Onat Gungor

Postdoctoral Scholar at UC San Diego (UCSD)

Personal Website | Google Scholar

Contact

ogungor@ucsd.edu

Research Interests

Cyber Physical Systems, Internet of Things, Artificial Intelligence (AI), Cybersecurity, Secure AI, Efficient AI, Reliable AI

Academic Work Experience

UC San Diego, Computer Science and Engineering, La Jolla, CA

Postdoctoral Scholar **January 2024 – Current**

- Efficient, secure, and reliable AI for dependable operation of cyber-physical systems and edge intelligence
- Sample projects include 1) continual intrusion detection [DAC'25], 2) robust adversarial defenses [DATE'24], 3) resilient brain-inspired learning [ICCAD'24], 4) reliable AI evaluation frameworks [ICPR'24], 5) multi-modal context-aware LLMs [MASS'25], 6) resource-efficient ML solutions [ASP-DAC'25], and 7) efficient AI system deployment [SenSys'25].

UC San Diego & San Diego State University, Electrical and Computer Engineering, San Diego, CA

Graduate Student Researcher **Sept 2019 – Dec 2023**

- Robust and secure machine learning for IoT and cyber-physical systems

Education

PhD in Electrical and Computer Engineering, UC San Diego & San Diego State University, 2023.

- Thesis: Towards Intelligent, Secure, and Efficient Industrial Internet of Things
- Advisors: Tajana Rosing (UCSD) and Baris Aksanli (SDSU)

BS in Computer Science and Engineering, Ozyegin University, 2019.

BS in Industrial Engineering, Ozyegin University, 2018.

Peer-Reviewed Publications

(*Equal contribution, ^Students I mentored)

Journal Articles

1. J. Chen^*, **O. Gungor*,** Z. Shang^, T. Rosing, "SAGE: Sample-Aware Guarding Engine for Robust Adversarial IoT Intrusion Detection," IEEE TDSC, 2025. (under review)
2. E. Li^*, **O. Gungor*,** Z. Shang^, T. Rosing, "CITADEL: Continual Anomaly Detection for Enhanced Learning in IoT Intrusion Detection," IEEE IoTJ, 2025. (under review)
3. C. I. Kocal^, **O. Gungor,** T. Rosing, and B. Aksanli, "ReLATE+: Unified Framework for Adversarial Attack Detection, Classification, and Resilient Model Selection in Time-Series Classification," IEEE TSMC, 2025. (under review)
4. **O. Gungor,** T. Rosing, B. Aksanli, "STEWART: Stacking Ensemble for White-Box Adversarial Attacks Towards More Resilient Data-driven Predictive Maintenance," Comput. Ind., 2022. (Impact factor: 9.1) PDF
5. **O. Gungor,** T. Rosing, B. Aksanli, "DOWELL: Diversity-induced Optimally Weighted Ensemble Learner for Predictive Maintenance of Industrial Internet of Things Devices," IEEE IoTJ, 2021. (Impact factor: 10.6) PDF
6. **O. Gungor,** T. Rosing, B. Aksanli, "RESPIRE++: Robust Indoor Sensor Placement Optimization under Distance Uncertainty," IEEE Sens. J., 2021. (Impact factor: 4.5) PDF
7. **O. Gungor,** B. Aksanli, R. Aydogan, "Algorithm Selection and Combining Multiple Learners for Residential Energy Prediction," FGCS, 2019. (Impact factor: 6.1) PDF

Conference Proceedings

1. R. Sood^, **O. Gungor,** H. Wang^, T. Rosing, "AQUA-LLM: Evaluating Accuracy, Quantization, and Adversarial Robustness Trade-offs in LLMs for Cybersecurity Question Answering," 2025. (under review)
2. I. Kale^, **O. Gungor,** J. Zhou^, T. Rosing, "LIGHT-HIDS: A Lightweight and Effective Machine Learning-Based Framework for Robust Host Intrusion Detection," 2025. (under review)
3. Y. Tian^, X. Ren, Z. Wang, **O. Gungor,** X. Yu, T. Rosing, "DailyLLM: Context-Aware Activity Log Generation Using Multi-Modal Sensors and LLMs," IEEE MASS, 2025. (Acceptance Rate: 29%) PDF
4. S. Fuhrman^, **O. Gungor,** T. Rosing, "CND-IDS: Continual Novelty Detection for Intrusion Detection Systems," ACM/IEEE DAC, 2025. (Acceptance Rate: 23%) PDF

5. N. Pandey^, S. Kulkarni, D. Wang, **O. Gungor,** F. Ponzina, T. Rosing, "DPQ-HD: Post-Training Compression for Ultra-Low Power Hyperdimensional Computing," ACM GLSVLSI, 2025. (Acceptance Rate: 27%) PDF
6. C. I. Kocal^, **O. Gungor,** A. Tartz, T. Rosing, B. Aksanli, "ReLATE: Resilient Learner Selection for Multivariate Time-Series Classification Against Adversarial Attacks," IEEE CSR, 2025. PDF
7. J. Chen^*, **O. Gungor*,** Z. Shang^, E. Li^, T. Rosing, "DYNAMITE: Dynamic Defense Selection for Enhancing Machine Learning-based Intrusion Detection Against Adversarial Attacks," ACM/IEEE SPW, 2025. **(Best paper)** PDF
8. L. Zhang^, Q. Zhao, R. Wang, S. Bian, **O. Gungor,** F. Ponzina, T. Rosing, "ORCA: Offload Rethinking by Cloud Assistance for Efficient Environmental Sound Recognition on LPWANs," ACM SenSys, 2025. (Acceptance Rate: 18%) PDF
9. Y. Tian^, **O. Gungor,** X. Yu, T. Rosing, "Poster Abstract: Fine-grained Contextualized Activity Logs Generation based on Multi-Modal Sensor Data and LLM," ACM SenSys, 2025. PDF
10. **O. Gungor,** A. Rios, N. Ahuja, T. Rosing, "TS-OOD: An Evaluation Framework for Time-Series Out-of-Distribution Detection and Prospective Directions for Progress," AAAI AI4TS, 2025. **(Oral)** PDF
11. E. Li^, Z. Shang^, **O. Gungor,** T. Rosing, "SAFE: Self-Supervised Anomaly Detection Framework for Intrusion Detection," AAAI AICS, 2025. **(Oral)** PDF
12. L. Zhang^, **O. Gungor,** F. Ponzina, T. Rosing, "E-QUARTIC: Energy Efficient Edge Ensemble of Convolutional Neural Networks for Resource-Optimized Learning," ACM/IEEE ASP-DAC, 2025. (Acceptance Rate: 28%) PDF
13. **O. Gungor,** A. Rios, P. Mudgal, N. Ahuja, T. Rosing, "A Robust Framework for Evaluation of Unsupervised Time-series Anomaly Detection," ICPR, 2024. PDF
14. F. Asgarinejad^, F. Ponzina, **O. Gungor,** T. Rosing, B. Aksanli, "HDXpose: Harnessing Hyperdimensional Computing's Explainability for Adversarial Attacks," ACM/IEEE ICCAD, 2024. (Acceptance Rate: 24%) PDF
15. **O. Gungor,** T. Rosing, B. Aksanli, "A^2HD: Adaptive Adversarial Training for Hyperdimensional Computing-Based Intrusion Detection Against Adversarial Attacks," IEEE CSR, 2024. PDF
16. **O. Gungor,** E. Li^, Z. Shang^, Y. Guo^, J. Chen^, J. Davis^, T. Rosing, "Rigorous Evaluation of Machine Learning-based Intrusion Detection Against Adversarial Attacks," IEEE CSR, 2024. PDF
17. **O. Gungor,** T. Rosing, B. Aksanli, "ROLDEF: Robust Layered Defense for Intrusion Detection Against Adversarial Attacks," ACM/IEEE DATE, 2024. (Acceptance Rate: 25%) PDF
18. **O. Gungor,** T. Rosing, B. Aksanli, "Adversarial-HD: Hyperdimensional Computing Adversarial Attack Design for Secure Industrial Internet of Things," IEEE/ACM Safe Things, CPS-IoT Week, 2023. **(Best paper runner-up)** PDF
19. X. Yu, M. Zhou, F. Asgarinejad^, **O. Gungor,** B. Aksanli, T. Rosing, "Private and Secure Learning at the Edge with Hyperdimensional Computing," ACM/IEEE DAC, 2023. PDF
20. M. Timken^, **O. Gungor,** T. Rosing, B. Aksanli, "Analysis of Machine Learning Algorithms for Cyber Attack Detection in SCADA Power Systems," IEEE SmartNets, 2023. PDF
21. **O. Gungor,** T. Rosing, B. Aksanli, "HD-I-IoT: Hyperdimensional Computing for Resilient Industrial Internet of Things Analytics," ACM/IEEE DATE, 2023. (Acceptance Rate: 25%) PDF
22. **O. Gungor,** T. Rosing, B. Aksanli, "DENSE-DEFENSE: Diversity Promoting Ensemble Adversarial Training Towards Effective Defense,", IEEE SENSORS, 2022. PDF
23. **O. Gungor,** T. Rosing, B. Aksanli, "CAHEROS: Constraint-Aware Heuristic Approach for Robust Sensor Placement," IEEE SENSORS, 2021. PDF
24. **O. Gungor,** T. Rosing, B. Aksanli, "ENFES: Ensemble Few-Shot Learning for Intelligent Fault Diagnosis with Limited Data," IEEE SENSORS, 2021. PDF
25. **O. Gungor,** T. Rosing, B. Aksanli, "OPELRUL: Optimally Weighted Ensemble Learner for Remaining Useful Life Prediction," IEEE ICPHM, 2021. PDF
26. **O. Gungor,** J. Garnier^, T. Rosing, B. Aksanli, "LENARD: Lightweight Ensemble Learner for Medium-term Electricity Consumption Prediction," IEEE SmartGridComm, 2020. PDF
27. **O. Gungor,** T. Rosing, B. Aksanli, "RESPIRE: Robust Sensor Placement Optimization in Probabilistic Environments," IEEE SENSORS, 2020. **(Best paper nominee)** PDF
28. **O. Gungor,** U. Cakan, R. Aydogan, P. Ozturk, "Effect of Awareness of Other Side's Gain on Negotiation Outcome, Emotion, Argument and Bidding Behavior," IJCAI ACAN, 2019. **(Best paper)** PDF

Honors and Awards

- Best paper, ACM/IEEE Internet of SafeThings, May 2025
- Best paper runner-up, ACM/IEEE Internet of SafeThings, May 2023
- San Diego State University, University Graduate Fellowship, August 2021

- Best paper nominee, IEEE SENSORS Conference, October 2020
- Best student paper, International Workshop on Agent-based Complex Automated Negotiations (ACAN), August 2019
- Ozyegin University, Computer Science and Engineering High Honor Degree, June 2019
- Ozyegin University, Valedictorian Award, June 2018

Industry Collaborations & Research Centers

- ***Intel Labs*** - Time-series Anomaly Detection and Out-of-Distribution Detection
- ***Google*** - LLM-Powered Personal Agents for Health Monitoring
- ***Lawrence Berkeley Lab*** - Automated large-scale network traffic classification
- *Jump 2*.0, SRC & DARPA Co-Sponsored Research Centers: PRISM and CoCoSys

Invited Talks

- *Continual Self-supervised Learning for Robust IoT Intrusion Detection,* SRC TECHCON, Sept. 2025
- *Collaborative Intelligence for Securing the IoT: Robust, Adaptive, and Secure AI-Driven Intrusion Detection Systems*, SRC JUMP 2.0 CoCoSys Theme 4 Meeting (Collaborative Intelligence), May 2025.
- *AI-Driven Cybersecurity: Advancing Intrusion Detection, LLM Security and Time-Series Anomaly Detection,* Invited Talk, Cisco Foundation AI Group, April 2025.

Teaching

Instructor

- *Software Tools and Techniques*, UCSD CSE 15L. Fa23, Sp22
- *Components and Design Techniques for Digital Systems*, UCSD CSE 140. Su22

Teaching Assistant

- *Embedded Systems Programming*, SDSU COMPE 375. Su21, Su22
- *Components and Design Techniques for Digital Systems*, UCSD CSE 140. Wi22

Guest Lecturer

- *Introduction to Embedded Systems*, UCSD CSE 147. Wi25
- *Cyber-Physical Systems*, SDSU COMPE 596. Sp23

Mentoring

I have mentored more than 30 students since 2020; selected mentees are listed below. († URM students)

- Nilesh Pandey (PhD): Efficient and Scalable Machine Learning for Edge Computing; **Publication: GLSVLSI'25**
- Ye Tian (PhD): Multimodal LLMs and Physical World Comprehension; **Publications: MASS'25, SenSys'25**
- Fatemeh Asgarinejad† (PhD): Hyperdimensional Computing Against Adversarial Attacks; **Publication: ICCAD'24**
- Sean Fuhrman (MS): Continual Novelty Detection for Network Intrusion Detection; **Publication: DAC'25**
- Le Zhang (MS): Efficient Edge AI for Resource-Optimized Learning; **Publications: SenSys'25, ASPDAC'25**
- Ipek Kocal† (MS): Resilient Time-series Classification Against Adversarial Attacks; **Publication: CSR'25**
- Mitchell Timken (MS): ML for Cyber Attack Detection in SCADA Power Systems; **Publication: SmartNets'23**
- Jing Chen (BS): Dynamic Defense Design for ML-based IDS Against Adversarial Attacks; **Publication: SPW'25**
- Elvin Li, Charlie Shang (BS): Self-supervised Continual Learning for Robust Intrusion Detection; **Publication: AICS'25**
- Ishaan Kale, Jiasheng Zhou (BS): Lightweight and Effective Anomaly-based Host Intrusion Detection
- Roshan Sood, Harry Wang (BS): Adversarially Robust LLM-Based Cybersecurity Question Answering
- Matilda Gaddi† (BS): Adaptive Edge-Cloud Framework for Cybersecurity Question Answering Using LLMs
- Johnathan Davis†, Yutong Guo (BS): ML-based Intrusion Detection Against Adversarial Attacks; **Publication: CSR'24**
- Jake Garnier (BS): Ensemble Learner for Electricity Consumption Prediction; **Publication: SmartGridComm'20**

Academic Service and Outreach

- **Journal Reviewer:** IEEE Internet of Things Journal, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Industrial Informatics, IEEE Transactions on Industrial Electronics, IEEE Transactions on Network and Service Management
- **Conference Reviewer:** ASPLOS'25, DATE'25, ECAI'24-25, MICRO'24, CODES+ISSS'23, DAC'23, SENSORS'22
- **Research Outreach Programs:** ENLACE bi-national summer research program, Early Research Scholars Program (ERSP)