ASHIM MAHARA

45 Hazel St, UP, Rochester, NY 14623
Ph no: 785-258-3288; Email: mr.maharaofficial@outlook.com, am7539@g.rit.edu

Education

Master of Science in **Computing Security**, Rochester Institute of Technology, Rochester, New York, USA;
June ’25 (expected graduation)

- Developing Cyber Security Intrusion Training Exercises for CEOs and Army Veterans funded by an NSF grant under Prof. Justin Pelletier
- Researching Applications of Large Language Models in Cyber Threat Intelligence at AI4SEC group under Prof. Nidhi Rastogi
- Participated in IRSEC ’23 and CCDC Tryouts ’23, Active Member of RIT Security Club (RITSEC)
- Published Poster in NDSS ’24 titled MORPH: Concept Drift Adaptation for Malware Detection
  - Won the highly competitive fully-funded Student Travel Grant (~$2000) for attending NDSS
  - Won the Best Poster Presentation Award

WORK EXPERIENCE

Cyber Range Jr Engineer, **Rochester Institute of Technology** ***Sept ’23 – May ‘24***

- Defined intended paths of exploitation for the environment by proposing and introducing vulnerabilities
- Configured a SMB server with insecure permissions (Anonymous Login) containing a zip with a rock-you password for Initial Access
- Utilized Terraform to provision 20+ Windows Machines for the Active Directory
- Installed and Configured a Graylog server for Log Aggregation and Visualization
- Configured a logging pipeline in Graylog for the Log Collection from machines using Ansible
- Created two CTF Webpages using React.js and hosted it using IIS Server
- Wrote 200+ lines of firewall rules for strict network segmentation to simulate realistic restrictions
- Configured RustDesk and Windows Remote Desktop for Remote Access for Analysts and Attackers
- Created Dashboards for Monitoring Active Directory logs

Consultant Data Engineer, **Shiva Technology, Kathmandu** ***Jun ’22 – Oct ‘22***

- Developed a NodeJS program to build threat intelligence data for the onion network from Tor consensus files with 26k IP addresses saved to date
- Built a scraper to collect data from the top 100k web pages using NodeJS and Puppeteer.
- Designed SQL database tables and relationships to accommodate millions of rows of data.
- Developed API to handle dozens of requests per second on a low-resource system.
- Set up the development environment for machine learning development operations using DVC, Minio, and Gitea.

Data Scientist, **Vairav Technology, Kathmandu** ***Jan’19 – Dec’21***

- Developed Machine Learning Models for the detection of exfiltration techniques abusing DNS protocol.
- Led a team of 13 developers in adopting an agile methodology for the development of the SIEM product.
- Mentored a team of 10 interns for a period of three months
- Built backend server and client software in Golang creating and serving thousands of requests/minute
- Implemented Apache Kafka for data queueing and ingestion of ~100+ GB of logs every day.
- Provided ad-hoc digital forensic services uncovering intrusion, such as remote access from the local network

Security Engineer, **Rigo Technologies, Kathmandu** ***Nov’17 – Dec’18***

- Designed High-Level Architecture for SIEM Products
- Integrated Systems into OSQuery Fleet for network-wide querying of host operating systems (100 + Systems, both Windows and Linux)
- Wrote custom Logstash pipelines for telemetry sources such as OSSEC/Wazuh and Windows Event logs
- Integrated MITRE ATT&CK Enrichment for Windows logs from Sysmon
- Applied Configuration updates to 20+ Windows Servers according to CIS benchmark

ACADEMIC PROJECTS

Title: MORPH: Towards Automated Concept Drift Adaptation for Malware Detection
Duration: Jan-Feb'24
Brief Description: This was a paper that I co-authored with a PhD student and another Masters student. In the paper, we used Self Supervised Learning and Active Learning to incrementally improve malware detection models over time. The paper primarily addressed the concept drift that occured in Android and Windows malware datasets.

Title: Covert Communications using Reserved Bits in TCP Headers
Duration: Oct-Dec'23
Brief Description: This was a group project for our course CSEC 750 Covert Communications at RIT. We developed a two-way communication channel using Reserved Bits in TCP Headers then implemented a Man-In-The-Middle proxy using Scapy on both ends to piggyback normal traffic for covert communications.

Title: Detection of Malware Beaconing in DNS Logs Using Deep Learning
Duration: Mar- Aug'21
Brief Description: This was a master's dissertation submitted in the final year of the course. It was aimed at detecting malware beaconing activity through DNS logs. Convolutional Neural Networks were used to achieve periodicity detection while a Transformer model was used for DGA detection.

Title: Feature Selection for Network Logs
Duration: Nov'18- Jan'19
Brief Description: A coursework project which filtered the most important features in an intrusion detection evaluation dataset, CIC-IDS 2017, it was aimed at the selection of core features providing max input while training a machine learning model. Thus the main features involved paring the initial 81 features to the most crucial 13.

RESEARCH PROJECTS

Title: Applications of Large Language Models in Threat Intelligence
Duration: Sept'23-Ongoing
Lab: AI4SEC at RIT
Brief Description: We are researching tasks that can be augmented by LLMs in the Threat Intelligence space.

Title: Computer Network Modeling
Duration: Mar- Dec'21
Brief Description: This was a self-supervised learning project with graph neural networks. It aimed to facilitate the generation of similar embeddings for similar devices via a graph neural network as the primary feature extractor for detection use cases.

Title: Detection with Fourier Transforms and Power Spectral Density Method
Duration: Sep'20- Feb'21
Brief Description: A research and development project, it targeted implementing algorithms that could find periodic activities in provided data. Its main aim was to find periodicities of different frequencies by performing windowing and applying FFTs on those windows to find the dominant frequency and their relative frequency strength.

Title: Algorithmically Generated Domains
Duration: Jul'20- Aug'20
Brief Description: This used Bi-Directional LSTMs to classify domains, leveraging an existing DGA domain dataset to build the deep learning classifier.

Title: Data Exfiltration by DNS Tunneling
Duration: Jan'20- Jun'20
Brief Description: This R&D project collected data by performing data exfiltration with DNS Tunneling and built a custom ML model using TensorFlow to detect it. It was able to detect DNS Tunneling in a computer network with high accuracy (>92%).

TECHNICAL SKILLS

- **Machine Learning**: PyTorch, Numpy, Pandas, TensorFlow, HuggingFace Transformers, Sklearn
- **Digital Forensics / Incident Response**: Microsoft Sysinternals, Microsoft Event Viewer
- **Network / Log Monitoring:** Wazuh, Kibana, Rsyslog, Sysmon, Suricata, Wireshark
- **Browser Automation:** Selenium, Puppeteer
- **Web Technologies:** Javascript, HTML, CSS
- **Database:** PostgreSQL, MariaDB, Elasticsearch
- **Cloud Technologies:** Terraform, Ansible, Docker
- **Programming Languages:** Python, Javascript, Golang, Bash, Powershell
- **Peneteration Testing:** NetExec/CrackMapExec, Netmap, BurpSuite, Metasploit, Google

CERTIFICATIONS

- Data Engineer - Datacamp through Data Fellowship, ’22
- Deep Learning Specialization - Coursera, ’20
- DeepLearning.AI TensorFlow Developer Specialization - Coursera, ’20
- Natural Language Processing Specialization - Coursera, ’20
- Micro degree in Deep Learning - FuseMachines, ’20
- Scrum Master - Scrum Alliance, ’19

AWARDS AND ACHIEVEMENTS

- Won the Best Poster Presentation Award at NDSS ’24 at San Diego
- Was awarded with NDSS Student Travel Grant (~$2000) for attending NDSS ’24 at San Diego
- Was selected from a pool of 100 applicants in ’21, for studying data science by Code for Nepal, a community of technological volunteers working to alleviate Nepal’s civic problems digitally
- Participated in Security Bootcamp conducted by Ing Skills Academy for 30+ prospective cybersecurity students, at Islington College ’18
- Was awarded a final year scholarship by Islington College with 50% tuition remission for scoring all As, ’17
- Founded a student empowerment club Change with Us that had 14 members at Islington College, ’16

WORKSHOPS, PRESENTATIONS, SEMINARS AND CONFERENCES

- Program Committee for Workshop On Security Operations and Construction (WOSOC) ’24 that was co-located with NDSS ’24
- Attended 5-day security conference called Network and Distributed Systems Symposium (NDSS) ’24 at San Diego, California, USA
- Attended a 2-day security conference called ThreatCon ’22 organized by ThreatNix held at Kathmandu, Nepal
- Attended a 3-day long ‘Cyber Warfare and Security Workshop’ conducted by the First Ranger Battalion, Nepal Army held at Ranger Battalion Barracks, Chauni, Kathmandu in April’19
- Attended a 1-day Security Workshop from David Venable organized by the US Embassy in ’18 held at iHub, Teku, Kathmandu, Nepal

LANGUAGES KNOWN:

- **English:** IELTS 8.0 Academic.
- **Nepali:** Mother Tongue.
- **Hindi:** Can understand and converse orally.

COMMUNITY SERVICE

- Volunteered at RIT during Collegiate Penetration Testing Competition, ’24