# INFA723 Class Project

There are three options for the class project, each described below. You can pick either one which may be interested to you. **The project can be a research paper, a case study, a simulation, or an implementation.** In either case, you are required to write a report about it. You may team up with other partners, if you choose to, in doing your projects. Naturally, a lot more will be expected from such collaborative projects!

The project deliverables are listed below:

* **Project middle report**: The middle report should include a title and team members if you choose to work as a group. The middle report should also identify the project scope, the research questions you plan to work on, and preliminary ideas about how you are going to address the research questions. The middle report has 5 points in the final grade.
* **Project Final report and other documents**: The final project report should be a comprehensive report including everything. The final project report has 15 points in the final grade.
* **Final project presentation:** everyone needs to prepare 10-15 slides for presenting their final project.

**I**f you are not sure what you want to do in the project, discuss your project ideas with me via emails, phone calls, face-to-face/online meetings, etc.

The project will be evaluated based on the following criteria:

* Originality and novelty
* Technical depth and soundness
* Presentation quality

The adoption of AI is rising. AI has changed the ways we explore science and conduct businesses:

* AlphaGo is the first computer program to defeat a professional human Go player, the first to defeat a Go world champion, and is arguably the strongest Go player in history.
* Google's DeepMind releases structure of every known protein.
* ChatGPT passes exams from law and business schools.
* Reinventing search with a new AI-powered Microsoft Bing and Edge, your copilot for the web.

However, many threats and attacks have also been reported targeting machine learning algorithms. For example,

* One pixel attack for fooling deep neural networks (J. Su, D. V. Vargas and K. Sakurai, "One Pixel Attack for Fooling Deep Neural Networks," in IEEE Transactions on Evolutionary Computation, vol. 23, no. 5, pp. 828-841, Oct. 2019, doi: 10.1109/TEVC.2019.2890858.)

As we expect AI continues to change businesses, consumers, and the economy, we would also like to investigate AI related cybersecurity issues.

**Option 1: Machine Learning Security**

In this project, you will conduct research on security and privacy issues related to machine learning. If you choose this option, you can explore any ML-related security and privacy issues. The topics include, but are not limited to:

* Threats and attacks in AI
* Threat modeling in AI
* An in-depth study of an attack on AI
* A case study of a cyber-attack on AI
* Security remediation in AI
* Risk assessment in AI
* Survey of cybersecurity in AI

Project deliverables:

* Project middle report
* Project final report
* Project presentation slides
* Other related project documents

**Option 2: Large Language Model (LLM) Security**

In this project, you will conduct research on security and privacy issues related to LLM. Examples of LLMs include GPT, Llama, and BERT. If you choose this option, you can explore any LLM-related security and privacy issues. The topics include, but are not limited to:

* LLM for offensive security
* LLM for defensive security
* LLM for risk management
* LLM for compliance and auditing
* Threats and attacks in LLM
* Threat modeling in LLM
* An in-depth study of an attack on LLM
* A case study of a cyber-attack on LLM
* Security remediation, e.g., defensive mechanism, in LLM
* Risk assessment in LLM
* Survey of cybersecurity in LLM

Project deliverables:

* Project middle report
* Project final report
* Project presentation slides
* Other related project documents

**Option 3: Self-Selected Research Topic**

You have options to select a research project on your own. However, the proposed project must have a focus on security and privacy issues. You proposed project is also subject to my approval to move forward. Self-selected research topic could be your job-related projects.

Project deliverables:

* Project middle report
* Project final report
* Project presentation slides
* Other related project documents

**If you want to extend the class project to a yearlong project (if you are also in one of my classes next semester), please indicate in your project middle report too**. I will work with you to define project scope so that we can achieve more outcomes after the project is completed.

## Project Advising

Class project is a good opportunity to demonstrate your understanding of the subject material and your abilities as a researcher. You are encouraged to discuss your project ideas with me. For campus students, we could set up regular meetings to discuss your projects. For distance students, you are welcome to discuss your projects with me through emails, phone calls, or skype. My contact information has been listed below. Please make appointment if you want to talk to me online.

* Office: East Hall Room 332
* Email: [yong.wang@dsu.edu](mailto:yong.wang@dsu.edu)
* Phone: 605-221 8193

## Project Middle Report Format

* 12-point standard font
* Single column
* Double spacing
* 3-5 pages (citation pages do not count)

## Project Final Report Format

* 12-point standard font
* Single column
* Double spacing
* An extension of the middle report
* 10 pages minimum (title and citation pages do not count): **project final report is a complete report of your class project. Project final report can be extended from your middle report.**

Note: you are welcome to use IEEE Manuscript Template for your final report. This is a good opportunity to practice academic writing and it may lead to publications too.

## Project Presentation (TBD)

On-campus students are required to give project presentations in the end of the semester. Students choosing the case studies are required to make videos presenting their work. The rest of students are not required to do the presentations but are welcome to present their projects via videos or online collaboration tools such as Google Hangouts and Skype. Presentation slides are required for all the students as part of the project deliverables.

All project works should be submitted through D2L. If you work as a group, submit one report per group according to the requirement.