Taha Eghtesad | PhD Candidate

✉ tahaeghtesad@psu.edu • www.tahaeghtesad.com
https://linkedin.com/in/tahaeghtesad

Education

Pennsylvania State University — **University Park, PA**
Doctor of Philosophy — *Aug 2022 – May 2026*
Informatics

University of Houston — **Houston, TX**
Master of Science, 3.81/4 — *Aug 2018 – May 2022*
Computer Science

Shahid Beheshti University — **Tehran, Iran**
Bachelor of Science, 17.17/20 — *Sep 2013 – May 2018*
Computer Engineering - Software

Areas of Expertiese

Machine Learning, Reinforcement Learning, Deep Learning, Software Engineering

Experiences

Research Experience

Pennsylvania State University — **University Park, PA**
Graduate Research Assistant — *Aug 2022 – Dec 2025*

- Spearheaded multiple PSU, NSF, ARO, and NIST-funded grants.
- Working at the intersection of machine learning to address cyber-security challenges. My responsibilities include researching for SOTA reinforcement learning algorithms, developing cyber-security simulations, and publishing academic articles.

University of Houston — **Houston, TX**
Graduate Research Assistant — *Aug 2018 – Aug 2022*

Industry Experience

Google — **Sunnyvale, CA**
Software Engineer — *Dec 2025 – Present*

Schneider Electric — **Lake Forest, CA**
Artificial Intelligence and Machine Learning Co-OP — *Jul 2024 – Aug 2024*

- Collaborated on US patents for Automated Layers of Protection Analysis (LOPA) by performing requirement analysis of safety controllers.
- Applied supervised and reinforcement learning solutions for LOPA of safety controllers of Industrial Control Systems.
- Applied adversarial reinforcement learning to mitigate safety hazards in Industrial Control Systems.

Hamisystem Sharif — **Tehran, Iran**
Fullstack Software Engineer — *Sep 2017 – Aug 2018*

- Added more than 100 software components and API to myMCI. myMCI is a customer-facing billing mobile application for the mobile communication company of Iran, which has more than 27 million customers. I was directly responsible for the development, operation, and testing during my appointment.

Teaching Experiences

Teaching Assistant

Database Administration
Pennsylvania State University, ETI 461
50 Students (Spring 2025)

Deep Reinforcement Learning
Pennsylvania State University, IST 597
20 Students (Spring 2025)

Computer Networks
Shahid Beheshti University
50 Students (Fall 2016), 30 Students (Spring 2016), 40 Students (Spring 2017)

Web Engineering
Shahid Beheshti University
70 Students (Spring 2017)

Advanced Programming
Shahid Beheshti University
40 Students (Spring 2014)

Introduction to Programming
Shahid Beheshti University
40 Students (Fall 2014)

Leading Instructor

LPIC-1
Shahid Beheshti University, Computer Lab
16 Students (Fall 2014), 20 Students (Fall 2015), 40 Students (Fall 2016)

Projects

Doctoral Dissertation

Pennsylvania State University
Deep Reinforcement Learning Applications in Cyberphysical Systems *Oct 2024*

- Applied reinforcement learning to solve cybersecurity challenges in transportation, chemical plants, and computer security by developing novel multi-agent RL algorithms for automated decision-making, enabling autonomous threat detection and mitigation.
- Developed and evaluated a hierarchical multi-agent reinforcement learning algorithm that successfully attacked a simulated transportation system, increasing total vehicle travel time by 50% compared to the no-attack baseline.
- Developed and evaluated a competitive multi-agent reinforcement learning algorithm that effectively mitigated attacks on chemical plants, limiting state deviation to only 17% under attack compared to nominal operating conditions.
- Leveraged software engineering principles and the Slurm workload manager to implement a scalable, distributed computing environment using MPI, enabling efficient evaluation of multi-agent reinforcement learning algorithms in the context of cyberattacks.
- Implemented AutoML features using Bayesian grid search for fine-tuning reinforcement learning models, enhancing their performance and adaptability in detecting and mitigating cyberattacks within the simulated environment.

Master Thesis

University of Houston
Adversarial Deep Reinforcement Learning for Moving Target Defense *May 2022*

- **Network reconnaissance attacks** is the initial step of sophisticated **adversarial persistent threats** against computer networks. To this extent, we developed a state-of-the-art **multi-agent reinforcement learning** framework that employs **game theoretic** modeling to obfuscate network architecture. This framework systematically alters network and component configurations, proactively defending against reconnaissance attacks by strategic and stealthy actors. The implemented solution enhances defense accuracy, reliability, and sophistication, surpassing the effectiveness of human-supervised (GitHub)

Bachelor Project

Shahid Beheshti University

SunHAS*: A Home Automation System for Smart Energy Monitoring* *Sep 2017*

- Developed a home automation system based on ESP8266 Microcontroller (C++), NodeJS, and Casandra for energy monitoring and routine actuation in smart homes. The limitations of Wifi range and number of connected nodes are tackled by turning the set of ESP8266 controllers into a **mesh grid**, enabling deployment of these systems on large-scale residential and commercial buildings reliably and wirelessly. (GitHub)

Select Research Projects

Blockchain-based Renewable Energy Trading Framework in Smart Communities

- Designed and implemented an **Ethereum-based smart contract** platform for **forward-trading renewable energy** within smart and connected communities. Developed software integration to facilitate seamless interaction between off-chain and on-chain components, maintaining authenticity and accountability of the energy trading contracts in an efficient manner. (GitHub)
- Expanded the framework to **processing outsourcing** at the computing edge where the possibility of collusion or misbehavior is deterred using monetary punishment devised by game theoretic analysis.

Computer Vision For Ridership Data Acquisition

- Ensured high-quality training and evaluation data for computer vision models by collaborating with the Chattanooga Area Transit Authority (CARTA) to acquire CCTV footage (24 x 30-second videos for tracking, 600 images for detection) and managing the annotation process.
- Developed and optimized YOLOv6 object detection models to achieve a 10-fold 91% detection rate for passengers in annotated images.
- Implemented and fine-tuned SORT object tracking algorithms to accurately assign boarding/alighting stops to passengers in 24 x 30-second videos, demonstrating an 84% assignment accuracy.
- Deployed a containerized solution of the trained models on the transit authority's infrastructure, enabling automated ridership data collection and analysis.

Toward Scalable Bug Bounty Brograms

- Surveyed 156 bug bounty hunters to understand **their motivations and challenges they face** while working in the crowdsourced vulnerability discovery markets. We interviewed 24 participants for a better understanding of the reasons for their dissatisfaction and leaving a program.
- With a **quantitative and qualitative** assessment, we summarized the key takeaways from the interviews with a numerical ranking. We provided **managerial bullet points** for program directors to improve their program, increasing participation and efficiency while decreasing the wasted time due to invalid reports.
- We concluded that **monetary rewards** are the bug hunters' main motivation while challenges arise due to the **competition** inherent in the market, i.e., only the first hunter to find a bug will be compensated.

Deep Reinforcement Learning for Model-Based Volt/VAR Optimization

- Devised a decentralized **deep reinforcement learning** platform based on **DDPG** algorithm for improving **Volt/VAR** optimization of **power grids** in smart and connected communities. **Decentralization** of the computational framework leads to improved training time and better accuracy of the models. Our analysis shows that our RL framework improves the Volt/VAR convergence time **from thousands** of computational steps to a few **hundred steps** to stabilize the power grid. (GitHub)

Select Software Project

Codebaz: Online judge for teaching programming to high school students (PHP)

SunCrawlers: A set of crawlers for Instagram, Twitter, Facebook, (Java, Neo4J, Python, ELKStack)

Ubuntu Release Party Website: Ubuntu 14.10 release party at Shahid Beheshti University (HTML)

SunTLS: A transport layer simulator for developing various error correction and sequencing schemes in computer networks. (Java)

SunJudge: A judge for running Shahid Behehsti AI Challenge (Java, Spring, Docker). This includes a solution for automating the setup, execution, and reporting of AI teams playing with each other.

Course Projects

SunBook: Search engine for jobs based on 25 Iranian job bulletins (Java, Lucene, Spring, Android)

SunViz: Ranking authors and co-authors in DBLP and visualizing them, based on PageRank(PR) algorithm and D3.js (Java, JS)

SunDrop: A scalable solution for secure transfer and storage of user files (Java, Spring, Docker)

SunBook: A social network for enterprise job finding like LinkedIn (Java, Spring)

SunProcessor: A 8 bit, 5 stage pipelined micro-processor (Verilog)

SunSocial: A simple social network with posts, comments, and likes. (Java, Servlet)

SunHotelier: Hotel management system (Java, Spring Core, Apache Cassandra)

SyncChronos: An ESP8266-based Internet Clock with DS3231 RTC backup, supporting both FUTABA VFD and MAX7219 LED Matrix displays.

Pensieve: Pensieve is a local AI chat assistant plugin for Obsidian. It's powered by Ollama and uses Retrieval-Augmented Generation (RAG) directly on your device.

Awards

Scholarship
Graduate Tuition Fellowship, Pennsylvania State University — *Aug 2022 – Dec 2024*

Distinguished Paper Award
Usenix Security 2023, Anaheim, CA — *July 2023*

Immigration Benefit
National Interest Waiver, I-140 Employment-Based 2nd-Preference — *Mar 2023*

Scholarship
Graduate Tuition Fellowship, University of Houston — *Aug 2018 – Aug 2022*

Waiver
Tuition Waiver 54.212, University of Houston — *Aug 2018 – Aug 2022*

Iranian University MSc entrance exam — **Rank 41**
Information Technology — *2018*
Among 10000 participants

Iranian University MSc entrance exam — **Rank 190**
Software Engineering — *2017*
Among 30000 participants

ACM ICPC Asian Regional Contest — **Rank 8**
Sharif University of Technology — *2016*
Team "Disqualified"

Iran Open 2D Soccer Simulation — **Rank 7**
Qazvin Islamic Azad University — *2016*
Team "Legen2Dary"

AI Challenge — **Rank 16**
Sharif University of Technology — *2016*
Team "Disqualified"

JavaCup **Rank 7**
Shahid Beheshti University *2016*
Among 200 participants

Urban Start-Up Weekend **Rank 3**
Shahid Beheshti University *2015*
Team “Just4Lunch”
The idea of a city hazard notification, such as building collapses, fires

Java Challenge
Sharif University of Technology, AI BOT Challenge *2015*
Team “Just4Lunch”

UTSec
University of Tehran, CTF *2015*
Team “Just4Lunch”

Iran Open 2D Soccer Simulation **Rank 5**
Qazvin Islamic Azad University *2015*
Team “Legen2Dary”

Iranian University BSc Entrance Exam **Rank 1428**
Mathematics *2013*
Among 250,000 participants

Service

Program Committee
The 40th Annual AAAI Conference on Artificial Intelligence *2025*

Auxilary Reviewer
22nd International Conference on Autonomous Agents and Multiagent Systems *2023*

Technical Committee
SBU AI Challenge *2017*
Online Judge for running the competition

Technical Committee
SBU AI Challenge *2015*
Wrote the game client for C++, and Online Judge for running the competition

Executive Committee
SBU Ubuntu 14.10 Release Party *2014*

Executive Committee
19th Computer Society of Iran Computer Conference, CSICC 2014 *2014*
Top computer conference in Iran

Organizations

Association for Computing Machinery **Professional Member**
ACM *Oct 2021 – present*

Institute of Electrical and Electronics Engineers **Student Member**
IEEE *Sep 2021 – present*

Talks

Doctoral Defense
College of Information Sciences and Technology, Pennsylvania State University *Feb 2026*
Adversarial Reinforcement Learning for Cyberattack Prevention, Detection, and Mitigation

Doctoral Comprehensive Exam (Proposal Defense)
College of Information Sciences and Technology, Pennsylvania State University *Mar 2024*

Adversarial Reinforcement Learning for Cyberattack Prevention, Detection, and Mitigation

Conference Presentation
GameSec 2020, University of Maryland – College Park (Virtual) *Oct 2020*
Adversarial Deep Reinforcement Learning based Adaptive Moving Target Defense

Publications

T. Eghtesad, Y. Vorobeychik, A. Laszka
17th ACM/IEEE International Conference on Cyber-Physical Systems *ICCPS 2026*
Adversarial Reinforcement Learning for Detecting False Data Injection Attacks in Vehicular Routing

T. Eghtesad, Y. Vorobeychik, A. Laszka
7th Games, Agents, and Incentives Workshop *GAIW @ AAMAS 2025*
A Game-Theoretic Deep Reinforcement Learning Approach for Detecting False Data Injection in Routing Algorithms

T. Eghtesad, Y. Vorobeychik, A. Laszka
The 23rd International Conference on Autonomous Agents and Multi-Agent Systems *AAMAS 2024*
Hierarchical Multi-Agent Reinforcement Learning for Assessing False-Data Injection Attacks on Transportation Networks

O Akgul, T Eghtesad, A. Elazari, O. Gnawali, J. Grossklags, M. Mazurek, D. Votipka, A. Laszka
23rd USENIX Security Symposium, ***Distinguished Paper Award*** *USENIX Security 2023*
Bug Hunters' Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem

S. Eisele, M. Wilbur, T. Eghtesad, K. Silvergold, F. Eisele, A. Mukhopadhyay, A. Laszka, A. Dubey
10th IEEE International Conference on Cloud Engineering *IC2E 2022*
Decentralized Computation Market for Stream Processing Applications

Scott Eisele, Taha Eghtesad, K. Campanelli, P. Agrawal, A. Laszka, A. Dubey
ACM Transactions on Cyber-Physical Systems *ACM TCPS 2020*
Safe and Private Forward-Trading Platform for Transactive Microgrids

S. Eisele, C. Barreto, A. Dubey, X. Koutsoukos, T. Eghtesad, A. Laszka, A. Mavridou
IEEE Computer Magazine *IEEE Computer 2020*
Blockchains for Transactive Energy Systems: Opportunities, Challenges, and Approaches

T. Eghtesad, Y. Vorobeychik, A. Laszka
International Conference on Decision and Game Theory for Security *GameSec 2020*
Adversarial Deep Reinforcement Learning based Adaptive Moving Target Defense

Omer Akgul, Taha Eghtesad, A. Elazari, O. Gnawali, J. Grossklags, D. Votipka, A. Laszka
6th Workshop on Security Information Workers *WSIW 2020*
The Hackers' Viewpoint: Exploring Challenges and Benefits of Bug-Bounty Programs

C. Barreto, T. Eghtesad, S. Eisele, A. Laszka, A. Dubey, X. Koutsoukos
Conference on Industrial Cyberphysical Systems *ICPS 2020*
Cyber-attacks and mitigation in blockchain based transactive energy systems

S. Eisele, T. Eghtesad, N. Troutman, A. Laszka, A. Dubey
International Conference on Distributed and Event-Based Systems *DEBS 2020*
Mechanisms for Outsourcing Computation via a Decentralized Market

Skillset

Languages: Python, Java, C, C++, C#, JavaScript, MATLAB

Machine Learning Algorithms: Decision Tree, SVM, Linear Regression, Linear Programming, Clustering, Bayesian, Deep Learning, Graph Convolution, Graph Attention, Convolutional Neural Network, RL (Q-Learning, DDPG, SAC, PPO)

Machine Learning Technologies: TensorFlow, PyTorch, Keras, Pandas, Numpy, SciKit Learn, Matplotlib, Seaborn

Software Development Technologies: J2EE, Kotlin, Spring, Hibernate, ASP.NET, Entity Framework, NodeJS, Express JS, SQL, NoSQL (Redis, Neo4j)

Big Data and Cloud Technologies: Information Retrieval, ELK Stack, Map Reduce, Apache Hadoop, Apache Spark, MongoDB, Kubernetes

Computer Engineering: Data Structures, Algorithms, Object Oriented Programming, Design Patterns, Computer Architecture, Computer Networks, Cryptography, Compilers

Misc: LaTeX, Git, Linux (LPIC-1), Windows (MCSA), CI/CD (Jenkins)