Hyunjae Lee 이현재

Information Security Engineer · AI Security

hyunjae@kaist.ac.kr
hyunjae-lee.github.io
github.com/hyunjae-lee · linkedin.com/in/hyunjaedev
Daejeon, Korea

I work where AI security meets day-to-day security operations. As principal investigator I built and validated an **LLM guardrail gateway** aligned with Korea's NIS N2SF framework, as a research project, and I run **web vulnerability assessment** and **certificate automation** across the university's websites. Before that I led **100+ security reviews a year** with the NIS and MSIT, and played a key role in a ~USD 130M next-generation information-system program.

EXPERIENCE

KAIST Engineer — 2020 — Present

Information Security Team · Web & AI Security — Jul 2026 — Present

- **Principal investigator, generative-AI guardrail research project** (team of 3; completed, not deployed to production): 8 outbound / 6 inbound inspection stages, RAG clearance control, canary tokens. A 205-prompt eval set with a CI gate took missed attacks 30%→0% and false blocks 2.6%→0% at 6 ms per check, no GPU. Mapped to OWASP LLM Top 10.
- Ran the **campus web vulnerability assessment**: 100% of mandated targets, scanner gaps closed with nuclei self-scans; individual remediation guidance and rescans for affected sites.
- Designed, built, and operate **certificate automation**: one-command ACME installer, self-updating agent, verification of the certificate actually served, DNS-01 for servers that can't open port 80. Zero certificate expiries.
- Designed a self-service security portal, IoC triage criteria for malicious URLs, and 47 automated server-baseline checks from the KISA guide; operate the WAF.

Information Security Team · Governance — Jul 2025 — Jul 2026

- **100+ security reviews a year** of major IT projects, including AI and cloud services, with the NIS and MSIT under the national cybersecurity guidelines.
- Led the MSIT security & privacy audit response (root-cause analysis, objections, evidence), **raising the institution's rating**; ran inspections, media security, and staff training.

Information Development Team · Academic Systems — 2020 — Jul 2025

- Core member of a ~USD 130M, 3-year **next-generation information system**: modernized 1,400+ graduation rules; 2,000+ graduations processed through the cutover without disruption (KAIST Special Commendation).
- Built in **security and privacy**: role-based access control, encryption and masking of personal data, privacy-impact-assessment and access-logging requirements, pre-launch vulnerability fixes and secure coding.

TmaxSoft Researcher — Jan — Jun 2020

- Spring-based enterprise products; cloud-native migration with Docker and Kubernetes.

Head Start, San Jose CA Data Scientist Intern — Jul — Aug 2019

- Built and evaluated machine-learning models.

Distributed Platforms & Security Lab, Chung-Ang Univ. Undergraduate Researcher — 2018 — 2019

- Blockchain double-spending research: IEEE paper and patent.

SKILLS

AI Security LLM guardrails · prompt-injection defense · RAG access control · AI red-team evaluation (promptfoo, garak) · OWASP LLM Top 10 · MITRE ATLAS · N2SF

Security Web vulnerability assessment (nuclei, AppScan) · TLS/PKI/ACME · WAF · threat intelligence · malware analysis · ATT&CK · security review & audit

Dev · Infra Python · FastAPI · Java/Spring · Docker · Kubernetes · CI/CD · Linux/Windows Server · DNS · ONNX (Korean NER)

EDUCATION

B.S. Computer Science & Eng., Chung-Ang Univ. — 2013 — 2020

Information Systems (Exchange), ECE Paris — 2018 — 2019

CERTIFICATIONS · LANGUAGES

Engineer Information Processing (2024)

OPIc English AL — highest grade (2025)

Korean native · English professional · Spanish, French elementary

TRAINING · CYBER SECURITY TRAINING CENTER

Local LLM Deployment & Application — 21 hrs (2026)

Security Review of Public IT Projects — 7 hrs (2026)

PUBLICATIONS · PATENT

Recipient-Oriented Transaction for Preventing Double Spending Attacks in Private Blockchain — IEEE SECON 2018

Patent KR 10-2018-0089040 — Recipient-oriented transaction verification for preventing double spending

HONORS

KAIST Special Commendation — next-generation system (2025)

Bronze Prize, SW Challenge — KOSA (2019)

Excellence Award, DaVinci SW TECH-FAIR (2019)