Hamid Bostani

June 2025

I am a well-organized, hard-working researcher with a passion for solving complex problems and a drive to achieve ambitious goals. I bring a unique blend of expertise in machine learning and systems security, with a particular focus on trustworthy AI. I am eager to apply my skills and contribute to the development of secure, reliable AI solutions for a safer digital future.

CONTACT INFORMATION

Hegdambroek 2305, 6546 WH Nijmegen, The Netherlands.

Email: hamidbostani.ac@gmail.com
Phone: +31 625440813
Google Scholar
Personal Homepage

RESEARCH INTERESTS

- **Adversarial Machine Learning**
- **Machine Learning**
- **Deep Learning**
- **Trustworthy AI**
- **Malware Detection Systems**
- **Intrusion Detection Systems**
- **Internet of Things**

EDUCATION

Radboud University, Nijmegen, The Netherlands. Oct. 2020 – Oct. 2024
Ph.D. Candidate in Computer Science.
Dissertation: **Rethinking the Security of Machine Learning in Malware Detection** (Supervisors: Prof. Veelasha Moonsamy and Dr. Erik Poll)
Dissertation has been approved by manuscript committee, and the defense is scheduled for Sep. 9, 2025

Islamic Azad University (IAU), South Tehran Branch, Tehran, Iran. Sept. 2012 - Sept. 2015
M. Sc. in Computer Engineering (Software Engineering), GPA: 17.55/20.
Thesis: **Intrusion Detection and Identification of Attacks on the Internet of Things (IoT) Using a Combination of Machine Learning Methods** (Supervisor: Prof. Mansour Sheikhan)
Master Seminar: **Using Collaborative Filtering in Recommender Systems** (Advisor: Prof. Ali Moeini)

Islamic Azad University (IAU), Shiraz Branch, Shiraz, Iran. Sept. 2004 - Sept. 2008
B. Sc. in Computer Engineering (Software Engineering), GPA: 16.73/20, Major GPA: 18.53/20.
Project: "**Developing E-Commerce System**s **(a Case Study in a Mobile Phone Store)**" (Supervisor: Dr. Mostafa Fakhrahmad)

HONORS AND AWARDS

- **Fully-Funded PhD** (Radboud University, Oct. 2020).
- **Best Employee Award** (NOET, Nov. 2019).
- **Certificate of Appreciation (**NOET, Feb. 2018).
- **Research Funding** (Iran National Science Foundation, Feb. 2018).
- **Outstanding Researcher Award** (IAU, South Tehran Branch, Dec. 2017).
- **Best Master Thesis Award** (the 5th Research, Scientific & Technological National Festival of IAU, May 2017).
- **Certificate of Appreciation** (IAU, South Tehran Branch, May 2017).
- **Outstanding Paper Award** (ICSPIS'2016).
- **Selected Paper** (IST'2016).

RESEARCH AND WORK EXPERIENCES

- **Ph.D. Candidate** Oct. 2020–Oct. 2024
  Digital Security Group, Institute for Computing and Information Sciences, Radboud University, Nijmegen, The Netherlands.
- **Visiting Scholar** Oct. 2023–March 2024
  Cybersecurity Group, King's College University, London, UK.
- **Visiting Scholar** Oct. 2023–March 2024
  Systems Security Lab, University College London, London, UK.
- **Research Assistant** Aug. 2017–Sept. 2020
  Young Researchers and Elite Club of IAU, South Tehran Branch, Tehran, Iran.
- **Research Assistant** Aug. 2016–March 2017
  Research Center of Modeling and Optimization in Science and Engineering, IAU, South Tehran Branch, Tehran, Iran.

Sep. 2012– Sep. 2020

- **Full-Stack Developer**
  Strategic Analysis and Information Security Group, Department of New Communications, National Organization for Educational Testing (NOET), Tehran, Iran.

- **Software Expert** April–Aug. 2012
  Software Systems Group, Department of Information and Communication Technology, Bank Hekmat Iranian, Tehran, Iran.

TEACHING ASSISTANT

- **Deep Learning**, Radboud University, 2023.
- **Networks & Security**, Radboud University, 2022.

PUBLICATIONS

Bibliographic indicators (Google Scholar June 2025) Citations: 705, h-index: 7.

Pre-prints

1. **H. Bostani**, J. Cortellazzi, D. Arp, F. Pierazzi, V. Moonsamy and L. Cavallaro. "On the Effectiveness of Adversarial Training on Malware Classifiers," under peer review (2024).

Journals

2. **H. Bostani** and V. Moonsamy. "Beyond Learning Algorithms: The Crucial Role of Data in Robust Malware Detection," Accepted for publication in IEEE Security & Privacy, March 2025.

3. **H. Bostani**, Z. Zhao, Z. Liu, and V. Moonsamy. "Level Up with ML Vulnerability Identification: Leveraging Domain Constraints in Feature Space for Robust Android Malware Detection," *ACM Transactions to Privacy and Security*, vol. 28 (2025), no. 2, pp.1-32. DOI: 10.1145/3711899 (Q1)

4. **H. Bostani** and V. Moonsamy, "EvadeDroid: A practical evasion attack on machine learning for black-box android malware detection," *Computers & Security*, vol. 139 (2024). DOI: 10.1016/j.cose.2023.103676, Impact Factor (2024) = 5.6 (Q1)

5. **H. Bostani**, M. Sheikhan, B. Mahboobi, "A Strong Coreset Algorithm to Accelerate OPF as a Graph-based Machine Learning in Large-Scale Problems," *Information Sciences*, vol. 555 (2021), pp. 424-441. DOI: 10.1016/j.ins.2020.10.009, Impact Factor (2020) = 5.9 (Q1)

6. **H. Bostani**, M. Sheikhan, "Hybrid of Anomaly-Based and Specification-Based IDS for Internet of Things Using Unsupervised OPF based on Map-Reduce Approach," *Computer Communications*, Elsevier, vol. 98 (2017), pp. 52-71. DOI: 10.1016/j.comcom.2016.12.001, Impact Factor (2016) = 3.3 (Q1)

7. **H. Bostani**, M. Sheikhan, "Modifying Supervised Optimum-Path Forest in Intrusion Detection Systems Using Social Network Approaches and Unsupervised Learning," *Pattern Recognition*, Elsevier, vol. 62 (2017), pp. 56-72.DOI: 10.1016/j.patcog.2016.08.027, Impact Factor (2016) = 4.6 (Q1)

8. **H. Bostani**, M. Sheikhan, "Hybrid of Binary Gravitational Search Algorithm and Mutual Information for Feature Selection in Intrusion Detection Systems," *Soft Computing*, Springer, vol. 21 (2017), no. 9, pp. 2307-2324.DOI: 10.1007/s00500-015-1942-8, Impact Factor (2016) = 2.5 (Q2)

9. M. Sheikhan, **H. Bostani**, "A Security Mechanism for Detecting Intrusions in Internet of Things Using Selected Features Based on MI-BGSA," *International Journal of Information & Communication Technology Research*, Iran Telecommunication Research Center (ITRC), vol. 9 (2017), no. 2, pp. 53-62. http://journal.itrc.ac.ir/article-1-42-en.html

Conferences & Workshops

10. **H. Bostani**, Z. Zhao, and V. Moonsamy. "Improving Adversarial Robustness in Android Malware Detection by Reducing the Impact of Spurious Correlations," *In Proceedings of the 29th European Symposium on Research in Computer Security Workshops (**ESORICS 2024 Workshops**)*.

11. Z. Moti, A. Senol, **H. Bostani**, F.Z. Borgesius, V. Moonsamy, A. Mathur, G. Acar, "Targeted and Troublesome: Tracking and Advertising on Children's Websites," *In Proceedings of the 45th IEEE Symposium on Security and Privacy (**IEEE S&P 2024**)*. DOI: 10.1109/SP54263.2024.00118

12. **H. Bostani**, M. Sheikhan, B. Mahboobi, "Developing a Fast Supervised Optimum-path Forest Based on Coreset," *In Proceedings of 19th International Symposium on Artificial Intelligence and Signal Processing* (***AISP'2017***), pp. 172-177, 2017. DOI: 10.1109/AISP.2017.8324076

13. **H. Bostani**, M. Sheikhan, "Modification of Optimum-Path Forest using Markov Cluster Process Algorithm," *In Proceedings of 2nd of International Conference on Signal Processing and Intelligent Systems (**ICSPIS'2016**)*, pp. 1-5, 2016. (***Winner of the Outstanding Paper Award***) DOI: 10.1109/ICSPIS.2016.7869874

14. M. Sheikhan, **H. Bostani**, "A Hybrid Intrusion Detection Architecture for Internet of Things," *In Proceedings of 8th International Symposium on Telecommunication (**IST'2016***), pp. 601-606, 2016. (***Selected as one of the Best Papers***) DOI: 10.1109/ISTEL.2016.7881893

Book Chapters

15. M. Sheikhan and **H. Bostani**, "Hybrid and modified OPFs for intrusion detection systems and large-scale problems," in Optimum-Path Forest (pp. 109-136). Elsevier (2022). https://doi.org/10.1016/B978-0-12-822688-9.00013-X

16. M. Sheikhan, **H. Bostani**, "Binary Gravitational Search Algorithm (BGSA): Improved Efficiency," *in Encyclopedia of Information Assurance,* Taylor & Francis (2016). https://www.taylorfrancis.com/books/9781351235808

ORAL/POSTER PRESENTATIONS

2024

- *Guest Talk:* **"Are We Truly Ready to Secure Malware Detection Against Adversarial Attacks?"** Machine Learning and Security Group, TU Berlin, Germany, December 2024.
- *Workshop Presentation:* **"Improving Adversarial Robustness in Android Malware Detection by Reducing the Impact of Spurious Correlations."** ESORICS 2024 Workshop on Security and Artificial Intelligence, Bydgoszcz, Poland, 20 September 2024. Watch the talk
- *Colloquium:* **"Rethinking Adversarial Machine Learning in the Context of Malware Detection,"** Lunch Colloquium, Digital Security Group, Radboud University, Nijmegen, The Netherlands, June 2024
- *Invited Talk:* **"Adversarial Robustness for Malware Classifiers."** KCL Cybersecurity Workshop, London, UK, February 2024.

2023

- *Webinar:* **"Adversarial Machine Learning: Challenges and Solutions in Malware Detection."** Iranian Society of Cryptology, December 2023. Watch the talk
- *Conference Presentation:* **"Improving Robustness of Machine Learning-based Android Malware Detection against Realizable Adversarial Examples."** ICT.OPEN'23, Utrecht, The Netherlands, April 2023.

2022

- *Colloquium:* **"Improving Robustness of Machine Learning-based Malware Detection against Realizable Android Adversarial Examples."** Lunch Colloquium, Digital Security Group, Radboud University, Nijmegen, The Netherlands, June 2022.

2020

- *Colloquium:* **"AI for Intrusion Detection."** Lunch Colloquium, Digital Security Group, Radboud University, Nijmegen, The Netherlands, October 2020.

2017

- *Conference Presentation:* **"Developing a Fast Supervised Optimum-path Forest Based on Coreset."** AISP'2017, Shiraz University, Shiraz, Iran, 25-27 October 2017.

2016

- *Conference Presentation:* **"Modification of Optimum-Path Forest using Markov Cluster Process Algorithm."** ICSPIS'2016, Amirkabir University of Technology, Tehran, Iran, 14-15 December 2016.

- *Conference Presentation:* **"A Hybrid Intrusion Detection Architecture for Internet of Things"** IST'2016, Iranian Research Institute for Information Science and Technology, Tehran, Iran, 27-28 September 2016.

ACADEMIC SERVICE

Program Committees

- 7th ACM Workshop on Artificial Intelligence and Security 2024

Sub-Reviewing

- NDSS, IEEE Euro S&P 2024
- USENIX Security 2023
- USENIX Security, IEEE Euro S&P, ACM Asia CCS 2022
- CANS 2021

TRAINING AND SKILLS

Training Courses

- **Education in a Nutshell**, Radboud University, Nijmegen, The Netherlands (2023).
- **Presentation Skills**, Radboud University, Nijmegen, The Netherlands (2023).
- **Summer School on Privacy-Preserving Machine Learning,** ITU Copenhagen and Aarhus University, Copenhagen, Denmark, (1-4 August 2022).
- **Advanced Conversation**, Radboud University, Nijmegen, The Netherlands (2021).
- **SQL Server Query Tuning and Optimization**, Faratar As Danesh Institute, Tehran, Iran (2018).
- **SQL Server 2016 – Design & Implementation**, Faratar As Danesh Institute, Tehran, Iran (2018).
- **Professional SCRUM Master**, Faratar As Danesh Institute, Tehran, Iran (2016).
- **MCSD Web Pack 2012**, Kahkeshane Noor Institute, Tehran, Iran (2016).
- **ETL (SSIS) and Data Mining (SSAS) 2012**, Faratar As Danesh Institute, Tehran, Iran (2014).
- **Data Warehousing & OLAP using SSAS 2012**, Faratar As Danesh Institute, Tehran, Iran (2014).
- **Win Application (C# & intro ADO.NET)**, South Industrial Management Institute, Shiraz, Iran (2008).

Computer Knowledge

- **Programming and Scripting:** Python, C/C++, C#, SQL, Java, JavaScript, HTLM & CSS, MATLAB.
- **Frameworks and Tools:** PyTorch, Scikit-Learn, Hugging Face Transformers, MATLAB Optimization, Fuzzy, and Neural Net Tools, Microsoft Visual Studio, SQL Server Management Studio, Visual Paradigm, Microsoft Office, Azure Boards.
- **Software Development Technologies:** C#.Net Windows Form, ASP.Net Web Form, APS.Net MVC, WCF Service, jQuery & AngularJS, ADO.NET Entity Framework, Java 2 Platform Micro Edition (J2ME), Microsoft BI Technologies (Data Quality, Integrated, Analysis, and Reporting Services).
- **Databases and Dataflow Systems:** SQL Server (programming).
- **Software Development Methodologies:** RUP, EUP, SCRUM.
- **OS:** Windows

Language Skills

- **Persian (Farsi):** Native language
- **English:** Fluent, TOEFL (Dec 2019) Internet-Based Test: 84/120 (Reading: 21/30, Listening: 22/30, Speaking: 21/30, Writing: 20/30)