Ahsan Ayub, PhD

linkedin.com/in/mdahsanayub | ahsanayub.github.io

Education

Tennessee Technological University — Cookeville, TN, USA
Doctor of Philosophy in the Department of Computer Science. CGPA 3.93 out of 4.0. — *Aug 2018 – May 2023*

Tennessee Technological University — Cookeville, TN, USA
Master of Science in the Department of Computer Science. CGPA 3.92 out of 4.0. — *Aug 2018 – May 2022*

American International University-Bangladesh — Dhaka, Bangladesh
Bachelor of Science in Computer Science & Engineering. CGPA 3.84 out of 4.0. — *May 2013 – Feb 2017*

Experience

Security Engineer — Jan 2024 – Present
Vanderbilt University Medical Center (VUMC) — *Nashville, TN*
- Contributed in security architecture development and management and risk assessment, analysis, and management.

Security Data Scientist — June 2023 – August 2023
Dropzone AI (Contractual) — *Seattle, WA*
- Integrated 4 security monitoring tools in the Company's alert investigation platform to perform analytical work in SOCs autonomously by leveraging the large language model (LLM)-based autonomous AI agents.
- Developed and refined prompts to specialize GPT language models in security operations without causing hallucination.

Graduate Research Assistant — Aug 2018 – May 2023
Cybersecurity Education, Research & Outreach Center (CEROC) — *Cookeville, TN*
- 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.
- Proposed a novel static-informed dynamic analysis approach for early detection of cryptographic windows ransomware and reported 97.67%, 92.38%, and 86.42% accuracy within 120, 60, and 30 seconds of their behavioral logs, respectively.
- Published 10 peer-reviewed scholarly articles in ransomware, cryptography, adversarial ML, DGA, and covert communication.

Security Engineer (Intern) — Jan, 2022 – Present
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
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.

Skills

Programming Languages: Proficient in Python, C/C++, and SQL. Familiar with JAVA, C#, R, Shell Scripting, JS, and PHP.
Frameworks and Tools: Metasploit, Splunk, Nmap, Nessus, Burp Suite, Matplotlib, Scikit-learn, Docker, Git, CI/CD, MySQL, RESTful API, Static Application Security Testing (SAST), and Dynamic Application Security Testing (DAST).
Cybersecurity Practices: Intrusion Analysis, Threat Modeling, API Security, Secure System Design and Architecture, Identity and Access Management (IAM), Disaster Recovery and Business Continuity, Secure Deployment Practices, and Cloud Security.

Certifications

- **AWS Certified Cloud Practitioner**, issued on Aug 2023 by Amazon Web Services (AWS).
- **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**, issued on Jun 2020 by DeepLearning.AI.
- **Neural Networks and Deep Learning**, issued on Feb 2020 by DeepLearning.AI.

Honors and Awards

- Best research paper award in the 2023 IEEE 9th International Conference on Collaboration and Internet Computing (CIC).
- 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.
- 2^{nd} prize for the 2015 Web Application Development/Showcasing intra-college competition at my undergraduate university.

Leadership

Competitive Programming Coach at Tennessee Tech University Oct 2021 – May 2023

- 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

- **PC Member**, 3rd Workshop on Rethinking Malware Analysis (WoRMA), co-located with IEEE EuroS&P 2024.
- **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**, A. Siraj, B. Filar, and M. Gupta, "RWArmor: a static-informed dynamic analysis approach for early detection of cryptographic windows ransomware," International Journal of Information Security (2023), pp. 1-24. (Manuscript)
- **M. A. Ayub**, A. Siraj, B. Filar, and M. Gupta, "Static-RWArmor: A Static Analysis Approach for Prevention of Cryptographic Windows Ransomware," 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Exeter, UK, pp. 1–10. (GitHub)
- **M. A. Ayub** and A. Siraj, "Understanding the Behavior of Ransomware: An I/O Request Packet (IRP) Driven Study on Ransomware Detection against Execution Time," 2023 IEEE 9th International Conference on Collaboration and Internet Computing (CIC), Atlanta, GA, USA, pp. 1–10. (Manuscript)
- **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.