Fatih Ilhan
Resume

School of Computer Science, College of Computing
Georgia Institute of Technology, Atlanta, GA, USA

e-mail: filhan@gatech.edu
web: fatih-ilhan.github.io
github: github.com/fatih-ilhan

Research Interests

- Memory/Computation-Efficient AI Systems
- Distributed/Federated Learning
- Edge-Cloud Computing
- Anomaly Detection, Time Series Prediction, Spatio-temporal Event Modeling

Academic Experience

Georgia Institute of Technology, Atlanta, GA, USA — August 2021 – Present

Ph.D. in Computer Science, CGPA: 3.88/4.00, Supervisor: Prof. Ling Liu

- Research focus areas: efficient inference for DNNs, memory-efficient finetuning for LLMs, federated learning, large language models, big data systems, adversarial machine learning
- Published nine papers in top venues such as CVPR, NeurIPS, WWW, WACV, ICDCS, ICDM
- Served as reviewer for CVPR, AAAI, ICML, ICDCS, IEEE TOIT
- Head TA for the Advanced Internet Systems and Applications course with 5 TAs and 100-150 students (January 2022 – Dec 2023)

Bilkent University, Ankara, Turkey — September 2019 – August 2021

M.Sc. in Electrical and Electronics Engineering, CGPA: 3.58/4.00, Supervisor: Prof. Serdar Kozat

- Thesis: Nonstationary Time Series Prediction with Markovian Switching RNNs
- Research focus areas: Nonstationary time series prediction, spatiotemporal event modeling, efficient learning for state-space models
- Published three papers in top IEEE journals, served as reviewer for IEEE TNNLS, IEEE TSP
- Served as grader for the Statistical Learning and Data Analytics, and Neural Networks courses

Nagoya University, Nagoya, Japan — April 2018 – August 2018

Exchange Program in Electrical and Electronics Engineering

- Studied intelligent systems for automobiles and traffic management systems.

Bilkent University, Ankara, Turkey — February 2015 – June 2019

B.S. in Electrical and Electronics Engineering, CGPA: 3.81/4.00

- Senior Project: 2D outdoor localization system completely independent of GPS.
- Undergraduate research experience on unsupervised video anomaly detection under the supervision of Asst. Prof. Hamdi Dibeklioglu and Prof. Serdar Kozat.

Ankara Science High School, Ankara, Turkey — September 2010 – June 2014

High School Degree, Natural Sciences Field, CGPA: 95.26/100

Industrial Experience

Research Scientist Intern
IBM Thomas J. Watson Research Center, Yorktown Heights, NY — May 2023 – Aug 2023
- Conducted research on efficient finetuning of large language models in resource-constrained environments

Research Scientist Intern
IBM Thomas J. Watson Research Center, Yorktown Heights, NY — May 2022 – Aug 2022
- Conducted research on computation-efficient federated learning under heterogeneous settings with resource-constrained devices (Filed a patent, and published two papers at CVPR23 and ICDCS23)

Machine Learning Engineer
DataBoss Analytics, Ankara, Turkey — June 2019 – July 2021
- Built end-to-end machine learning architectures for large-scale online temporal/spatio-temporal prediction and anomaly detection systems

- Worked in a DevOps environment managing purpose-built, distributable and scalable services.

Data Scientist
DataBoss Analytics, Ankara, Turkey August 2018 – June 2019
- Analyzed complex spatio-temporal data, including traffic, crime and weather data.
- Reported and presented the results to project managers, engineers and clients.

Intern Engineer
DataBoss Analytics, Ankara, Turkey January 2018 – March 2018
- Implemented models for face detection and panic detection in crowd scenes.

Intern Engineer
Roketsan, Ankara, Turkey June 2017 – July 2017
- Wrote a Labview program that enables communication with a GPS receiver and displays/records the position, velocity, heading and time data.
- Worked on integration of GPS and INS using Extended Kalman Filter.

Conference Papers

[C15] **F. Ilhan**, G. Su, S. F. Tekin, T. Huang, S. Hu, and L. Liu, "Resource-Efficient Transformer Pruning for Finetuning of Large Models", *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2024.

[C14] **F. Ilhan**, KH. Chow, S. Hu, T. Huang, S. F. Tekin, W. Wei, Y. Wu, M. Lee, R. Kompella, H. Latapie, G. Liu, L. Liu, "Adaptive Deep Neural Network Inference Optimization with EENet", *IEEE/CVF Winter Conference on Applications of Computer Vision (WACV)*, 2024.

[C13] S. Hu, T. Huang, **F. Ilhan**, S. F. Tekin, L. Liu, "Large Language Model-Powered Smart Contract Vulnerability Detection: New Perspectives", *IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS-ISA)*, 2023.

[C12] T. Huang, S. Hu, KH. Chow, **F. Ilhan**, S. F. Tekin and L. Liu, "Lockdown: Backdoor Defense for Federated Learning with Isolated Subspace Training", *Thirty-seventh Conference on Neural Information Processing Systems (NeurIPS)*, 2023.

[C11] W. Wei, L. Liu, KH. Chow, **F. Ilhan** and Y. Wu, "Model Cloaking against Gradient Leakage", *IEEE International Conference on Data Mining (ICDM)*, 2023.

[C10] **F. Ilhan**, G. Su, Q. Wang and L. Liu, "Scalable Federated Learning with System Heterogeneity", *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2023. *(demo)*

[C9] **F. Ilhan**, G. Su and L. Liu, "ScaleFL: Resource-Adaptive Federated Learning with Heterogeneous Clients", *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2023.

[C8] KH. Chow, L. Liu, W. Wei, **F. Ilhan** and Y. Wu, "STDLens: Securing Federated Learning Against Model Hijacking Attacks", *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2023.

[C7] **F. Ilhan**, S. F. Tekin, S. Hu, T. Huang, KH Chow, L. Liu, "Hierarchical Deep Neural Network Inference for Device-Edge-Cloud Systems", *ACM International World Wide Web Conference (WWW)*, 2023. *(poster)*

[C6] **F. Ilhan**, S. F. Tekin and B. Aksoy, "Spatio-Temporal Crime Prediction via Temporally Hierarchical Convolutional Neural Networks", *28th IEEE Signal Processing and Communications Applications Conference*, 2020.

[C5] **F. Ilhan**, N. M. Vural and S. S. Kozat, "LSTM-Based Online Learning with Extended Kalman Filter Based Training Algorithm", *28th IEEE Signal Processing and Communications Applications Conference*, 2020.

[C4] **F. Ilhan** and E. Mumcuoglu, "Performance Analysis of Semi-Supervised Learning Methods under Different Missing Label Patterns", *28th IEEE Signal Processing and Communications Applications Conference*, 2020.

[C3] **F. Ilhan**, S. F. Yilmaz and S. S. Kozat, "A Two-Stage Multi-Class Classification Approach Based on Anomaly Detection", *28th IEEE Signal Processing and Communications Applications Conference*, 2020. *(poster)*

[C2] N. M. Vural, B. Altas, **F. Ilhan** and S. S. Kozat, "Shortest Path Learning in Non-Stationary Environments via Online Convex Optimization", *28th IEEE Signal Processing and Communications Applications Conference*, 2020.

[C1] N. M. Vural, B. Altas, **F. Ilhan** and S. S. Kozat, "Online Shortest Path Learning via Convex Optimization", *28th IEEE Signal Processing and Communications Applications Conference*, 2020.

Journal Papers

[J3] **F. Ilhan**, O. Karaahmetoglu, I. Balaban and S. S. Kozat, "Markovian RNN: An Adaptive Time Series Prediction Network with HMM-based Switching for Nonstationary Environments", *IEEE Transactions on Neural Networks and Learning Systems*, 2021.

[J2] N. M. Vural, **F. Ilhan**, S. F. Yilmaz, S. Ergüt and S. S. Kozat, "Achieving Online Regression Performance of LSTMs with Simple RNNs", *IEEE Transactions on Neural Networks and Learning Systems*, 2021.

[J1] **F. Ilhan** and S. S. Kozat, "Modeling of Spatio-Temporal Hawkes Processes with Randomized Kernels", *IEEE Transactions on Signal Processing*, 2020.

Preprints

[P7] T. Huang, S. Hu, **F. Ilhan**, S. F. Tekin, W. Wei, and L. Liu, "Silencer: Pruning-aware Backdoor Defense for Decentralized Federated Learning", *under review*, 2024.

[P6] S. F. Tekin, **F. Ilhan**, T. Huang, S. Hu and L. Liu, "FusionShot: Boosting Few Shot Learners with Focal-Diversity Optimized Ensemble Method", *under review*, 2024.

[P5] KH. Chow, S. Hu, T. Huang, **F. Ilhan**, S. F. Tekin and L. Liu, "Diversity-driven Privacy Protection Masks Against Unauthorized Face Recognition", *under review*, 2024.

[P4] KH. Chow, **F. Ilhan**, W. Wei, Y. Wu, M. Lee, G. Liu, R. Kompella and L. Liu, "Focal Diversity-Optimized Object Detection Ensembles", *under review*, 2024.

[P3] Y. Wu, KH. Chow, S. Hu, **F. Ilhan**, W. Wei and L. Liu, "An Error Diversity Optimization Framework for Creating Efficient Ensemble Learning Systems", *under review*, 2024.

[P2] S. Hu, T. Huang, KH. Chow, **F. Ilhan**, S. F. Tekin and L. Liu, "Linking Ethereum Accounts with Pseudo-supervised Pre-trained Language Models", *under review*, 2024.

[P1] O. Karaahmetoglu, **F. Ilhan** and S. S. Kozat, "Unsupervised Online Anomaly Detection On Irregularly Sampled Or Missing Valued Time-Series Data Using LSTM Networks", 2020.

Awards and Honors

- Received the **191st** rank among 2M high school graduates in University Entrance Examination.
- Received the **80th** rank among 0.2M university graduates in ALES (National GRE).
- Full **TUBITAK Scholarship** for the M.Sc. studies.
- **JASSO Scholarship** for Exchange Program at Nagoya University.
- **Full Scholarship** from Bilkent University during M.Sc. and Ph.D. Studies.
- **Comprehensive Full Scholarship** from Bilkent University during B.S. studies.
- Bilkent University High Honor Student during B.S. Studies.

Projects

Source codes with more details are available on: *github.com/fatih-ilhan* and *github.com/git-disl*

Memory-Efficient Deep Learning Systems:

- ScaleFL: Scalable federated learning under resource heterogeneity with two-dimensional model scaling *(Available on: github.com/git-disl/scale-fl) (Demo: scalefl.herokuapp.com)*. [C9, C10]
- RECAP: Memory-efficient finetuning of large transformer models with pruning and sparse model updates. [C15]

Adaptive Neural Network Inference:

- EENet: Early-exit policy optimization for adaptive inference *(Available on: https://github.com/git-disl/EENet)*. [C14]
- HiDEC: Hierarchical inference for device-edge-cloud hierarchies with early exiting based on sample difficulty and prediction confidence. [C7]

Robust Deep Learning Systems:

- Defense algorithms against gradient leakage, model hijacking, and backdoor attacks. [C8, C11, C12, P5, P7]
- Efficient and robust ensemble learning systems. [P3, P4]

AI for Blockchain Security and Applications:

- Smart contract vulnerability detection using LLMs. *(Available on: https://github.com/git-disl/GPTLens)*. [C13]
- Linking Ethereum accounts over transaction networks using transformer-based models. [P2]

Time Series Prediction and Anomaly Detection:

- Predy: Worked in the design and development of a time series prediction framework for data from business domains such as economy, retail, and energy.
- Real-time Anomaly Detection: Worked on the design and development of an anomaly detection framework for time series and social media data.

Spatio-temporal Event Modeling:

- Spatio-temporal Crime Analysis and Prediction: Designed and implemented a spatio-temporal crime analysis and prediction framework with statistical and machine learning-based approaches.
- Hurricane Trajectory Prediction: Developed a deep learning architecture to predict hurricane trajectories. The introduced model is based on TrajGRU architecture and uses weather images and past trajectory data. *(Available on: github.com/fatih-ilhan/hurricane-hunters)*

Computer Vision Application Systems:

- Facial Attractiveness Estimation: Implemented a CNN-based deep learning architecture to estimate attractiveness from frontal facial images. Currently working on providing more interpretability to help the users to understand which factors (pose, emotion, illumination etc.) make their photos more attractive. *(Available on: github.com/fatih-ilhan/facial-attractiveness-prediction)*
- Facial Emotion Recognition: Implemented three machine learning and active appearance modeling-based architectures, including CNN-based and autoencoder-based approaches, for emotion recognition from frontal face images.

Electronics:

- LocInCampus: Designed and implemented a 2D outdoor localization system completely independent of GPS, for the industrial design project. The system uses TDOA and CDMA techniques to perform robust and precise localization.
- Touchpad Controlled Audio Processing Unit: Designed an audio processing system that consists of active filters and an amplifier controlled by a touchpad. Available features are volume control, equalizer, reverb, and delay.
- Levitating Light Bulb: Designed an LED light bulb powered with electromagnetic induction and levitated using electromagnetic suspension. A feedback control system based on magnetic field changes performs high-frequency switching to perform stabilization.
- Ion Craft: Designed and made an ion craft that levitates under high voltage between its poles. The designed system utilizes the Biefeld-Brown effect to create ion wind.

Miscellaneous:

- Hotel Booking Reservation System: A web application on Django for managing hotel reservations. *(Available on: github.com/fatih-ilhan/hotel_booking_system)*
- Pong Game with Gesture Control: Implemented Pong game on an 8x32 LED Matrix coded with assembly language on an 8051 microcontroller. Players can control their paddles using hand gestures. *(Available on: github.com/fatih-ilhan/pong)*
- Pacman Game: Implemented a full version of the classical game Pacman, coded with VHDL. *(Available on: github.com/fatih-ilhan/pacman)*
- Pixelium: Implemented a multi-functional painting application for the Android platform. In addition to standard Paint features, Pixelium provides additional features such as note-taking, child lock, and

alarm lock with drawing puzzles. *(Available on: github.com/fatih-ilhan/pixelium)*

SKILLS

Programming: Python, SQL, R, C++, Java, MATLAB, Assembly (8051), VHDL
Tools: Deep Learning Libraries (Tensorflow, PyTorch, Keras), MLOps Tools (Kubernetes, Polyaxon, MLFlow), Other Tools (Docker, Flask, Django, Kafka, Spark), Agile (Gitlab, Atlassian Tools)
Test Scores: TOEFL iBT: 108, GRE: 149/170/3.5
Languages: Turkish (Native), English (Advanced), Japanese (Lower intermediate ∼N4)

SOCIAL ACTIVITIES

- Bass Guitarist in "Parallel Park" (2022-2023)
- Bilkent University Music Club Member (2014-2017)
- Bass Guitarist in "Freud Goes Technical" (2014-2017)
- Bilkent IEEE Student Branch Member (2014-2016)
- Bilkent University Open Software and Internet Technologies Club Member (2014-2015)
- Ankara Science High School Electronics Club Member (2012-2014)
- Ankara Science High School Physics Olympiads Team Member (2010-2012)

HOBBIES

- Backpacking, overnight camping, being on the road
- Playing bass, discovering new music genres