Dr. Shayan (Sean) Taheri's Outline for Medical-AI-IoT-Security Proposal

Candidate Venue for Submission: **NSF Secure and Trustworthy Cyberspace (SaTC)**

Task 1: Emerging Security-Associated Medical Errors (Application-Level).

- Analyzing the existing and emerging medical errors in terms of the causes, forms, risks, and prevalence based on the international databases and evaluating their prevalence using the statistical analysis software, such as Stata and SAS [1].
- Finding the educational and practical medical procedures for prevention and detection-correction against medical errors.
- Developing a taxonomy of medical errors and solutions.
- Identifying association of security threats with medical errors (MRs) [2].
- Proposing novel (AI/Computer Vision/Digital Twin) technology-driven medical procedures as security countermeasures for the MR-based security threats and evaluating their impacts on healthcare system.

Task 2: Vulnerability Assessment of Medical Devices at Software and Hardware-Level (Device-Level).

- Discovering the relationship between medical devices with the medical errors.
- Studying security tests and the attacks demonstrated by the researchers on a conclusive number of devices.
- Identifying hardware/software vulnerabilities and loopholes present in the medical devices by physical inspection to be exploited for developing detrimental attacks.
- Proposing efficient and intelligent cross-layer solutions and countermeasures based on the novel methods from physical assurance.
- Developing a taxonomy of security attacks and defenses for medical devices.

Task 3: AI Utilization in Medical-Based Cyber Attacks and Defenses (Device-Level).

- Identifying the opportunities from the existing cyber-attacks for the medical devices (along with similar types of devices) and proposing new dynamically evolving attacks accordingly. Targeting both data- and control-path of the devices for malicious operations.
- Finding the trends and behavior of known attacks (i.e., training data) acquired from physical inspection to build knowledgeable and protected AI-driven defenses.

Task 4: Intelligent Testing of Security-Enhanced Medical Devices (Device-Level).

- Introducing different security metrics for evaluating the medical devices.
- Conducting comprehensive test and analysis on the security-enhanced medical devices for measuring their performance and defense strength.
- Integrating digital twins of patients into the testing framework for performance augmentation.
- Prevention, recognition, monitoring, and control by the security-enhanced medical devices in confronting the post-enhancement attacks.

Task 5: AI-Driven Software-Hardware Recognition for Effective Drugs and Vaccines (Application-Level).

- Developing a novel cross-layer medical recognition system for the medical devices with the aim of providing prescriptions and recognizing medicines, realized using a hardware accelerator.
- Security assessment of the recognition system based on different malicious medical scenarios.
- Analyzing the dangerous impacts of system misrecognition of medical data on healthcare system.

[1] Prevalence of medical errors in Iran: a systematic review and meta-analysis
[2] Assessment of Physician Sleep and Wellness, Burnout, and Clinically Significant Medical Errors