PRAJNA BHANDARY

prajna.bhandary.22@gmail.com | (443)-527-5965 | https://www.linkedin.com/in/pjbhandary/ | https://github.com/prajbh

EDUCATION

University of Maryland, Baltimore County (UMBC) Expected Graduation: December 2025
Ph.D. Candidate (ABD), Computer Science (Available to start full-time: December 2025)

SKILLS

Programming/Scripting: Python, PowerShell, C++, C, Java
Automation & Data Analysis: Jupyter, Scikit-Learn, PyTorch, TensorFlow, HuggingFace, Pega
Cloud/Container Platforms: Azure, IBM Cloud, Docker
Analysis Tools: Ghidra, Wireshark, YARA (basic), Scapy, VirusTotal, Proxmox, Cofense Triage
Reverse Engineering & Debugging: (familiar) IDA Pro, Ghidra, GDB, x64dbg, WinDbg
Version Control & Dev Tools: Git, Visual Studio, IntelliJ IDEA, ServiceNow
Databases: MySQL, MongoDB, Cloudant

WORK EXPERIENCE

Graduate Assistant - Teaching Assistant - *UMBC* Feb 2019 - present
- **Courses:** Introduction to Machine Learning, Software Reverse Engineering, Computer Networks, Artificial Intelligence, Introduction to Network Security, Data Structure, Programming languages, Object Oriented Programming(C++), Assembly language.

Threat Intel Research Intern - *Palo Alto Networks Unit42 - Threat Intel Research* May 2024 - August 2024
- Developed a proof-of-concept (PoC) using Llama3 and Mistral models to simulate Command and Control (C2) operations in ransomware attacks, demonstrating advanced AI-driven scenarios.
- Fine-tuned AI models and applied prompt engineering to simulate autonomous attacks, showcasing potential vulnerabilities and improving defense strategies.

Summer Associate - *Navy Federal Credit Union - Automation & Special Projects* May 2023 - August 2023
- Developed a tool to cluster text messages and extract actionable data insights, improving analysis speed and accuracy.
- Explored the application of large language models (LLMs) to accelerate incident resolution, optimizing incident management processes and improving resolution times.

Software Developer/Cybersecurity Specialist - *IBM CISO Innovation & Remediation* May 2021 - May 2023
- Designed and implemented PoCs to detect unknown threats and enhance internal network visibility.
- Developed tools for attack path detection and external connection analysis using the MITRE ATT&CK Framework, reducing manual analysis time by $\sim 15\%$.
- Built an NLP-powered IBM Cloud application to automate dynamic response generation, improving efficiency by $\sim 50\%$.

PUBLICATION AND RESEARCH WORK

Cybersecurity Research with Machine Learning Focus August 2020 – Present
- Conducted behavioral analysis of ransomware families (BlackMatter, Conti, LockBit, Midnight) using Windows Event Logs in an Active Directory environment.
  Published: ISDFS 2025 – *A Behavioral Analysis of Ransomware in Active Directory. Paper*
- Applied unsupervised clustering (HDBSCAN) and feature similarity techniques to uncover ransomware evolution patterns.
  Published: CAMLIS 2024 – *Ransomware Evolution: Unveiling Patterns Using HDBSCAN. [Paper])*
- Built similarity-based feature vectors using PE headers and API call analysis to detect malware behavior trends.
  Presented: MTEM 2023 – *Malware Trends Using Similarity Matrix.[Poster]*
- Utilized tensor decomposition to analyze antivirus scan data and mine latent malware pattern structures.
  Presented: MTEM 2022 – *Malware Antivirus Scan Pattern Mining via Tensor Decomposition.[Poster]*

Cybersecurity and AI August 2023 – Present
- Investigated generative AI influence on ransomware design and evolving threat models.
  Presented: CODEBOT 2025 – *AI-Driven Ransomware Tactics.[]Position Paper]*
- Reflected on the impact of AI tools on education, academic integrity, and the TA experience. []Position Paper]
  Presented: CODEBOT 2025 – *From Assistance to Dependence: A Graduate Teaching Assistant's Take on AI in Education.*

Cryptographic Protocol Shapes Analyzer (CPSA) August 2019 – August 2023
- Formally analyzed TLS 1.3 protocols using CPSA to identify structural vulnerabilities in cryptographic handshakes.
  Published: Searching for Selfie in TLS 1.3 with the Cryptographic Protocol Shapes Analyzer, Protocols, Strands, and Logic (Springer, 2022).[]Paper]