Pooria Lakzian

Neyshaboor, Iran
Phone: (+98)9377851319
Email: poorialakzian@gmail.com

Research Interests

AI/ML for Security	Trustworthy AI	AI Security
Computer Vision	Adversarial Machine Learning	Explainable AI

Education

Iran University of Science and Technology Sep 2020 – Sep 2024
Bachelor's in Computer Science
Tehran, Iran
GPA: 16.1/20 (Dept. Average: 13.77)

National Organization for Development of Exceptional Talents Sep 2014 – June 2020
Diploma in Mathematics and Physics
Neyshaboor, Iran
GPA: 18.81/20

Publications

Under Review:
*Malware Detection via Memory Dumps: Investigating the Role of Uneven Kernel Filters in CNNs with Visual Explainability.*Mohammadhadi Alaeiyan, Pooria Lakzian, Submitted to *the Journal of Computer Virology and Hacking Techniques(Springer)*, Nov 2024

Manuscript in preparation:
On the Resilience of ML-based Intrusion Detection Systems Against Backdoor Attacks. Mohammadhadi Alaeiyan, Pooria Lakzian, Expected: Feb 2025

Research Experience

Research Assistant Fall 2023 - Present
Advisor: Dr. Mohammadhadi Alaeiyan

- **ML-based Malware Detection**: We proposed a novel deep learning-based approach to detect and classify malware using the images created from memory dumps of PE files with visual explanation. We also gathered a malware image dataset and made it publicly available.
- **On the Resilience of ML-based Intrusion Detection Systems Against Backdoor Attacks**: Working on improving the robustness of ML-based intrusion detection systems against backdoor attacks by embedding a Trojan within the model. Using adversarial training as a defense strategy to improve our system's resilience.
- **Attention Guided Data Augmentation for Image-based Malware Detection**: Working on a data augmentation method for identifying and cropping the most salient region of a malware image instance using attention heat map to use in model training.

Final Undergraduate Project Spring 2024
Advisor: Dr. Mehdi Alaeiyan

- **Malware Detection Using Transfer Learning Approach**: Utilized various pre-trained models to evaluate their performance on the malware detection task. Conducted extensive comparative analysis to determine the top-performing models and proposed a novel architecture that integrates key characteristics from these models.

Teaching Experience

- **Data Structure and Algorithms** Fall 2022
  Teaching assistant of Dr. Javad Vahidi *Iran University of Science and Technology*

- **Database Design** Fall 2023
  Teaching assistant of Dr. Fatemeh Baharifard *Iran University of Science and Technology*

Work Experience

Backend Developer Intern at Pardazesh Sazan Summer 2023
Supervisor: Dr. Javad Vahidi
As a member of the development team, I primarily focused on developing backend functionalities for our E-commerce platform, implementing features such as user authentication.

Test Scores

Test	Scores	Date
IELTS Academic	Overall: 7.5 (L:8.0, R:8.5, W: 6.5, S: 7.0)	09/09/2024

Skills

Programming Languages:
Python, R, C++, JavaScript, SQL, HTML, CSS, LaTeX
Tools and Frameworks:
TensorFlow, Keras, PyTorch, Scikit-Learn, Pandas, Matplotlib, NumPy, Django

Honors and Awards

- Ranked Among the top 1% of the National University Entrance Exam in Iran
- Finalist in the Startup Contest at the Azad University of Neyshaboor: Built a Web application for selling second-hand goods.