# MEHRGAN KHOSHPASAND FOUMANI

83 Biggs St., Fredericton, NB
(506)471-2778 ⋄ me.khoshpasand@gmail.com

## HIGHLIGHTS OF QUALIFICATIONS

- Enthusiastic Machine Learning Researcher with more than **6 years** of programming experience.
- **+2** years of industrial experience as a **Machine Learning Researcher** and **Software Engineer**.
- Strong programming skills in **Python**, **Java**, **C/C++**, **and Web Development**.
- Strong knowledge in **Data structure** and **Algorithms**.
- Highly experienced in applying Deep Learning to the **Computer Vision**, **NLP**, and **Time Series** problems.
- In-depth knowledge of **Security** and **Privacy**.

## EDUCATION

**University of New Brunswick** Fredericton, NB, Canada September 2018 - Present
**Master of Computer Science** CGPA: 4.3/4.3
**Supervisor: Dr. Ali Ghorbani**, Canada Research Chair in Cybersecurity & Director of the CIC
Thesis: **On the Evaluation of Adversarial Vulnerabilities in Deep Neural Networks.**
Awarded New Brunswick Innovation Foundation graduate Scholarships two times in a row.
Description: Developed a library that contains Pytorch implementation of common adversarial attacks. Performed an comprehensive analysis on multiple recently proposed adversarial defenses. Proposed an unrestricted adversarial attack based on generative adversarial networks that bypasses multiple state-of-the-art defenses.

**University of New Brunswick** Fredericton, NB, Canada September 2015 - August 2018
**First-class Honours Bachelor of Computer Science** CGPA: 4.0/4.3
Thesis: **Smart-Phone Based Human Fall Detection Using Recurrent Neural Networks**.
Dean's list 2015, 2016, 2017, and 2018.
Won NSERC Undergraduate Student Research Award (USRA)-2016.
Awarded N. Myles Brown Undergraduate Scholarship and Edwin Jacob Special University Scholarship.
1st place, UNB Programming Competition-March 2018.

## PROFESSIONAL EXPERIENCE

**University of New Brunswick** September 2018 - Present
*Research Assistant*

- **Project: "Fake News Detection"**: Conducted research and development on machine learning and data mining techniques for Fake News detection project.
- **Project:"Anomaly detection on streaming data"**: Developed machine learning-based solutions for anomaly detection on streaming data.

**Canadian Institute for Cybersecurity** May 2017 - September 2017
*Research Assistant*

- **Project: "Machine learning-based Android malware detection"**: Studying the behaviour of Android malware families. Finding the necessary triggers for each malware family and writing a script that activates the malware on real phones. Gathering malware samples from various sources. Writing a script that generates a dataset containing Android malware behaviours. Applying Machine Learning techniques to detect Android malware and to classify malware based on their categories.

**Fitpath** September 2016 - January 2017
*Software Developer*

- Developed a chat-bot that automates the communication between fitness coaches and their clients. Additionally, developed a web app that helps fitness coaches to manage their client's progress.

## PROJECTS

**Smart-Phone Based Human Fall Detection Using Recurrent Neural Networks**
Built a cloud based framework that predicts human falls using smart-phone's sensors. Trained A deep learning model to predict falls up to 0.5 second before happening.

**A Survey on Deep Reinforcement Learning**
Conducted research about deep reinforcement learning; covering the recent algorithms and techniques.

**A Benchmark to Evaluate the performance of Big Spatial Data Frameworks**
Developed a benchmark to compare big data solutions for spatial data based on Spark. Performed experiments on GeoSpark, Magellan, SpatialSpark and Postgresql using 10 spatial join operations over several datasets.

**Python Implementation of Machine Learning Techniques**: Vanilla Python implementation of KNN, Naive Bayes, ID3, Adaboost, Random Forest.

**Python Implementation of Encryption Techniques**: Vanilla Python implementation of BGN, Elgamal, Paillier.

## PUBLICATIONS

1. Mehrgan Khoshpasand and Ali Ghorbani. On the generation of unrestricted adversarial examples. *The DSN Workshop on Dependable and Secure Machine Learning (DSML)*, 06 2020
2. Mehrgan Khoshpasand, Ali Ghorbani, Samaneh Mahdavifar, and Hessam Mohammadian. Deep learning in adversarial settings. *Book chapter submitted for publication.*, 2020
3. Mehrgan Khoshpasand and Alireza Manashty. Smart-phone based human fall detection using recurrent neural networks. *26th Annual Graduate Research Conference, UNB*, 2019

## TECHNICAL STRENGTHS

| | |
|---|---|
| **Languages** | Python (certified, advanced), Java (advanced), C (intermediate), and JS (intermediate) |
| **ML Frameworks** | Pytorch, TensorFlow, Fastai, Scikit-learn, Pandas, and Numpy |
| **Version Control** | Git |