Research Statement

I aspire to pursue Computer Security as an enduring academic subject. In particular, I am interested in studying **Anti-censorship Internet Measurement**, **Secure Designs for Infrastructure Systems**- such as **Supervisory Control and Data Acquisition** (SCADA), **Cloudless Computing**, and **Internet of Things** (IoT)- and **Privacy-Preserving Adversarial Methods** to defend against privacy violation attacks from commercial Machine Learning (ML) models. These topics captivate me for they directly adhere not only to my technical interest in building reliable systems, but also address the challenges of information freedom and data privacy that have been central to my commitment to employ computing as a levitation towards the betterment of societal well-being.

Future Research Agenda: First and foremost, **my core agenda is to guardrail technology to serve the betterment of human rights**. However, to be specific:

Decentralized Censorship Circumvention: I plan to base my future Censorship Circumvention research direction on the rationale stated in the paper, *"The Parrot Is Dead,"* by **Prof. Amir Houmansadr** et al. as the ground truth, where the authors contemplated that seeking obfuscation methods beyond mimicry at a higher layer of covert communication, i.e., network binary data into a sound wave, is direly essential [1]. As a doctoral researcher, I aim to continue my research on developing novel circumvention models based on distributed systems against regional Internet censorship. One example would be to further my design of utilizing the sheer number of IoT devices in the wild for network routing purposes with **fragmented packets sent in parallel (parallelism)**, paralyzing real-time packet-pair or traffic correlation surveillance techniques without significant performance cost.

Privacy-preserving Methods Against ML Models: I look forward to expanding upon the project, *"Glaze,"* by **Shawn Shan** and **Prof. Ben Zhao** et al., where they utilized a data augmentation technique that applies imperceptible perturbations to artists' images and protects them from diffusion-based text-to-image models from mimicking their unique artistic styles [2]. I would also like to explore **ML masking or watermarking techniques** further as defensive mechanisms for individuals subjected to unsolicited ML training data collections.

IoT Security and Novel Applications: I want to investigate the IoT security of governmental, infrastructural, and commercial venues. For instance, despite extensive research efforts in Smart City initiatives, severe embedded-level protocol vulnerabilities still haunt governmental and civilian users [3; 4]. Another overlooked Cybersecurity area in this domain is the vulnerability of military-related IoT devices, namely the **Internet of Battlefield Things** (IoBT) and **Internet of Medical Things** (IoMT), which are subjected to heavy interference during Cyberwarfare and on battlefields [5].

References

[1] A. Houmansadr, C. Brubaker, and V. Shmatikov, "The parrot is dead: Observing unobservable network communications," in *2013 IEEE Symposium on Security and Privacy*, pp. 65–79, 2013.

[2] S. Shan and et al., "Glaze: Protecting artists from style mimicry by text-to-image models," in *Proceedings of the 32nd USENIX Security Symposium*, 2023.

[3] J. Ahamed and A. V. Rajan, "Internet of things (IoT): Application systems and security vulnerabilities," in *2016 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA)*, (Ras Al Khaimah, United Arab Emirates), pp. 1–5, 2016.

[4] B. Babu, T. Ijyas, P. Muneer, and J. Varghese, "Security issues in SCADA-based industrial control systems," in *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, (Abha, Saudi Arabia), pp. 47–51, 2017.

[5] O. Westerlund and R. Asif, "Drone hacking with raspberry-pi 3 and wifi pineapple: Security and privacy threats for the internet-of-things," in *2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS)*, (Muscat, Oman), pp. 1–10, 2019.