Sagnik Chakraborty

Email: sagnikchakraborty212@gmail.com **Address:** 74 Andrews Way, Piscataway, NJ, 08854 **Phone:** (813)-838-4648
Github: github.com/RedFlame2112 **Website:** https://quaternion-universe.vercel.app **LinkedIn:** sagnik-chakraborty-2112

EDUCATION

University of Illinois at Urbana-Champaign | Champaign, IL Expected: MAY 2027
M.C.S - Computer Science

University of Illinois at Urbana-Champaign | Champaign, IL Graduated MAY 2025
B.S. - Computer Engineering

Coursework: CS445 Computational Photography, CS412 Data Mining, CS225 Data Structures, CS374 Algorithms/Models of Computation, CS425 Distributed Systems, CS461 Computer Security, INFO 490 Digital Forensics, ECE498DN Trust in Critical Infrastructures, CS440 Artificial Intelligence, ECE391 Computer Systems Programming, ECE479 IoT and Cognitive Computing, CS483 Applied Parallel Programming, ECE313 Statistics, ECE310 Digital Signal Processing, CS407 Cryptography, CS415 Game Development, ECE 385 Digital Systems Laboratory

SKILLS & TECHNICAL TOOLS

Programming Languages: Golang, C/C++, Java, Rust, Python, Perl, SQL, Lua, Javascript, C#, Powershell, Ocaml
Technologies: Git, (Py)torch, TensorFlow, GreenGrass, Azure, GCP, AWS, Splunk, Snyk, Apache Spark, ESXi, Proxmox, Docker, Kubernetes, Terraform, neo4j, Unix, Linux, GDB, EMACS, Windows, x64dbg, Wireshark, tcpdump, Snort, IDA Pro, Ghidra, Radare2, Jadx, Cyberchef
Other Skills: AI/ML Design & Development, Operating Systems, Distributed Systems Architecture, Software Engineering, Object-oriented development, Data science, Data analytics, Data analysis, cybersecurity, mathematics, communication, teamwork, technical skills and knowledge

EXPERIENCE

Healthcare Product Consulting - Software Development/Architecture Intern | Cognizant Technology Solutions
Jun 2023 - Aug 2023

- Designed and unit tested data mapping workflows in C# converting healthcare claims (Facets DB) to HL7 FHIR standards, increasing data accuracy by 25%.
- Deployed secure, cost-efficient cloud infrastructure on Kubernetes & Docker; automated CI/CD with Azure DevOps, reducing deployment times
- Integrated Snyk for real-time vulnerability detection, safeguarding sensitive information of over thousands of users of FACETS
- Worked independently to identify pipeline bottlenecks and propose process improvements that improved time-to-market for finance-grade data systems.

Administrator and Infrastructure Developer| SIGPwny (ACM @ Illinois) *Jan 2021 - Current*

- Managed and optimized 4 ESXi platforms serving over 100 active users, reducing incident response time by 40% and ensuring high availability.
- Designed CTF badge PCB boards using MicroPython for FallCTF 2023 and 2024 for around 300 people, incorporating reverse engineering and debugging techniques.
- Configured and deployed CTF challenge infrastructure on Google Kubernetes Engine (GKE), with focus on network traffic analysis and security software deployment.
- Produced and scheduled weekly content, maintaining organization records and media for over 600 YouTube subscribers.

Cofounder of Purple Team | SIGPwny (ACM @ Illinois) *Aug 2024 - Current*

- Provisioned and secured OVH cloud infrastructure and Proxmox environments for purple team operations, including attack/defense exercises for ~30 people as part of the team
- Led initiatives in reverse engineering, penetration testing, and malware analysis during security assessments and CTF events.

CTF Lead| SIGPwny (ACM @ Illinois) *Jan 2024 - Current*

- Developed STARVE—an automated MITRE EMB3D-based embedded attack simulation and vulnerability testing platform, lowering manual testing by around 30% and contributing to our team's 5th-place finish at the 2025 MITRE eCTF.
- Led automated attack meetings for MITRE eCTF2025, enhancing team processes through structured reverse engineering and security assessment sessions.
- Secured 2nd place overall at MITRE eCTF2024 as a key member of the Embedded team, demonstrating advanced skills in penetration testing and embedded system security.
- Authored detailed design reports and implemented GitHub issue tracking to streamline project management and collaborative vulnerability testing efforts.

ACHIEVEMENTS AND CERTIFICATIONS

- Mitre eCTF 2nd place team in 2024 and 2023, 5th in 2025
- 6th Place Countrywide team on CTFtime (2022), 11th in 2023
- Top 15 team in Hivestorm 2024
- CSAW Quals 2024: 4th place

PROJECTS & Research

CS445 Final Project: Depth-aware Neural Style Transfer | *IPython, Pytorch* | RedFlame2112/CS445_FinalProject

- Developed a pipeline for extending Gatys-style neural style transfer (VGG19 + L-BFGS) with MiDaS v3 monocular depth estimation to apply depth-dependent stylization across foreground/midground/background via soft, Gaussian-feathered masks and normalized alpha blending.
- Implemented depth-aware compositing with tuned layer stylization strengths (30% foreground / 70% midground / 100% background) to preserve foreground detail while increasing abstraction in distant regions.
- Built an evaluation harness (SSIM, PSNR, LPIPS, pixel/VGG losses) over 100 content images × 5 styles (1,000 outputs), improving SSIM 0.225→0.409 (+0.184) and PSNR 10.51→13.62 dB (+3.11) while reducing LPIPS by 0.089 vs. baseline.
- Created an interactive GUI for manual depth-threshold refinement and mask autosave to handle depth-estimation failure cases.

GRADAR NIDS | *IPython, Pytorch/Keras, ApacheSpark* | RedFlame2112/GRADAR-NIDS

- Developed a Network Intrusion Detection System (NIDS) for IoT and cognitive computing, employing a hybrid LSTM/Convolutional Neural Network to classify potential cloud network attacks from PCAP data.
- Implemented rigorous data collection, network traffic analysis, and machine learning techniques to enhance malware analysis.

RainStorm | *Golang*

- Designed and implemented a stream processing framework analogous to Apache Spark, built on a hybrid distributed file system (HyDFS).
- Enabled robust data extraction, transformation, and aggregation functions to support real-time data mining and security assessments.

RESEARCH PROJECT – Automated Vulnerability Detection in Embedded Systems

- Conducted comprehensive research integrating both static and dynamic analysis techniques to detect vulnerabilities in embedded and IoT systems.
- Developed a novel framework that leverages reverse engineering, data mining, and machine learning to accurately classify security threats in network traffic.
- Executed extensive testing using real-world datasets, showcasing significant improvements in malware analysis, penetration testing, and security assessments.
- Contributed actionable insights for process improvement and enhanced global security protocols, supporting robust critical infrastructure protection.