

Behzad Ousat

✉ behzad.ost@gmail.com
in 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	01/2022 – Present
---	-------------------

ML/DL Pipeline Development

- Developed end-to-end ML pipelines using **Pandas**, **PyTorch**, and **Scikit-Learn** to collect and analyze billions of real-world noisy browser interaction artifacts, classifying human vs automated agents with 95% (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.

LLM and ML-based Adversarial Web Automation

- 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

- 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).

Tapsi - Platform Technical Team Lead Tehran	12/2017 – 10/2021
---	-------------------

Production Infrastructure Orchestration & Security

- **Led platform team** to migrate 60+ microservices to Kubernetes, **Coordinated** with backend teams, onboarded developers on technical workflows through workshops, and presented improvements to stakeholders.
- Maintained 99% uptime for microservices by operating infrastructure of over 100 **Ubuntu** servers for compute clusters and databases across **Kubernetes**, **PostgreSQL**, and **MongoDB**.
- Established **On-call Program** to handle ad hoc requests, shielding infrastructure engineers from interruptions.
- Reduced deployment errors and established automated rollouts by implementing **CI/CD** pipelines to include canary-testing, staging, and production environments utilizing **Bash** and **Ansible**.

Software Engineering & Monitoring

- 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%.
- 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.
- Designed and implemented a low-latency **WebSocket** service backed by **Redis** pub/sub to deliver critical data to mobile apps in real-time (<50ms), providing guaranteed delivery and engagement in high-traffic conditions.

Fraunhofer IDMT - Machine Learning Engineer Intern Germany	09/2019 – 12/2019
--	-------------------

- Built **Multimodal Modeling** and classification pipeline for studio scene frames by developing a Deep Learning pipeline (OpenCV and CNN) to analyze over 100 hours of news broadcast data with 95% accuracy.

SKILLS

Programming: Python, Node.JS, Java

Data Stores: PostgreSQL, MongoDB, RabbitMQ

DevOps: Ubuntu, Networks, Bash, Ansible

Monitoring: Prometheus, Grafana, Graylog

Machine Learning: PyTorch, Scikit-Learn, Tensorflow, Pandas

Orchestration: Github Actions, Kubernetes, Docker, MLFlow

Cloud: AWS EC2, Beanstalk, GCP AppEngine, Vertex AI

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 Gen AI	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

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 image processing workflows.	

SELECTED PUBLICATIONS

B. Ousat, L. Rampersaud, D. Bailey, N. Turkmen, S. Uluagac, A. Kharraz, Cracking the Web: Analyzing LLM-Based Browsers and Automated Solvers in the Web. To be Submitted to USENIX Security, 2026.

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

D. C. Hoang, **B. Ousat**, A. Kharraz, C. V. Nguyen, EnSolver: Uncertainty-Aware Ensemble Captcha Solvers with Theoretical Guarantees. Under Review IEEE Transactions on Pattern Analysis and Machine Intelligence, 2024. Available as arXiv preprint arXiv:2307.15180

L. Rampersaud, **B. Ousat**, C. Brown, S. Uluagac, A. Kharraz, On the Effectiveness of End-Users' Data Backup Practices Against Data Corruption. Accepted for IEEE 16th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2025.

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.

B. Ousat, M. A. Tofighi, A. Kharraz, An End-to-End Analysis of Covid-Themed Scams in the Wild. In the 18th ACM ASIA Conference on Computer and Communications Security (ASIACCS), 2023.

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.