Applied Programming Learning Series (APL)
CSEE5590/490-0005: Cybersecurity & AI

University of Missouri-Kansas City, School of Computing and Engineering, CSEE Department

Course Coordinator: Dr. Yugyung Lee

Instructor: Gharib Gharibi
Office: 519 Robert H. Flarsheim Hall
Email: ggk89@mail.umkc.edu
Office Hours: Tuesday and Thursday 3:00 - 4:00 PM or by appointment
Class Time: Tuesday & Thursday 5:30 PM – 8:15 PM, June 3 – July 27 (Summer 2019)
Class Location: Cockefair Hall-Rm 104

- Email is the preferred way of communication
- If you send me an email related to this course, include the course name in the email subject

Applied Programming Learning Series (APL) Description:
Each course in this APL series is for a graduate student or undergraduate (Senior) in the School of Computing & Engineering (SCE) who want to build programming skills in a specialized area. Students must have permission to enroll in any course of this series. The courses in this series will be counted toward fulfilling the course requirement for students' degree at SCE.

Course Description

Learning Cybersecurity technologies and tools for the development of Cybersecurity applications. This course teaches students to build Cybersecurity Programming techniques and programming skills to build secure neural networks using deep learning algorithms (Part 1) and to provide cybersecurity and privacy for the SOTA predictive models (Part 2). Students will develop applied programming skills using case studies from sensing, actuation, processing, and communication.

The course format is lecture and the instructional model is classroom based.

Prerequisite: prior knowledge and experience with Python, JavaScript, and Deep Learning.

Required Textbooks:

No textbook is required. However, several lectures and assignments will focus on research-based activities such as reading, reviewing, analyzing, and summarizing research papers.

Evaluation Plan		
Exams x 2	30%	Exam 1: June 27 (15%)
		Exam 2: July 25 (15%)
Assignments x 2	20%	Google Form including Github & Canvas Turnitin (Similarity <30%)
Presentation	10%	In class presentation
ICP x 7	35%	In class projects
Attendance	5%	Attendance Sheets & Feedbacks
Total	100%	

Schedule (tentative)

Part 1 (Week 1 – 4): Secure Deep Learning

- Building Deep Neural Networks
- Programming for Cybersecurity Applications
- Programming for Deep Learning Applications in Cybersecurity
- Federated Learning

Part 2 (Week 5 - 8): Cybersecurity Programming for Data/Deep Learning

- Programming for Data Privacy and Security
- Information Systems Security Programming and Audit
- Hacking Deep Learning Models
- Securing Deep Learning Models
- Data Privacy and Security

HOMEWORK

- The late policy on assignments is 10% off the grade if late within one day, 20% off the grade for two days late, 30% off the grade for three days late. Assignments that are submitted more than three days late will no longer be accepted
- DO NOT EMAIL your homework
- Your homework should be an original and independent work
- Homework points will be awarded on 100% for an honest effort to work each problem.

Grading (tentative; this grading criteria may change depending on the class overall performance)

95 -100	A
90 -94	A-
87- 89	B+
83 - 86	B
80 – 82	B-

77 – 79	C+
73 -76	C
70 – 72	C-
0 – 59	F

ICP Submission Guidelines (for In Class students):

1. ICP Submission is in pairs of two students.
2. Once completed, it must be presented to Instructor before the end of the class
3. Submission after class is considered as a late submission. (Check the late submission policy)
4. ICP Code with brief explanation should be pushed to GitHub. Submit the GitHub link through the Feedback Form: https://forms.gle/87zbbnxfVewBJEj98

Online Submission Guidelines (for Online students):

1. Submit your source code and documentation to GitHub and represent the work through wiki page properly (submit your screenshots as well. The screenshot should have both the code and the output)
2. Comment your code appropriately
3. Video Submission (2 – 3 min video showing the demo of the ICP, with brief voice-over on the code explanation)
4. Submission after class is considered as a late submission. (Check the late submission policy in the syllabus)
5. Use the following Google link to submit your ICP: https://forms.gle/87zbbnxfVewBJEj98

ICP Evaluation Criteria:

1. Completeness of Features
2. Code Quality (https://en.wikipedia.org/wiki/Best_coding_practices)
3. Time
4. Feedback Submission

Assignment Submission Guidelines (for both In Class and Online students):

1. LAB submission is in pairs of two students.
2. Submit your source code and documentation to GitHub and represent the work through wiki page properly (submit your screenshots as well.

1. The screenshot should have both the code and the output)
2. Comment your code appropriately
3. Video Submission (2 –3 min video showing the demo of the LAB, with brief voice-over on the code explanation)
4. Submit report and source code at Turnitin in UMKC blackboard
5. Remember that similarity score should be less than 15%
6. Use this link to submit your LAB#: https://forms.gle/vLhf86AZ3FbcEjcs6

The report should include below details

- Introduction
- Objectives
- Approaches/Methods
- Workflow
- Datasets
- Parameters
- Evaluation & Discussion
- Conclusion

RULES OF CONDUCT: Academic dishonesty will be addressed in accordance with UMKC regulations as presented in the "Policies and Procedures" section of the University catalog which is available online http://www.umkc.edu/catalog/Student_Conduct.html

Academic dishonesty includes cheating, plagiarism, or sabotage as defined in the above mentioned regulations. Please note that any behavior that might disrupt the learning process and environment (use of electronic devices, independent side conversation, habitual or extreme tardiness) while class is in session will not be tolerated and will result in dismissal.

By attending this class, you are acknowledging that you have read, understand and are fully committed to the required codes of conduct and are aware of the consequences of breaching them. Please contact the instructor if you have any questions regarding this or any other issues related to this class.

ATTENDANCE:

Students are expected to attend and participate in classes. Students who have an *excused absence* are expected to make arrangements with the instructor for alternative or make-up work. Such arrangements should be made in advance of the absence, where possible. Each student should make every attempt to get to class on time. The instructor is willing to circulate a sign-in sheet at every class and missing more than two class sessions may result in a reduced grade. With the exception of documented emergencies, medical reasons or out of town travel related to work, make-ups will not be possible. Whenever possible, advance notification is required.

RULES OF CONDUCT: Academic dishonesty will be addressed in accordance with UMKC regulations as presented in the "Policies and Procedures" section of the University catalog which is available online http://www.umkc.edu/catalog/Student_Conduct.html

CAMPUS SAFETY, MASS NOTIFICATION, EMERGENCY RESPONSE, and INCLEMENT WEATHER POLICIES:

http://www.umkc.edu/umkc alert/ http://www.umkc.edu/police **Police: 816-235-1515 or 911**

DISABILITY SUPPORT SERVICES: To obtain disability-related accommodations and/or auxiliary aids, students with disabilities must contact the Office of Services for Students with Disabilities (OSSD) as soon as possible. To contact OSSD call 816-235-5696. Once verified, OSSD will notify the course instructor and outline the accommodation and/or auxiliary aids to be provided. For more information go to: http://www.umkc.edu/disability/.

ENGLISH PROFICIENCY STATEMENT: Students who encounter difficulty in their courses because of the English proficiency of their instructors should speak directly to their instructors. If additional assistance is needed, they may contact the UMKC Help Line at 816-235-2222.

GRADE APPEAL POLICY: Students are responsible for meeting the standards of academic performance established for each course in which they are enrolled. The establishment of the criteria for grades and the evaluation of student academic performance are the responsibilities of the instructor. This grade appeal procedure is available only for the review of allegedly capricious grading and not for review of the instructor's evaluation of the student's academic performance.
http://www.umkc.edu/catalo g/gradeappeals

Title IX: Under the University of Missouri's Title IX policy, discrimination, violence and harassment based on sex, gender, and gender identity are subject to the same kinds of accountability and support applied to offenses based on other protected characteristics such as race, color, ethnic or national origin, sexual orientation, religion, age, ancestry, disability, military status, and veteran status. If you or someone you know has been harassed or assaulted, you can find the appropriate resources by visiting UMKC's Title IX Office webpage (http://info.umkc.edu/title9/) or contacting UMKC's Title IX Coordinator, Mikah K. Thompson (816.235.6910 or thompsonmikah@umkc.edu). Additionally, you can file a complaint using UMKC's online discrimination complaint form, which is located at http://info.umkc.edu/title9/reporting/report-online/.

While most UMKC employees are required to report any known or suspected violation of Title IX, students may seek confidential guidance from the following campus locations:

UMKC Counseling Service **Volker Campus** 4825 Troost Ave, Suite 206 Kansas City, MO 64110 Phone – (816) 235-1635	**UMKC Counseling Service** **Health Sciences Campus** Health Sciences Building 1418 2464 Charlotte Kansas City, MO 64108 Phone – (816) 235-1635 (open Tuesdays, 1-5pm)	**Student Health and Wellness** 4825 Troost Ave., Suite 115 Kansas City, MO 64110 Phone - (816) 235-6133