# Seyedhamidreza Mousavi

*PhD in Computer Engineering*

✉ hamidmousavi0@gmail.com
✉ seyedhamidreza.mousavi@mdu.se
hamidmousavi0.github.io/
hamidrezamousavi
hamidmousavi0

## Summary

## Education

2022–Present **PhD. in Computer Engineering**, *(Estimated Graduation: May 2027) Malardalen University*, Vasteras, Sweden

2016–2019 **M.Sc. in Computer Engineering**, *Shahid Bahonar University of Kerman*, Kerman, Iran

2012–2016 **B.Sc. in Computer Engineering**, *Shahid Bahonar University of Kerman*, Kerman, Iran

## Research Interests

My research interests focus on trustworthy deep learning, encompassing areas such as adversarial robustness, fairness, and reliability in both discriminative and generative models. I am also deeply engaged in tiny deep learning, exploring techniques like pruning, quantization, and neural architecture search to enable efficient deployment of deep neural networks on resource-constrained devices.

## Selected Publications

[1] M. H. Ahmadilivani, S. **Mousavi**, J. Raik, M. Daneshtalab, and M. Jenihhin. Cost-effective fault tolerance for cnns using parameter vulnerability based hardening and pruning. In *2024 IEEE 30th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, pages 1–7. IEEE, 2024.

[2] S. Ali Mousavi, H. **Mousavi**, and M. Daneshtalab. Farmur: fair adversarial retraining to mitigate unfairness in robustness. In *European Conference on Advances in Databases and Information Systems*, pages 133–145. Springer, 2023.

[3] S. M. Ebrahimipour, B. Ghavami, t. **Mousavi**, M. Raji, Z. Fang, and L. Shannon. Aadam: A fast, accurate, and versatile aging-aware cell library delay model using feed-forward neural network. In *Proceedings of the 2020 ACM/SIGDA International Conference On Computer Aided Design (ICCAD)*, pages 1–9, 2020.

[4] B. Ghavami, S. **Mousavi**, Z. Fang, and L. Shannon. Stealthy attack on algorithmic-protected dnns via smart bit flipping. In *2022 23rd International Symposium on Quality Electronic Design (ISQED)*, pages 1–7. IEEE, 2022.

[5] M. Loni, t. **Mousavi**, M. Riazati, M. Daneshtalab, and M. Sjodin. Tas: Ternarized neural architecture search for resource-constrained edge devices. In *To appear in the Design, Automation and Test in Europe Conference (DATE 2022), Mar*, 2022.

[6] S. Mousavi, S. **Mousavi**, and M. Daneshtalab. Proard: progressive adversarial robustness distillation: provide wide range of robust students. *arXiv preprint arXiv:2506.07666*, 2025.

[7] H. **Mousavi**, M. Loni, M. Alibeigi, and M. Daneshtalab. Dass: differentiable architecture search for sparse neural networks. *ACM Transactions on Embedded Computing Systems*, 22(5s):1–21, 2023.

[8] S. **Mousavi**, M. H. Ahmadilivani, J. Raik, M. Jenihhin, and M. Daneshtalab. Proact: Progressive training for hybrid clipped activation function to enhance resilience of dnns. *arXiv preprint arXiv:2406.06313*, 2024.

## Research Projects

- **AutoDeep: Automatic Design of Safe, High-Performance and Compact Deep Learning Models for Autonomous Vehicles** Deep Neural Networks (DNN) are increasingly being used to support decision-making in autonomous vehicles. In this project, we develop a framework called AutoDeep to achieve performance, compactness, and robustness in the design and customization of DNN for intention detection and behavior prediction as two safety-critical applications in road and construction autonomous vehicles
- **Security and Reliability of Deep Learning:** We have developed a method to analyze the adversarial robustness and reliability of deep learning models. We consider simultaneously adversarial attacks and bit-flip attacks.

## Selected Honors and Awards

2019 Selected as the **Best Student** in Computer Engineering Department, Shahid Bahonar University of Kerman

2019 **Ranked first GPA** among my Masters graduation class (30 students)

2018 **Erasmus+ Winter School**, Gradana EU Project Scholarship, Universit of Bonn, Germany

2016 **Ranked first GPA** among my Bachelors graduation class (70 students)

## International Research Collaborations

*Reconfigurable Computing LAB*, **Simon Fraser University**, British Columbia, Canada
Collaboration on reliability in FPGAs and hardware accelerators research projects.
https://www.sfu.ca/~zhenman/

*DeepHero LAB*, **Mälardalen University**, Västerås, Sweden
Collaboration on Automatic Design of Safe, High-Performance and Compact Deep Learning Models for Autonomous Vehicles.
http://www.es.mdh.se/staff/3303-Masoud_Daneshtalab

*Dependable Computing Systems*, **Tallinn University of Technology (TUT)**, Tallinn, Estonia
Collaboration on Reliable deep learning models.
https://jaanraik.wordpress.com/

# Details

## Education

### PhD

2022–Present **PhD. in Computer Engineering,Artificial Intelligence** , *DeepHero LAB, Mälardalen University*, Västerås, Sweden

Thesis Title *Automatic design of high-performance, compact, robust and reliable deep neural networks*

Supervisor Professor Masoud Daneshtalab

**Selected Courses**

- Diffusion Models
- Foundations of Deep Learning
- TinyML and Efficient Deep Learning Computing
- Algorithms for Optimization
- Deep Learning and Neural Networks
- Programming Reliable Embedded Systems

### Master

2016–2019 **M.Sc. in Computer Engineering,Artificial Intelligence** , *Department of Computer Engineering, Shahid Bahonar University of Kerman*, Kerman, Iran, 🎓18.13/20

Thesis Title *Reliability and Security Analysis of Deep Learning Models*

Thesis GPA 19.40/20

Supervisor Professor Mahdi Eftekhari and Professor Behnam Ghavami

**Selected Courses and GPAs:**

- Digital Signal Processing: 19.25/20
- Digital Image Processing: 19.4/20
- Deep Learning: 19.75/20
- Machine Learning: 17/20
- Fuzzy Sets and Systems: 19/20
- Fault Tolerant Computing: 19/20
- Evolutionary Computing: 16.6/20

### Bachelor

2012–2016 **B.Sc. in Computer Engineering, Computer Hardware**, *Department of Computer Engineering, Shahid Bahonar University of Kerman*, Kerman, Iran, 🎓17.66/20

Thesis Title *Design and Implementation of ARM7-TDMIS on Xilinx Spartan 6 FPGA*

Thesis GPA 20/20

Supervisor Professor Behnam Ghavami

**Selected Courses and GPAs:**

- Computer Architecture: 20/20
- Embedded and Real-time Systems: 20/20
- Logic Circuits: 19.5/20
- VLSI System Design: 19.5/20
- Artificial Intelligence: 16.1/20
- Engineering Mathematics: 20/20
- Operating System: 19.5/20
- Mathematics I: 20/20
- Electronic Digital: 18.5/20
- Programming Language Design: 19.25/20

## Awards and Honors

2019 Selected as the **Best Student** in Computer Engineering Department, Shahid Bahonar University of Kerman

2019 **Ranked first GPA** among my Masters graduation class (30 students)

2018 Erasmus+ Winter School, **Gradana EU Project Scholarship**, Universit of Bonn, Germany

2016 Received **full Scholarship** for Masters degree (Tuition waiver), Shahid Bahonar University of Kerman

2016 **Ranked first GPA** among my Bachelors graduation class (70 students)

2016 **Exempted** from Iranian University Entrance Exam as an exceptional talent

2012 Received **full Scholarship** for Bachelors degree (Tuition waiver), Shahid Bahonar University of Kerman

## Publications

### Published Papers

[1] Seyed Milad Ebrahimipour, Behnam Ghavami, **Hamid Mousavi**, Mohsen Raji, Zhenman Fang, Lesley Shannon, "Aadam: A Fast, Accurate, and Versatile Aging-Aware Cell Library Delay Model using Feed-Forward Neural Network", *IEEE/ACM International Conference on Computer-Aided Design* ***(ICCAD '20)***, *2020*.

[2] Behnam Ghavami, **Hamid Mousavi**, Zhenman Fang, Lesley Shannon, "Stealth Attack on Protected DNNs: Compromising Robustness without Losing Accuracy via Smart Bit Flipping", *Design Automation Conference 2021* ***(DAC 2021 WIP)***, *2021*.

[3] Mohammad Loni, **Hamid Mousavi**, Mohammad Riazati , Masoud Daneshtalab and Mikael Sjodin "TAS: Ternarized Neural Architecture Search for Resource-Constrained Edge Devices", *Design, Automation and Test in Europe Conference* ***(DATE 2022)*** , *2022*.

[4] Behnam Ghavami, **Hamid Mousavi**, Zhenman Fang, and Lesley Shanno " Stealthy attack on algorithmic-protected dnns via smart bit flipping.", *International Symposium on Quality Electronic Design* ***(ISQED 2022)*** , *2022*.

[5] **Hamid Mousavi**, Mahdi Eftekhari, Behnam Ghavami, "Training a Deep extreme learning machine by integrated structure and efficient learning algorithm for a deep autoencoder. ", ***Electronics Industries***, *2020*. (In Persian).

[6] **Hamid Mousavi**, Mahdi Eftekhari, Behnam Ghavami, "A Supervised Learning Algorithm to Train Deep Extreme Learning Machine ", The $23^{rd}$ Annual National Conference of the Iranian Computer Association **(CSICC)**, *2018*, Tehran, Iran (In Persian).

[7] **Hamid Mousavi**, Mahdi Eftekhari, Behnam Ghavami, "Provide a hierarchical neural network and a combined training algorithm for classification ", The $4^{rd}$ Conference on Contemporary Issues in Computer Information and Science,**(CICIS)** *2019*, Tehran, Iran (In Persian).

[8] **Hamid Mousavi**, Mahdi Eftekhari, Behnam Ghavami, "An Efficient Learning Algorithm to Train Multi layer Extreme Leaning Machine ", The $4^{rd}$ 4TH IRANIAN CONFERENCE ON SIGNAL PROCESSING AND INTELLIGENT SYSTEMS, **(ICSPIS)***2018*, Tehran, Iran (In Persian).

[9] Seyed Ali Mousavi,**Hamid Mousavi** and Masoud Daneshtalab, "FARMUR: fair adversarial retraining to mitigate unfairness in robustness", European Conference on Advances in Databases and Information Systems, **ADBIS** *2023*.

[10] **Hamid Mousavi**, Mohammad Loni ,Mina Alibeigi and Masoud Daneshtalab , "DASS: Differentiable Architecture Search for Sparse Neural Networks", ACM Transactions on Embedded Computing Systems, *2023*.

[11] Mohammad Hasan Ahmadilivani, **Seyedhamidreza Mousavi**, Jaan Raik, Masoud Daneshtalab, Maksim Jenihhin, "Cost-effective fault tolerance for cnns using parameter vulnerability based hardening and pruning", IEEE 30th International Symposium on On-Line Testing and Robust System Design , **IOLTS** *2024*.

[12] **Seyedhamidreza Mousavi**, Mohammad Hasan Ahmadilivani, Jaan Raik, Masoud Daneshtalab, Maksim Jenihhin, "Proact: Progressive training for hybrid clipped activation function to enhance resilience of dnns", **Arxiv** *2024*.

[12] **Hamid Mousavi**, Ali Zoljodi, Masoud Daneshtalab, "Analysing robustness of tiny deep neural networks", European Conference on Advances in Databases and Information Systems, **ADBIS** *2023*.

[13] Bostan Khan, **Hamid Mousavi**, Masoud Daneshtalab, "HeRD: Modelling Heterogeneous Degradations for Federated Super-Resolution in Satellite Imagery", European Conference on Advances in Databases and Information Systems, **IEEE Access** *2025*.

[14] **Hamid Mousavi**, Ali Mousavi, Masoud Daneshtalab, "ProARD: Progressive Adversarial Robustness Distillation: Provide Wide Range of Robust Students", International Joint Conference on Neural Networks, **IJCNN** *2025*.

[15] Amin Yoosefi, **Hamid Mousavi**, Masoud Daneshtalab, "Efficient On-device Transfer Learning using Activation Memory Reduction", Eighth International Conference on Fog and Mobile Edge Computing, **FMEC** *2023*.

[16] HamidReza Mahini, **Hamid Mousavi**, Masoud Daneshtalab, "GTFLAT: Game Theory Based Add-On For Empowering Federated Learning Aggregation Techniques", **Arxiv** *2023*.

## Skills

- **Programming Languages:** Python, C++
- **Deep Learning:** PyTorch
- **HDL:** VHDL (B.Sc. thesis)
- **Machine Learning:** Scikit-Learn, Numpy, Pandas
- **Simulation:** Xilinx ISE Toolset (B.Sc. Thesis), Modelsim (B.Sc. Thesis)
- **document preparation:** LaTeX
- **Version Control Management:** Git

## Experience

### Research Experience

2016–2020 **Research Assistant**, *Reliable Embedded System Design and Machine Learning Laboratory*, Shahid Bahonar University of Kerman, Kerman, Iran
- **Supervisor:** Professor Mahdi Eftekhari and Professor Behnam Ghavami
- **Master Thesis:** Reliability and Security Analysis of Deep Learning Models
- **Contributed** in **7** papers

2020–Present **Research Assistant**, *Heterogeneous systems - hardware software co-design research group*, Mälardalen University, Västerås, Sweden
- **Supervisor:** Professor Masoud Daneshtalab
- **Contributed** in **10**

## Teaching Experience

2022 **Teacher**, *IDT*, Malardalen University

**Courses:**

- Deep Learning
  - Fall 2022, 2023, 2024
- Computer Architecture and VHDL
  - Spring 2022, 2023, 2024

2016–2019 **Laboratory Instructor**, *Department of Computer Engineering*, Shahid Bahonar University of Kerman

**Courses:**

- Machine Learning Laboratory
  - Fall 2018, Winter 2018
- Deep Learning Laboratory
  - Fall 2019, Winter 2019

2019–2019 **Teaching Assistant**, *Department of Computer Engineering*, Shahid Bahonar University of Kerman

**Courses:**

- Machine Learning
  - Fall 2019, Winter 2019
- Computer Architecture
  - Fall 2017

## References


Professor Masoud Daneshtalab
*Full-Professor*
Heterogeneous systems research group
**Mälardalen University, Sweden**
✉ masoud.daneshtalab@mdh.se

Professor Jaan Raik
*Full-Professor*
Dependable Computing Systems
**Tallinn University of Technology (TUT)**
✉ jaan.raik@taltech.ee