**Secure AI Systems – Instructor: Dr. Shayan (Sean) Taheri**

**Topics:**

1. Introduction to Secure AI Systems.
2. Review of Statistical Analysis (Signal Processing), Artificial Intelligence, and Machine/Deep Learning.
3. AI in Cybersecurity Domain: Introduction, Considerations, Technology, and Principles.
4. Positive and Negative Applications of AI for Cybersecurity and People’s Lives.
5. Trustworthy Versus Reliability of AI Systems.
6. Hardware and Software Attacks and Defenses using AI Techniques.
7. AI Systems for Malicious Anomaly Detection.
8. AI-Enabled Cryptographic Algorithms.
9. Intelligent Hardware and Software Trojans.
10. AI-Based Side-Channel Analysis.
11. Leveraging AI in Network Security.
12. Security Aspects of Reinforcement Learning.
13. Testing and Security of Deep Neural Networks (DNNs).
14. Usage of DNNs in Emerging Cyber Attacks.
15. Secure Explainable and Ethical AI Systems.