(412) 499-4176
ymalhi@andrew.cmu.edu

Yuvraj Singh Malhi

github.com/yuvraj-malhi
linkedin.com/in/yuvraj-malhi

EDUCATION

M.S. in Information Security	**Carnegie Mellon University**	**Aug 2022 – Dec 2023**

- *Coursework:* 15-513 (Introduction to Computer Systems), 14-741 (Introduction to Information Security), 14-761 (Applied Information Assurance), 14-829 (Mobile and IoT Security).

B.E. in Electronics & Instr.	**BITS Pilani**	**Aug 2018 – May 2022**

- *Coursework:* Network programming, Data Structures & Algorithms, Credited Security Research.
- *Co-curricular:* Hockey Team (Left Half), Punjab Cultural Association (Bhangra Team), Volunteer Teacher.

SKILLS AND TECHNOLOGIES

- *Languages:* **Proficient –** C, C++, Python, MATLAB, LaTeX. **Basics –** HTML, Assembly language.
- *Tools:* Metasploit, WireShark, Tensorflow, Scikit-Learn Git, GitHub, VScode, Jupyter.

TECHNICAL EXPERIENCE

Network and Systems Intern	**Samsung R&D Bangalore**	**July 2021 – Jan 2022**

System Automation and ML Log Analysis
- Worked on **ML-based log analysis** for **system fault detection** and post-mortem **root cause analysis**.
- Designed an **anomaly detection** system to monitor system background information and take pre-emptive action before hard failure. **Saved service teams 20 hrs/week** and completed implementation in stipulated 2 months deadline.

Project Assistant	**BITS Pilani**	**Jan 2021 – July 2021**

Intrusion Detection Systems for IoT using ML (Link to Paper)
- Designed and implemented **network IDS for IoT** to overcome few design flaws of existing IDS. This design can detect 22 types of attacks with help of 3 ML based modules using **Random Forest, ANN, Decision Tree, and XGBoost**.
- Central Module used for attack detection & classification with F1 Score **94.41%**. One among two edge modules used for only attack detection at IoT edge with F1 scores of **99.98%** and **99.87%**.

Project Assistant	**BITS Pilani**	**Jan 2021 – May 2021**

Mitigating DoS/DDoS attacks in SDN Data Planes
- Surveyed and analyzed methods used to **detect and mitigate** Denial-of-Service (**DoS**) and Distributed Denial-of-Service (**DDoS**) attacks at **Data Plane** level in Software Defined Networks (SDN) using P4 language.
- Identified **limitations of P4** for attack detection and mitigation such as: No support for loops and for complex functions, and minimal support for mathematical analysis.

Cybersecurity Research Intern	**IIT Kanpur, c3i Division**	**May 2021 – June 2021**

Intrusion Detection of Encrypted Traffic
- Among **top 5** students from India selected to be a part of the **Intrusion Detection Team** of IIT's cybersecurity division.
- Surveyed and categorized **non-encrypted/encrypted traffic analysis** solutions based on application and mechanism.

PROJECTS

Ultra-fast URL Port Scanner   **Link to Project**
- Scans URL open ports up to **10X faster** than traditional scanners by using up to 100 of child scanners **concurrently**.
- The scanner also **lists all IPv4 and IPv6 addresses** allotted to each URL.

Concurrent TFTP Servers   **Link to Projects**
- Created a TFTP single process server to handle multiple clients using **listen** call on multiple FDs. Speed: **~25 Mbps**.
- Created a TFTP **multi process server** to handle clients by spawning a child server for each client. Speed: **~50 Mbps**.

Ultra Fast Trace-route   **Link to Project**
- A concurrent traceroute server for multiple domains to give results within **3 sec – 10X faster** than standard traceroute.
- A TCP client runs on a separate window to find **longest common routing path** among a given set of domains.