Weekly Calendar (Subject to Change)

Code Assignments are due to **5:00 pm every Friday**. **Papers Assignments** are due 12 pm before each class.

	Topic	Readings/Watching	Assignments	Notes
Week 1	Introduction, Syllabus, Introduction to Machine Learning, Classification Model: K-Nearest Neighbors.	Intro to ML models - Jupyter Notebook #1 (ML + KNN)		- Install Jupyter - Overview Python - Overview Numpy
Week 2	Basic ML algorithm: Support Vector Machines (SVM), Decision Trees, and Random Forests	Intro to fundamental/classical ML algorithms - Jupyter Notebook #2 (SVM + DT + RF)	Code Assignment #1	
Week 3	Linear Classification, Optimization, Stochastic Gradient Descent	Jupyter Notebook #3 (Linear Models) Jupyter Notebook #4 (Optimization Technique)		
Week 4	Backpropagation	Jupyter Notebook #5 (Optimization Technique)	Code Assignment #2	
Week 5	Introduction to Deep Neural Network	Jupyter Notebook #6 (Neural Network Model)	Code Assignment #3	
Week 6	Adversarial Machine Learning	**Monday:** - Intriguing properties of neural networks - Explaining and Harnessing Adversarial Examples **Wednesday:** - Towards Evaluating the Robustness of Neural Networks - Transferability in Machine Learning **See Also:** - Adversarial Learning - Generative Adversarial Networks - Generating Adversarial Examples with Adversarial Networks	**Monday**: Papers Assignment 1 **Wednesday**: Papers Assignment 2	- How to Read a Paper - Efficient Reading - How to Give a Great Talk - How to Write a Great Research Paper - How to Give a Great Research Talk
Week 7	Data poisoning, Defenses and detection: challenges	**Monday (Data Poisoning):** - Poisoning Attacks against Support Vector Machines - Poison Frogs! Targeted Clean-Label Poisoning Attacks on Neural Networks **Wednesday (Detection Challenges):** - Adversarial Examples Are Not Easily Detected: Bypassing Ten Detection Methods - Towards Deep Learning Models Resistant to Adversarial Attacks **See Also:** - Targeted Backdoor Attacks on DNN	**Monday**: Papers Assignment 3 **Wednesday**: Papers Assignment 4 Code Assignment #4	
Week 8	Data Privacy and Reconstruction Attack	**Monday (Data Privacy):** - The Secret Sharer **Wednesday (Privacy Attack)** - Membership inference attacks against MLs. **See Also:** - On Taxis and Rainbows - Some Useful Probability Facts - Reconstruction Attacks (Notes) - The Algorithmic Foundations of Differential Privacy (Section 8.1, overview Section 1)	**Monday**: Papers Assignment 5 **Wednesday**: Papers Assignment 6	

Week 9	Differential Privacy, a firm mechanism for private computations	**Monday:** - The Algorithmic Foundations of Differential Privacy (Section 2, Section 3.1 and 3.2) - The Complexity of Differential Privacy (Section 1.4-1.6) **Wednesday:** - The Algorithmic Foundations of Differential Privacy (Section 3.3) - The Complexity of Differential Privacy (Section 2) **See Also:** - Lunchtime for Differential Privacy - A Firm Foundation for Private Data Analysis - Data Privacy Foundations and Applications	**Project Summary** - Title, Group - 2-pages Summary. **(Due to Friday 12 March)** Code Assignment #5	
Week 10	Algorithmic Fairness	**Monday:** - 50 Years of Test (Un)fairness: Lessons for ML - Fairway: a way to build fair ML software **Wednesday:** - Fairness through Awarness - Equality of Opportunity in Supervised Learning **See Also:** - Fairness and ML (Sections 1 & 2)	**Monday**: Paper Assignment 7 **Wednesday**: Papers Assignment 8	
Week 11	Causal Inferences	**Monday:** - Pearl's Book (Ch 2) - Pearl's Book (Ch 3) **Wednesday:** Causality Paper #1 Causality Paper #2 **See Also** - WebPPL (Probabilistic Programming Language)	**Monday**: Paper Assignment 9 **Wednesday**: Paper Assignment 10	
Week 12	White-box and Gray-box methods for testing ML Models	**Monday (Testing DNN):** - DeepXplore - DeepTest **Wednesday (Bugs in DNN):** - Taxonomy of Real Faults in Deep Learning Systems - A Comprehensive Study on Challenges in Deploying Deep Learning Based Software	**Monday**: Papers Assignment 11 **Wednesday**: Papers Assignment 12	
Week 13	ML-assisted Software Testing	**Monday:** - Fuzzing: Hack, Art, and Science - Fuzzing: Challenges and Reflections **Wednesday:** - Automatic analysis of malware behavior using machine learning - On Training Robust PDF Malware Classifiers	**Monday**: Paper Assignment 13 **Wednesday**: Papers Assignment 14	
Week 14	ML-assisted Debugging, Project Presentation	**Monday:** - Differential Performance Debugging with Discriminant Regression Trees - Detecting and Understanding Real-World Differential Performance Bugs in Machine Learning Libraries **Wednesday:** Final Project Presentations (TBA)		
Week 15	Project Presentations	Final Project Presentations (TBA)	**Final Project Submission**	