





# Unat Teksen

 [unatteksen.com](https://unatteksen.com)  [LinkedIn](#)  [Github](#)  [Google Scholar](#)

Email : [unatteksen@gmail.com](mailto:unatteksen@gmail.com)

Mobile : +90 5382052020

## Research Statement

My research interests lie in security and privacy in machine learning, as well as trustworthy AI. 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 LLMs, HCI, and applying AI solutions to address real-world problems and social issues.

## 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

- 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.
- Developing policy authorization tools using REST APIs. Implementing and optimizing gRPC & HTTP services for system functionality. Contributed to the integration of the Spark data management into an e-commerce platform.

### 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 **Prof. Alptekin Küpçü** and **Asst. Prof.ERCÜMENT ÇİÇEK**.
- Developed novel defensive mechanisms against attacks in privacy-preserving machine learning systems. Specifically, focusing on split learning frameworks implemented in **PyTorch**. Prepared a repo on **Github**.
- 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 **The Scientific and Technological Research Council of Türkiye (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. 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 **1<sup>st</sup>** 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 National University Entrance Exam performance.

## 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]  
• Hugging Face open-source models, Cohere ReRank, BS4 scraping, RAGAS evaluation, and optimization.

**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.

**Title Generator from Abstract with LLM & PEFT (LoRA)**      [Transformers](#), [Huggingface](#), [PyTorch](#), [LoRa](#) [Github]

**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](#), [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 + Security, React, SQL/MySQL, Tkinter

## Certificates & Courses

---

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

## References

---

- **Prof. Alptekin Küpçü**, Koç University & Crypto, Security, Privacy Lab      [akupcu@ku.edu.tr](mailto:akupcu@ku.edu.tr)
- **Prof. Tamer Dag**, BSc Thesis Advisor      [tamer.dag@aum.edu.kw](mailto:tamer.dag@aum.edu.kw)
- **Prof. Taner Arsan**, Department Chair      [arsan@khas.edu.tr](mailto:arsan@khas.edu.tr)
- **Prof. Nima Jafari Navimipour**, Dpt. of Computer Eng.      [nima.navimipour@khas.edu.tr](mailto:nima.navimipour@khas.edu.tr)

## Activities

---

**Social Media Content Creator & Event Organizer**, [Kadir Has University Social Support and Solidarity Community](#)  
• Creating content for social media announcements and events; volunteering in charity event organization.

**Organizing Coding Contests & Problem Recitations**, [Kadir Has University Engineering Club](#)

*Updated on January 2, 2025*