Saeyeon Hong

sally99h@gmail.com | LinkedIn | saeyeonhong.github.io/

EDUCATION

Ewha Womans University **Seoul, Korea**
MS in Artificial Intelligence | Advisor: Se Eun Oh Mar 2025 – Present
Selected Course: Deep Learning Security, Information Security, Computer Vision(Intro & Special Topics)

Ewha Womans University **Seoul, Korea**
BE in Mechanical and Biomedical Engineering Mar 2019 – Aug 2024

Hong Kong Baptist University **Kowloon Tong, Hong Kong**
Exchange Student Program Sep 2022 – May 2023

RESEARCH INTERESTS

- Network security anonymity systems and traffic analysis
- Privacy focus on privacy risks in machine learning systems.

PUBLICATIONS

Scalable Tor Traffic Correlation Attack via Approximate Nearest Neighbor Search Jun 2026
Saeyeon Hong, Hyewon Kim, Saidur Rahman Mohammad, Se Eun Oh CISC-S (in Korean)

PRESENTATIONS

LLM Guided Adversarial Feature-to-Executable Malware Generation Dec 2025
Saeyeon Hong, Hyejin Woo, Md Mahmuduzzaman Kamol, Se Eun Oh, Md Saidur Rahman ACSAC

RESEARCH EXPERIENCE

Scalable Tor Traffic Correlation Attack via Approximate Nearest Neighbor Search Sep 2025 – Jun 2026

- Reframed pairwise matching in Tor end-to-end correlation attacks as an approximate nearest neighbor search task
- Reduced complexity from $O(N^2)$ to $O(N \log N)$ using GPU-accelerated CAGRA and HNSW indexing
- Analyzed the Genuine Tor Traces dataset to quantify the realistic traffic scale an adversary must handle
- Proposed a traffic-scale-focused threat model for Tor traffic correlation attacks

Duration Loss as a privacy proxy in Text-to-Speech Model Jan 2025 – May 2026

- Investigated whether duration prediction loss leaks training membership in TTS models
- Conducted membership inference attacks using speaker embeddings and alignment-based duration signals
- Surveyed the evolution of TTS architectures across autoregressive, non-autoregressive, and duration-based models

KV Cache in AutoPyTorch Sep 2024 – Dec 2024

AutoML Lab, Leibniz University of Hannover Hannover, Germany

- Implemented key–value caching for self-attention blocks in AutoPyTorch decoders (Transformer, TCN, and LSTM)
- Performed computational complexity analysis of the caching mechanism, reducing time complexity from $O(N^2) \rightarrow O(N)$ for Transformers and from O(2^L) → O(L) for TCN-based decoders

WORK EXPERIENCE

Machine Learning Engineer Intern Jun 2024 – Aug 2024

FPT Software Hanoi, Vietnam

- Develop Text-to-SQL for processing natural language to generate SQL Script by pipelining LLM, OpenSearch and MSSQL
- Construct the context RAG pattern with text-embedding the documents by BERT on OpenSearch with kNN Search
- Reduce the 90% of response time for general conversation query by adding decision layer with Semantic Router
- Utilize Conversation Memory from LangChain to remember the history while checking token length
- Tailor prompts to constraint LLM output in JSON format to pipeline SQL Script, DB execution result and error explanation

TEACHING

Teaching Assistant

Ewha Womans University — Seoul, Korea

Introduction to Artificial Intelligence — Sep 2025 – Dec 2025

- Led hands-on laboratory sessions (python) and guide students through practical exercises to improve technical proficiency
- Graded programming assignments, providing clear feedback to help students strengthen problem-solving skills

Computer Algorithm — Mar 2026 – Jun 2026

- Delivered lecture about Number theory
- Graded Assignments and proctor Exams

Undergraduate Tutor

Ewha Womans University - Solid Mechanics — Mar 2021 – Jun 2021

- Lead hands-on laboratory sessions and guide students step by step through practical exercises to improve technical proficiency

SCHOLASHIP

- Academic Encouragement Scholarship (2026)
- Outstanding Ewha Scientist Scholarship (2025)
- Artificial Intelligence Convergence Scholarship (2025)
- Ewha Woman's University Academic Scholarship for Overseas Experience (Sep 2022)

SKILLS

- Machine Learning Libraries: PyTorch, Sci-kit Learn
- Languages: Korean (native), English (fluent)