Unat Teksen

unatteksen.com LinkedIn Github Google Scholar

Email : unatteksen@gmail.com
Mobile : +90 5382052020

Research Statement

My research interests lie in the alignment, explainability, and trustworthiness of language models (LMs). Additionally, I am focused on studying attacks and defenses in distributed machine learning models, an area I have previously worked on. My broader interests include exploring the intersection of privacy and LMs, as well as applying LMs to address real-world problems.

Education

Kadir Has University **2018 – 2023**

Bachelor of Science in Computer Engineering, Full Scholarship *Istanbul, Turkey*

GPA: 4.0/4.0 (Valedictorian)

Experience

Avinga **Sept. 2023 – Present**

Freelance Software Developer *Istanbul, Turkey & (remote) Serbia*

- Developing policy authorization tools leveraging REST APIs. Implementing and optimizing new gRPC & HTTP services to enhance system functionality.
- Delivering full-stack web solutions for the avinga.com CMS project. Providing end-to-end integration of CMS's with payment gateways, email platforms, and dealership systems, successfully serving over 20 clients.

Koç University **June 2022 – June 2024**

Research Intern *Istanbul, Turkey*

- Conducted research at **Koç University Cryptography, Security, and Privacy Research Group**, under the supervision of **Assoc. Prof. Alptekin Küpçü** and **Asst. Prof. Ercüment Çiçek**.
- Developed novel defensive mechanisms against attacks in privacy-preserving machine learning systems. Specifically, focusing on split learning frameworks implemented in **PyTorch**.
- Designed and implemented anomaly detection models in **scikit-learn** from scratch to detect and mitigate the impacts of a specific attack in a distributed and private deep learning model. Contributed as a **co-author** to research papers.
- Achieved **100% accuracy in detecting** all known attacks, and **21.8x and 50x faster** than the leading two leading approaches in existing literature.
- Conducted analysis of various attack vectors using **dimension reduction methods** (t-SNE, PCA).
- Tools and libraries: *PyTorch, scikit-learn, NumPy, Pandas, Matplotlib.*

ASELSAN **June 2022 – July 2022**

Software Engineering Intern *Ankara, Turkey*

- Worked at *Dpt. of Avionics Software* which designs and develops a graphical user interface for aircraft systems.
- Developed an **interface for the unit testing,** integrated with the specific aircraft's GUI, to facilitate acknowledgment and processing of protocol commands. ***C/C#*** *are used throughout the project.*

Kadir Has University **Nov. 2021 – June 2022**

Research Intern *Istanbul, Turkey*

- Worked on **dimension reduction methods** and graph-based manifold learning algorithms for open-source Sca-ML project supported by TÜBİTAK. The project *"Developing a New Method Based on Eigenvalue Distribution Slicing and Contour Integral for Manifold Learning and Analysis of Big Data"* was supervised by **Asst. Prof. E. Fatih Yetkin**.
- Implemented and utilized PETSc/SLEPc Python libraries, developing custom functions to solve **eigenvalue problems in dimensionality reduction methods**, including **PCA and SVD**.
- Tools and libraries: *scikit-learn, NumPy, Pandas, SciPy, PETSc/SLEPc, Matplotlib, Plotly, Seaborn*

Publications & Preprints

1. Ege Erdogan, **Unat Teksen**, M. Salih Celiktenyildiz, Alptekin Kupcu, A. Ercument Cicek. **"SplitOut: Out-of-the-Box Training-Hijacking Detection in Split Learning via Outlier Detection"**, 2023; arXiv:2302.08618. *International Conference on Cryptology And Network Security (CANS '24).*
2. Ege Erdogan, **Unat Teksen**, M. Salih Celiktenyildiz, Alptekin Kupcu, A. Ercument Cicek. **"Defense Mechanisms Against Training-Hijacking Attacks in Split Learning"**, 2023; arXiv:2302.08618v1.
3. **Unat Teksen**, Mert Yagmur, M. Buket Darici, Tamer Dag. **"Interpretability in Deep Learning-Based Cancer Detection: Effects of Augmentation and Image Processing"**, 2025; *[In writing phase]*

Honor & Awards

- **Valedictorian** - Ranked **1st** student in Kadir Has University
- **TÜBİTAK Star Scholarship** - Awarded for an internship in a funded project for 6 months
- **Merit-Based Full Scholarship (BSc)** - Awarded for B.Sc. education due to the performance in the National University Entrance Exam

Professional Activities

- **Reviewer at IEEE T-IFS** (IEEE Transactions on Information Forensics and Security)
- **Subreviewer at ESORICS 2023** (European Symposium on Research in Computer Security 2023)
- **Reviewer at TJEECS** (TUBITAK Turkish Journal of Electrical Engineering and Computer Sciences)

Projects

RAG Evaluation Pipeline + Reranker + HuggingFace Models | LangChain, Huggingface, RAGAS, LoRa [Github]
- This project includes RAG pipeline with HuggingFace open-source models, Cohere ReRank module and evaluation with RAGAS, scrapping of web pages with BS4 and RAG optimization script

Title Generator from Abstract with LLM & PEFT (LoRA) | Transformers, Huggingface, PyTorch, LoRa [Github]
- Fine-tuning of T5 & BART with arXiv CS-related articles. Training with LoRA, evaluation with rouge-score.

ML/NN Models from Scratch and Tutorials | Transformers, PyTorch [Github]
- Exploring and coding NN models (Transformers, CLIP, AE/VAE, etc.) from scratch that I am curious about.

dynbatcher - Dynamic Batch Size Dataloader Generator | PyTorch, matplotlib [Github] [PyPI]

LDA Topic Modeling for Bloomberg News | Gensim, NLTK, pyLDAvis, Pandas, Numpy [Github]

Social Media Platform with JWT Authentication | Java SpringBoot, React, MySQL, JWT, Axios, Maven, BS [Github]

Skills & Technical Strengths

Human Languages: Turkish *(native)*, English *(fluent)*, Italian *(elementary)*

Programming Languages: Python, Java, Go, JavaScript, C/C#, PHP, Matlab, CSS

Machine Learning/Data Science: PyTorch, scikit-learn, NumPy, Pandas, Matplotlib, LangChain

Web Development: Java Spring, Spring Security, React, jQuery, Bootstrap, Maven, SQL/MySQL, Tkinter, Swing

Typesetting: LaTeX

Certificates & Courses

- Sequence Models[1], Improving Deep Neural Networks (Hyperparameter Tuning, Regularization, and Optim.)[2], Neural Networks and Deep Learning[3], Machine Learning[4] (Coursera & DeepLearning.AI)
- CCNA: Introduction to Networks [5] (Cisco)

Activities

Social Media Content Creator & Event Organizer @Kadir Has University Social Support and Solidarity Community
- Designing and creating content specific to regular announcements and events for social media platforms. Volunteering in the organization of charity events.

Updated on November 28, 2024