Md. Ahsan Ayub

Atlanta, GA 30318, USA | mayub42@tntech.edu | linkedin.com/in/mdahsanayub | ahsanayub.github.io

Education

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

Experience

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

- Executed experimental research of static and dynamic ransomware analysis to develop multi-layered endpoint protection for prompt and robust detection on Windows environment by incorporating Data Science and Reverse Engineering techniques.
- Published 6 peer-reviewed scholarly articles in ransomware, cryptography, adversarial ML, DGA, and covert communication.

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

- Processed a large number of geographical security events on SIEM to document security incidents and to present actionable insights on the anomalous IP ranges for the incident response and risk mitigation tasks.
- Utilized open-source tools to discover trends and emerging threats and identify known/unknown web applications security vulnerabilities including cross-site scripting, cross-site request forgery, SQL injection, DoS attacks, and API attacks.
- Developed custom methodologies, payloads, and exploits to detect and remedy security issues, such as OWASP Top 10.

Graduate Teaching Associate — Aug 2021 – Dec 2021
Tennessee Tech University — *Cookeville, TN*

- Instructed a class of 75+ CS undergraduate students to teach Introduction to Problem Solving and Programming in C++.

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

- Led Dev and UI/UX teams to build a scalable and reliable sales learning app for 1,500+ users of a pharmaceutical company.

Projects

Detection of Windows-based Cryptographic Ransomware (GitHub: 1, 2, and 3) — Mar 2020 - Present

- Examined the structural dissimilarities (PE metadata) between 2,436 ransomware and 3,014 benign application with built machine learning models and reported accuracy, precision, recall, and F_1 scores in low 90s using Random Forest classifier.
- Identified a unique list of suspicious indicators based on the structural information of 727 active ransomware.
- Achieved 10.04% of testing error with the Local Outlier Factor algorithm to investigate structural similarities of ransomware samples based on Imports, Function Names, and PE Sections feature spaces.
- Extracted data-driven encryption patterns of 272 ransomware based on 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 an Artificial Neural Network architecture using Keras to detect 21 ransomware families (multiclass classification) based on IRP logs and obtained 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 (GitHub) — 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 (GitHub) — Jun 2019 - Aug 2019

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

Skills

Proficient with: Python, Firewall, Metasploit, Nmap, Nessus, Burp Suite, Offensive Security, Vulnerability Assessment, Git, Object Oriented Programming, C/C++, Agile, MySQL, Matplotlib, Scikit-learn, Network Analysis, and Web Development.
Familiar with: Android App Development, Docker, RESTful API, Secure Development Lifecycle (SDLC), JavaScript, AWS, Software Design Patterns, Static Application Security Testing (SAST), and Dynamic Application Security Testing (DAST).

Certifications

- **eLearnSecurity Junior Penetration Tester (eJPT)**, issued on Aug 2022 by eLearnSecurity - an INE Company.
- **CompTIA Security+**, issued on Feb 2022 by CompTIA.
- **Sequences, Time Series, and Prediction** & **Neural Networks and Deep Learning** by DeepLearning.AI in 2020.

Leadership

Competitive Programming Coach at Tennessee Tech University — Oct 2021 – Present

- Taught mathematics, data structure, and algorithms-related problem-solving topics through lectures and practice contests.

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

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

Honors and Awards

- Best poster in the 2021 Student Research and Creative Inquiry Day (CS Graduate Track) at Tennessee Tech University.
- 2^{nd} prize for the 2015 Web Application Development/Showcasing intra-college competition at my undergraduate university.

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.
- M. M. Rayhan and **M. A. Ayub**, "An Experimental Analysis of Classification Techniques for Domain Generating Algorithms (DGA) based Malicious Domains Detection," 2020 23rd International Conference on Computer and Information Technology (ICCIT), Dhaka, 2020, pp. 1-5.
- S. M. Hossain and **M. A. Ayub**, "Parameter Optimization of Classification Techniques for PDF based Malware Detection," 2020 23rd International Conference on Computer and Information Technology (ICCIT), Dhaka, 2020, pp. 1-6.
- R. N. Chowdhury, M. M. Chowdhury, S. Chowdhury, M. R. Islam, **M. A. Ayub**, A. Chowdhury, and K. A. Kalpoma, "Parameter Optimization and Performance Analysis of State-of-the-Art Machine Learning Techniques for Intrusion Detection System (IDS)," 2020 23rd International Conference on Computer and Information Technology (ICCIT), Dhaka, 2020.

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.