COSC 6580 – Data Security and Privacy

Course Description

We will discuss the fundamental and advanced topics in data security and privacy, including differential privacy, secure multi-party computation, homomorphic encryption, data perturbation, data anonymization, security and privacy in AI, and location privacy. Students are expected to read selected papers and submit reading summaries. Participation in class discussions is highly encouraged. Students will need to finish a term project. Each project team can have 1~2 people.

Class meeting times and venue: 5-6:15 pm, Cudahy 412

Prerequisite:

Basic knowledge of statistics, databases, machine learning/data mining, and distributed systems

Learning Outcomes:

We expect the following learning outcomes:

- Students will learn the basic principles and methods for protecting data security and privacy in an open, collaborative computing environment.
- Students can implement and experiment with some methods.
- Students can apply the learned methods to applications and research projects.

Textbook and Materials

No textbook is used. All materials will come from recent research papers or online references.

Assignments and exams

Reading assignments. Students should submit reading summaries for reading assignments. Each paper summary consists of a few paragraphs with less than one page, including the research problem, technical contributions, strengths, and weaknesses of the approach.

Term project. It has three parts: project proposal, implementation, and final report (and presentation). The instructor will give some project topics. Ph.D. students are also encouraged to try their research ideas.

Final exam. It will be a take-home exam.

Grading Policy

Reading summaries	30%
Term project (proposal 10%, implementation 10%, presentation 10%, final report 10%)	40%
final exam	30%

A [90, 100], A- [84, 89], B+ [78, 83], B [73, 77], B- [67, 72], C+ [62, 66], C [56, 61], C- [51, 55], D [45, 50], F [0, 44]
The instructor will not curve the grades.

Selected Topics (tentative)

1. Introduction
2. Data perturbation
3. Differential privacy
4. Data anonymization
5. Basic data encryption methods
6. Secure multi-party computation (garbled circuits, secret sharing)
7. Homomorphic encryption
8. Private information retrieval and oblivious RAM
9. Trusted execution environment
10. Security and privacy in AI
11. Location privacy

Course Policies

1. Late Assignments (homework and project): no penalty within one hour, 30% penalty for one hour to 12-hour late, and 50% penalty for 12-hour to one day late. Submissions late for more than one day will not be graded.
2. Study groups are encouraged. However, the work submitted for grading must be the student's or project team's work. Plagiarism will result in a score of zero on the exam or assignment. You can review the document on the Academic honesty policy in the student handbook or from http://bulletin.marquette.edu/
3. Any course-related communication will be made to the student's official Marquette email address. It is the student's responsibility to check their emails.

About COVID-19

Please check the University's current policy about COVID-19 https://today.marquette.edu/2022/08/covid-19-mitigation-protocols-to-begin-the-fall-2022-semester/. Students are encouraged to wear masks in the classroom in alignment with the university recommendation and city guidance.