BRANDON SINGH

New York, NY | 347-255-0892 | brandon@bbot.nyc | bbot.nyc | linkedin.com/in/brandon-s-4752b3181

EDUCATION

St. John's University New York, NY
M.S., Cyber and Information Security 2023 - 2025
GPA: 4.0 | NSA- and ABET-accredited program
Relevant Coursework: Network Security, Cryptography, Digital Forensics, Secure Software Engineering

St. John's University New York, NY
B.S., Computer Science - Concentration: Cyber Security Systems 2018 - 2022
GPA: 3.32 | Relevant Coursework: Algorithms, Systems Programming, Applied Security

EXPERIENCE

National Science Foundation I-Corps New York, NY
Entrepreneurial Lead *Apr 2024 - Nov 2024*
* Analyzed network security and architecture requirements for vehicular cloud computing across 100+ stakeholder interviews; progressed from Regional to National Cohort on technical depth
* Developed threat modeling and risk assessment methodology for decentralized edge environments, directly informing co-authored IEEE publication on distributed trust-based authentication

PROJECTS

AI Infrastructure Platform 2024 - Present
* Architected a self-hosted platform on a single server (i5-12400, RTX 3050, 64 GB RAM, 11 TB) running 38 containerized services - Nextcloud, Matrix, privacy-focused media frontends - with VLAN-based network segmentation, Caddy reverse proxy with TLS, and 6 public-facing domains
* Configured GPU passthrough for local LLM inference via Ollama; manage 4 VMs for IoT automation (Home Assistant), network simulation (GNS3), remote desktop, and dedicated AI agent workloads

Samsung Camera Reverse Engineering 2025 - Present
* Reverse engineered Samsung Galaxy S25 Camera2 APIs by decompiling Samsung Camera app and mapping vendor-specific device IDs, discovering undocumented Log gamma capture via private vendor tag (35,5,0)
* Built an Android Camera2 app with 10-bit BT.2020 video pipeline: hardware HEVC encoding via MediaCodec, MPEG-TS muxing, and SRT live-streaming through NDK native bridge

Autonomous AI Agent Platform 2024 - Present
* Deployed a persistent AI agent on a Linux VM with Telegram integration for autonomous web research, browser automation, code execution, and file management across multiple LLM backends (Ollama, Anthropic)
* Integrated Model Context Protocol (MCP) for tool orchestration with execution approval policies, scheduled automation, and multi-platform integrations including smart home and webhooks

PUBLICATION

Singh, B., Ghazizadeh, P., Choudhury, P., & Ebrahimi, A. (2024). Assessing Cooperative Trust-Based Authentication within Micro Vehicular Clouds. IEEE SmartNets 2024. | ieeexplore.ieee.org/document/10577698

TECHNICAL SKILLS

Security: Threat Modeling, Risk Assessment, Cryptography, Digital Forensics, Reverse Engineering, Vulnerability Analysis, Secure Network Architecture, Cloud and Edge Security
Infrastructure: Linux Administration (CLI), Docker, KVM/QEMU, GPU Passthrough, Caddy, Unraid, VLANs
AI & Agents: LLM Integration, MCP, Agent Orchestration, Ollama, Anthropic API, Tool-Use Design
Mobile/Android: Camera2 API, Kotlin, Jetpack Compose, MediaCodec, NDK, HEVC, SRT Protocol
Networking: TCP/IP, DNS, Edge Computing, Distributed Systems, Tailscale VPN
Tools: Git, Wireshark, GNS3, Home Assistant, PostgreSQL