

# Fatih İlhan

## Resume

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

*e-mail:* [filhan@gatech.edu](mailto:filhan@gatech.edu)  
*web:* [fatih-ilhan.github.io](http://fatih-ilhan.github.io)  
*github:* [github.com/fatih-ilhan](https://github.com/fatih-ilhan)  
*google scholar profile:* [DHB3X18AAAAJ](https://scholar.google.com/citations?user=DHB3X18AAAAJ)  
*orcid id:* [0000-0002-0173-7544](https://orcid.org/0000-0002-0173-7544)

RESEARCH INTERESTS	Efficient Inference/Fine-tuning for Large Language/Multi-modal Models, Computer Vision, Distributed/Federated Learning, Ensemble Learning, AI Safety and Alignment	
ACADEMIC EXPERIENCE	<b>Georgia Institute of Technology</b>	<b>Atlanta, GA, USA</b>
	Ph.D. in Computer Science, CGPA: 3.84/4.00, Supervisor: <a href="#">Prof. Ling Liu</a>	Aug 2021 – Present
	<ul style="list-style-type: none"><li>- Published 13 papers (5 as first author) in top venues such as CVPR, NeurIPS, ICLR, EMNLP.</li><li>- Served as reviewer for CVPR, ICCV, AAAI, ICML, ICDCS, IEEE PAMI and IEEE TOIT.</li><li>- Head TA for the Advanced Internet Systems course with 5 TAs and 100-150 students, selected as the outstanding Head TA for OMSCS program.</li></ul>	
	<b>Bilkent University</b>	<b>Ankara, Türkiye</b>
	M.Sc. in EEE, CGPA: 3.58/4.00, Supervisor: <a href="#">Prof. Serdar Kozat</a>	Sep 2019 – Aug 2021
	<ul style="list-style-type: none"><li>- Thesis: Nonstationary Time Series Prediction with Markovian Switching RNNs</li><li>- Published 3 papers in top IEEE journals, served as reviewer for IEEE TNNLS and IEEE TSP.</li><li>- TA for the courses: Statistical Learning and Data Analytics, Neural Networks.</li></ul>	
	B.Sc. in Electrical and Electronics Engineering, CGPA: 3.81/4.00	Aug 2014 – Jun 2019
	<ul style="list-style-type: none"><li>- Senior Project: GPS-independent outdoor localization system</li><li>- Specialization in signal processing, machine learning, communications</li><li>- Attended exchange program at Nagoya University, Japan (Spring 2018) and studied intelligent automobile systems.</li></ul>	
	<b>Ankara Science High School</b>	<b>Ankara, Türkiye</b>
	High School Degree, Science Track, CGPA: 95.26/100	Sep 2010 – Jun 2014
WORK EXPERIENCE	<b>IBM Thomas J. Watson Research Center</b>	<b>Yorktown Heights, NY</b>
	Researcher Intern, Mentors: Dr. Gong Su, Dr. Donna Dillenger	May-Aug 2022/23/24
	<ul style="list-style-type: none"><li>- Worked on memory-efficient decoding with KV cache compression for long-context inference with LLMs, filed a patent application.</li><li>- Researched efficient pruning for LLM fine-tuning through CPU/GPU workload balancing. Our work led to a publication at CVPR24.</li><li>- Worked on computation-efficient federated learning under heterogeneous settings with on-premise deployments, filed a patent. Our work led to two publications at CVPR23 and ICDCS23.</li></ul>	
	<b>DataBoss Analytics</b>	<b>Ankara, Türkiye</b>
	Machine Learning Engineer	Aug 2018 – Jul 2021
	<ul style="list-style-type: none"><li>- Built <a href="#">Predy.AI</a>, an end-to-end pipeline for real-time spatio-temporal prediction and anomaly detection, within a team of three engineers. Analyzed retail data from customer businesses to provide procurement and logistics insights, reduced consumption forecast errors by up to 40%.</li></ul>	
	<b>Roketsan</b>	<b>Ankara, Türkiye</b>
	Electronics Engineer Intern	Jun 2017 – Jul 2017
	<ul style="list-style-type: none"><li>- Integrated GPS and INS data using Extended Kalman Filter for navigation systems and enhanced localization precision by 85%. Built a Labview application for fast and simultaneous communication with eight GPS receivers.</li></ul>	

SKILLS	<p><b>Programming:</b> Python, C++, CUDA, Triton, SQL, R, Java, MATLAB, Assembly (8051), VHDL</p> <p><b>Tools:</b> Deep Learning Frameworks PyTorch, Keras, Tensorflow, vLLM), MLOps Tools (Kubernetes, Polyaxon, MLFlow), Other Tools (Docker, Flask, Django, Kafka, Spark), Agile (Gitlab, Atlassian Tools)</p> <p><b>Test Scores:</b> TOEFL iBT: 108, GRE: 149/170/3.5</p>
PROJECTS	<p>Source codes with more details are available on: <a href="https://github.com/git-disl">github.com/git-disl</a> and <a href="https://github.com/fatih-ilhan">github.com/fatih-ilhan</a></p> <p><b>Efficient Inference/Fine-tuning:</b></p> <ul style="list-style-type: none"> <li>- Memory-efficient federated learning/fine-tuning: ScaleFL [C12, C13], RECAP [C18], Fed4LM [P1]</li> <li>- Adaptive inference: HiDEC [C11], EENet [C17]</li> <li>- KV cache compression for long-context inference [P2, P3]</li> <li>- Efficient ensemble learning: LLM-TOPLA [C15]</li> </ul> <p><b>Robust Deep Learning Systems:</b></p> <ul style="list-style-type: none"> <li>- Defense algorithms against adversarial attacks. [C8, C9, C10, C14]</li> <li>- LLM safety and alignment [C16, C19]</li> </ul> <p><b>Time Series Prediction and Anomaly Detection:</b></p> <ul style="list-style-type: none"> <li>- Online time series analysis [J3, C1, C2, C5]</li> <li>- Spatio-temporal event prediction [J1, C6]</li> <li>- Anomaly detection [J2, C3]</li> </ul>
CONFERENCE PAPERS	<p>[C19] T. Huang, S. Hu, <b>F. Ilhan</b>, S. F. Tekin, and L. Liu, “Booster: Tackling Harmful Fine-tuning for Large Language Models via Attenuating Harmful Perturbation”, <i>International Conference on Learning Representations (ICLR)</i>, 2025. (oral)</p> <p>[C18] <b>F. Ilhan</b>, G. Su, S. F. Tekin, T. Huang, S. Hu, and L. Liu, “Resource-Efficient Transformer Pruning for Fine-tuning of Large Models”, <i>IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)</i>, 2024.</p> <p>[C17] <b>F. Ilhan</b>, 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”, <i>IEEE/CVF Winter Conference on Applications of Computer Vision (WACV)</i>, 2024.</p> <p>[C16] T. Huang, S. Hu, <b>F. Ilhan</b>, S. F. Tekin and L. Liu, “Lazy Safety Alignment for Large Language Models against Harmful Fine-tuning”, <i>Thirty-seventh Conference on Neural Information Processing Systems (NeurIPS)</i>, 2024.</p> <p>[C15] S. F. Tekin, <b>F. Ilhan</b>, T. Huang, S. Hu and L. Liu, “LLM-TOPLA: Efficient LLM Ensemble by Maximising Diversity”, <i>ACL Conference on Empirical Methods in Natural Language Processing (EMNLP Findings)</i>, 2024.</p> <p>[C14] KH. Chow, Sihao Hu, Tiansheng Huang, <b>Fatih Ilhan</b>, Wenqi Wei, and Ling Liu, “Diversity-driven Privacy Protection Masks Against Unauthorized Face Recognition”, <i>Privacy Enhancing Technologies Symposium (PETS)</i>, 2024</p> <p>[C13] <b>F. Ilhan</b>, G. Su, Q. Wang and L. Liu, “Scalable Federated Learning with System Heterogeneity”, <i>IEEE International Conference on Distributed Computing Systems (ICDCS)</i>, 2023. (demo)</p> <p>[C12] <b>F. Ilhan</b>, G. Su and L. Liu, “ScaleFL: Resource-Adaptive Federated Learning with Heterogeneous Clients”, <i>IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)</i>, 2023.</p> <p>[C11] <b>F. Ilhan</b>, S. F. Tekin, S. Hu, T. Huang, KH Chow, L. Liu, “Hierarchical Deep Neural Network Inference for Device-Edge-Cloud Systems”, <i>ACM International World Wide Web Conference (WWW)</i>, 2023. (poster)</p> <p>[C10] T. Huang, S. Hu, KH. Chow, <b>F. Ilhan</b>, S. F. Tekin and L. Liu, “Lockdown: Backdoor Defense for Federated Learning with Isolated Subspace Training”, <i>Thirty-seventh Conference on Neural Information Processing Systems (NeurIPS)</i>, 2023.</p> <p>[C9] KH. Chow, L. Liu, W. Wei, <b>F. Ilhan</b> and Y. Wu, “STDLens: Securing Federated Learning Against Model Hijacking Attacks”, <i>IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)</i>, 2023.</p> <p>[C8] W. Wei, L. Liu, KH. Chow, <b>F. Ilhan</b> and Y. Wu, “Model Cloaking against Gradient Leakage”, <i>IEEE International Conference on Data Mining (ICDM)</i>, 2023.</p>

	<p>[C7] S. Hu, T. Huang, <b>F. Ilhan</b>, S. F. Tekin, L. Liu, “Large Language Model-Powered Smart Contract Vulnerability Detection: New Perspectives”, <i>IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS-ISA)</i>, 2023.</p> <p>[C6] <b>F. Ilhan</b>, S. F. Tekin and B. Aksoy, “Spatio-Temporal Crime Prediction via Temporally Hierarchical Convolutional Neural Networks”, <i>28th IEEE Signal Processing and Communications Applications Conference</i>, 2020.</p> <p>[C5] <b>F. Ilhan</b>, N. M. Vural and S. S. Kozat, “LSTM-Based Online Learning with Extended Kalman Filter Based Training Algorithm”, <i>28th IEEE Signal Processing and Communications Applications Conference</i>, 2020.</p> <p>[C4] <b>F. Ilhan</b> and E. Mumcuoglu, “Performance Analysis of Semi-Supervised Learning Methods under Different Missing Label Patterns”, <i>28th IEEE Signal Processing and Communications Applications Conference</i>, 2020.</p> <p>[C3] <b>F. Ilhan</b>, S. F. Yilmaz and S. S. Kozat, “A Two-Stage Multi-Class Classification Approach Based on Anomaly Detection”, <i>28th IEEE Signal Processing and Communications Applications Conference</i>, 2020. (poster)</p> <p>[C2] N. M. Vural, B. Altas, <b>F. Ilhan</b> and S. S. Kozat, “Shortest Path Learning in Non-Stationary Environments via Online Convex Optimization”, <i>28th IEEE Signal Processing and Communications Applications Conference</i>, 2020.</p> <p>[C1] N. M. Vural, B. Altas, <b>F. Ilhan</b> and S. S. Kozat, “Online Shortest Path Learning via Convex Optimization”, <i>28th IEEE Signal Processing and Communications Applications Conference</i>, 2020.</p>
JOURNAL PAPERS	<p>[J3] <b>F. Ilhan</b>, O. Karaahmetoglu, I. Balaban and S. S. Kozat, “Markovian RNN: An Adaptive Time Series Prediction Network with HMM-based Switching for Nonstationary Environments”, <i>IEEE Transactions on Neural Networks and Learning Systems</i>, 2021.</p> <p>[J2] N. M. Vural, <b>F. Ilhan</b>, S. F. Yilmaz, S. Ergüt and S. S. Kozat, “Achieving Online Regression Performance of LSTMs with Simple RNNs”, <i>IEEE Transactions on Neural Networks and Learning Systems</i>, 2021.</p> <p>[J1] <b>F. Ilhan</b> and S. S. Kozat, “Modeling of Spatio-Temporal Hawkes Processes with Randomized Kernels”, <i>IEEE Transactions on Signal Processing</i>, 2020.</p>
PREPRINTS	<p>[P3] <b>F. Ilhan</b>, S. F. Tekin, S. Hu, T. Huang and L. Liu, “Neural Cache Compression for Memory-Efficient Inference with Large Vision-Language Models”, <i>in progress</i>, 2025.</p> <p>[P2] <b>F. Ilhan</b>, G. Su and L. Liu, “Memory-Efficient Decoding with KV Cache Compression for Long-Context LLMs”, <i>in progress</i>, 2025.</p> <p>[P1] <b>F. Ilhan</b>, S. F. Tekin, S. Hu, T. Huang and L. Liu, “Fed4LM: Efficient Federated Fine-tuning under Data and Resource Heterogeneity with a Mixture of Masked Adapters”, <i>in progress</i>, 2025.</p>
PATENTS	<p>[T2] <b>F. Ilhan</b>, G. Su, “Memory-Efficient Decoding with KV Cache Compression for Large Language Models”, (filed), 2025.</p> <p>[T1] <b>F. Ilhan</b>, G. Su, “Computation-Efficient Federated Learning System for Resource Heterogeneity”, P20240403701, 2023.</p>
AWARDS AND HONORS	<ul style="list-style-type: none"> <li>- Outstanding Head TA Award in OMS CS program by Georgia Tech (2024)</li> <li>- Full Scholarship from the Scientific and Technological Research Council of Türkiye for M.Sc. studies.</li> <li>- Full Scholarship from Bilkent University during B.Sc. and M.Sc. Studies.</li> <li>- 80th among 0.2M university graduates in ALES (National GRE).</li> <li>- JASSO Scholarship for Exchange Program at Nagoya University.</li> <li>- Bilkent University High Honor Student during B.Sc. Studies.</li> <li>- 191st among 2M high school graduates in University Entrance Examination.</li> </ul>