Ayesha Binte Mostofa : ayeshathoi.github.io : ayeshaathoi62@gmail.com

Statement of Purpose

of Ayesha Binte Mostofa (CS, PhD applicant for Fall–2025)

In the modern era of the digital revolution, electronic devices have become integral to our daily lives, storing all sensitive information related to our everyday activities. These devices are becoming more capable day by day with the integration of sophisticated operating systems and advanced machine learning techniques. A single vulnerability within these intelligent systems can lead to catastrophic consequences, ranging from financial losses in the billions to the loss of lives. The 2023 data breach on a Bangladesh Government website[1], which exposed the personal data of over 5 crore citizens was an eye-opener for me. This is my primary reason for pursuing a PhD in security. I want to analyze the security challenges of modern computational systems and design solutions to mitigate these challenges during my PhD.

Prior Works:

Security Coursework: My interest in cybersecurity began to grow after thoroughly implementing and documenting the functionalities of the threat intelligence tool, MISP for my security term project. I was impressed by the tool's usability and felt motivated to explore further. As part of my coursework, I implemented a public key cryptography system using AES, incorporating Diffie-Hellman and RSA key exchange algorithms, all interconnected via a client-server socket. I have completed the seedlabs assignments exploring firewall configuration and evasion techniques, using C language for buffer-overflow vulnerability, and Python for malware modification within the docker environment. Furthermore, I independently implemented steganography techniques to conceal messages within images and audio.

Data Provenance & Threat Detection: Currently I am working with Professor Dr. Md. Shohrab Hossain and Dr. Shahrear Iqbal (NRC Canada) on a cybersecurity research project. Our objective is to investigate the prediction accuracy of Large Language Models (LLMs) in detecting attack behaviors within computer system logs. Detecting APTs from system logs is challenging, due to their nature as zero-day attacks. Our approach involves constructing provenance graphs and reverse trees (children-to-parent relationships) using random walks. We then generate event traces, classify them, and label the data as benign or malicious to guide Language models in accurately detecting attack behaviors. We are currently exploring the question: could utilizing Retrieval-Augmented Generation in language models enhance the precision of attack behavior detection in our research? We are also exploring whether more efficient algorithms could be developed to construct provenance graphs.

Automating Code Review with NLP and Semantic Metadata: During my undergrad thesis with Professor Dr. Anindya Iqbal and Dr. Toufique Ahmed (IBM Research), we focused on liberating developers from the labor-intensive and time-consuming task of manual code reviews. Acquaintance with prompt engineering, requiring less time than fine-tuning since it doesn't involve extensive retraining for a specific task, led us to the question: Could prompt engineering be deployed to make LLMs focus on semantic metadata, allowing them to grasp the whole essence of the work? This idea led to generating the call graph and code summaries from the codebase, providing the models with a concise understanding of the vast codebase. We evolved our prompts, augmenting few-shot examples with and without instructions, and experimented using GPT and Gemini models. To retrieve the best n few-shot examples, we utilized the BM25 algorithm. We also experimented with parameter-efficient fine-tuning, where we supervised the model with instructions and employed QLoRA, effectively balancing performance and memory usage with Llama and CodeLlama models. While all our models outperformed the baseline model CodeReviewer, the best model surpassed the result by achieving over **90% BLEU** in this task. To validate our results, we conducted a human evaluation study through a web portal, where developer feedback confirmed the superiority of our model over the baseline. We also validated the result through self-reflection and GraphCodeBert. I was actively involved in the entire research, but my major contributions were in prompt evolution and the development of the

[1] 2023 Bangladesh Government website data breach - Wikipedia

web portal. I also made significant contributions to the codebase for call graph generation and code summary, and co-authored a paper [1] detailing the findings.

Machine Learning Projects: Inspired by the application of CycleGAN and VGG19 in an existing article, I employed VGG16, CycleGAN, and ResNet50 to transfer artistic styles from paintings to landscape images, in a project **Paint like Your Favorite Artists**. This project, documented in a detailed report, utilized perceptual loss to achieve high-quality style transfer through calculations of style and content loss with minimal computational resource. Our current question is whether this approach can effectively transform text into calligraphy. I also participated in the SUST Deep Learning Enigma 2024 competition, focusing on **vehicle object detection** where we secured 8th place among approximately 100 competitors from other universities. We fine-tuned vision transformer models, including YOLOv6L6, YOLOv8, Faster R-CNN, and CoDETR, by leveraging transformer learning techniques. I also contributed to developing an Android App for **Client-side verification of National ID Card images**, using Android Studio, openCV, and TensorflowLite, as a machine learning intern in one of BD company. Additionally, I worked on a research project with Dr. A. B. M. Alim Al Islam on **forecasting ground level water** by utilizing artificial neural networks and regression models.

Faculty of Interest: I believe the University of Massachusetts Amherst is an excellent fit for my aspirations, given the diverse expertise and strengths of its faculty. I am particularly interested in the work of **Dr. Pubali Datta**. One of her papers, *"ALASTOR: Reconstructing the Provenance of Serverless Intrusions"*, is especially insightful as I am currently engaged in research involving provenance graphs. I find her work closely aligned with my interests. I have built a strong foundation in systems through various coursework projects. These projects include building a C compiler from scratch using bison and flex, learning assembly x86 language, and the 8086 as well as MIPS architecture, implementing various functionalities of the xv6 operating system, including the paging mechanism for memory management. I have also developed an embedded systems project, *Health Monitoring System*, designed to assess the health conditions of COVID-19 patients.

I am also eager to work with **Dr. Amir Houmansadr**, as I am impressed by his research on *"ProxyGPT: Enabling Anonymous Queries in AI Chatbots with (Un)Trustworthy Browser Proxies"*. I have prior experience with GPT and AI models and a strong curiosity about exploring security aspects in them. Additionally, during my computer networks coursework, I configured VLANs, simulated networks in NS2, implemented a multi-threaded web server, and enhanced TCP Cubic-FIT simulations. I believe I can gain valuable insights by working with him. It would also be a privilege to work with **Dr. Eugene Bagdasarian**. His study on cross-modal injection attacks in language models, *"Soft Prompts Go Hard: Steering Visual Language Models with Hidden Meta-Instructions"*, is highly illuminating. I am very interested in working on similar projects. I am also interested to work with **Dr. Shiqing Ma**. My solid foundation in Artificial Intelligence and systems, combined with my research motivation, aligns closely with Dr. Ma's areas of interest.

Goals: Nothing inspires me more than the thought that my contributions could someday lead to developing more efficient systems, ultimately serving countless individuals. As a woman dedicated to research in a third-world country, I know how it feels to be a part of the minority. Post-PhD, I aim to remain in academia as a faculty member, conducting impactful research and creating pathways to support individuals from underrepresented backgrounds. I believe pursuing a PhD at the University of Massachusetts Amherst will help me turn my aspirations into reality.

References

[1] *Md. Asif Haider, ***Ayesha Binte Mostofa**, *Sk. Sabit Bin Mosaddek, Anindya Iqbal, and Toufique Ahmed. Prompting and fine-tuning large language models for automated code review comment generation, 2024. https://arxiv.org/abs/2411.10129.

[2] *Equal contribution.