

# Yujin Choi

The College of Computing and Data Science, Nanyang Technological University | [cs-yujin.choi@ntu.edu.sg](mailto:cs-yujin.choi@ntu.edu.sg)

## RESEARCH POSITIONS

---

- Apr. 2026  
– Present      **Postdoctoral Researcher**, Nanyang Technological University, Singapore  
*The College of Computing and Data Science*  
Host: Prof. Jaehong Yoon
- Mar. 2026  
– Present      **Postdoctoral Researcher**, Ulsan National Institute of Science and Technology  
*Department of Industrial Engineering*  
Mentor: Prof. Saerom Park

## EDUCATION

---

- Mar. 2021  
– Feb. 2026      **Ph.D.** in Industrial Engineering, **Seoul National University**, Seoul, Korea  
Dissertation: *Trustworthy Generative Models: from Privacy to Fairness*  
Advisor: Prof. Jaewook Lee | GPA: 3.84 / 4.3
- Mar. 2017  
– Feb. 2021      **B.Eng.** in Industrial Engineering & **B.Sc.** in Mathematics (Double Major)  
**Yonsei University**, Seoul, Korea  
GPA: 3.91 / 4.3

## PUBLICATIONS

---

(†: equal contribution.; underline = 1<sup>st</sup>/corr. author.)

### Journals

- [J8] Y. Choi, J. Park, Y. Park, J. Lee, & J. Byun. Differentially Private Upsampling for Enhanced Anomaly Detection in Imbalanced Data. *Engineering Applications of Artificial Intelligence* (2026). IF: 8.0, top 2.8%
- [J7] Y. Choi, D. Kim, & J. Lee. Temporal Consistency Ensemble Empirical Mode Decomposition for Forecasting Practical Metal Price. *Engineering Applications of Artificial Intelligence*, 158, 111490 (2025). IF: 8.0, top 2.8%
- [J6] J. Byun, Y. Choi, & J. Lee. Improving the Utility of Differentially Private Clustering through Dynamical Processing. *Pattern Recognition*, 157, 110890 (2025). IF: 7.6, top 9.0%
- [J5] J. Byun, Y. Choi, J. Lee, & S. Park. Privacy-Preserving Inference Resistant to Model Extraction Attacks. *Expert Systems with Applications*, 256, 124830 (2024). IF: 7.5, top 6.6%
- [J4] J. Park, H. Kim, Y. Choi, W. Lee, & J. Lee. Fast Sharpness-Aware Training for Periodic Time Series Classification and Forecasting. *Applied Soft Computing*, 144, 110467 (2023). IF: 6.6, top 13.7%
- [J3] J. Byun, S. Park, Y. Choi, & J. Lee. Efficient Homomorphic Encryption Framework for Privacy-Preserving Regression. *Applied Intelligence*, 53(9), 10114–10129 (2023). IF: 3.5, top 41.2%
- [J2] Y. Choi, J. Park, J. Lee, & H. Kim. Exploring Diverse Feature Extractions for Adversarial Audio Detection. *IEEE Access*, 11, 2351–2360 (2023). IF: 3.6, top 35.0%
- [J1] J. Park, Y. Choi, J. Byun, J. Lee, & S. Park. Efficient Differentially Private Kernel Support Vector Classifier for Multi-Class Classification. *Information Sciences*, 619, 889–907 (2023). IF: 6.8, top 8.1%

### Top Conferences

- [C8] H. Kim, J. Park, Y. Choi, & J. Lee. Stability Analysis of Sharpness-Aware Minimization. *International Conference on Machine Learning (ICML)*, accepted (2026)
- [C7] J. Park, S. Lee, W. Jeong, Y. Choi, & J. Lee. Leveraging Priors via Diffusion Bridge for Time Series Generation. *SIGKDD Conference on Knowledge Discovery and Data Mining (KDD) 2026*
- [C6] J. Park, Y. Choi, & J. Lee. Multi-Class Support Vector Machine with Differential Privacy. *Advances in Neural Information Processing Systems (NeurIPS) 2025*
- [C5] Y. Choi†, Y. Park†, J. Byun, J. Lee, & J. Park. Safeguarding Privacy of Retrieval Data against Membership Inference Attacks: Is This Query Too Close to Home?. *Findings of EMNLP 2025, Suzhou, China*
- [C4] J. Park†, Y. Choi†, & J. Lee. In-Distribution Public Data Synthesis with Diffusion Models for Differentially Private Image Classification. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern*

*Recognition (CVPR), 12236–12246 (2024)*

- [C3] **Y. Choi**<sup>†</sup>, J. Park<sup>†</sup>, H. Kim, J. Lee, & S. Park. Fair Sampling in Diffusion Models through Switching Mechanism. *Proceedings of the AAAI Conference on Artificial Intelligence (AAAI)*, 38(20), 21995–22003 (2024)
- [C2] H. Kim, J. Park, **Y. Choi**, & J. Lee. Fantastic Robustness Measures: The Secrets of Robust Generalization. *Advances in Neural Information Processing Systems (NeurIPS)*, 36, 48793–48818 (2023)
- [C1] J. Park, H. Kim, **Y. Choi**, & J. Lee. Differentially Private Sharpness-Aware Training. *International Conference on Machine Learning (ICML)*, 27204–27224 (2023)

## PATENTS

---

- 2025.05.28 Clustering Method and Apparatus Supporting Differential Privacy  
Reg. No. 10-2815746 | App. No. 1020220185186, filed 2022.12.27
- 2023.06.07 Apparatus and Method for Learning Differential Privacy Multi-Classification Based on Kernel Support Vector  
App. No. 10-2023-0073178
- 2023.07.05 Method and System for Detecting Adversarial Speech Example  
App. No. 1020230087024

## PREPRINTS & UNDER REVIEW

---

- [5] **Y. Choi**, J. Park, Y. Park, & J. Lee. Multiple Hyperplanes with Dual Encoding Support Vector Machine for Industrial Anomaly Detection. *2nd major revision, IEEE Transactions on Industrial Informatics* (IF: 9.9)
- [4] **Y. Choi**, J. Park, J. Byun, & J. Lee. Leveraging Programmatically Generated Synthetic Data for Differentially Private Diffusion Training, *Under review, Pattern Recognition* (IF: 7.6)
- [3] J. Park, **Y. Choi**, Y. Park, & J. Lee. Privacy-Preserving Asymmetric Banach Kernel Encoding for Support Vector Classification. *Submitted to Pattern Recognition* (IF: 7.6)
- [2] H. Kim, J. Park, **Y. Choi**, S. Lee, & J. Lee. BayesNAM: Leveraging Inconsistency for Reliable Explanations. *Under review, Pattern Recognition* (IF: 7.6)
- [1] H. Kim, J. Park, W. Lee, J. Lee, & **Y. Choi**. Exploring the Effect of Multi-Step Ascent in Sharpness-Aware Minimization. *Submitted to IEEE Access* (IF: 3.6)

## SCHOLARSHIPS AND FELLOWSHIPS

---

- 2025 Youlchon AI Scholarship, Youlchon AI Star
- 2023–2025 Doctoral Student Research Grant, Ministry of Science and ICT, Korea (Graduate Research Fellowship in Science and Engineering)
- 2019–2020 National Science and Technology Scholarship (full tuition), Ministry of Science, Korea

## TEACHING EXPERIENCE

---

### Lecturer

- Spring 2025 Financial Machine Learning, Soongsil University, Seoul, Korea
- Fall 2024 Financial Programming 2, Soongsil University, Seoul, Korea

### Teaching Assistant (TA), Industrial Engineering (Prof. Jaewook Lee), SNU

- 2022 Mathematical Methods for Industrial Management, Seoul National University

### TA & Instructor, Corporate Education Programs, SNU

- 2023–2024 HD Hyundai: Nonlinear Time Series Analysis
- 2022 Woori Bank: Big Data Analysis with Python and Deep Learning with PyTorch
- 2022–2024 SNU Big Data FinTech: Optimization and Machine Learning
- 2024–2025 SNU Big Data AI CEO Program
- 2021–2025 Samsung Data Scientist for Device Solution: Optimization
- 2021–2022 Samsung Data Scientist for Device Solution: Linear Algebra
- Samsung Best TA Award, 2021**

## REFERENCES

---

- Jaewook Lee** Professor of Industrial Engineering, Seoul National University  
[jaewook@snu.ac.kr](mailto:jaewook@snu.ac.kr)
- Saerom Park** Assistant professor of Industrial Engineering, UNIST  
[srompark@unist.ac.kr](mailto:srompark@unist.ac.kr)
- Hoki Kim** Assistant professor of Industrial Security, Chung-Ang University  
[hokikim@cau.ac.kr](mailto:hokikim@cau.ac.kr)