Hesamodin Mohammadian

Ph.D. Candidate, Computer Science, University of New Brunswick,
h.mohammadian@unb.ca
+1 506 230 6994

Summary

I am currently a Ph.D. candidate at the University of New Brunswick. I am also an AI researcher and developer at Canadian Institute for Cybersecurity (CIC). I was involved with several industrial collaborative projects between CIC and (DnD, Scotia Bank, and ADGA Group) for the past four years. My research studies mainly concentrate on adversarial machine learning and security vulnerabilities of deep learning models, especially in the network and cybersecurity domains.

EXPERIENCES

- **Canadian Institute for Cybersecurity**, Fredericton, Canada
  - **Research Assistant**, *Jan 2019 - Present*
  - **Researcher in a security research team in collaboration with ADGA Group Consultants Inc.**, *Jan 2022 - present*
    - In the first phase of this project, I was part of a team performing comprehensive research on different cybersecurity aspects and vulnerabilities of the supply chain. Also, I participated in preparing a detailed survey document covering an in-depth review of critical applications of the supply chain and traditional and innovative technologies used to overcome security vulnerabilities.
    - In the second phase, based on the previous findings, blockchain was selected as a suitable solution for supply chain security and I developed a proof of concept application based on the blockchain using Hyperledger Fabric, Java, and smart contracts.
  - **Researcher in a security research team in collaboration with Scotiabank**, *Nov 2019 - Jan 2022*
    - I was part of a research team generating a threat landscape report about security vulnerabilities s of financial institutions with a focus on malware and ransomware.
    - In the second phase our team conducted a detailed review of different available solutions for cyber threat intelligence sharing using different sources such as companies' websites and interviews. Also, we proposed a customer-orientated ranking system using an AHP-based approach.
    - Then we conducted research about the vulnerabilities of financial institution operations against different detected CVEs and proposed a scoring system with deep learning and word embedding developed using Python and PyTorch.
    - In the last phase in order to predict an attacker's next step and break the kill chain, a comprehensive dataset of different TTPs was collected from various sources, and an application for extracting association rules was developed using Apriori and Python.
  - **AI researcher and developer in a project for Department of National Defence (DnD) - Hostile new detection project**, *Jul 2019 - Feb 2020*
    - I used different deep learning techniques (RNN and LSTM) and NLP which were developed using Python, PyTorch, and Scikit Learn to detect hostile news from different textual documents.

        - Also in this project huge amount of tweets and user information was crawled from Twitter and stored in the database using Kafka and Elastic search. A community detection algorithm was developed using Python and graph-related information such as K_core, closeness, etc were extracted for different users.

- **University of New Brunswick**, Fredericton, Canada
    - **Graduate Teaching Assistant**, *Jan 2021 - Jan 2022*
        - **CS1003** Programming & Problem Solving for Engineers
    - **Computer Science Graduate Students Association Treasurer (CS-GSA)**, *Nov 2019 - Dec 2020*
        - Represent the CS-GSA at GSA meetings
        - Preside over any meeting of the CS-GSA
        - Supervise the financial affairs of the CS-GSA
- **17th International Conference on Privacy, Security, and Trust (PST)**, Fredericton, Canada

  Executive Group Member, *Aug 2019*
- **Sepanta**, Tehran, Iran:

  Software Developer, *Aug 2012 - Aug 2013*
    - Designed and developed a web-based automation system for a large company using ASP.Net and C#.
    - Designed and developed a large-scale database using SQL server.

EDUCATION

- **University of New Brunswick**, Fredericton, Canada

  Ph.D. Candidate, Computer Science, *Jan 2019 - Jul 2023 (expected)*
- **Kharazmi University**, Tehran, Iran

  M.Sc., Artificial Intelligence, *Sep 2012 - July 2015*

  Thesis Title: Image Classification Based on Bag of Words Method
- **Iran University of Science and Technology**, Tehran, Iran

  B.Sc., Software Engineering, *Sep 2007 - Sep 2012*

  Thesis Title: Distributed AI in Video Games

LICENCES & CERTIFICATIONS

- **Neural Networks and Deep Learning**, *deeplearning.ai, Oct 2020*
- **Improving Deep Neural Networks: Hyperparameter tuning, Regularization and Optimization**, *deeplearning.ai, Oct 2020*
- **Structuring Machine Learning Projects**, *deeplearning.ai, Nov 2020*
- **Sequence Models**, *deeplearning.ai, Nov 2020*
- **Convolutional Neural Networks**, *deeplearning.ai, Dec 2020*

PUBLICATIONS

- **Hesamodin Mohammadian**, Arash Habibi Lashkari, and Ali A. Ghorbani. ”Evaluating Deep Learning-based NIDS in Adversarial Settings.” In ICISSP, pp. 435-444. 2022.
- **Hesamodin Mohammadian**, Ali A. Ghorbani, and Arash Habibi Lashkari. ”A Gradient-based Approach for Adversarial Attack on Deep Learning-based Network Intrusion Detection Systems.”(Submitted to Applied Soft Computing Journal).
- **Hesamodin Mohammadian**, Sajjad Dadkhah, Mohammed Al-Darwbi, Ehab Alkhateeb, and Ali A. Ghorbani. ”Cyber Threat Intelligence Sharing Solution: A Survey.”(Submitted).

TECHNICAL SKILLS

- **Programming Languages**
  Python, Java, C#, C++, MATLAB
- **Tools and Libraries**
  PyTorch, Scikit-Learn, Numpy, Pandas
- **Operating System**
  Windows Family, Ubuntu