

Behzad Ousat

7+ Years in Applied ML, Software, and DevOps

✉ behzad.ost@gmail.com
🌐 linkedin.com/in/behzad-ousat
📍 Miami, FL - Open to relocate

📞 786-824-6705
🌐 behzad-ost.github.io

EDUCATION

Ph.D. Computer Science, Florida International University	01/2022 – 04/2026
M.Sc. Computer Engineering, Sharif University of Technology	08/2018 – 08/2021
B.Sc. Computer Engineering, University of Tehran	08/2014 – 08/2018

EXPERIENCES

Florida International University - Applied ML Graduate Researcher Miami, FL ML/DL Pipeline Development <ul style="list-style-type: none">Developed end-to-end ML pipelines using Pandas, PyTorch, and Scikit-Learn to collect billions of real-world browser interaction artifacts, classifying human vs automated agents with 95% accuracy (arXiv).Trained and fine-tuned deep learning models on terabytes of PCAP data to detect zero-day network attack classes, deploying Open Set Recognition models to classify unknown traffic with 85% accuracy (Journal). LLM and ML-based Adversarial Web Automation <ul style="list-style-type: none">Built and evaluated LLM-powered Browser Agents with prompt optimization, achieving >90% success in web crawling tasks and producing large-scale labeled behavioral datasets for downstream modeling.Developed large-scale Object Detection pipelines trained on millions of text CAPTCHAs, achieving 80%+ solve rates across 1M+ production websites, enabling empirical analysis of CAPTCHA prevalence (WWW '24). Large-Scale Data Analysis & Measurement <ul style="list-style-type: none">Built large-scale web crawling and analysis pipelines for nearly 30K reported vulnerabilities from across 10+ package ecosystems, identifying trends, malicious packages, and supply-chain attack patterns (arXiv).Investigated development practices, code reuse, and popular packages in over 300K Phishing websites in collaborations with Microsoft Security, enabling scalable detection of malicious websites (DIMVA '24).	01/2022 – Present
Tapsi - Software and Site Reliability Engineer Tehran Platform Technical Team Lead <ul style="list-style-type: none">Developed scalable Node.js and Python message passing libraries based on gRPC and RabbitMQ, integrating Prometheus and Grafana dashboards, reducing Mean Time to Resolution (MTTR) by 50%.Designed and implemented a low-latency WebSocket service backed by Redis to deliver critical data to mobile apps in real-time (<50ms), providing guaranteed delivery and engagement in high-traffic conditions.Established On-call Program to handle external requests, shielding infra engineers from interruptions. Senior Infrastructure Engineer <ul style="list-style-type: none">Migrated 60+ microservices to Kubernetes, Coordinated with backend teams, onboarded developers on technical workflows through workshops, and presented improvements to stakeholders.Built and optimized scalable data pipelines with Kafka and Apache Spark to process 10K events/second across services, including Python ML microservices and data analytics workflows. Infrastructure Engineer <ul style="list-style-type: none">Maintained 99% uptime for microservices by operating infrastructure of over 100 Ubuntu servers for compute clusters and databases across Kubernetes, PostgreSQL, and MongoDB.Reduced deployment errors and established automated rollouts by implementing CI/CD pipelines to include canary-testing, staging, and production environments utilizing Bash and Ansible.	12/2017 – 10/2021
Fraunhofer IDMT - Machine Learning Engineer Intern Germany <ul style="list-style-type: none">Built Modeling and classification pipeline to detect studio scene frames by developing a Face Recognition Deep Learning pipeline using (OpenCV and CNN), analyzing over 100 hours of news broadcast data.	09/2019 – 12/2019

SKILLS

Programming: Python, Node.JS, Java	Machine Learning: PyTorch, Scikit-Learn, Pandas
Data Stores: PostgreSQL, MongoDB, RabbitMQ	Orchestration: Git Actions, Kubernetes, Docker, MLFlow
DevOps: Ubuntu, Networks, Bash, Ansible	Cloud: AWS EC2, Beanstalk, GCP AppEngine, Vertex AI
Monitoring: Prometheus, Grafana, Graylog	Security: Web attacks, Bot Detection, Adversarial Analysis

CERTIFICATES AND HONORS

Google Cloud Skillboost ML Engineer Path , 100+ hands-on hours with Vertex AI, AutoML, and GenAI	2025
Conference Reviewer , RAID, DIMVA, MadWeb (20-25% Acceptance Rate)	2024, 2025
Journal Reviewer , IEEE Transactions on Information Forensics & Security (TIFS, IF 8.0)	2024
Scholarship Recipient , Student Government Association Graduate Scholarship	2024
Cisco Certified Network Associate (CCNA)	2021
University of Tehran ACM Student Chapter , Vice President	2016-2017

PROJECTS

LLM-Powered Chat System utilizing RAG on PDF Documents - Personal Project	06/2025 – 08/2025
<ul style="list-style-type: none">Created a LLM-driven pipeline to extract information from unstructured documents and developed a Chat-with-PDF feature using Retrieval-Augmented Generation (RAG) to enable interactive querying.	
Adversarial Analysis of Behavioral Bot Detection Framework - WWW' 24 Short Paper	08/2023 – 05/2024
<ul style="list-style-type: none">Implemented Adversarial Machine Learning attacks, including FGSM and Genetic Algorithm, to evaluate the robustness of developed deep learning models and investigate limitations in practical scenarios.	
Remote DevOps Engineer to Migrate Legacy Java System - Image Analysis Group	08/2020 – 12/2020
<ul style="list-style-type: none">Migrated legacy DICOM medical image analysis software to Google Cloud Platform App Engine, integrating PostgreSQL and Kafka, improving scalability, fault tolerance, and maintainability of workflows.	

SELECTED PUBLICATIONS

S.A. Akhavani*, **B. Ousat***, A. Kharraz, Open Source, Open Threats? Investigating Security Challenges in Open-Source Software. To be Submitted to USENIX Security, 2026. Available as arXiv preprint arXiv:2506.12995

B. Ousat, M. Shariatnasab, E. Schafir, F. Shirani, A. Kharraz, WebGuard: Detecting Evasive Web Scanners via a Multi-Modal Forensics Engine. Under Review ACM Web Conference (WWW), 2026. Available as arXiv preprint arXiv:2412.07005

L. Rampersaud, **B. Ousat**, S. A. Akhavani, J. Zandi, S. Uluagac, A. Kharraz, Evaluating Security Checks Against Malicious Payloads with Forged Signatures. Accepted for IEEE 16th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2025.

M. A. Tofighi, **B. Ousat**, J. Zandi, E. Schafir, A. Kharraz, Constructs of Deceit: Exploring Nuances in Modern Social Engineering Attacks. In 21st Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), 2024.

Behzad Ousat, Dongsheng Luo, Amin Kharraz, Breaking the Bot Barrier: Evaluating Adversarial AI Against Multi-Modal Defenses. In the ACM Web Conference (WWW), 2024.

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

M. Soltani, **B. Ousat**, M. Jafari Siavoshani, A. H. Jahangir, An Adaptable Deep Learning-based Intrusion Detection System to Zero-day Attacks. Journal of Information Security and Applications, 2023.