Behzad Ousat

Ph.D. Research Engineer | Applied ML & LLMs

behzad.ost@gmail.com | 786-824-6705
linkedin.com/in/behzad-ousat | Google Scholar
github.com/behzad-ost | Miami, FL - Open to relocate

Applied machine learning researcher and software engineer specializing in LLM-based agents, automated evaluation, and large-scale ML systems. Experienced in building web-scale measurement pipelines, developing and evaluating ML and LLM-based models, and analyzing adversarial robustness. Bringing eight years of software and DevOps engineering experience alongside applied research in AI/ML. Available to start in **December 2026**.

SKILLS

ML & Research

PyTorch - TensorFlow - Transformers - scikit-learn - CNN - OpenCV - Pandas - NumPy - Adversarial ML - Open Set Recognition - Time Series Analysis

Generative AI & LLMs

LLM Agents - Prompt Engineering - RAG - Prompt Chaining - LLM Evaluation - OpenAI API - Vertex AI - Hugging Face - Ollama

Data & Streaming

PostgreSQL - MongoDB - Redis - Kafka - RabbitMQ - Pinecone - PySpark - Elasticsearch

Engineering & Observability

Ansible - Linux - Git - GitHub Actions - CI/CD - gRPC - Prometheus - Grafana - Data Dog

Languages

Python - Node.js - TypeScript - Bash - C++

Cloud & Platform

AWS - GCP - Kubernetes - Docker - Terraform

EDUCATION

Ph.D. Computer Science, Florida International University **01/2022 – 12/2026**
M.Sc. Computer Engineering, Sharif University of Technology **08/2018 – 08/2021**
B.Sc. Computer Engineering, University of Tehran **08/2014 – 08/2018**

EXPERIENCE

Florida International University - Research Assistant, Applied ML | Miami, FL **01/2022 – Present**

- Engineered **LLM-powered browser agents** by varying the reasoning backend, orchestration, and browser-automation layers, achieving over 95% bypass rate against 4 commercial bot defenses.
- Crawled **30K reported vulnerabilities** across 10+ package ecosystems with custom crawling pipelines, surfacing CWE patterns, malicious packages, and software supply-chain trends.
- Evaluated **prompting strategies** across 10 LLM backends for automated vulnerability analysis, measuring precision, recall, and latency on patched and vulnerable packages.
- Developed Python-based **LLM evaluation pipelines** that automated prompt execution, output parsing, metric computation, and model comparison for vulnerability analysis in CI/CD workflows.
- Trained **LSTM** and **Transformer** models in **PyTorch** on browser-interaction time series to classify automated agents at 95% accuracy, ablating each input modality to isolate its contribution.
- Operated multi-modal collection pipelines capturing **1.6B+ browser interaction artifacts** (DOM, screenshots, event streams) into terabytes of NoSQL storage.
- Measured Captcha deployment across **1M+ websites**, then built an **object-detection** pipeline that solved 12 unique Captcha schemes at 80%+ accuracy.

Tapsi (ride-hailing service) **- Platform Technical Team Lead | Tehran** **12/2019 – 10/2021**

- Created **internal platform tooling** in Python and Bash that let developers run a single microservice locally against shared **Kubernetes** staging environments, cutting local resource needs by 80%.
- Developed **Node.js** and Python message-passing libraries over **gRPC** and **RabbitMQ** that sustained 10K events per second, instrumented with **Prometheus** and **Grafana**.

Fraunhofer IDMT - Machine Learning Engineer Intern | Ilmenau, Germany **09/2019 – 12/2019**

- Trained a **CNN**-based face-recognition model with **OpenCV** and built a Python annotation tool to label news video by anchor identity and scene type, generating ground truth across hundreds of hours.

Tapsi (ride-hailing service) **- Senior Infrastructure Engineer | Tehran** **12/2017 – 09/2019**

- Migrated 60+ microservices to **Kubernetes**, establishing Dockerization and cluster processes, coordinating with backend teams, and onboarding developers through internal workshops.
- Engineered production data pipelines with **Kafka** and **Apache Spark** to automate collection, processing, and reporting for Python ML microservices and analytics workflows.
- Implemented **CI/CD** pipelines in Bash and **Ansible** across staging, canary, and production environments, using A/B testing to de-risk releases.

PROJECTS

LLM Browser Agent Evaluation of Commercial Bot Services – Ph.D. Thesis **2026**

- Led research on autonomous web agents and bot-management systems, designing controlled experiments across model reasoning, agent orchestration, browser profiles, and automation stacks.

Adversarial Analysis of Web Bot Defenses – Short Paper **2024**

- Applied **FGSM** and genetic algorithms against behavioral bot detectors to measure evasion robustness and establish the practical limits of multi-modal defenses.

Open-Set Intrusion Detection on Network Traffic – Master's Thesis **2023**

- Built distributed training and inference workflows over terabytes of **PCAP** data, applying **open set recognition** to detect zero-day network attack classes and apply unsupervised learning for further analysis.

DevOps Consultant – Image Analysis Group **2020**

- Built and maintained a scalable application platform on **Google Cloud**, combining a **Java App Engine** runtime and deployment pipeline with **PostgreSQL** and **Kafka** data infrastructure.

MENTORING, SERVICES, AND HONORS

Teaching Assistant, Software Vulnerability; Data Structures & Python Programming, FIU **2022–Present**

Dissertation Year Fellowship Award, Florida International University **2026**

SGA Graduate Scholarship, Florida International University **2025**

Graduate Mentor, Research methodology, coding practices, and project planning **2022–2025**

Journal Reviewer, IEEE Transactions on Information Forensics & Security (TIFS, IF 8.0) **2024**

Conference Reviewer, RAID, DIMVA, MadWeb **2024, 2025**

SELECTED PUBLICATIONS

B. Ousat, N. Turkmen, L. Rampersaud, D. Bailey, S. Uluagac, A. Kharraz, From Puzzles to Profiles: A Cross-Stack Study of Solver Services and LLM Browser Agents Against Bot Management Systems. Submitted to USENIX Security Symposium, 2027.

B. Ousat, L. Rampersaud, D. Bailey, N. Turkmen, A. Kharraz, Broken Gates: Re-evaluating Web Bot Defenses in the Age of LLM Agents. Preprint, 2026. arXiv:2607.18659

S. A. Akhavani, **B. Ousat**, A. Kharraz, Vulnerability Evolution and the Promise of Automated Gatekeeping in Open-Source Software. International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2026.

B. Ousat, M. Shariatnasab, E. Schafir, F. Shirani, A. Kharraz, In-Application Defense Against Evasive Web Scans through Behavioral Analysis. Preprint, 2025. arXiv:2412.07005

B. Ousat, D. Luo, A. Kharraz, Breaking the Bot Barrier: Evaluating Adversarial AI Against Multi-Modal Defenses. ACM Web Conference (WWW), 2024.

B. Ousat, E. Schafir, D. C. Hoang, M. A. Tofighi, S. Arshad, C. Nguyen, S. Uluagac, A. Kharraz, The Matter of Captchas: An Analysis of a Brittle Security Feature on the Modern Web. ACM Web Conference (WWW), 2024.