Mati Ur Rehman

Phone: [+14342576136] — Email: [mati@virginia.edu]
LinkedIn: https://www.linkedin.com/in/mati-ur-rehman-02949a157

Professional Summary:

Applied researcher with strong expertise in machine learning, privacy, and cybersecurity. Extensive industry experience in developing advanced anomaly detection systems leveraging Graph ML, federated learning, and large language models. My work has been published in top-tier security conferences, including IEEE Security & Privacy.

Education

University of Virginia - MS Computer Science - GPA: 4.00 — Charlottesville, Virginia | January 2023 - May 2025
  Selected Coursework: LLMs Fairness & Security, NLP, Network Security

Lahore University of Management Sciences - BS Computer Science- GPA: 3.80 — Lahore, Pakistan | September 2018 - May 2022

Experience

Corvic Inc - Graph ML Intern — Mountain View, California | June 2024 - Present
- Implemented an unsupervised GNN encoder for the Corvic embedding engine.
- Designed a specialized temporal graph network model for trend forecasting using time-series graph data.

University of Virginia- Research Assistant - Machine Learning & Security — Charlottesville, Virginia | January 2023 - Present
- Research focused on developing host intrusion detection systems for detecting cyber threats using Machine learning technologies including **Federated Learning**, **Graph Neural Networks** and **Large Language Models (LLMs)**.

Katana Graph Inc - Machine Learning Engineer — Austin, Texas | June 2022 - December 2022
- Developed an **anomaly** based **IDS** leveraging Graph Representaion Learning
- Solution adopted by tech companies including Microsoft and Cisco
- Research paper published at **IEEE Security & Privacy 2024**

Publications

1. Rehman, M. U., Ahmadi, H., & Hassan, W. U. (2024, February). FLASH: A Comprehensive Approach to Intrusion Detection via Provenance Graph Representation Learning. In 2024 IEEE Symposium on Security and Privacy (SP) (pp. 139-139). IEEE Computer Society.
2. Rehman, M. U., & Hassan, W. U. (2024). TRUSTWATCH: A privacy-aware approach to system intrusion detection. In submission.
3. Liu, Q., Shoaib, M., Rehman, M. U., Bao, K., Hagenmeyer, V., & Hassan, W. U. (2024). Accurate and Scalable Detection and Investigation of Cyber Persistence Threats. arXiv preprint arXiv:2407.18832.
4. Gui, J., Nie, M., Guo, J., Zou, F., Rehman, M. U., & Hassan, W. U. (2024). A principled approach for detecting APTs in massive networks via multi-stage causal analytics. In submission.

Projects

Privacy Preserving Anomaly Detection System *(Python, Pytorch, Gensim, Matlab)*
- Integrated federated learning with graph representation learning to detect malicious processes in user machines
- Introduced an advanced encryption scheme and ensemble framework to solve Non-IID data problem, optimizing for heterogeneous system logs data

Distributed End Point Audit Logs Collection Tool *(C++, Javascript, Zeek Scripting)*
- Developed a Linux-based tool for distributed endpoint log collection. Worked on a complex C++ codebase designed to collect Linux Auditd logs from individual machines and transmit them to a central server

Technical Skills

- Machine Learning Expertise: Graph Representation Learning, Large Language Models, Natural Language Processing
- Programming Languages: Python, C/C++, HTML, CSS, JavaScript, SQL
- Frameworks: LangChain, Streamlit, React, Node.js, Flask, PyTorch, torch-geometric, Keras

Volunteer Work

- Helped organize the DMV security Workshop 2024
- External paper reviewer for IEEE Security & Privacy and Network Distributed System Security conferences
- Teaching Assistant for undergraduate courses (Network Security, Advanced Programming, Operating Systems)