Yashaswi Malla - Curriculum Vitae

Email: yashaswi.malla@nyu.edu
Website: https://yashaswiim.github.io/

EDUCATION

2019 - 2023 **Bachelor of Science**, Computer Science, New York University Abu Dhabi, UAE
Minor: Applied Mathematics, Interactive Media
Honors: cum laude, GPA: 3.933
Capstone Advisor: Dr. Christina Pöpper
Title: Bypassing Secure VPN Tunnels through Local IP Camouflage

2017 - 2019 **IB Diploma Programme**, Ullens School, Nepal
Score: 43

RESEARCH EXPERIENCE

Oct 2025 – Present **Research Assistant**, Haven Lab, New York University Abu Dhabi, UAE

- Investigating security and privacy issues in LLM-based agentic systems
- Developing defense mechanisms to secure LLM agents against sophisticated attack vectors

May 2023 – Jul 2023 **Post-graduate Research Assistant**, Cyber Security and Privacy Lab, New York University Abu Dhabi, UAE

- Investigated the evolution of media coverage of privacy-related issues over 10 years across regions
- Analyzed the emotions and tones conveyed in 100K articles using IBM's Watson Tone Analyzer
- Worked on integration of LLMs into the pipeline for article classification to extend the scope of the research

Feb 2022 – May 2023 **Student Researcher**, Cyber Security and Privacy Lab, New York University Abu Dhabi, UAE

- Worked on finding how vulnerabilities in VPN applications can be actively exploited by adversaries
- Developed a novel attack that cause VPN clients to leak traffic outside the protected VPN tunnel
- Conducted 195 experiments against 66 of the most representative VPN providers on multiple OS
- Revealed vulnerability in 64.6% providers and researched countermeasures to mitigate the vulnerability

Oct 2022 – May 2023

Student Researcher for Automation, Genetic Heritage Group, New York University Abu Dhabi, UAE

- Developed automated workflow on HPC for bioinformatics analyses using Bash and Python scripts
- Integrated 12 metagenomics analysis tools like kraken, metawrap, fastANI into the automated pipeline

PROFESSIONAL EXPERIENCE

Sep 2023 – Jul 2025

Lead AI Engineer, Cypherleak Limited, UAE

- Oversaw end-to-end development lifecycle of AI projects, from ideation to deployment
- Conducted R&D for integrating AI to introduce new features in the company's cyber risk scoring platform
- Worked on designing and maintaining custom LLM-based agentic systems, ensuring seamless integration into existing system
- Implemented cost-effective algorithms in LLM engineering, resulting in at least 25% reduction in LLM inference costs

TEACHING EXPERIENCE

Sep 2021 – Dec 2021

Teaching Assistant, Computer Science, New York University, US

- Supported the primary instructor of the course CSCI-UA.0202: Operating Systems (Undergrad)
- Evaluated and provided constructive feedback on students' academic performance through grading of homework, lab assignments, and examination papers
- Facilitated student comprehension of fundamental course concepts by conducting weekly office hours, offering personalized guidance
- Fostered an engaging learning environment by addressing students' queries and providing additional explanations during one-on-one consultations

LEADERSHIP & OUTREACH

Mar 2022 – Dec 2022

Vice President, Nepali Student Association, New York University Abu Dhabi, UAE

- Involved in event planning and organization for and about the Nepali community at NYUAD

Aug 2020 – Aug 2021	**Initiative Leader, ADvocacy Student Interest Group**, New York University Abu Dhabi, UAE • Initiated a pilot program STRIVE (STRength in Vocational Education) with UNHCR and NYUAD Community Outreach and lead a team of 19 NYUAD student volunteers • Organized sessions for People of Concern spread across the UAE to improve their conversational English skills

PUBLICATIONS

2023	*Nian Xue, Yashaswi Malla, Zihang Xia, Christina Pöpper, and Mathy Vanhoef. Bypassing Tunnels: Leaking VPN Client Traffic by Abusing Routing Tables. In 32nd USENIX Security Symposium (USENIX Security 23)*

HONOR & AWARDS

2025	AI-Powered Security Pioneer *awarded by UAE Cybersecurity Council to Cypherleak*
2023	NYU Honors Scholar (Founders' Day) *awarded to top 40% of graduating class*

RESEARCH INTERESTS

Security and privacy issues in AI-based agentic systems, AI security, Role of AI in cybersecurity, Cyber forensics, Software and systems security, Network security, Web security

RELEVANT COURSEWORK

Computer Security, Network Security, Security and Human Behavior, Operating Systems, Computer Networks, Object-Oriented Programming, Algorithms, Multivariable Calculus, Linear Algebra, Probability and Statistics, Ordinary Differential Equations

SKILLS

Coding	Python, C/C++, Java, JavaScript, Bash, SQL
Software	Microsoft Office, Google Suite, Arduino, Processing, Figma, Wireshark, GDB, Ghidra
Language	Nepali (first language), English (fluent), Hindi (spoken), French (intermediate)