Instructor Information

Instructor(s):
Shirin Nilizadeh

Office Number:
ERB 530

Email Address:
shirin.nilizadeh@uta.edu

Faculty Profile:
http://crystal.uta.edu/~shirin/

Office Hours:
Thursdays 9-11 am

Course Information

Section Information:
CSE 5388/6388

Time and Place of Class Meetings:
Thursdays 11-1:50 pm, WH 221

Description of Course Content:
This course is about the role of data and data analytics in security and privacy. It covers applications of machine learning and big data analytics to various security and privacy problems, and also discusses the security and privacy problems associated with machine learning and big data. The topics include: the use of machine learning for making decisions related to security and privacy; misuse detection on social media; tracking technologies; data (de-)anonymization; anomaly detection; privacy-preserving machine learning algorithms, and adversarial machine learning.

Required Textbooks and Other Course Materials:
No required textbook. All course readings will be scientific papers. Each week the instructor lists these papers for students to read before the class.

Descriptions of major assignments and examinations:
In this course, we will read and discuss a few papers every week. Every student must complete the assigned reading prior to the class so that they can participate fully in class discussions. Students will be the discussion leader for class discussions of two different papers (on two different days). Students will also work on a major project in groups of size 2–3.
Grading Information

Grading:
Course grades will be based on the following:

- **Class Participation** 15%
- **Leading two class discussions** 15%
- **Paper summaries** 20%
- **Research project** 50%
  - Project draft proposal 10%
  - Project proposal presentation 5%
  - Project final proposal 10%
  - Weekly project progress updates 10%
  - Project written progress report 20%
  - Project presentation 10%
  - Final project report 35%

This class will have **no exams**. Final project presentations will be held on the last day of class.

Class participation
This is a discussion-based graduate seminar course. You are expected to attend all class meetings and to participate actively in the discussion. Students need to inform the instructor in advance, if they cannot attend a class due to a conference or other major personal or professional obligation.

Reading reviews
We will read and discuss 2 or 3 papers every week. Every student must complete the assigned reading prior to the class so that they can participate fully in class discussions. To facilitate productive class discussions, students must submit a review of each of the assigned papers to Canvas on **Wednesdays by 11:59 pm**. Reviews should consist of three brief paragraphs in students’ own words with the following structure:

Paragraph 1:
- Explain the problem and motivation.
- Explain the main ideas and technical contributions of the work.
- Compare this work with the main prior work.
- Explain the methodology used for evaluation.

Paragraph 2:
- List three key strengths and three key weaknesses of this paper. Focus should be more on approach and evaluation.

Paragraph 3:
- List any future work that you might consider in this line of research.

Leading two class discussions
Students will be the discussion leader for class discussions of two different papers (on two different days). As the discussion leader, the student must prepare a 30-minute presentation that covers the main technical contributions of the paper, plus at least 10 discussion questions. Prior to the beginning of class, the student should upload their slides as a PDF to the Canvas folder for that reading assignment.

Research Project
Students will work on a major project in groups of size 2–3. Students should propose their own projects, however, if needed some projects will be suggested by the instructor. Here is the timeline for the projects:
- **Wednesday, February 5th (11:59 pm)**: Every student submits at least two project ideas for their project. Explain each idea in one or two paragraphs: state your research questions, motivation and general approach.
- **Thursday, February 6th**: Every student has 10 minutes to present their ideas in the class. At the end of this class students will decide about their projects and their groups.
- **From Friday, February 7th, to Wednesday, February 12th**: The instructor schedules meetings with each group to discuss and refine their idea.
- **Friday, February 14th (11:59 pm)**: Group submit a finalized version of their project proposal in 2-3 pages. The proposal should state their research questions; hypotheses (if any); general approach; and evaluation metrics. It should also include a timeline with checkpoints and deliverables at those checkpoints. Describe what you hope to accomplish by the end of the semester.
- **Every week in class**: Each group gives an oral progress report (~5 minutes). Describe your progress, and discuss your plan for the next week.
- **Wednesday, March 25th (11:59 pm)**: Groups submit a written progress report. Their written progress report should describe their progress to date relative to their proposed timeline, note any problems they have run into, describe your updated plan for the rest of the semester, and include any preliminary results or technical accomplishments. This written report should also include a draft related work section for your final paper.
- **Thursday, May 7th**: Give a 25-minute final project presentation in class.
- **Monday, May 11th (11:59 pm)**: Submit a paper including an abstract, introduction (including research questions), related work, methodology, results, discussion, conclusions, and references.

Students are encouraged to submit their project as a full paper to a conference with an appropriate deadline. A paper submission will likely require additional work after the end of the semester.

Your final paper should be written in a style suitable for publication at a conference or workshop. Papers should be in double-column ACM format (see [https://www.acm.org/publications/proceedings-template](https://www.acm.org/publications/proceedings-template)).

**Late paper reviews policy**: To accommodate for unavoidable circumstances, you get four automatic 1-day extensions for individual paper summaries without having to ask me for an extension. Just note the extension request on the summary. Finally, you can drop 2 summaries, but at most 1 for a given week. Save these for circumstances such as falling ill or interviewing.

**Late report policy**: Students will be penalized 25% for every day it is late beyond the designated deadline. You are required to submit satisfactory versions of your project reports within 4 days of the deadline to pass the class. This policy will be used for each of the project proposals, progress report, and final report.

**Course Schedule**
**Check the website:**
[http://crystal.uta.edu/~shirin/specialTopics2020.html](http://crystal.uta.edu/~shirin/specialTopics2020.html)
Institution Information

UTA students are encouraged to review the below institutional policies and informational sections and reach out to the specific office with any questions. To view this institutional information, please visit the Institutional Information page (http://www.uta.edu/provost/administrative-forms/course-syllabus/index.php) which includes the following policies among others:

- Drop Policy
- Disability Accommodations
- Title IX Policy
- Academic Integrity
- Student Feedback Survey
- Final Exam Schedule

Additional Information

Emergency Exit Procedures:
Should we experience an emergency event that requires evacuation of the building, students should exit the room and move toward the nearest exit. When exiting the building during an emergency, do not take an elevator but use the stairwells instead. Faculty members and instructional staff will assist students in selecting the safest route for evacuation and will make arrangements to assist individuals with disabilities.

Student Success Programs:
UT Arlington provides a variety of resources and programs designed to help students develop academic skills, deal with personal situations, and better understand concepts and information related to their courses. Resources include tutoring by appointment, drop-in tutoring, etutoring, supplemental instruction, mentoring (time management, study skills, etc.), success coaching, TRIO Student Support Services, and student success workshops. For additional information, please email resources@uta.edu, or view the Maverick Resources website.

The English Writing Center (411LIBR):
The Writing Center offers FREE tutoring in 15-, 30-, 45-, and 60-minute face-to-face and online sessions to all UTA students on any phase of their UTA coursework. Register and make appointments online at the Writing Center (https://uta.mywconline.com). Classroom visits, workshops, and specialized services for graduate students and faculty are also available. Please see Writing Center: OWL for detailed information on all our programs and services.

The Library’s 2nd floor Academic Plaza (http://library.uta.edu/academic-plaza) offers students a central hub of support services, including IDEAS Center, University Advising Services, Transfer UTA and various college/school advising hours. Services are available during the library’s hours of operation.

Librarian to Contact:
Each academic unit has access to Librarians by Academic Subject that can assist students with research projects, tutorials on plagiarism and citation references as well as support with databases and course reserves.

Emergency Phone Numbers

In case of an on-campus emergency, call the UT Arlington Police Department at 817-272-3003 (non-campus phone), 2-3003 (campus phone). You may also dial 911. Non-emergency number 817-272-3381