

I hold a strong background in **Artificial Intelligence** and **Cybersecurity**, with particular focus on **cyber-attack detection and localization in smart grids** using advanced deep learning techniques. As a research assistant at prominent labs including **ASC Lab**, **PSS Lab**, and **CReaTech**, I contributed to the development of AI-driven models—such as **Autoencoders**, **CNNs**, **Transfer Learning**, **Kolmogorov-Arnold Networks (KAN/CKAN)**—to detect and localize anomalies in both numerical and visual data. My work has led to multiple publications and has equipped me with hands-on skills in **Python**, **MATLAB**, **TensorFlow**, **PyTorch**, and working with large-scale cybersecurity datasets like the **Mississippi dataset**.

I also **completed a volunteer course in Meta-Learning**, where I developed a deep understanding of **learning to learn paradigms**. This included exposure to and hands-on experience with various meta-learning models such as:

- **Model-Agnostic Meta-Learning (MAML)**
- **Reptile**
- **Prototypical Networks and Matching Networks**
- **SNAIL**
- **Few-shot learning and meta-optimization frameworks**

This training enriched my understanding of how meta-learning techniques can improve model generalization in low-data regimes—a key advantage for cybersecurity systems where labeled attack data is scarce. I'm confident in applying these strategies to design **adaptive and robust AI systems**, particularly in domains like intrusion detection, real-time anomaly recognition, and autonomous control.

Additionally, I completed a graduate-level **Reinforcement Learning** course, which enhanced my capabilities in **decision-making algorithms** such as **Q-learning**, **SARSA**, **DQN**, and **PPO**, applied to dynamic simulations and cybersecurity scenarios.

Looking forward, I aim to focus my research on **secure and adaptive AI systems in autonomous vehicles** and **smart grids**, using:

- **Self-Supervised Learning** (e.g., Contrastive Learning, Masked Autoencoding, Temporal prediction)
- **Online Learning** (e.g., Continual Learning, Contextual Bandits, Streaming Anomaly Detection)
- **Meta-Learning** (to build rapidly adaptable security models across multiple deployment environments)
- **Reinforcement Learning** (for adaptive, policy-driven intrusion response and system control)

By combining these AI domains, my goal is to build **resilient, generalizable, and real-time intelligent defense systems** for critical cyber-physical infrastructures.