ABHAY PRATAP SINGH (Software Development / Cybersecurity / AI-ML)

Scientist ‘B’ @C-DOT (DoT, GoI) | Research @YorkU | WhizHack | Microsoft CyberEngage’22 | IIT Jodhpur

Work Experience

Centre for Development of Telematics (DoT, GoI) – Scientist ‘B’ (Software Developer and Architect) *Jun’24 - Present*

National Scale Packet Processing Solution

- **Designed and developed** high-performance Data Plane Development Kit **(DPDK)** & Vector Packet Processor **(VPP)** based **packet processing application (C based)** in single-box solution sustaining **400 Gbps** Rx/Tx at ISP gateway edges for **national network security** enforcement reducing rack-space cost.
- **Implemented DPI (C based)** to surface **eSNI** within UDP flows by parsing Initial ClientHello and TLS extensions via **nDPI** and integrated a **two-phase stateful** pipeline (a fast-path stateless step, followed by a deep inspection stage), maintaining per-flow state to **correlate packets** and trigger actions with minimal latency.
- Engineered end-to-end **DPI strategy** and **architecture**, expanding application coverage by **200%** leading to PoC acceptance by an **Inter-ministerial** committee (GoI).
- **Optimized packet processing code** to leverage NIC offloads, pre-built packets, and batched Tx; achieving **10× throughput uplift** and **15× reduction** in CPU utilization.

Corporate Security & Threat Intelligence

- **Deployed** DNS Response Policy Zone **(DNS RPZ)** across corporate DNS infrastructure in Delhi & Bangalore, blocking **thousands** of requests to blacklisted domains and known/listed C&C servers improving **corporate security posture**.
- **Designed and developed** highly optimized, large-scale crawlers for **Telegram** and **Reddit** using **Playwright/Python** (**70% improvement** over previous solution) to gather multi-format data for **threat intelligence** on various Darknet marketplaces enhancing cyberspace awareness.

York University (Toronto, Canada) – MITACS Research Intern (AI-ML and Cybersecurity Researcher) *Jun’23 - Aug’23*

Automated Intelligence-Driven Malware Detection and Analysis

- Implemented ***Artificial Intelligence & Machine Learning techniques*** like **information-gain selection** and **three-layer Random Forest** architecture plus **weighted score fusion core** for multi-source behavioural analysis over network flows and memory dump features.
- **Developed** an automated **Python + QEMU testbed** where one Windows 10 VM per sample (8 vCPU/8 GB RAM) is “aged” for one week to defeat sandbox evasion, then 2000 malware samples are executed across 8 families, generating a **17TB database** of pcaps and memory dumps.
- **Performance**: L1 (network binary) macro **P/R/F1 ≈ 0.96/0.96/0.95**; L2 (network family) **macro F1 ≈ 0.98** with ~15% Unknown; L3 (memory family) macro **F1 ≈ 0.98**.

VolMemLyzer-V2

- **Designed and developed** a feature extractor tool - VolMemLyzer(V2) **(Python based)** with **250+** supported Memory Analytics Features (compared to <75 in V1) using **Volatility3** framework to provide in-depth memory forensics capabilities.
- **Implemented** modular pipeline which reduces processing duration of stored memory snapshots by **20–30%**, and producing CSVs for downstream **Machine Learning**.

WhizHack Technologies – Security Consultant (Cybersecurity Intern) *Nov’22 - Dec’22*

- Contributed to the **Operational Technology (OT)** security module by implementing **standards (RFC 5424/5425)** for their next-gen SIEM system, TRACE.
- Designed and deployed **3 customized honeypots** for increased efficacy using **CONPOT**, implemented within **containerized Docker environments**.

Microsoft Cybersecurity Engage 2022 – Mentee (Cybersecurity Intern) *May’22 - Jul’22*

- **Ranked 1st (All India)** on the program leaderboard based on performance in assignments and final project on defending **Critical Infrastructure** (chose **Delhi SLDC**, Electricity DISCOM Infrastructure) from Stuxnet-like cyber-attacks.
- Conducted **OSINT** and identified 10 most probable **attack vectors**, proposing a comprehensive Solution Architecture with 15 **security controls/policies** to minimize the attack surface and implement Defence-in-Depth/Zero Trust principles, alongside incident response and legal considerations.
- Presented 5 functional prototypes/PoCs, including **Machine Learning model** to detect botnet attacks, building **enumeration tools** from scratch, etc.

Technical Skills & MOOCs

Programming/Scripting	C/C++, Python, Bash, PowerShell, JAVA, MATLAB	**MOOCs**	• Introduction to Digital Forensics by Security Blue Team • Data & Tools for Defense Analysts by Splunk STEP • SOC Essentials: Investigating with Splunk by Splunk STEP
Cybersecurity Tools/Frameworks	Volatility, Metasploit, Wireshark, NMap, YARA, BurpSuite, Autopsy, Splunk, Chronicle, Suricata, OSINT, NIST CSF RMF		
Network Software Development	Data Plane Development Kit, Vector Packet Processor, nDPI, BGP, DNS RPZ, QUIC, TCP, DNS, ICMP, OSI Model	**CI/CD Tools**	Docker, Docker Swarm, Github Workflows, QEMU, VMware Tools integration, Kubernetes, Playwright

Education & Certification

Degree	Institute	Grade	Remarks	Year
B. Tech. (CSE)	**Indian Institute of Technology, Jodhpur**	7.88/10.0	Institute Silver Medal	2020-2024
AISSCE (Class XII)	**Army Public School, Birpur**	93.80%	Top 0.1% nationally	2018-2019
AISSE (Class X)	**Army Public School, Birpur**	10.0/10.0	School Topper	2016-2017

Certifications	Issuing Body	Year
Certified Ethical Hacker v13 (Training Completion Certificate)	EC Council	2025*
CompTIA Security+ (SY0-701)	CompTIA	2025
Certified in Cybersecurity	ISC2	2024
Google Professional Cybersecurity Certificate	Google	2023

*Employer Sponsored (Exam Pending)

Publications

Unveiling Evasive Malware Behavior: Towards Generating a Multi-Sources Benchmark Dataset and Evasive Malware Behavior Profiling Using Network Traffic and Memory Analysis | The Journal of Supercomputing (Springer)

Achievements

- Received **Student Distinguished Services Award** and **Institute Silver Medal** for my contributions to Student Senate IITJ in AY 2022-23.
- **Contingent Leader** of 150 IIT-J students in the 55th INTER IIT SPORTS MEET 2022; personally led Runner-Up awardee **Best Marching Contingent** at IIT Delhi.
- Achieved **All India Rank 1** in Microsoft Cybersecurity Engage 2022.
- **State Rank 3** (Uttarakhand) in NSTSE-2019 conducted by Unified Council.

Position of Responsibilities/Recognition

C-DOT	• Led the core **DPI track** (3 members including interns) of National Scale Packet Processing Solution. • **Highest KRA** points of all **<3 YoE** team members in National Scale Packet Processing Solution Team.
IIT Jodhpur	• **Vice-President of Board of Student Sports** (Highest student position in sporting fraternity of IITJ); headed investments and events worth **2.1 Cr (INR)** successfully with 95% budget utilization expanding from just 9 to 15 societies/clubs, which **tripled** student engagement. • Spearheaded successful events like **VARCHAS** (Inter-College), **KRIDANSH** (Inter-Hostel), etc; leading 100s of students hierarchically. • Bagged **4th position** out of 23 IITs; leading a team of 4 members in INTER IIT TECH MEET 12.0 in Cybersecurity PS at IIT Madras. • Google Developer Student Clubs (GDSC) Cybersecurity Coordinator; conducted training sessions, research review, etc.

Phone : +91-9560949946 | **Email** : sengar.abhayps@gmail.com | **Github** : Abhay-Sengar | **LinkedIn** : abhay-pratap-singh-sengar