ITMS 527 SYLLABUS

ITMS 527 AI for Cybersecurity

Hours: 3 credit hours / 45 contact hours

Instructor: Marwan Omar, Ph.D.

Textbook, title, author, and year:
Machine Learning for Cybersecurity Cookbook, Emmanuel Tsukerman, 2019

Specific course information
a. **Catalog description:** This course is designed to equip students with knowledge and skills necessary to understand, implement, and leverage artificial intelligence (AI) techniques in the realm of cybersecurity. In an era where cyber threats continue to evolve and grow in complexity, AI has emerged as a powerful tool to defend against and mitigate these threats. This course explores the intersection of AI and cybersecurity, providing a comprehensive understanding of how AI technologies can be used to protect computing systems. By the end of this course, students will be well-equipped to leverage the power of AI to enhance cybersecurity efforts, making them valuable assets in the ever-evolving landscape of digital security. Join us on this exciting journey into the world of "AI for Cybersecurity" and prepare to defend against the digital threats of tomorrow. The course is intended for students with a basic understanding of computing and cybersecurity concepts.
b. **Prerequisites:** ITMD 514 or ITMS 514

Specific goals for the course
a. **Course Outcome:** The goal of this course is for students to learn how to apply artificial intelligence (AI) techniques to the problems of controlling cybersecurity risk to enterprise information assets. Students will learn the applications, benefits, limitations, and concerns regarding the use of AI in cybersecurity contexts. The course consists of lectures, hands-on lab exercises, group discussions, and assignments, which will give students the opportunity to work with AI tools and datasets relevant to cybersecurity. Guest speakers from industry and academia may also provide insights into cutting-edge developments in the field.
b. **Course Student Outcomes:**
Upon successful completion of the course the student should be able to do the following:

- Recall and describe fundamental concepts of cybersecurity, to include
  ○ threat landscapes;
  ○ attack vectors;
  ○ security protocols.
- Describe the role of AI in cybersecurity, including its applications, benefits, and limitations.
- Use AI algorithms and tools to detect, analyze, and respond to cyber threats.

- Explain the ethical and legal considerations surrounding the use of AI in cybersecurity.
- Employ critical thinking and problem-solving skills to address emerging cyber threats.
- Manage and deploy information resources applicable to each student's particular area of focus in an enterprise setting.

Topics to be covered
a. Introduction to cybersecurity
b. Fundamentals of AI
c. AI Applications in Cybersecurity
d. AI-driven security analytics
e. Ethical & Legal aspects of AI in Cybersecurity
f. Real-world case studies
g. Future trends

Each ITM Departmental Syllabus *represents a recent offering of the course. The instructor, textbook(s), course outcomes, and course student outcomes/learning objectives may vary in future semesters.*

February 1, 2024