Abdullah Garra

0525006769 | garra0702@gmail.com
linkedin.com/abdullahgarra | github.com/abdullahgarra

Education

B.Sc. Computer Science at **Tel-Aviv University**

M.Sc. Computer Science at **Tel-Aviv University** **GPA: 96** **Supervisor**: Dr.Mahmood Sharif
Thesis: Reliable Security-Incident Prediction from Text and Network measurements

Research & Projects

Forecasting Cyber Threats with LLMs — TAU (Thesis) (Submitting to **ESORICS 2026**)

- Designing and implementing a full pipeline to forecast cyber incidents based on monthly news data, malicious activity feeds, and network-level indicators.
- I processed the CC-NEWS archives with Hugging Face's DataTrove (filtering, deduplication, and cleaning) and uploaded the cleaned dataset to Hugging Face. [link]
- **Fine-tuned** Longformer (MLM); developed snapshotting and checkpointing for robust long runs.
- Built scalable distributed training system with PyTorch Distributed Data Parallel (DDP) across multiple GPUs.

Model Identification for Embedding-Based Retrieval (In Preparation)

- Developing input–output–level profiling methods for model fingerprinting under black-box and cross-model transfer settings.
- Investigating the stability and transferability of semantic similarity patterns across embedding models.

AdvEGI – Machine Learning with Graphs Course [GitHub]

- Adversarial Training & Transfer on EGI (**NeurIPS'21** revisit)
- Reproduced EGI on the airport-role benchmark; implemented a **PGD**-style score-and-flip adversarial pretraining that perturbs edges under budgeted constraints.
- Takeaways: transfer gains are inconsistent.
  Simple degree-aware baselines compete, suggesting EGI's "transfer" mostly reflects centrality signals rather than robust structure.

Layoff Prediction Language Model – NLP Course [GitHub]

- Developed a hybrid prediction model combining structured financial data and unstructured news data using BiLSTM and FinBERT to forecast layoff percentages with a Mean Absolute Error (MAE) of 8.74.
- Implemented advanced text processing techniques, including embedding-based filtering and cosine similarity ranking, to integrate financial news insights within various time windows.

DNS Port Randomization Analysis

- Developed a Linux-based authoritative nameserver using **BIND** (Berkeley Internet Name Domain) to facilitate testing of port randomization for a list of recursive resolvers.
- Used **Scapy** and **nslookup** scripts to execute experiments, querying recursive resolvers with random subdomains of the authoritative domain.
- Used **ZMap** and **Censys CLI** for large-scale scanning of the internet IP space.
- Implemented **MongoDB** for efficient mapping between sent and received requests, enabling analysis of method reliability (Scapy vs nslookup) across varying batch sizes and resolver order (iterative vs round-robin).

Extension for Phishing Email Detection [GitHub]

- Co-authored a technical report and a user study to document pipeline design, UX choices, and common error modes
- Developed a chrome extension for Gmail that uses machine learning models to identify phishing E-mails.
- Utilized Flask as the backend framework. Gained familiarity in **GCP** (Google Cloud Platform) services, JavaScript, machine learning techniques, and Gmail API while working on the project.
- Trained and methodologically compared the performance of different (classic) machine learning models.

Experience

Teaching Assistant, TAU February 2025 – Present

- Mentoring students through real-world ML-based security projects in:
  - Workshop on Usable Security and Privacy (Dr. Mahmood Sharif).
  - Workshop on Intrusion Detection with ML (Dr. David Movshovitz)

Software Project Grader, TAU April 2024 – October 2024

- Tested C and Python code implementing different variations of the K-Means algorithm, verifying correctness and using **Valgrind** to verify memory allocations.

Calculus for Mathematicians Tutor, TAU September 2022 –April 2023

- Provided 1:1 tutoring clarifying core topics and guiding homework and formal writing.
- Tailored study plans to each student while tracking progress in addition to preparing them for the final exams.

External Research

Between Reflection and Construction: AI as the New Orientalism November 2023

Co-authored with Dr. Hama Abu-Kishk and Dr. Michael Dahan (Mike)

- Collaborated with researchers in the social sciences to systematically query ChatGPT's API and analyze outputs in the context of cultural and geopolitical bias
- Designed and executed the automated querying methodology

Talks & Presentations

Israel Internet Association (ISOC-IL) Seminar at Reichman University, 2023

- Presented research methodology for "Between Reflection and Construction: AI as the New Orientalism," focusing on systematic prompting techniques to evaluate cultural bias in LLMs

Skills & Abilities

- **Languages:** Python, C, C++, Bash, Java, SQL
- **Frameworks & Tools**: PyTorch, HuggingFace, Flask, GCP, AWS, MongoDB, Scapy, ZMap, DDP, Git
- **Topics:** NLP, Machine Learning, Cybersecurity, RAG, Embedding Models, Distributed Training, Time-Series Forecasting, Networks
- **Languages:** Arabic (native), English (fluent), Hebrew (fluent)