

YASHASWI MALLA

Saadiyat Island, Abu Dhabi, UAE • 971-505302514 • yashaswi.malla@nyu.edu

EDUCATION

New York University Abu Dhabi

Abu Dhabi, UAE

B.S. in Computer Science

May 2023

Minors: *Applied Mathematics, Interactive Media*

Honors: cum laude (GPA 3.933)

Capstone Advisor: Christina Pöpper

RESEARCH INTERESTS

Security and privacy issues in LLM-based agentic systems, LLM safety, Application of LLMs for cybersecurity

RESEARCH EXPERIENCE

New York University Abu Dhabi

Abu Dhabi, UAE

Research Assistant, Haven Lab

October 2025 – Present

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

Post-graduate Research Assistant, Cyber Security and Privacy Lab

May 2023 – July 2023

- 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

Student Researcher, Cyber Security and Privacy Lab

Feb. 2022 – May 2023

- 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

Student Researcher for Automation, Genetic Heritage Group

Oct. 2022 – May 2023

- 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
- Increased the speed of metagenomics data analysis by 60%

TEACHING EXPERIENCE

New York University

New York, US

Teaching Assistant, Computer Science

Sep. 2021 – Dec. 2021

- 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

PUBLICATIONS

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).

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

HONORS & AWARDS

AI-Powered Security Pioneer (awarded by UAE Cybersecurity Council to Cypherleak)

2025

Founders Day Award

2023

LEADERSHIP & OUTREACH

New York University Abu Dhabi

Abu Dhabi, UAE

Vice President, Nepali Student Association

Mar. 2022 – Dec. 2022

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

Initiative Leader, ADvocacy Student Interest Group

Aug. 2020 – Aug. 2021

- 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.

PROFESSIONAL EXPERIENCE

Cypherleak Limited

Abu Dhabi, UAE

AI and LLM Engineering Lead

Sep. 2023 – July 2025

- 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

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)

REFERENCES

Sandra Siby

New York University Abu Dhabi
 Assistant Professor of Computer Engineering
 Haven Lab
 Email: sandra.siby@nyu.edu

Christina Pöpper

New York University Abu Dhabi
 Program Head of Computer Science
 Cyber Security & Privacy Lab (CSP-lab)
 Email: christina.poepper@nyu.edu

Aashish Jha

New York University Abu Dhabi
 Assistant Professor of Biology
 Email: jhaar@nyu.edu