Alireza Bahramali

abahramali@cs.umass.edu
4132308939

LinkedIn
Google Scholar

Education

University of Massachusetts Amherst — Amherst, MA
PhD, Computer Science, GPA: 3.93 — Sep 2017 – Dec 2022 (Expected)

University of Massachusetts Amherst — Amherst, MA
Master of Science, Computer Science, GPA: 3.94 — Sep 2017 – Sep 2020

University of Tehran — Tehran, Iran
Bachelor of Science, Electrical Engineering, GPA: 3.68 — Sep 2012 – Jun 2017

Interests

Machine Learning in Security & Privacy, Natural Language Processing in Healthcare

Publications

Robust Adversarial Attacks Against DNN-Based Wireless Communication Systems
Bahramali A., Nasr M., Houmansadr A., Goeckel D., Towesly D.
The ACM Conference on Computer and Communications Security, 2021

Defeating Deep Neural Network (DNN)-Based Traffic Analysis Systems in Real-Time With Blind Adversarial Perturbations
Nasr M., Bahramali A., Houmansadr A.
The USENIX Security Symposium, 2021

Practical Traffic Analysis Attacks on Secure Messaging Applications
Bahramali A., Soltani R., Houmansadr A., Goeckel D., Towesly D.
The Network and Distributed System Security Symposium, 2020

DeepCorr: Strong Flow Correlation Attacks on Tor Using Deep Learning
Nasr M., Bahramali A., Houmansadr A.
The ACM Conference on Computer and Communications Security, 2018

Experience

Graduate Research Assistant — Sep 2017 – Present
The SPIN Research Group, UMass Amherst — Amherst, MA

- Implemented a framework to perform traffic analysis on Tor connections using **Deep Learning (DL)**, **Python**, and **PyTorch**. Improved the state-of-the-art by **92%**.
- Designed **Universal Adversarial Examples** to preserve privacy against traffic analysis attacks using **Python** and **PyTorch**. Reduced the accuracy of such attacks by **90%** by only adding **10%** bandwidth overhead.
- Implemented limited-data network traffic analysis attacks using **Semi-Supervised** and **Self-Supervised** machine learning techniques and **Diffusion Probabilistic Models**.

Machine Learning Engineer Intern — Jun 2022 – Aug 2022
Truevta – AI/ML Team — Seattle, WA

- Designed a knowledge graph for clinical notes and ontologies using T5 sequence-to-sequence transformer.
- Improved the state-of-the-art in clinical ontology mapping task by 2% using back-translation.
- Reduced the fine-tuning inference time for clinical notes entity detection task by a **factor of 10**.

Data Science Intern Jun 2021 – Aug 2021
Faire – Search and Recommendation Team San Francisco, CA

- Implemented a recommender system using XGBoost binary classifier to recommend products from the same brand.
- **Improved** the impression_to_click_rate of the recommender system by **12%**.
- Performed user analytic and data model reviews for different parts of the Faire website.

Technical Skills

Programming Languages: Python, PyTorch, SQL, C/C++, TensorFlow.
Developer Tools: GitHub, scikit-learn, Keras, Hugging Face, pandas DataFrame, CUDA, Linux, Git, REST API, Docker, Selenium, Tor, Jupyter Notebooks.
Expertise: Data Structures, Deep Learning, Machine Learning, Natural Language Processing, Self-Supervised Learning, Semi-Supervised Learning, Diffusion Probabilistic Models, Generative Adversarial Networks (GAN), Adversarial Examples, Contrastive Learning, Security and Privacy.

Projects

Social Network | *C++, Object Oriented Programming, QT*

- Developed a social network similar to LinkedIn using C++ and Qt as the user interface.

Packet Scheduling | *C++, Object Oriented Programming, Graph Theory*

- Implemented and compared packet scheduling algorithms in network switches using C++ and graph theory.

English Premier League Prediction | *Python, PyTorch*

- Designed a DL classifier to predict English Premier League soccer matches using PyTorch.

Top-K Insights From Multi-Dimensional Data | *Python, pandas, MySQL*

- Automated the process of extracting useful insights from multi-dimensional data.

Messaging Application Bots | *Python, REST API, Selenium, Docker*

- Automated message sending and receiving in Telegram, Signal, and Wickr using Python and REST API.

Relevent Courses

Machine Learning, Deep Learning, Database & Design Implementation, Pattern Recognition, Advanced Algorithms, Advanced Computer Netowrks, Advanced Information Assurance

Honours

Ranked 70th among 260000 participants in Iran's National Universities Entrance Exam (Konkur), 2012.