Md. Ahsan Ayub

Cookeville, TN 38501, USA | mayub42@tntech.edu | linkedin.com/in/mdahsanayub | ahsanayub.github.io

Education

Tennessee Tech University — Cookeville, TN
(Master's leading to) Ph.D. Student in the Department of Computer Science. CGPA 3.93/4.00. — *Aug 2018 – May 2023*

Experience

Security Engineer (Intern) — Jan 2022 – Present
AllianceBernstein — *Nashville, TN*

- Administered the networking devices, e.g., Firewall, Proxy Server, Domain Name Server (DNS), Intrusion Detection System (IDS), and Load Balancer, to safeguard the Company's global infrastructure from insider and outsider security threats.
- Processed the security logs/events (indexed in an SIEM) from devices across the Company's global infrastructure to present actionable analytical insights to the team to aid the incident management/operation and risk mitigation tasks.

Graduate Research Assistant — Aug 2018 – Present
Cybersecurity Education, Research & Outreach Center (CEROC) — *Cookeville, TN*

- Contributed to the experimental research of both static and dynamic malware analysis for ransomware to propose multi-layered endpoint protection by incorporating Data Science, Machine Learning, and Reverse Engineering techniques.
- Partnered with the external security researchers in industry, U.S. national labs, and other universities in a collaborative research environment to initiate and review the research project, perform experiments, and analyze the empirical findings.

Graduate Teaching Associate — Aug 2021 – Dec 2021
Department of Computer Science, Tennessee Tech University — *Cookeville, TN*

- Instructed a class of 75+ students to teach Introduction to Problem Solving and Programming in C++ in Fall 2021.
- Developed class materials, exam/quiz questions, and programming assignments/challenges; initiated automated programming assessments with online judging tools; and managed online quizzes and grading.

Software Project Manager — Feb 2017 – July 2018
Appinion BD Limited — *Dhaka, Bangladesh*

- Led the software development and UI/UX team to a successful launch of a learning app (Android & Web) with 1,500+ users for the sales department of one of the renowned pharmaceutical companies, *Renata Limited* (Operated by Pfizer until 90s).
- Coordinated with the largest NGO in the world, *BRAC*, to automate the business process of *Human Rights and Legal Aid Services* by conceptualizing the software development scope to facilitate the nationwide adaptation of digitization.

Projects

Static Analysis of Ransomware to Find Similarities on PE File Metadata — Dec 2020 - Nov 2021

- Identified a unique list of suspicious indicators on the generated Portable Executable (PE) file metadata of 727 active ransomware samples based on the exploratory data analysis tasks and our domain knowledge.
- Applied One-Class Classification techniques on several feature spaces, including Imports, Libraries, and PE Sections, to find out the similarities and achieved 10.04% of testing error with the Local Outlier Factor algorithm.

I/O Request Packet (IRP) Logs Driven Ransomware Detection — Mar 2020 - Sep 2020

- Extracted data-driven encryption patterns based on time series analysis through IRP, a low-level file system I/O logs, to detect unseen ransomware samples within 15 mins of execution (testing error of 6.25%) by using One-Class SVM algorithm.
- Constructed Neural Networks architecture using Keras to effectively detect IRP logs of 21 ransomware families and achieved accuracy, precision, recall, and F_1 scores in the range of $99.7\% \pm 0.2\%$.

Adversarial Machine Learning on network-based Intrusion Detection System — Sep 2019 - Jan 2020

- Developed a Multilayer Perceptron (MLP) using Keras for an improved intrusion detection system (target) to launch the model evasion attack by sending adversarial network packets, crafted from the Jacobian-based Saliency Map method.

Parallelization of RSA Encryption Algorithm in High Performance Computing — Jun 2019 - Aug 2019

- Demonstrated significant performance improvements of the parallel implementation of RSA algorithm by using the OpenMP library comparing with its serial implementation (achieved 4.4 speed up with 8 threads).

Skills

Proficient with: Python, Object Oriented Programming (OOP), Firewall, Git, Problem Solving, C/C++, Agile, MySQL, Splunk, Matplotlib, Scikit-learn, Network Analysis, Web Development, and Software/Technical Documentation.
Familiar with: Android App Development, PHP, RESTful API, Software Design Patterns (e.g., MVC), and Cloud Computing.

Honors and Awards

- Best poster in the 2021 Student Research and Creative Inquiry Day (CS Graduate Track) at Tennessee Tech University.
- Represented (50+) Graduate Students in the Computer Science Strategic Planning Core Group during Spring 2021.

Certifications

- **CompTIA Security+**, issued on Feb 2022 by CompTIA.
- **Advanced SQL for Data Scientists**, issued on Feb 2021 by LinkedIn.
- **Learning Amazon Web Services (AWS) for Developers**, issued on Feb 2021 by LinkedIn.
- **Data Analysis and Visualization (Python)**, issued on Jun 2020 by Udemy.
- **Sequences, Time Series, and Prediction**, issued on Jun 2020 by DeepLearning.AI.
- **Neural Networks and Deep Learning**, issued on Feb 2020 by DeepLearning.AI.
- **Machine Learning A-Z: Hands-on Python & R in Data Science**, issued on Jun 2019 by Udemy.

Leadership

Competitive Programming Coach at Tennessee Tech University Oct 2021 – Present

- Taught implementation, mathematics, data structure, and algorithms-related topics to prepare 10+ Computer Science undergraduate students for International Collegiate Programming Contest (ICPC).
- Hosted several intra-university competitive programming contests using online judging platform to promote awareness and raise interest in the department, as well as university.

President of the Computer Science Graduate Student Club at Tennessee Tech University Sep 2019 – Aug 2021

- Organized bi-weekly seminars to promote research environment and enable the club members to network and exchange ideas.

Professional Services

- **Sub-reviewer**, Lightning Talks, Women in CyberSecurity (WiCyS 2022).
- **Sub-reviewer**, IEEE International Conference on Big Data (IEEE BigData 2021).
- **Program and Organization Committee Member**, Workshop on Smart Farming, Precision Agriculture, and Supply Chain (SmartFarm 2021), held in conjunction with the 2021 IEEE International Conference on Big Data.

Publications

- **M. A. Ayub** and A. Siraj, "Similarity Analysis of Ransomware based on Portable Executable (PE) File Metadata," 2021 IEEE Symposium Series on Computational Intelligence (SSCI), Orlando, FL, USA, 2021, pp. 1-6. (GitHub)
- **M. A. Ayub**, S. Smith, A. Siraj, and P. Tinker, "Domain Generating Algorithm based Malicious Domains Detection," 2021 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), Washington DC, USA, 2021, pp. 77–82. (GitHub)
- **M. A. Ayub**, A. Continella, and A. Siraj, "An I/O Request Packet (IRP) Driven Effective Ransomware Detection Scheme using Artificial Neural Network," 2020 IEEE International Conference on Information Reuse and Integration (IRI), Las Vegas, NV, USA, 2020, pp. 319-324. (GitHub)
- **M. A. Ayub**, W. A. Johnson, D. A. Talbert, and A. Siraj, "Model Evasion Attack on Intrusion Detection Systems using Adversarial Machine Learning," 2020 54th Annual Conference on Information Sciences and Systems (CISS), Princeton, NJ, USA, 2020, pp. 1-6. (GitHub)
- **M. A. Ayub**, Z. A. Onik, and S. Smith, "Parallelized RSA Algorithm: An Analysis with Performance Evaluation using OpenMP Library in High Performance Computing Environment," 2019 22nd International Conference on Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 2019, pp. 1-6. (GitHub)
- **M. A. Ayub**, S. Smith, and A. Siraj, "A Protocol Independent Approach in Network Covert Channel Detection," 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), New York, NY, USA, 2019, pp. 165-170. (GitHub)
- **M. A. Ayub**, K. A. Kalpoma, H. T. Proma, S. M. Kabir, and R. I. H. Chowdhury, "Exhaustive study of essential constraint satisfaction problem techniques based on N-Queens problem," 2017 20th International Conference of Computer and Information Technology (ICCIT), Dhaka, 2017, pp. 1-6.