Curriculum Vitae

PERSONAL DATA

Full name	Yujin Choi
Affiliation	The College of Computing and Data Science, Nanyang Technological University
Email	cs-yujin.choi@ntu.edu.sg

PROFESSIONAL EXPERIENCE

April. 2026 - Current: Postdoctoral Researcher
Nanyang Technological University, Singapore
The College of *Computing and Data Science*
Host: Prof. Jaehong Yoon

Mar. 2026 - Current: Postdoctoral Researcher
Ulsan National Institute of Science and Technology
Department of *Industrial Engineering*
Mentor: Prof. Saerom Park

EDUCATION

Mar. 2021 - Feb. 2026: Seoul National University, Seoul, Korea
Ph.D. candidate *in Industrial Engineering*
Advisor: Prof. Jaewook Lee
Cumulative GPA *3.84/4.3*
Dissertation:
Trustworthy Generative Models: from Privacy to Fairness

Mar. 2017 - Feb. 2021: Yonsei University, Seoul, Korea
Bachelor of Engineering *in Industrial Engineering*
Bachelor of Science *in Mathematics (Double Major)*
Cumulative GPA *3.91/4.3*

PUBLICATIONS

[Journals]

[J1] **Choi, Y.**, Park, J., Park, Y., Lee, J., & Byun, J. (2026). Differentially Private Upsampling for Enhanced Anomaly Detection in Imbalanced Data, *Engineering Applications of Artificial Intelligence*. **(IF: 8.0, top 2.8%)**

[J2] **Choi, Y.,** Kim, D., & Lee, J. (2025). Temporal Consistency Ensemble Empirical Mode Decomposition for forecasting practical metal price, *Engineering Applications of Artificial Intelligence*, *158*, 111490. **(IF: 8.0, top 2.8%)**

[J3] **Choi, Y.**, Park, J., Lee, J., & Kim, H. (2023). Exploring diverse feature extractions for adversarial audio detection. *IEEE Access*, *11*, 2351-2360. **(IF: 3.6, top 35.0%)**

[J4] Byun, J., **Choi, Y.**, & Lee, J. (2025). Improving the utility of differentially private clustering through dynamical processing. *Pattern Recognition*, *157*, 110890. **(IF: 7.6, top 9.0%)**

[J5] Byun, J., **Choi, Y.**, Lee, J., & Park, S. (2024). Privacy-preserving inference resistant to model extraction attacks. *Expert Systems with Applications*, *256*, 124830. **(IF: 7.5, top 6.6%)**

[J6] Park, J., **Choi, Y.**, Byun, J., Lee, J., & Park, S. (2023). Efficient differentially private kernel support vector classifier for multi-class classification. *Information Sciences*,*619*, 889-907. **(IF: 6.8, top 8.1%)**

[J7] Park, J., Kim, H., **Choi, Y.**, Lee, W., & Lee, J. (2023). Fast sharpness-aware training for periodic time series classification and forecasting. *Applied Soft Computing*, *144*, 110467. **(IF: 6.6, top 13.7%)**

[J8] Byun, J., Park, S., **Choi, Y.**, & Lee, J. (2023). Efficient homomorphic encryption framework for privacy-preserving regression. *Applied Intelligence*, 53(9), 10114-10129. **(IF: 3.5, top 41.2%)**

[Top Conferences]

[C1] **Choi, Y.***, Park, Y.*, Byun, J., Lee, J., & Park, J. (2025). Safeguarding Privacy of Retrieval Data against Membership Inference Attacks: Is This Query Too Close to Home?. In *Findings of the Association for Computational Linguistics: EMNLP 2025, pages 8241–8258, Suzhou, China. Association for Computational Linguistics.*

[C2] **Choi, Y.***, Park, J.*, Kim, H., Lee, J., & Park, S. (2024, March). Fair sampling in diffusion models through switching mechanism. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 38, No. 20, pp. 21995-22003).

[C3] Park, J.*, **Choi, Y.***, & Lee, J. (2024). In-distribution Public Data Synthesis with Diffusion Models for Differentially Private Image Classification. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 12236-12246).

[C4] Park, J., **Choi, Y.**, & Lee, J. (2025). Multi-Class Support Vector Machine with Differential Privacy*., accepted for Advances in Neural Information Processing Systems*

[C5] Park, J., Kim, H., **Choi, Y**., & Lee, J. (2023, July). Differentially private sharpness-aware training. In *International Conference on Machine Learning* (pp. 27204-27224). PMLR.

[C6] Kim, H., Park, J., **Choi, Y.**, & Lee, J. (2023). Fantastic robustness measures: The secrets of robust generalization. *Advances in Neural Information Processing Systems*, *36*, 48793- 48818.

[C7] Park, J., Lee, S., Jeong, W., **Choi, Y.**, & Lee, J. (2024). Leveraging priors via diffusion bridge for time series generation. Accepted for *KDD 2026.*

*: equal contribution

PATENT

[1] Clustering method and apparatus supporting differential privacy, Application No. 1020220185186, filed 2022.12.27, Registration No. 10-2815746, registered 2025.05.28

[2] Apparatus and Method for Learning Differential Privacy Multi-Classification Based on Kernel Support Vector, Application No. 10-2023-0073178, filed 2023-06-07

[3] Method and system for detecting adversarial speech example, Application No. 1020230087024, filed 2023.07.05

PREPRINT AND UNDER REVIEW PAPERS

[1] **Choi, Y.**, Park, J., Byun, J., & Lee, J. (2024). Leveraging Programmatically Generated Synthetic Data for Differentially Private Diffusion Training. *arXiv preprint arXiv:2412.09842.*

[2] **Choi, Y.**, Park, J., Park, Y., & Lee, J. (2025). Multiple Hyperplanes with Dual Encoding Support Vector Machine for Industrial Anomaly Detection, *2nd major revision at IEEE Transactions on Industrial Informatics.*

[3] Kim, H., Park, J., Lee, W., Lee, J., & **Choi, Y.** (2023). Exploring the Effect of Multi-step Ascent in Sharpness-Aware Minimization. *arXiv:2302.10181., submitted to IEEE Access.*

[4] Park, J., **Choi, Y.**, Park, Y., & Lee, J. (2025). Privacy-Preserving Asymmetric Banach Kernel Encoding for Support Vector Classification, *submitted to Pattern Recognitions.*

[5] Kim, H., Park, J., **Choi, Y.**, Lee, S., & Lee, J. (2024). BayesNAM: Leveraging Inconsistency for Reliable Explanations. *arXiv preprint arXiv:2411.06367., submitted to Pattern Recognitions* .

[6] Kim, H., Park, J., **Choi, Y.**, & Lee, J. (2023). Stability Analysis of Sharpness-Aware Minimization. *arXiv preprint arXiv:2301.06308., under review at IEEE Transactions on Pattern Analysis and Machine Intelligence.*

SCHOLARSHIP AND FELLOWSHIPS

[Scholarship]

- National Science and Technology Scholarship (full tuition), Ministry of Science, Korea, 2019-2020
- Youlchon AI Scholarship, Youlchon AI Star, 2025

[Fellowship]

- Doctoral Student Research Grant, Ministry of Science and ICT, Korea (Graduate Research Fellowship in Science and Engineering), 2023-2025

LECTURES AND TEACHING ASSISTANT EXPERIENCE

[Lecturer]

- Financial Programming 2, Soongsil University (2nd semester, 2024)
- Financial Machine Learning, Soongsil University (1st semester, 2025)

[Teaching Assistant]

- **Industry training programs**
  - Samsung Data Scientist for Device Solution for Prof. Jaewook Lee
    - Optimization and Linear Algebra (2021-2022) **- Best TA Award, 2021**
    - Optimization (2023-2025)
  - Woori Bank: Big data analysis with Python and deep learning with PyTorch (2022**)**
  - HD Hyundai: Nonlinear Time Series Analysis (2023-2024)
- **National training programs**
  - SNU Big-Data FinTech: Optimization and Machine Learning for Prof. Jaewook Lee (2022-2024)
  - Big Data AI CEO Program (2024-2025)
- **University Courses**
  - Mathematical Methods for Industrial Management, Seoul National University (2nd semester, 2022)