academic integrity as stated in the USC Student Handbook. All students are expected to submit assignments that are their own original work and prepared specifically for this course and section in this academic term. You may not submit work written by others or "recycle" work prepared for other courses without obtaining written permission from the instructor(s). Students suspected of engaging in academic misconduct will be reported to the Office of Academic Integrity.

Other violations of academic misconduct include, but are not limited to, cheating, plagiarism, fabrication (e.g., falsifying data), knowingly assisting others in acts of academic dishonesty, and any act that gains or is intended to gain an unfair academic advantage.

Academic dishonesty has a far-reaching impact and is considered a serious offense against the university. Violations will result in a grade penalty, such as a failing grade on the assignment or in the course, and disciplinary action from the university itself, such as suspension or even expulsion.

For more information about academic integrity see the student handbook or the Office of Academic Integrity's website, and university policies on Research and Scholarship Misconduct.

Please ask your instructor if you are unsure what constitutes unauthorized assistance on an exam or assignment or what information requires citation and/or attribution.

Course Content Distribution and Synchronous Session Recordings Policies

USC has policies that prohibit recording and distribution of any synchronous and asynchronous course content outside of the learning environment.

Recording a university class without the express permission of the instructor and announcement to the class, or unless conducted pursuant to an Office of Student Accessibility Services (OSAS) accommodation. Recording can inhibit free discussion in the future, and thus infringe on the academic freedom of other students as well as the instructor. (Living our Unifying Values: The USC Student Handbook, page 13).

Distribution or use of notes, recordings, exams, or other intellectual property, based on university classes or lectures without the express permission of the instructor for purposes other than individual or group study. This includes but is not limited to providing materials for distribution by services publishing course materials. This restriction on unauthorized use also applies to all information, which had been distributed to students or in any way had been displayed for use in relation to the class, whether obtained in class, via email, on the internet, or via any other media. Distributing course material without the instructor's permission will be presumed to be an intentional act to facilitate or enable academic dishonestly and is strictly prohibited. (Living our Unifying Values: The USC Student Handbook, page 13).

Statement on University Academic and Support Systems

Students and Disability Accommodations:
USC welcomes students with disabilities into all of the University's educational programs. The Office of Student Accessibility Services (OSAS) is responsible for the determination of appropriate accommodations for students who encounter disability-related barriers. Once a student has completed the OSAS process (registration, initial appointment, and submitted documentation) and accommodations are determined to be reasonable and appropriate, a Letter of Accommodation (LOA) will be available to generate for each course. The LOA must be given to each course instructor by the student and followed up with a discussion. This should be done as early in the semester as possible as accommodations are not retroactive. More information can be found at osas.usc.edu. You may contact OSAS at (213) 740-0776 or via email at osasfrontdesk@usc.edu.

Student Financial Aid and Satisfactory Academic Progress:
To be eligible for certain kinds of financial aid, students are required to maintain Satisfactory Academic Progress (SAP) toward their degree objectives. Visit the Financial Aid Office webpage for undergraduate- and graduate-level SAP eligibility requirements and the appeals process.

Support Systems:
Counseling and Mental Health - (213) 740-9355 – 24/7 on call
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention.

988 Suicide and Crisis Lifeline - 988 for both calls and text messages – 24/7 on call
The 988 Suicide and Crisis Lifeline (formerly known as the National Suicide Prevention Lifeline) provides free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week, across the United States. The Lifeline consists of a national network of over 200 local crisis centers, combining custom local care and resources with national standards and best practices. The new, shorter phone number makes it easier for people to remember and access mental health crisis services (though the previous 1 (800) 273-8255 number will continue to function indefinitely) and represents a continued commitment to those in crisis.

Relationship and Sexual Violence Prevention Services (RSVP) - (213) 740-9355(WELL) – 24/7 on call
Free and confidential therapy services, workshops, and training for situations related to gender- and power-based harm (including sexual assault, intimate partner violence, and stalking).

Office for Equity, Equal Opportunity, and Title IX (EEO-TIX) - (213) 740-5086
Information about how to get help or help someone affected by harassment or discrimination, rights of protected classes, reporting options, and additional resources for students, faculty, staff, visitors, and applicants.

Reporting Incidents of Bias or Harassment - (213) 740-2500
Avenue to report incidents of bias, hate crimes, and microaggressions to the Office for Equity, Equal Opportunity, and Title for appropriate investigation, supportive measures, and response.

The Office of Student Accessibility Services (OSAS) - (213) 740-0776
OSAS ensures equal access for students with disabilities through providing academic accommodations and auxiliary aids in accordance with federal laws and university policy.

USC Campus Support and Intervention - (213) 740-0411
Assists students and families in resolving complex personal, financial, and academic issues adversely affecting their success as a student.

Diversity, Equity and Inclusion - (213) 740-2101
Information on events, programs and training, the Provost's Diversity and Inclusion Council, Diversity Liaisons for each academic school, chronology, participation, and various resources for students.

USC Emergency - UPC: (213) 740-4321, HSC: (323) 442-1000 – 24/7 on call
Emergency assistance and avenue to report a crime. Latest updates regarding safety, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible.

USC Department of Public Safety - UPC: (213) 740-6000, HSC: (323) 442-1200 – 24/7 on call
Non-emergency assistance or information.

Office of the Ombuds - (213) 821-9556 (UPC) / (323-442-0382 (HSC)
A safe and confidential place to share your USC-related issues with a University Ombuds who will work with you to explore options or paths to manage your concern.

Occupational Therapy Faculty Practice - (323) 442-2850 or otfp@med.usc.edu
Confidential Lifestyle Redesign services for USC students to support health-promoting habits and routines that enhance quality of life and academic performance.