

『4단계 BK21』 혁신인재 양성사업 인공지능 분야 교육연구단 사업신청서

사업분야	신산업분야			접수번호	2120251015523
신청분야	세부분야		산업·기술분야	단위	전국
	디지털		인공지능		
학술연구분야 분류코드	구분	관련분야(1순위)	관련분야(2순위)	관련분야(3순위)	
	대분류	공학	공학	공학	
	중분류	컴퓨터학	컴퓨터학	공학일반	
	소분류	인공지능	정보보호	공학교육	
	비중(%)	60	25	15	
신청학과(부) 정보	신청 대학명	이화여자대학교	신설(예정) 학과	신설(예정)학과 여부	
	학사 조직 유형	일반 학과(부)		학과 개설(예정)일	
	학과(부)명		대학 간 연합 여부	N	
		인공지능소프트웨어학부	연합 대학명		
교육 연구단명	국문	고신뢰 고효율 인공지능 교육연구단			
	영문	Trustworthy and Resource-efficient Unified Evolving AI			
교육 연구단장	소속		이화여자대학교 인공지능대학 사이버보안학과		
	직위		정교수		
	성명	국문	양대현	전화	02-3277-4289
				팩스	
		영문	DAEHUN NYANG	이동전화	010-5132-2714
				E-mail	nyang@ewha.ac.kr
총 사업기간		2025. 9. 1 ~ 2027. 8. 31 (24개월)			

본인은 『4단계 BK21』사업 지원을 신청서와 같이 신청하며, 지원이 결정될 경우 관련 법령, 귀 재단과의 협약, 귀 재단이 정한 제반 사항 등을 준수하고 성실하게 사업을 추진하여 소정의 사업 성과를 거두도록 노력하겠습니다. 아울러, 신청서에는 사실과 다른 내용이 포함되지 아니하였으며 만약 허위 사실이나 중대한 오류가 발견될 경우에 그에 상응하는 불이익을 감수하겠습니다.

2025년 월 일

작성자	교육연구단장	(인)
확인자	산학협력단장	(인)
확인자	총장	(인)

한국연구재단 이사장 귀하

혁신인재
(인공지능 분야)



- 4단계 두뇌한국(BK)21 사업 -
혁신인재양성사업
인공지능 분야 선정평가 신청서

2025. 7.

교 육 부
한국연구재단

신청서 표지

『4단계 BK21사업』 혁신인재양성사업 인공지능 분야
교육연구단 사업신청서

사업분야	신산업 분야		접수번호		
신청분야	세부분야	산업·기술분야	단위 전국		
	D. 디지털	인공지능			
학술연구 분야 분류코드	구분	관련분야(1순위)	관련분야(2순위)	관련분야(3순위)	
	대분류	공학	공학	공학	
	중분류	컴퓨터학	컴퓨터학	공학일반	
	소분류	인공지능	정보보호	공학교육	
	비중(%)	60	25	15	
신청 학과(부) 정보	신청 대학명	이화여자대학교	신설(예정) 학과	□신설학과	
				□신설예정학과	
	학사 조직 유형	□대학원	학과 개설(예정)일	YYYY.MM.DD.	
		■ 일반 학과(부)			
		□학과(부) 내 전공			
		□협동과정	대학 간 연합 여부	□대학 간 연합 해당	
		□융합전공			
학과(부)명	인공지능• 소프트웨어학부	연합 대학명			
교육 연구단명	국 문	고신뢰 고효율 인공지능 교육연구단			
	영 문	Trustworthy and Resource-efficient Unified Evolving AI			
교육 연구단장	소 속	이화여자대학교 인공지능대학 사이버보안학과			
	직 위	정교수			
	성명	국문	양대현	전화	02-3277-4289
				팩스	
		영문	DaeHun Nyang	이동전화	010-5132-2714
				E-mail	nyang@ewha.ac.kr
총 사업기간	2025. 9. 1. ~ 2027. 8. 31. (24개월)				

본인은 『4단계 BK21』 사업 지원을 신청서와 같이 신청하며, 지원이 결정될 경우 관련 법령, 귀 재단과의 협약, 귀 재단이 정한 제반 사항 등을 준수하고 성실하게 사업을 추진하여 소정의 사업 성과를 거두도록 노력하겠습니다.

아울러, 신청서에는 사실과 다른 내용이 포함되지 아니하였으며 만약 허위 사실이나 중대한 오류가 발견될 경우에는 그에 상응하는 불이익을 감수하겠음을 서약합니다.

2025년 8 월 4 일

작성자	교육연구단장	양대현
확인자	이화여자대학교 산학협력단장	조월령
확인자	이화여자대학교 총장	이향숙
한국연구재단 이사장 귀하		

* 선정 일정에 따라 지원 시점은 변동될 수 있음

<신청서 요약문>

중심어	인공지능	고효율 AI	고신뢰 AI
	거대AI모델	멀티모달AI	온디바이스AI
	AI 하드웨어	데이터 합성	차분프라이버시
고신뢰 고효율 인공지능 교육연구단			
(TRUE-AI: Trustworthy and Resource-efficient Unified Evolving AI)			
교육연구단의 비전과 목표	<ul style="list-style-type: none"> ○ 신뢰도 높고 효율적인 인공지능 연구의 필요성 (1장 1.1) <ul style="list-style-type: none"> - 초거대 · 멀티모달 AI의 연산 자원 소모 급증으로 모델 효율성이 크게 주목받음 - 사이버 공격, 정보 유출로 인한 AI 모델의 신뢰성 결여 - 고신뢰 · 고효율 AI 고급 인재에 대한 수요 대비 부족한 공급 		
	<ul style="list-style-type: none"> ○ TRUE-AI 교육연구단의 비전 및 목표 (1장 1.2) <ul style="list-style-type: none"> - <u>고효율 AI</u>(경량화, 제약 환경 학습, 분산처리)와 <u>고신뢰 AI</u>(프라이버시 보호, 적대적 방어)를 양대 축으로 특화 교육 · 연구 트랙 구성 - AI SW-HW-보안 분야가 유기적으로 연계된 다학제 기반 교육체계 구축 - 산학협력, 글로벌 교류, 현장 실무교육을 위한 통합 생태계를 통해 산업 수요와 국제 경쟁력을 겸비한 AI 인재 양성 ○ 연구진 구성: 컴퓨터공학전공, 사이버보안전공, 인공지능융합전공의 참여 교수진은 멀티모달/생성형 AI, AI 시스템, 최적화, 보안 AI 분야 전문가 (1장 1.3) 		
교육역량 영역	<ul style="list-style-type: none"> ○ 교육연구단의 교육목표: 고신뢰 · 고효율 AI 인재 양성을 위한 통합된 교과과정 ○ 교육과정: <u>효율적 AI</u>와 <u>보안 AI</u> 교육 트랙은 아래와 같이 구성 (1장 1.2.2, 2장 1.1.2) <ul style="list-style-type: none"> - AI공통과목: AI 전공 기본 역량 확보 (예: AI개론, AI시스템) - 트랙핵심과목: 트랙별 전문성과 심화 역량 강화 (예: 컴퓨터비전, 딥러닝보안) - 트랙선택과목: 수요 기반 응용기술 선택 학습 (예: 고성능컴퓨팅, 시스템보안특론) - 프로젝트과목: 산학협력 기반 실전 문제 해결 (예: AI융합프로젝트) 		
	<ul style="list-style-type: none"> ○ 교육 트랙 1: <u>효율적 인공지능 교육</u> <ul style="list-style-type: none"> - 트랙 교육목표: 자율주행, 로봇, 엣지 컴퓨팅 등 제약된 환경에서 고성능 AI 모델을 설계하고 구현할 수 있는 교육 프로그램 - 핵심 역량: 경량화, 분산처리, 자기지도/준지도 학습, 시스템 최적화 등 - 예시 과목: 분산컴퓨팅, On-Device AI, 고성능컴퓨팅 ○ 교육 트랙 2: <u>보안 인공지능 교육</u> <ul style="list-style-type: none"> - 트랙교육목표: 적대적 공격, 프라이버시 침해 등 보안 위협을 AI로 해결하는 실전형 보안 AI 인재 양성 - 핵심 역량: 적대적 공격/방어, 정보보호, 차등 프라이버시, 신뢰 기반 생성형 AI - 예시 과목: 딥러닝보안, 개인정보보호, 기반코드분석, 암호기술특론 등 		
연구역량 영역	<ul style="list-style-type: none"> ○ 연구 트랙 1: <u>효율적 인공지능 연구</u> (1장 1.2.3) <ul style="list-style-type: none"> 연구목표: 인공지능 모델의 학습 효율성 향상을 위한 SW/HW 융합 인재 양성 [세부연구목표 1-1] 거대 모델을 위한 <u>효율적 학습</u> <ul style="list-style-type: none"> - 거대 모델의 연산 효율성과 데이터 활용 최적화를 위해, 사전학습 · 정제 · 정렬 · 파인튜닝 기법, 고성능 AI 모델 설계, 실무 데이터 역량을 갖춘 전문 인재 양성 		

	<p>[세부연구목표 1-2] 엣지 디바이스를 위한 효율적 학습 연구</p> <ul style="list-style-type: none"> - 엣지 디바이스 기반의 분산 학습, 약지도·자기지도 등 저자원 학습, 도메인 적응 및 시뮬레이션 기반 기술을 통해, 다양한 제약 환경에서 AI 구현하는 인재 양성 <p>[세부연구목표 1-3] AI 시스템의 성능/자원 효율성 극대화를 위한 HW 구조 연구</p> <ul style="list-style-type: none"> - UVM 기반 메모리 최적화와 비표준 정밀도(Bit Slicing) 연산 구조 연구를 통해 AI 연산 병목을 해소하고, HW/SW 융합 고효율 시스템 설계 역량을 갖춘 인재 양성 <p>○ 연구 트랙 2: 보안 인공지능 연구 (1장 1.2.3)</p> <p>연구 목표: 인공지능 모델 공격/보호 및 프라이버시 침해/보호 연구 인력 양성</p> <p>[세부연구 목표 2-1] 인공지능 모델 공격 및 보호 연구</p> <ul style="list-style-type: none"> - 적대적 공격 및 Membership Inference Attack, Memorization과 같은 프라이버시 침해에 대응하기 위해, 고신뢰 AI 모델 방어·보호 기법을 연구하는 인재 양성 <p>[세부연구 목표 2-2] 인공지능 모델의 프라이버시 침해/보호 연구</p> <ul style="list-style-type: none"> - 차분 프라이버시 기반 데이터 합성과 AI 기반 암호 트래픽 분석 기술을 통해, 민감정보보호와 데이터 활용의 균형을 달성하고 프라이버시 중심 보안 인재 양성
산학협력 영역	<p>○ 교과 프로그램: 본 교육연구단의 교과과정을 산학협력으로 확장 (4장 1.1)</p> <ul style="list-style-type: none"> - “교과 ↔ 비교과 ↔ 실증 프로젝트”를 연계한 3단계 문제해결 루프 구축 - 산업체 전문가가 강의·멘토·평가에 상시 참여, 실전성과 평가 신뢰성 확보 <p>○ 도메인 기반 전문화 교육 (4장 1.1)</p> <ul style="list-style-type: none"> - 헬스케어, 스마트제조, 모빌리티, 클라우드 4대 분야로 도메인 구성 - 각 도메인에서 실제 기업 데이터를 활용하여 문제 해결 및 규제·윤리 교육 병행 <p>○ 현장 중심 프로젝트 기반 학습 (4장 1.1)</p> <ul style="list-style-type: none"> - AI융합프로젝트(6-12개월)로 산업체와 공동 PoC 수행 → KPI 점검·데모데이·IP 검토하고, 산업 적용성과 사업화 가능성을 함께 확보 <p>○ 비교과 프로그램 및 현장 연계 (4장 3.1)</p> <ul style="list-style-type: none"> - 자율연구, 해커톤, 인턴십, 창업 탐색 등 4단계 비교과 프로그램 운영 - 기업 PM의 직무 요구를 반영한 현장 실습을 통해 취업 연계 강화
기대효과	<p>[학문] 산업 수요 기반의 융합 교육과 최신 연구를 연계해 실전형 AI 인재 양성</p> <p>[사회] 사회적 현안 해결 및 디지털 전환을 선도할 보안·프라이버시 역량 확산</p> <p>[경제] 고부가가치 기술 창출과 기업 맞춤형 교육을 통한 취업·기술이전 성과</p> <p>[국제] 국제공동연구와 교육 융합으로 글로벌 AI 허브로 도약</p> <p>○ 교육연구단의 정량/정성 목표</p> <p>[교육] AI 분야에 특성화된 박사과정 중심의 국내 최고의 연구 중심 대학원 (지표) 신입생 유치 (괄호 안: 박사/통합): 1차년도 15명(7명) → 2차년도 20명(10명) (2장 2.1.1)</p> <p>[연구] AI 모델 효율성, 보안 AI 분야에서 세계적 경쟁력을 가진 연구 성과 창출 (지표) H-index 20 이상 참여교수 비율: 현재 33% → 1차년도 38% → 2차년도 45% (3장 1.3)</p> <p>[산학] 산업체 수요 기반의 실용 연구/인재 양성을 통한 산학 연계의 선순환 체계 (지표) 인턴 1차년도 10건 → 2차년도 15건, 기술이전 2건 (2차년도) (4장 1.1, 3.1)</p> <p>[국제화] 국제 공동연구 및 학술 활동을 통해 글로벌 연구 허브로 도약 (지표) 국제 공동연구 총 24건(2년), 인적교류 총 12건(2년) (2장 4.1.3, 4.2, 3장 2.2, 2.3)</p>

목 차

I. 교육연구단의 구성, 비전 및 목표	1
1. 교육연구단 구성, 비전 및 목표	2
1.1 교육연구단의 필요성	2
1.2 교육연구단의 비전 및 목표	5
1.3 교육연구단의 구성	13
1.4 기대효과	26
II. 교육역량 영역	28
1. 교육과정 구성 및 운영	29
1.1 교육과정 구성 및 운영 계획	29
2. 인력양성 계획 및 지원 방안	44
2.1 교육연구단의 우수 대학원생 확보 및 지원 계획	44
2.2 대학원생 학술활동 지원 계획	46
2.3 우수 신진연구인력 확보 및 지원 계획	48
3. 참여교수의 교육역량	50
3.1 참여교수의 교육역량 대표 실적	50
4. 교육의 국제화 전략	52
4.1 교육 프로그램의 국제화 계획	52
4.2 대학원생 국제공동연구 계획	59
III. 연구역량 영역	62
1. 참여교수 연구역량	63
1.1 중앙정부 및 해외기관 연구비	63
1.2 연구업적물	63
1.3 교육연구단의 연구역량 향상 계획	66
2. 연구의 국제화 현황 및 계획	71
2.1 참여교수의 국제적 학술활동 참여 실적 및 현황	71
2.2 참여교수의 국제공동연구 실적 및 계획	73
2.3 외국 대학 및 연구기관과의 연구자 교류 실적 및 계획	77
IV. 산학협력 영역	81
1. 산학공동 교육과정	82
1.1 산학공동 교육과정 구성 및 운영 계획	82
2. 참여교수 산학협력 역량	86
2.1 국내 및 해외 산업체, 지자체 연구비	86
2.2 특허, 기술이전, 창업 실적의 우수성	86
2.3 산학협력을 통한 (지역)산업문제 해결 실적의 우수성	86
3. 산학 간 인적/물적 교류	93
3.1 산학 간 인적/물적 교류 실적과 계획	93
<부록> 첨부자료	

I . 교육연구단의 구성, 비전 및 목표

I. 교육연구단의 구성, 비전 및 목표

1. 교육연구단의 구성, 비전 및 목표

1.1 Ewha TRUE-AI 교육연구단의 필요성

TRUE-AI: Trustworthy and Resource-efficient Unified Evolving AI

1.1.1 신뢰도 높고 효율적인 인공지능 연구의 필요성

○ 인공지능 모델의 연산 효율성 · 에너지 최적화: 국가 경쟁력의 핵심 과제

- ✓ 초기대 AI 모델 학습에는 막대한 비용과 에너지가 소요되며, GPT-3의 경우 학습 비용은 약 470만 달러, 탄소배출량은 500톤 이상으로 보고됨 (Strubell et al., 2019; OpenAI, 2020)
- ✓ GPT-4는 정확한 파라미터 수는 비공개지만, 업계 분석에 따르면 약 1.8조 파라미터로 추정되며, Mixture-of-Experts(MoE) 기반의 선택적 계산 구조를 통해 연산 효율성과 성능 간 균형을 달성함.
- ✓ 특히, GPT-4o(2024)는 음성 · 영상 · 텍스트를 하나의 통합 모델로 처리하면서도, GPT-4 대비 2배 빠르고 50% 저렴한 추론 비용을 실현함 (OpenAI, 2024)
- ✓ 중국 DeepSeek-V2는 236B 파라미터와 2.6조 토큰을 학습하였으며, 효율적 토큰 라우팅, KV 캐싱 등을 활용해 GPT-4 및 LLaMA 2 대비 높은 연산 효율성을 달성함 (DeepSeek AI, 2024)
- ✓ 국내 초기대 언어모델 HyperCLOVA X는 300B(3,000억 개) 이상의 파라미터를 보유하며, 고성능 GPU 자원 확보, 연산 최적화, 맞춤형 모델 설계가 경쟁력의 핵심으로 작용함.
- ✓ 중국 Moonshot AI의 Kimi K2는 1.8조 파라미터 규모로, MoE 구조 기반의 선택적 expert 활성화를 통해 연산량을 획기적으로 절감함 (Kimi K2, 2024).
- ✓ 본 교육연구단은 “모델 경량화-학습 최적화-AI 가속기 친화형 설계”를 위한 통합형 SW/HW 교육 · 연구 체계를 구축하고, 해당 분야의 고효율 · 고신뢰 AI 기술 인재 양성을 목표로 함

○ AI 서비스 확산에 따른 사이버보안 위협 대응: 국가 안전과 산업 보호의 필수 조건

- ✓ AI 기술은 의료, 금융, 국방, 교육 등 다양한 분야에 빠르게 확산되며, 사회 전반에 큰 변화를 일으키고 있지만, 개인정보 유출, 편향된 의사결정, 설명 불가능한 알고리즘의 위협 등 정보보호 및 프라이버시 침해에 대한 우려도 심각해지고 있음
- ✓ 생성형 AI(ChatGPT, Claude, Gemini 등)의 등장으로 인해 민감한 정보의 무단 수집 및 사용, AI 모델에 의한 프라이버시 침해 가능성, 훈련 데이터의 보안 위협은 사회적 문제로 부각되고 있음.
- ✓ UN, OECD, EU를 비롯한 국제기구들은 “신뢰할 수 있는 AI”, “프라이버시 보호 중심 AI 설계”를 강조하고 있으며, 국내에서도 과학기술정보통신부와 개인정보보호위원회를 중심으로 AI 보안 및 프라이버시 가이드라인 마련을 추진하고 있음.
- ✓ AI 기술이 고도화될수록 보안 및 프라이버시 위협도 정교해지고 있으며, 특히 다음과 같은 정량적 지표는 AI 보안 분야의 기술적 대응 역량이 시급히 필요함을 보여줌:
 - A) 2025년 7월 18일 MIT Technology Review 기사에 따르면, 주요 AI 훈련 데이터 셋이 수백만개의 개인 정보를 포함하고 있다고 지적하고 있음.
 - B) Alizadeh et al. (2025) 연구에 따르면, 단순한 프롬프트 인젝션 공격만으로도 LLM이 평균 15~20% 확률로 민감 정보를 유출할 수 있음이 실험적으로 확인됨.
- ✓ 이러한 위협은 AI 기술이 도입된 공공 서비스, 금융, 의료 등 민감 정보가 집약된 분야에서 더욱 치명적인 문제로 연결될 수 있기에, 인공지능 기술의 정보보호 · 프라이버시 보호 역량은 기술 생태계의 지속가능성을 좌우하는 핵심 요소임

- ✓ 본 교육연구단은 이를 반영하여 “강건한 보안 AI 모델 설계-적대적 방어 훈련-차등 프라이버시 보호형 학습 프레임워크”를 위한 교육·연구 체계를 구축하고, 해당 분야 인재 양성을 목표로 함

○ 고효율·고신뢰 인공지능 기술 인력에 대한 수요 대비 부족한 공급

- ✓ 한국고용정보원에 따르면, 2025년까지 국내 AI·데이터 고급 인재는 9만 명 이상 부족할 것으로 추정됨 (디지털 인재 현황 분석, 2022)
 - ✓ AI 전공자 중 박사급은 6%에 불과하며, SW/HW 최적화 및 보안 특화 인력은 극소수에 불과함.
 - ✓ 산업계는 “AI 모델 성능” 뿐 아니라 “에너지 절감, 응답속도, 보안성”을 종합적으로 고려한 기술 인재를 요구함.
 - ✓ 정부 및 민간 조사에 따르면 AI 보안 및 프라이버시 보호 분야 인력은 매우 부족한 상황임.
 - A) 전자신문 보도(2024.12.26)에 따르면, 정보보호기업 10곳 중 3곳, 인재 확보 어려움을 겪고 있음
 - B) 미국 NIST (National Institute of Standards and Technology) 및 EU AI Act 등은 AI 신뢰성 확보를 위해 “보안과 프라이버시 전문 인력의 확보를 정책 필수 조건”으로 명시
 - ✓ 이를 고려하여 본 교육연구단은 단순한 AI 개발을 넘어, 고효율, 고신뢰 AI를 설계·운영할 수 있는 인력의 양성을 위해 학제 간 융합형 커리큘럼 + 실증 중심 연구 프로젝트를 통해 산업체가 요구하는 복합형 인재 양성 체계를 구축하려고 함
- ※ 고신뢰: 일반적으로 정보의 정확성(예: 할루시네이션 방지), 사이버 공격·방어, 프라이버시 등을 포함하지만, 본 연구단은 사이버공격 대응 및 프라이버시 보호에 중점을 둠

1.1.2 Ewha TRUE-AI 교육연구단의 필요성 (그림 1-1)

○ 국내 최고의 여성 중심 고등교육기관으로서 AI 고급 인재의 다양성 확보

- ✓ 국내 이공계 박사 중 여성은 약 22%(2021년 기준)에 불과하며, AI 분야는 그보다 낮다고 추정됨
- ✓ 이화여대는 국내 최고의 여성 중심 이공계 고등교육기관으로서, AI 분야의 성별 불균형 해소 및 인재 다양성 확보에 전략적 역할을 수행할 수 있음
- ✓ 본 교육연구단은 고급 AI 인력 양성에 있어 성별 다양성과 포용성을 실현함으로써, 국가 차원의 AI 인력 수급 불균형 문제 해결에도 기여할 수 있음
- ✓ 여성 AI 고급인재 육성은 UN 지속가능발전목표(SDGs; Sustainable Development Goals)의 성평등·교육 접근성 강화와 과기정통부의 디지털 포용 정책 기조에 부합하며, 지속 가능한 AI 인재 생태계 구축을 위한 핵심 대안으로 자리할 수 있음
- ✓ AI와 보안/프라이버시 분야는 사회적 민감성과 기술적 판단이 동시에 요구되는 융합 영역으로, 다양한 배경의 인재 참여가 중요하지만, 여성 인재의 참여는 심각하게 저조한 상황임:
 - A) 세계경제포럼(WEF) “Gender Gap Report 2023”에서는 AI·데이터 분야의 젠더 격차 해소까지 131년이 소요될 수 있다고 전망
 - B) (ISC)² (International Information System Security Certification Consortium) 및 Cybersecurity Ventures 보고서에 따르면 전 세계 사이버보안 직무에서 여성 비중은 2022년 기준 약 22-25%
- ✓ 이는 단지 수치의 문제를 넘어, AI 기술이 특정 집단의 경험과 시각에만 의존할 위험성을 시사하며, 특히 AI의 자동화된 의사결정이 개인정보 보호, 감시 기술, 사회적 편향에 직접 영향을 미치는 만큼, 여성 인재의 관점이 반영된 균형 잡힌 기술 설계는 필수적임.

○ 인공지능·소프트웨어학부의 유기적으로 통합된 연구 및 교육 체계 활용

- ✓ 컴퓨터공학전공, 사이버보안전공, 인공지능융합전공으로 구성된 인공지능 소프트웨어학부의 유기적 구조를 바탕으로 AI 핵심 기술과 응용을 아우르는 교육 및 연구역량 확보가 가능함.

I. 교육연구단의 구성, 비전 및 목표

혁신인재양성사업 인공지능 분야 교육연구단 사업

- ✓ 컴퓨터공학전공은 인공지능 뿐만 아니라, 고성능 컴퓨팅, 시스템 최적화, SW 아키텍처 등 기반 기술 연구에 강점이 있음.
- ✓ 사이버보안전공은 AI 보안, 적대적 학습, 개인정보 보호 등 보안 중심 AI 연구에 특화된 전공임.
- ✓ IITP 인공지능 융합혁신인재양성사업(2022-2025, 이하 AIX사업)을 통해 2022년에 개설된 인공지능 융합전공은 생성형 AI, 멀티모달 모델 분야의 핵심 인재를 양성하고 있음.
- ✓ 이처럼, 본교는 모델 최적화-보안-응용을 아우르는 융합형 인재 양성 커리큘럼을 이미 운영 중임.

○ 대형 정부 과제 수행 실적 기반의 안정적 연구 인프라 보유

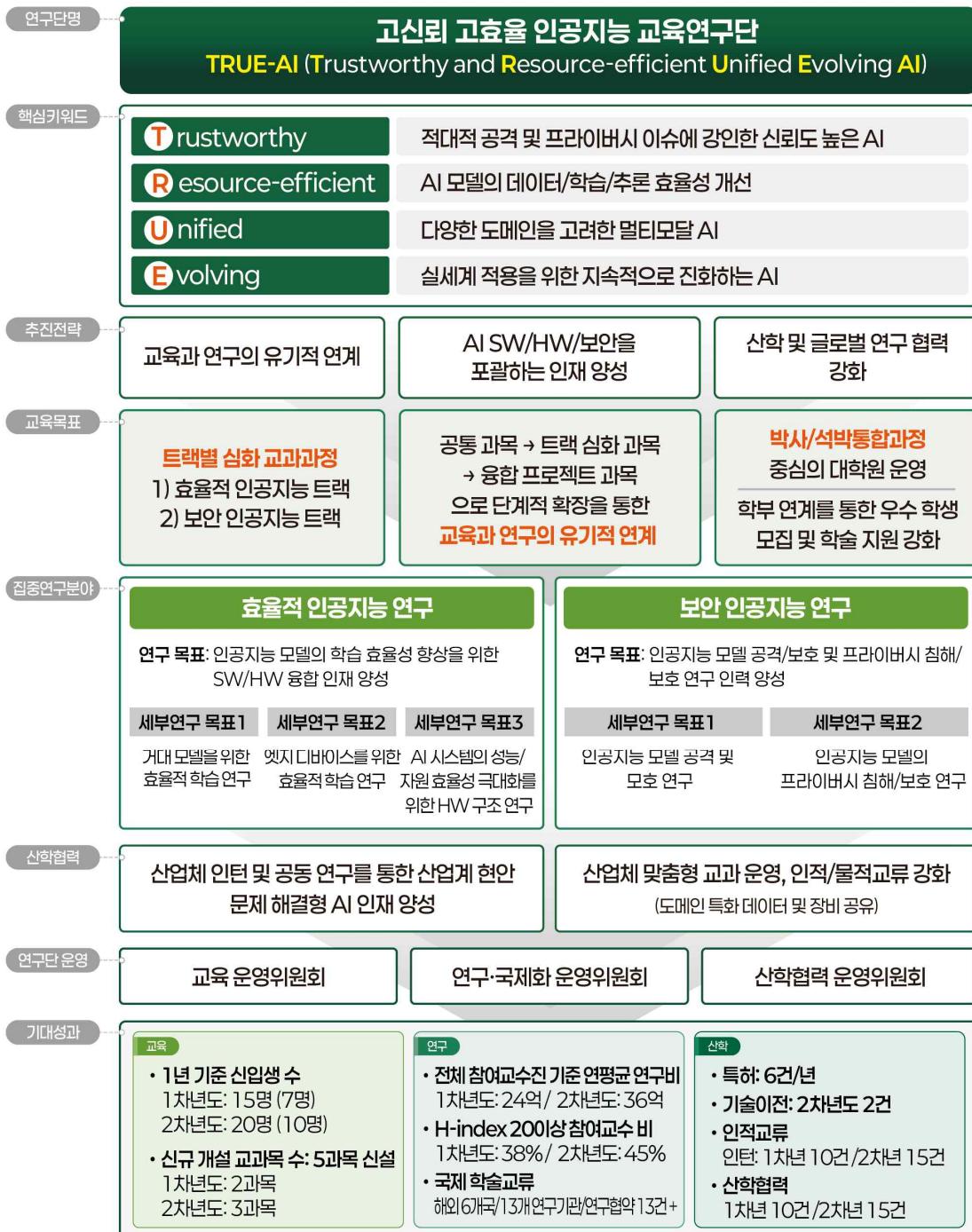
- ✓ 인공지능 · 소프트웨어학부에서 운영 중인 IITP AIX사업을 통해 고성능 GPU 클러스터, 산학연계 연구 네트워크, AI 실증 교육 플랫폼 등 첨단 교육 · 연구 인프라를 성공적으로 구축함.
- ✓ 해당 과제를 통해 컴퓨터공학전공, 사이버보안전공, 인공지능융합전공 간의 융합 교육 체계를 이미 마련하였고, 국내 유수의 AI 기업과 공동 연구 및 산학 프로젝트를 다수 운영하였음.
- ✓ 특히, 고도화된 컴퓨팅 인프라를 활용하여 거대 모델 학습, AI 보안 시뮬레이션, 분산 학습 등의 실전형 교과과정을 운영하였고, 이를 통해 석 · 박사급 인력의 현장 적용성을 극대화하였음.
- ✓ 본 교육연구단은 이러한 실적 기반 위에서, 고효율 · 고신뢰 AI 기술을 주제로 한 SW/HW 융합 연구 및 보안 중심 AI 연구를 안정적으로 추진할 수 있으며, 교육-연구-성과 확산-산업 연결로 이어지는 선순환 구조를 체계적으로 실현할 수 있는 운영 역량을 이미 확보함.



<그림 1-1> Ewha TRUE-AI 교육연구단의 필요성

1.2 교육연구단의 비전 및 목표

1.2.1 교육연구단의 비전



<그림 1-2> Ewha TRUE-AI 교육연구단의 비전

○ TRUE-AI 교육연구단의 비전 (그림 1-2 참조)

- ◆ 높은 신뢰성과 자원 효율성을 갖춘 AI 모델 개발에 필요한 인재 양성 및 연구체계 구축
- ◆ 해외 유수 교육기관인 MIT, CMU, Toronto의 교육/연구 모델을 참고하되, 이화여대만의 교육 환경을

기반으로 선정한 AI 특화 분야(신뢰성과 효율성)의 핵심 인재 양성에 집중함.

○ 교육연구단이 속한 인공지능·소프트웨어학부의 현재

- ◆ 인공지능·소프트웨어학부의 학부생 정원 증가
 - ✓ 본교는 2018년도 대학입시부터 정시모집 정원의 20%를 호크마 교양대학으로 입학시키고, 2학년 진학 시에 자유롭게 전공을 선택할 수 있는 자유학부제를 실시하고 있음
 - ✓ 2022년 호크마 교양대학에서 ‘인공지능 소프트웨어학부’를 전공으로 선택한 학부생의 수가 경영학부를 제치고 1위를 차지하며 2022년 2학년 정원이 기존 105명에서 187명으로 증가함
- ◆ 상대적으로 낮은 대학원 진학률
 - ✓ 대학원 신입생 수가 학부 정원 대비 낮으며, 특히 박사과정 지원자가 크게 저조함
 - ✓ 낮은 대학원 진학률 원인: 1) 높은 학부 취업률, 2) AI 분야 대학원 커리큘럼, 3) 타 대학원 진학

○ 세계 저명대학 벤치마킹 분석

- ◆ MIT - Stephen A. Schwarzman College of Computing
 - ✓ 2020년 신설된 MIT 컴퓨팅 대학은 AI 중심의 융합 교육을 위해 EECS, CSAIL, IDSS 등 총 11개 단위 조직을 통합하고, 모든 학문 분야에 AI를 접목하는 “AI+X 융합 인재” 양성을 목표로 함
- ◆ CMU - Carnegie Mellon AI (CMU AI)
 - ✓ 2017년 설립된 AI 단과대학은 컴퓨터공학, 로보틱스, 언어기술, HCI 등 기존 전공을 통합하여 AI 전주기 교육체계를 구축하고, AI Core, AI Systems, AI for Social Good 다양한 융합 프로그램 운영
- ◆ University of Toronto - Vector Institute
 - ✓ 캐나다 정부, 산업체, 대학이 공동으로 운영하는 AI 인재 양성 허브로 산업 수요 기반의 AI Professional Master’s Program은 실무형 고급 인재 양성의 대표 사례임

○ 세계 저명대학 벤치마킹을 바탕으로 한 이화여대 인공지능대학의 추진 전략

AI Core/System/융합을 중심으로 AI 인재 양성 체계를 고도화한 MIT, CMU, Toronto를 참조하여 다음과 같은 방향으로 교육연구단을 운영하고자 함

- ◆ AI 핵심기술과 사회적 책임을 아우르는 융합형 인재 양성
 - ✓ AI 모델의 효율성, 보안성, 신뢰성 등 기술적 전문성과 데이터 책임성, 사용자 중심 설계 중점
- ◆ 여성 중심 고등교육기관의 특성을 살린 포용적 AI 인재 생태계 조성
 - ✓ 낮은 여성 AI 인력 비율(13~14%)을 고려할 때, AI 교육 플랫폼으로 차별적 역할 수행 가능
- ◆ 실전 기반 교육과 산학연 협력을 통한 현장형 리더 양성
 - ✓ 산업체와의 공동연구, 프로젝트 기반 수업, 고성능 GPU 인프라를 통한 실무 중심 교육 강화
 - ✓ 국내외 AI 기업과 연계한 현장형 고급 인재 배출 체계 구축
- ◆ 글로벌 모델을 반영하되, 이화여대만의 교육 시스템 정립
 - ✓ 컴퓨터공학전공, 사이버보안전공, 인공지능융합전공의 연계 교육을 통해 특화 융합교육 모델 구축

1.2.2 교육연구단의 교육 목표 및 내용

○ 교육과정 구성 및 운영 계획

- ◆ 교육과정 개요
 - ✓ 기본 교육연구단의 교육과정은 AI 모델의 효율성과 보안성을 핵심 축으로 설정
 - [효율적 AI 트랙] 제한된 자원으로 높은 성능을 내는 경량화·최적화된 AI 모델 설계·구현
 - [보안 AI 트랙] AI 기술의 보안 취약점 대응 및 프라이버시 보장 연구
 - ✓ 석사(24학점), 박사(36학점), 석박통합(60학점) 과정에 걸쳐 다음 4가지 유형의 과목으로 구성됨

- (AI공통과목) AI 전공 기본 역량 확보를 위한 기초 이론 교육
- (트랙핵심과목) 트랙별 전문성과 심화 역량 강화를 위한 핵심 기술 교육
- (트랙선택과목) 수요 기반 응용기술 선택 학습을 통한 역량 다양화
- (프로젝트과목) 산학협력 기반 실전 문제 해결 중심 프로젝트 수행

◆ 효율적 AI 트랙

- ✓ 교육 목표: 자율주행 · 로봇 · 엣지 컴퓨팅 등 제약 환경에서 고성능 AI 모델 설계/구현 능력 배양

과목 분류	목적	과목명 예시
AI공통과목	기초 역량 확보 후 고도화된 응용기술 학습 가능	인공지능개론, 딥러닝, 인공지능시스템 설계
트랙핵심과목	효율성 중심의 설계 기술 및 경량화 기법 교육	컴퓨터비전, 분산컴퓨팅, On-Device AI, 효율적학습특론
트랙선택과목	실제 시스템 적용 사례 기반 학습	지능형시스템SW/HW, 엣지컴퓨팅개론, 고성능컴퓨팅
프로젝트과목	기업 연계 과제를 통한 문제해결 능력 강화	AI융합프로젝트(효율성×보안 AI), AI융합기술상용화(효율성×보안 AI)

◆ 보안 AI 트랙

- ✓ 교육 목표: 적대적 공격 · 프라이버시 위협 등 AI 기반 보안 문제 해결 역량 및 융합 능력 배양

과목 분류	목적	과목명 예시
AI공통과목	AI 보안 응용을 위한 기초 지식 확보	자연어처리특론, 생성형인공지능
트랙핵심과목	생성형 AI 위협, 모델 취약점 분석 및 방어 기술 학습	보안개론, 딥러닝보안, 차세대보안특론, 정보보호론
트랙선택과목	암호 · 네트워크 보안 등 산업 적용 중심 과목 운영	개인정보보호, 시스템보안특론, 최신암호기술특론, AI기반코드분석
프로젝트과목	기업 연계 과제를 통한 문제해결 능력 강화	AI융합프로젝트(효율성AI×보안 AI), AI융합기술상용화(효율성×보안 AI)

◆ 트랙 간 연계 과목 구조

- ✓ 공통 기반 학보 → 트랙 심화 → 융합 프로젝트 확장의 3단계 구조로 구성
- ✓ 1단계: 모든 학생이 이수하는 AI 공통과목을 통해 수학 및 알고리즘 기반 역량 함양
- ✓ 2단계: 트랙별 핵심/선택과목으로 효율성과 보안 분야의 전문성 심화
- ✓ 3단계: 트랙 간 협업 프로젝트 과목 운영 (예: LLM 효율화와 데이터 유출 방지 통합)

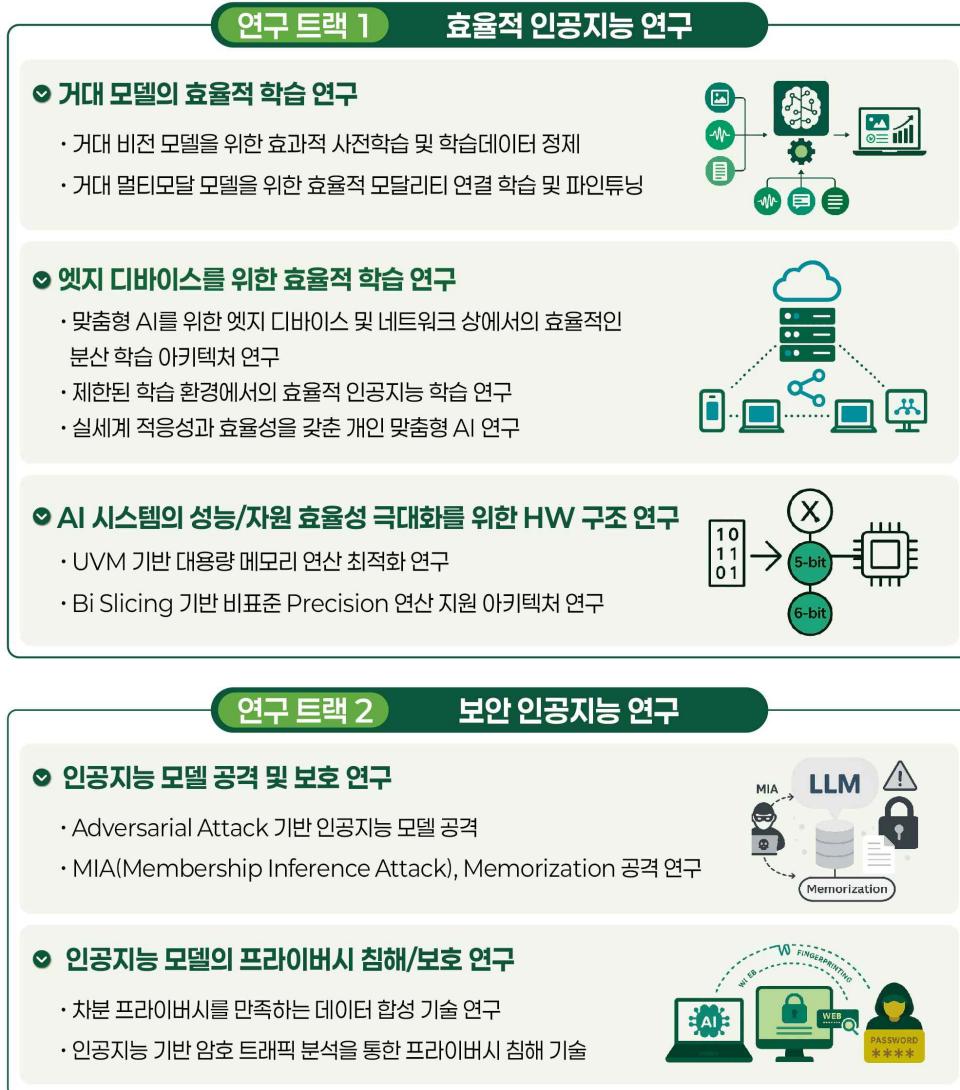
○ 교육과정 운영을 위한 추진 전략

- ◆ 산업체 수요 기반 맞춤형 트랙 운영 (예: NVIDIA, 네이버클라우드, 현대차 등과 연계한 과목 기획)
- ◆ 트랙 융합 프로젝트 활성화: LLM, IoT, 클라우드 등 공통 기술 기반 교차 트랙 협력 유도
- ◆ 품질관리 강화: 산업체 전문가-교수진 협력 ‘교육과정위원회’ 운영, 정기 워크숍 통한 개선
- ◆ 연구-교육 연계 및 국제 협력 교육 추진: 교수 연구실 기반 프로젝트 과목 운영

1.2.3 교육연구단의 연구 목표 및 내용

고신뢰 고효율 AI 수요에 부응하기 위해 1) 효율적 인공지능, 2) 보안 인공지능의 특화 방향으로 구성함

※ 고신뢰: 일반적으로 정보의 정확성(예: 할루시네이션 방지), 사이버 공격 · 방어, 프라이버시 등을 포함하지만, 본 연구단은 사이버공격 대응 및 프라이버시 보호에 중점을 둠.



<그림 1-3> 교육연구단의 연구목표: 1) 효율적 인공지능 연구, 2) 보안 인공지능 연구

○ 연구 트랙 1: 효율적 인공지능 연구

연구 목표: 인공지능 모델의 학습 효율성 향상을 위한 SW/HW 융합 인재 양성

[세부연구 목표 1] 거대 모델을 위한 효율적 학습 연구

- ◆ 거대 비전 모델을 위한 효과적 사전학습 및 학습데이터 정제
- ✓ 거대 비전 모델 확산으로 대규모 데이터 기반 사전학습의 중요성이 증가하였으나, 높은 계산량으로 인해 사전학습의 효율성 개선이 필수적임
- ✓ 도메인 특성과 태스크에 따라 학습데이터를 자동 선별 · 정제할 수 있는 AI 모델 개발 역량 필요
- ✓ 고성능 AI 모델을 효율적으로 설계하고 다양한 도메인에 적응할 수 있는 인재를 양성하며, 학습데이터의 품질과 구성 전략에 대한 실무 능력을 함께 배양함
- ◆ 거대 멀티모달 모델을 위한 효율적 모달리티 연결 학습 및 파인튜닝
- ✓ 멀티모달 AI 모델의 크기와 복잡도가 급증함에 따라, 연산 자원, 에너지 소비 등 비용 문제 해결

- 을 위한 효율적 AI 개발과 전문 인재 양성이 중요한 과제로 떠오름
- ✓ 멀티모달 정렬, 경량화, 인과 추론 기반 시뮬레이션 효율적 AI 연구 경험을 교육과정에 반영함
 - ✓ 다양한 입력 데이터를 융합한 상호 보완적 학습, 인과 관계 추론 활용, 실제 산업에 적용을 위한 효율적 파인튜닝 방식에 대한 인재를 양성함

[세부연구 목표 2] 엣지 디바이스를 위한 효율적 학습 연구

- ◆ 맞춤형 AI를 위한 엣지 디바이스 및 네트워크 상에서의 효율적인 분산 학습 아키텍처 연구
 - ✓ 개인 맞춤형 AI 학산과 함께 엣지 디바이스 내 경량 학습 및 디바이스 간 선택적 지식 전이를 통한 효율적 모델 학습이 핵심 과제로 부상함
 - ✓ 연합학습은 데이터 공유 없이 학습 가능하지만, 중앙 서버 의존성과 멀티모달 처리의 한계가 있음
 - ✓ 저성능 디바이스에서도 고성능 AI 구현이 가능하도록 효율적 모델 설계 및 멀티모달 학습, 선택적 지식 전이 기반 분산 학습 구조를 중심으로 실무형 인재를 양성하고자 함
- ◆ 제한된 학습 환경에서의 효율적 인공지능 학습 연구
 - ✓ 데이터 라벨링 비용 증가로 약지도, 준지도, 자기지도 등 효율적 학습 방식이 중요해지고 있음
 - ✓ 약지도 · 준지도 · 자기지도 학습은 라벨 없이도 가능해 의료 · 로봇 등 현장 활용도가 높음
 - ✓ 능동학습, 자기지도 학습을 중심으로 자원 제약과 라벨 부족 상황에서도 높은 학습 효율성과 성능을 보장하는 AI를 구현할 수 있는 역량을 갖춘 인재 양성
- ◆ 실세계 적용성과 효율성을 갖춘 개인 맞춤형 AI 연구
 - ✓ 실제 환경에서 데이터 부족, 클래스 불균형, 도메인 차이로 인해 AI 모델 성능 저하가 빈번함
 - ✓ 특히 디지털 헬스, 자율주행, 제조, 국방 등에서는 입력 조건이 수시로 변화하며 복수의 다운스트림 작업이 요구되기에, 이에 적응할 수 있는 범용 AI의 중요성이 커지고 있음.
 - ✓ 도메인 적응, 멀티모달 · 생성형 AI, 시뮬레이션 기반 학습을 교육과정에 반영하여, 일반화 성능과 자원 효율을 모두 갖춘 차세대 AI 인재를 양성함.

[세부연구 목표 3] AI 시스템의 성능/자원 효율성 극대화를 위한 HW 구조 연구

- ◆ UVM (Unified Virtual Memory) 기반 대용량 메모리 연산 최적화 연구
 - ✓ 수백 GB 데이터를 처리하는 AI 워크로드의 병목 현상 해결을 위해 다수의 GPU 메모리를 연계하는 UVM이 활용되고 있으나, 여전히 메모리 접근 지연과 데이터 이동 오버헤드가 존재함
 - ✓ 시스템 구조 이해 및 최적화 역량을 바탕으로 성능 병목을 해결할 인재를 양성하고자 함.
 - ✓ AI 모델 실행 패턴 분석과 SW/HW 통합 최적화 교육을 연계하여 고성능 시스템 AI 인재 양성
- ◆ Bit Slicing 기반 비표준 Precision 연산 지원 아키텍처 연구
 - ✓ 초거대 AI의 추론 효율 향상을 위해, 작업 특성에 따른 정밀도 조절 방식의 중요성이 부각됨
 - ✓ 특히, 6-bit, 5-bit 등과 같은 비표준 정밀도를 지원하는 유연한 연산 구조에 대한 수요가 증가하고 있으며, 이는 고효율 AI 하드웨어 설계의 핵심 기술로 간주됨
 - ✓ 다양한 비트폭 연산 구조 설계 · 시뮬레이션 교육을 통해 차세대 AI 연산 아키텍처 역량을 강화하고, HW-SW 융합형 고효율 시스템 최적화 인재를 양성할 계획임

○ 연구 트랙 2: 보안 인공지능 연구

연구 목표: 인공지능 모델 공격/보호 및 프라이버시 침해/보호 연구 인력 양성

[세부연구 목표 1] 인공지능 모델 공격 및 보호 연구

- ◆ Adversarial Attack 기반 인공지능 모델 공격
 - ✓ AI 모델은 미세한 입력 교란에도 취약하며, 약 80%가 적대적 공격에 노출되는 것으로 보고됨
 - ✓ Google Brain, OpenAI, MIT 등에서 공격·방어 기술을 NeurIPS, ICLR에서 활발히 발표하고 있음
 - ✓ 적대적 공격 탐지 및 방어 알고리즘 설계, 적대적 훈련(adversarial training) 등의 기술을 기반으로 신뢰할 수 있는 AI 시스템 개발 능력을 갖춘 고급 인재를 양성하고자 함
- ◆ MIA(Membership Inference Attack), Memorization 공격 연구
 - ✓ ChatGPT, Gemini 등 대규모 언어모델(LLM)의 확산과 함께, 훈련 데이터의 존재 여부를 추론하는 MIA 공격과 모델의 과잉기억(Memorization) 문제가 프라이버시 위협으로 부각됨
 - ✓ Carnegie Mellon, OpenAI, Google 등에서 LLM의 안전성/프라이버시 설계가 주목받고 있음
 - ✓ LLM 구조에 대한 이해, 정보 유출 위험 탐지, 모델 내 데이터 보호 전략 수립을 위한 인력 양성

[세부연구 목표 2] 인공지능 모델의 프라이버시 침해/보호 연구

- ◆ 차분 프라이버시를 만족하는 데이터 합성 기술 연구
 - ✓ Differential Privacy(DP)는 민감 정보 보호와 AI 학습을 병행하는 핵심 기술로, Stanford, MIT, Google 등에서 활발히 연구 중임
 - ✓ Diffusion 기반 데이터 합성과 DP 결합으로 프라이버시와 데이터 활용 간 균형 연구가 증가
 - ✓ 프라이버시 보존 데이터 생성 및 성능-보호 간 트레이드오프 최적화를 위한 인재 양성
- ◆ 인공지능 기반 암호 트래픽 분석을 통한 프라이버시 침해 기술
 - ✓ “The world in data breach”에 따르면, 2024년 기준 매일 약 700만 건의 비암호화 데이터가 침해되며, 암호 통신에서도 트래픽 패턴 분석을 통한 민감 정보 노출이 심각한 위협으로 부상함
 - ✓ TOR 네트워크의 암호화 트래픽에 대한 AI 기반 팽거프린팅, 트래픽 패턴 분류가 활발히 연구됨
 - ✓ 암호 트래픽 분석 특화 연구를 기반으로, 보안 프로토콜과 익명성 네트워크 이해, 트래픽 분석 알고리즘 설계 등을 포함한 교육을 통해 네트워크 보안 전문가를 양성하고자 함

1.2.4 교육연구단의 산학협력 목표 및 내용

○ 산학협력 목표: 산업체 수요 기반 교육과정과 인턴십 연계를 통한 현장 맞춤형 AI 인재 양성

○ 본 교육연구단의 산학협력 현황

참여 교수진은 지난 5년 간 다양한 기업 및 기관과의 산학 공동 연구, 기술 자문, 보안 교육, 오픈 강의, 인턴십 연계를 통해 AI·보안 분야 실무 역량을 갖춘 인재 양성과 기술 확산을 동시에 추진하고 있음.

- ◆ 산학 공동 연구: 큐빅(생성형 AI 합성데이터), LG전자·현대차(로봇·차량 AI), 유니와이즈솔루션즈(홈 피트니스 AI), DXR(제조 합성데이터), 비엠스마일(IoT-펫 헬스케어), 스포터(조리로봇 비전 AI), Wordbricks(노코드 플랫폼), 병원 연계 의료 AI 등 다양한 기업 및 기관과 협력 연구 수행
- ◆ 기술 자문 및 이전: 네이버(HyperClova-X 음성 LLM 구축 자문), 현대차(생성형 AI 자문), 유니와이즈 솔루션즈·에스프레스토·Wordbricks (특허, 기술이전, 알고리즘 고도화 자문)
- ◆ 강의 및 교육 콘텐츠 제공: KOCW, 타이젠 오픈강의, 소스코드·데이터셋 공개 (누적 조회 95만 회)
- ◆ 보안 특화 교육 및 실습: 랜섬웨어 실습교육, ChatGPT 보안위협 특강, Amazon Alexa/Google Assistant 도청 탐지, Tor 트래픽 보호 연구 등 보안 특화 실습·교육 운영
- ◆ 학생 연계 활동: 대학원생의 다양한 기업 인턴십 참여(DXR, 병원 등), 연구 결과 오픈소스 공개, 정규 교과 과정과 연계한 프로젝트 참여 등 실무 기반 교육

○ 산학공동 교육과정 구성 및 운영 계획

◆ 공동 교육과정 체계적 구성

- ✓ LG전자, 현대차, 네이버 등 산업체 수요 반영한 AI, 보안, 시스템 분야 특화 맞춤형 교육과정 구성
- ✓ 캡스톤디자인 및 현장실습, 인턴십 프로그램을 정규 교육과정에 통합하고, 산학협력을 수행 중인 회사와의 프로젝트와 대학원생의 매칭을 주선함

◆ 산업체 전문가 참여

- ✓ 실무 중심 특강과 문제해결 기반 교과목 공동 운영 (예: 네이버 클라우드의 멀티모달 LLM 경량화)
- ✓ 현장기반 프로젝트 수행형 수업을 통해 산업 현장의 문제를 직접 해결하는 수업모델을 정착시킴

◆ 교육과정 품질관리 및 개선

- ✓ 산학협의체(기업 파트너 포함)를 통한 정기적 평가와 피드백 회의를 통해 교육과정의 유효성과 산업체 적합성을 지속 점검함
- ✓ 교과목의 운영 결과 분석 후 반영 (예: 로봇청소기 On-device AI 과제를 교육과정에 반영)

◆ 인재 수요 대응형 교과 운영

- ✓ 산업체가 필요로 하는 핵심 기술·역량 중심 과목 운영 (예: 음성 LLM, 보이스피싱 대응 탐지)
- ✓ 산업체 맞춤형 교육과정을 통해 대학원생의 취업 연계 강화
예: Microsoft Research · Adobe Research · 네이버 등과의 프로젝트 참여 경험을 교육과정에 반영

○ 산학 간 인적/물적 교류 계획

- ◆ 삼성, LG, 현대차 등 산업체 전문가가 수업 공동 운영 및 기술 세미나에 참여한 사례 기반 교육
- ✓ 교수진과 기업 간 협업을 통해 Amazon Alexa · Google Assistant 트래픽 분석, 랜섬웨어 실습 교육, IoT 기반 보안 시스템 등 고도화된 산학 캡스톤 프로젝트를 지속 확대
- ✓ 병원 및 스타트업과 연계하여 연구협력 확대 (예: DXR, 에스프레스토, 서울대병원, Wordbricks 등)
- ✓ 산학 공동연구 시 기업이 제공한 실제 데이터셋과 장비를 실습과 연구에 활용

1.2.5 교육연구단의 국제화 목표 및 내용

○ 국제화목표: 국제공동연구 활성화/졸업생 해외 진출 지원을 통한 국제경쟁력을 갖춘 인재 양성

○ 국제화목표 달성을 위한 추진전략

◆ 국제 학술활동 및 해외 진출 지원 체계 강화

- ✓ 대학원생 연구 실적 평가를 통해 최우수 학술대회 연 1회 참석 비용 지원 대학원생 선정
- ✓ 해외 저명 연구그룹과의 인턴십, 공동 연구를 통해 대학원생의 국제화 역량 증진
- ✓ 졸업생의 글로벌 AI 기업 및 연구소 진출을 위한 멘토링 네트워크 구축

◆ 글로벌 연구 네트워크 강화를 위한 학술 교류 기반 조성

- ✓ 해외 석학 정기 초청 세미나 시리즈 운영: 연 4회 이상 해외 저명 연구자 초청 세미나 개최
- ✓ 글로벌 공동 강의 및 단기 교육과정 운영: 해외 대학 교수진과의 단기 집중 강의 운영
- ✓ Horizon Europe, NSF 등 해외 연구비 수주를 위한 국제 공동과제 사전 기획
- ✓ 산학 국제 협력 확대: 산업체와 함께 Global AI Challenge, 공동 논문 발표로 실질적 협력 확대

◆ 글로벌 커뮤니케이션 및 문화 적응 역량 강화

- ✓ AI 전공 대학원생을 위한 영문 논문 작성 특강, 발표 클리닉, peer-review 워크숍 정기 운영
- ✓ 대학 간 협정을 통한 교환 연구/방문 프로그램 운영 (3~6개월 단기 파견 포함)
- ✓ 글로벌 환경에서 협업 가능한 연구자의 소양 교육 병행 (문화 다양성, 저작권, 데이터 윤리 등)

1.2.6 교육연구단의 학사 단위로서의 안정화 및 지속가능성 제고 방안

- ✓ (인공지능 · 소프트웨어학부의 안정된 구조) 컴퓨터공학전공, 사이버보안전공, 인공지능융합전공이 협력하여 AI 핵심, 보안, AI 융합이라는 상호보완적 특성을 통해 안정적이고 교육연구 기반 형성
- ✓ (학부-대학원 연계 강화 및 SW중심대학사업과의 유기적 연결) 인공지능대학 내 세 전공이 참여하는 SW중심대학사업과 연계하여, 학부생의 진로 탐색 및 연구 관심을 유도하며, 본 교육연구단의 대학원 과정으로의 자연스러운 진학을 유도하는 선순환 구조를 구축하고 있음.
- ✓ (산학연계형 인턴십 및 실무 연계 강화) 국내외 유수의 대학, 연구소, 산업체와 연계한 AI 관련 인턴십 프로그램 참여를 적극 장려하여, 실무 경험을 축적하고 진로 확장성을 확보함.
- ✓ (졸업생-재학생 네트워크 구축 및 멘토링 시스템) 졸업생 멘토링 프로그램, AI+보안 분야의 리더십 아카데미, 졸업생 취업/창업 사례 공유를 통해 진로 확장성과 교육연구단의 외연 확장 유도

1.2.7 교육연구단의 대표적 미래 목표에 대한 달성 방안

- [교육목표] 인공지능 분야에 특성화된 박사과정 중심의 국내 최고의 연구 중심 대학원으로 발전
 - ✓ (핵심지표) 신입생 유치 실적 (괄호 안: 박사/통합과정): 1차년도 15명(7명) → 2차년도 20명(10명)
 - ✓ 컴퓨터공학전공, 사이버보안전공, 인공지능융합전공이 협력하여 AI 기초부터 응용까지 아우르는 교육 체계를 설계하고, 효율성 · 프라이버시 · 공격/방어 등 고도화 주제를 다루는 교과과정을 통해 실질적 역량을 갖춘 인재를 양성함.
 - ✓ 박사과정 유도 강화: BK21 장학금, 연구 인턴 장려금, 학술활동비 지원을 통한 재정적 지원
 - ✓ 우수 학부생을 대상으로 학석연계형 AI · 보안 융합 설명회 및 진로 컨설팅 진행
 - ✓ 통합과정 이수자의 연구성과(논문 · 특허 등)를 성과기반 장학제도와 연계하여 지속가능성 확보
- [연구목표] 인공지능 모델의 효율성, 보안 인공지능 분야에서 세계적 경쟁력을 가진 연구 성과 창출
 - ✓ (핵심 지표) H-index 20 이상 사업단 참여교수 비율: 현재 33% → 1차년도 38% → 2차년도 45%
 - ✓ 효율적인 AI 모델 설계, 적대적 공격 대응, 프라이버시 보장 등 핵심 기술을 보유한 연구진 간의 협업을 통해 상호보완적이고 시너지를 창출하는 융합 연구를 활성화함
 - ✓ 제한된 자원 환경에서도 고성능을 발휘할 수 있는 효율적인 AI 모델 설계를 위한 핵심 기술을 집중 연구하여, 자원 효율성과 성능을 동시에 확보함
 - ✓ 시스템 보안, AI 기반 프라이버시 보호, 적대적 공격 대응 등 사회적 파급력이 큰 이슈에 대해 선제적으로 대응할 수 있는 기술적 해법을 제시하여 기술의 사회적 책임을 실현함
- [산학목표] 산업체 수요 기반의 실용 연구 및 인재 양성을 통해 산학 연계의 선순환 체계 구축
 - ✓ (핵심 지표) 인턴 1차년도 10건 → 2차년도 15건, 기술이전 2건 (2차년도)
 - ✓ 국내 주요 AI 산업 분야와의 공동연구 및 기술이전을 통해 현장 적용이 가능한 연구성과 도출
 - ✓ 산업체 수요를 반영한 맞춤형 연구 주제를 발굴하고, 이를 박사과정의 산학 프로젝트와 연계
 - ✓ 현장 중심형 산학 인턴십을 확대하고, 참여 기업과의 정기 기술 교류회를 통해 협력 체계 유지
 - ✓ 산학 공동 연구실 및 기술협력센터를 통해 산업체와의 공동기술개발, 지식재산 창출, 창업 연계
- [국제화 목표] 국제 공동연구 및 학술 활동을 통해 글로벌 연구 허브로 도약
 - ✓ (핵심 지표) 국제 공동연구 총 24건(2년), 인적교류 총 12건(2년)
 - ✓ 국제학회 참여, 공동연구 수행, 해외 연구자 초청 세미나를 촉진하기 위한 인센티브 체계 구축
 - ✓ 우수 해외 연구기관과의 협력을 확대하고, 공동 과제 수행을 통한 글로벌 연구 네트워크를 강화
 - ✓ 국제 학술단체 활동 및 글로벌 AI 컨소시엄 참여를 장려하여, 교육연구단의 국제적 위상 제고

1.3 교육연구단의 구성

① 교육연구단장의 교육·연구·행정 역량

성명	한글	양대현	영문	DaeHun Nyang
소속기관	이화여자대학교	인공지능대학	인공지능·소프트웨어학부	
원소속기관	이화여자대학교	인공지능대학	사이버보안학과	

<표 1-1> 교육연구단장 최근 5년간 연구실적

연번	저자/수상자/ 발명자/창업자	논문 제목/ 저서 제목/ book chapter 제목	학술지명/학술대 회명/ 출판사명/행사명	권(호), 페이지/ISSN/ ISBN(pp. **-**)	제재/출판/ 행사 연도	DOI 번호 (해당 시)
1	Sian Kim, Seyed Mohammad Mehdi Mirnajafizadeh, Bara Kim, Rhongho Jang, DaeHun Nyang	SketchFeature: High-Quality Per-Flow Feature Extractor Towards Security-Aware Data Plane	ISOC Network and Distributed System Security Symposium (NDSS 2025)	979-8-9894372-8-3	2025	https://doi.org/10.14722/ndss.2025.241071
2	Sian Kim, Changhun Jung, Rhongho Jang, David Mohaisen, DaeHun Nyang	A Robust Counting Sketch for Data Plane Intrusion Detection	ISOC Network and Distributed System Security Symposium (NDSS 2023)	1-891562-83-5	2023	https://doi.org/10.14722/ndss.2023.2323102
3	Changhun Jung, Sian Kim, Rhongho Jang, David Mohaisen, DaeHun Nyang	A Scalable and Dynamic ACL System for In-Network Defense	ACM Conference on Computer and Communications Security (ACM CCS 2022)	978-1-4503-9450-5/22/11	2022	https://doi.org/10.1145/3548606.3560606
4	RhongHo Jang, DaeHong Min, SeongKwang, Aziz Mohaisen, DaeHun Nyang	SketchFlow: Per-Flow Systematic Sampling Using Sketch Saturation Event	IEEE INFOCOM 2020 - IEEE Conference on Computer Communications	978-1-7281-6413-7 / 978-1-7281-6412-0	2020	https://doi.org/10.1109/infocom41043.2020.9155252
5	Sungha Baek, Youngdon Jung, David Mohaisen, Sungjin Lee, DaeHun Nyang	SSD-assisted ransomware detection and data recovery techniques	IEEE Transactions on Computers	Vol. 70, No. 10, pp. 1762-1776	2021	https://doi.org/10.1109/tc.2020.3011214

○ 교육연구팀장의 교육역량

- ◆ 2003년부터 현재까지 22년째 컴퓨터공학 분야에서 후학을 양성하고 있음
- ◆ 알고리즘 중심의 사고를 위한 새로운 교육 방법론을 개발하고, ‘문제해결기법’ 교과목을 개설하여 6년 동안 학생들을 교육하며 매우 좋은 반응을 이끌어 냈음
- ◆ 우수강의상, 한국공학교육학회 우수강의 교수상을 포함하여 3건의 교육관련 수상 실적 보유
- ◆ 2003년부터 대학원 연구실을 운영 중으로 최근 5년간 박사 4명, 석사 11명을 배출함
- ◆ 미국대학과의 Dual Degree 프로그램을 주도적으로 개설하고 운영하여 3명의 UCF (University of Central Florida) 박사를 배출함
- ◆ 5명의 박사가 미국 유수 대학의 컴퓨터과학과 조교수 (Wayne State University, Loyola University Chicago), 부교수 (University of Central Florida), 국내외 유수 대학의 조교수 (성균관 대학교, The Erdenet Institute of Technology)로 활동 중임

○ 교육연구팀장의 연구역량

- ◆ 2019-현재까지 40편의 연구 논문을 빅데이터, 사이버 보안/프라이버시 관련 최우수 학술대회 및 학술지인 IEEE INFOCOM (BK21+ IF-4), ACM CCS (BK21+ IF-4), NDSS (BK21+ IF-2), USENIX SECURITY, ICDCS (BK21+ IF-3), PETS (BK21+ IF-2), IEEE Comm Surveys and Tutorials (IF-35.6), IEEE IoT J (IF-10.6), IEEE TDSC (IF-7.3), FGCS (IF-7.5), IEEE TMC (IF-7.9) 등에 출판함
- ◆ 최근 연구 결과물은 보안/프라이버시를 위한 분야에 집중되어 있는데, AI 기술의 취약성, AI를 활용한 보안/프라이버시 분야에서 ACM CCS, Usenix Security, NDSS 등 관련 분야 최우수 학술대회와 저널에 연구성과를 게재하였음.
- ◆ 특히, 인공지능 기반 네트워크 침입탐지기술에서 네트워크 데이터 처리/분석은 처리 시간, 요구되는 컴퓨팅 용량, 메모리 사용량 등의 오버헤드를 고려한 효율적 수행을 위해 필수적인 분야이며, 교육연구팀장은 관련 연구 분야에서 국제적으로 최고의 성과를 거두고 있음
- ◆ 특히, 교육연구팀의 목표인 데이터 중심 보안 및 프라이버시를 위한 핵심 연구분야에 대한 오랜 경험을 바탕으로 해당 분야의 교육과 연구 부분을 리드할 역량을 보유하고 있음

○ 교육연구팀장의 행정역량

- ◆ 연구기간 2년, 총 사업비 15억 원, 총 4개의 참여기관, 참여인력 약 40명의 IIITP 과제를 주관기관의 사업책임자로서 성공적으로 수행함
- ◆ 연구기간 6년, 총 사업비 28억 원, 총 2개의 연구실, 참여인력 약 50명의 한국연구재단 과제를 사업책임연구자로서 성공적으로 함 (3개년 단계 평가 결과: S등급)
- ◆ 정보통신처 처장 대행, 정보통신처 부처장, 정보통신처장, 학과장으로 학교의 행정 업무를 수행함
- ◆ 3년 동안 한국연구재단 전문위원으로 정보과학회 우수학술대회 목록 개편 위원으로 활동함
- ◆ 17년 동안 한국정보보호학회 논문지 편집위원으로 활동한 후, 2020-2025년까지 정보보호학회 논문지 편집위원장으로 활동 중임
- ◆ 2017년부터 ETRI Journal (SCI-indexed) 정보보호 섹션 편집위원장으로 활동 중임
- ◆ 관련 연구분야 최우수학술대회인 IEEE ICDCS, IEEE DSC, IEEE MSN/MASS, ICISC에 프로그램위원으로 활동하고 있음

② 대학원 신청학과 소속 전체 교수 및 참여교수

<표 1-3> 교육연구단 신청학과 소속 전체 교수 및 참여교수 현황

기준일	신청학과명	전체 교수 수			참여교수 수 (단위: 명)						합계	
					기존교수 수			신임교수 수				
		전임	겸임	계	전임	겸임	계	전임	겸임	계		
접수 마감일	인공지능 · 소프트웨어학부	0	12*	12	0	7*	7	0	5*	5	12	

*본교 규정상 학부 소속의 이들 전임 교수진은 대학원 과정인 인공지능 · 소프트웨어학부에 겸임으로 등재되어 있음

③ 교육연구단 구성의 적절성

<표 1-4> 참여교수진의 인공지능 분야 교육 실적 및 연구 분야

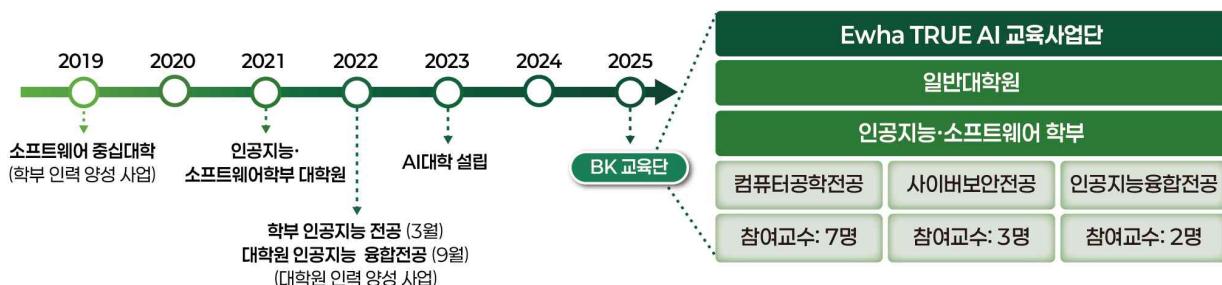
연번	성명 (한글/영문)	직급	연구자등록번호	소속 대학 및 소속 학과	세부전공분야	인공지능 관련 대학원 교과목 개설 실적
	인공지능 관련 연구분야와의 연계성					
1	양대현 DaeHun Nyang	정교수	10116341	이화여자대학교 인공지능소프트 웨어학부	인공지능시스템 및응용	침입탐지시스템 (2023년 1학기) 사이버보안특론Ⅲ (2025년 1학기)
	<ul style="list-style-type: none"> - 인공지능 기반 침입탐지를 위한 네트워크 모니터링, 특징 추출 알고리즘 원리를 AI 탐지 모델에 적용 - 네트워크에서 발생하는 다양한 보안 문제 제기와 이를 해결하기 위한 인공지능 기반의 최신 연구 수행 					
2	김종길 Jongkil Kim	부교수	12961764	이화여자대학교 인공지능·소프 트웨어학부	정보보호	AI기반IoT보안 (2024년 2학기) 차세대보안특론 (2024년 1학기)
	<ul style="list-style-type: none"> - 데이터 프라이버시 보호를 위한 영지식증명 및 암호화 관련 연구 수행 - 인공지능을 이용한 침입탐지알고리즘 개발과 관련한 연구 수행 					
3	배호 Ho Bae	조교수	11635105	이화여자대학교 인공지능소프트 웨어학부	기계학습및지식 처리	인공지능보안특론 (2024년 2학기)
	<ul style="list-style-type: none"> - LLM 모델 공격, 코드 보안, 모델 포이즈닝 등 인공지능 모델에 대한 공격 및 방어에 대한 연구를 수행 중. - AI 시스템의 신뢰성과 안전성을 확보하기 위한 모델 취약점 분석 및 대응 기법을 중심으로 연구를 수행 중. 					
4	오세은 Se Eun Oh	조교수	12880629	이화여자대학교 인공지능소프트 웨어학부	인공지능시스템 및응용	딥러닝보안 (2025년 1학기)
	<ul style="list-style-type: none"> - 멤버십 추론, 학습데이터 복원 등 인공지능 모델의 보안/프라이버시 문제 해결위한 연구 수행 - 인공지능 모델을 활용한 악성코드 탐지, 익명화 네트워크 모니터링 등 보안 솔루션 개발 연구 수행 					
5	노준혁 Junhyug Noh	조교수	11436386	이화여자대학교 인공지능소프트 웨어학부	시각정보처리	인공지능개론 (2024년 2학기)
	<ul style="list-style-type: none"> - 제한적인 학습 환경에서도 성능을 확보하기 위한 준지도/약지도 학습, 능동 학습, 도메인 적응 기법 등 의 연구 수행 - 모델의 학습 효율성 및 해석 가능성을 높이기 위한 신뢰 가능한 인공지능 및 설명 가능한 AI(XAI) 기법 연구 수행 					
6	민동보 Dongbo Min	부교수	10190916	이화여자대학교 인공지능소프트 웨어학부	시각정보처리	컴퓨터비전특론 (2025년 1학기) 컴퓨터비전개론 (2023년 2학기)
	<ul style="list-style-type: none"> - 컴퓨터비전 분야에서 자율주행, 로봇을 위한 효율적 장면이해(3차원 깊이, 객체 분할, 모델 경량화)와 실세계 적용을 위한 도메인 일반화 연구 수행 - 거대 비전 모델의 효율적 사전학습 및 이를 멀티모달 모델로 확장하는 연구 수행 					
7	반효경 Hyokyung Bahn	정교수	10091721	이화여자대학교 인공지능소프트 웨어학부	인공지능시스템 및응용	AI융합기반기술주제연구 I (2024년 2학기)
	<ul style="list-style-type: none"> - 현대의 AI 워크로드가 전통적인 워크로드와 어떻게 다른지 참조 패턴 및 자원 사용 특성 등을 분석하고 시스템 SW가 이를 효율적으로 대처하기 위한 각종 전략을 연구함 					

I. 교육연구단의 구성, 비전 및 목표

혁신인재양성사업 인공지능 분야 교육연구단 사업

8	윤명국 Myung Kuk Yoon	조교수	11089187	이화여자대학교 인공지능소프트 웨어학부	프로세서및분산 /병렬컴퓨터구 조	고급컴퓨터구조 (2025년 1학기)
	<ul style="list-style-type: none"> - 그래픽 처리 장치(GPU) 및 머신러닝 가속기의 아키텍처 최적화 연구 수행 - 이기종 연산 지원(GPU/NPU)을 활용한 고성능 AI 소프트웨어 구현 및 시스템 수준 최적화 연구 수행 					
9	이지영 Jiyoung Lee	조교수	11564062	이화여자대학교 인공지능소프트 웨어학부	인공지능시스템 및응용	
	<ul style="list-style-type: none"> - 멀티모달 분야에서 영상, 음성, 자연어를 이해하고 서로의 정보를 생성하는 생성형 모델 개발 연구 - 거대 멀티모달 모델의 효율적 학습을 위한 학습 경량화 방법 및 멀티모달 임베딩 정렬 연구 					
10	이형준 Hyungjune Lee	교수	11091991	이화여자대학교 인공지능소프트 웨어학부	인공지능시스템 및응용	엣지 컴퓨팅개론 (2025년 1학기)
	<ul style="list-style-type: none"> - 엣지컴퓨팅, 엣지 네트워크, 엣지 AI 분야에서 디바이스 및 디바이스간의 네트워크를 활용한 분산 학습, 경량 학습, 멀티모달 학습 연구 수행 - 연합학습, 디바이스간 선택적 전이 학습 및 효율적 경량 멀티모달 학습 모델 아키텍처 및 시스템 개발 연구 수행 					
11	오유란 Uran Oh	부교수	11812138	이화여자대학교 인공지능소프트 웨어학부	인공지능시스템 및응용	인간컴퓨터상호작용특론 (2023년 2학기)
	<ul style="list-style-type: none"> - 사용자의 멀티모달 입력 (제스처, 음성, 표정 등) 인식 모델을 응용한 지능형 인터페이스 개발 연구 - 멀티모달거대언어모델(MLM)을 활용한 사용자맞춤형 추천 및 개인화 시스템 설계 및 구현 연구 - 감성컴퓨팅기반 인간-로봇 상호작용 및 Human-in-the-loop기반의 인간-AI 상호작용 연구 					
12	황의원 Uiwon Hwang	조교수	11462992	이화여자대학교 인공지능소프트 웨어학부	컴퓨터/인공지 능	
	<ul style="list-style-type: none"> - 데이터 결측, 클래스 불균형, 라벨 부족 등 실세계 데이터의 제약을 극복하기 위한 생성형 인공지능 연구 수행 - 다양한 모달리티와 도메인 간 이질성을 극복하고 범용 인공지능을 구현하기 위한 멀티모달 AI 및 도메인 적용 연구 수행 					

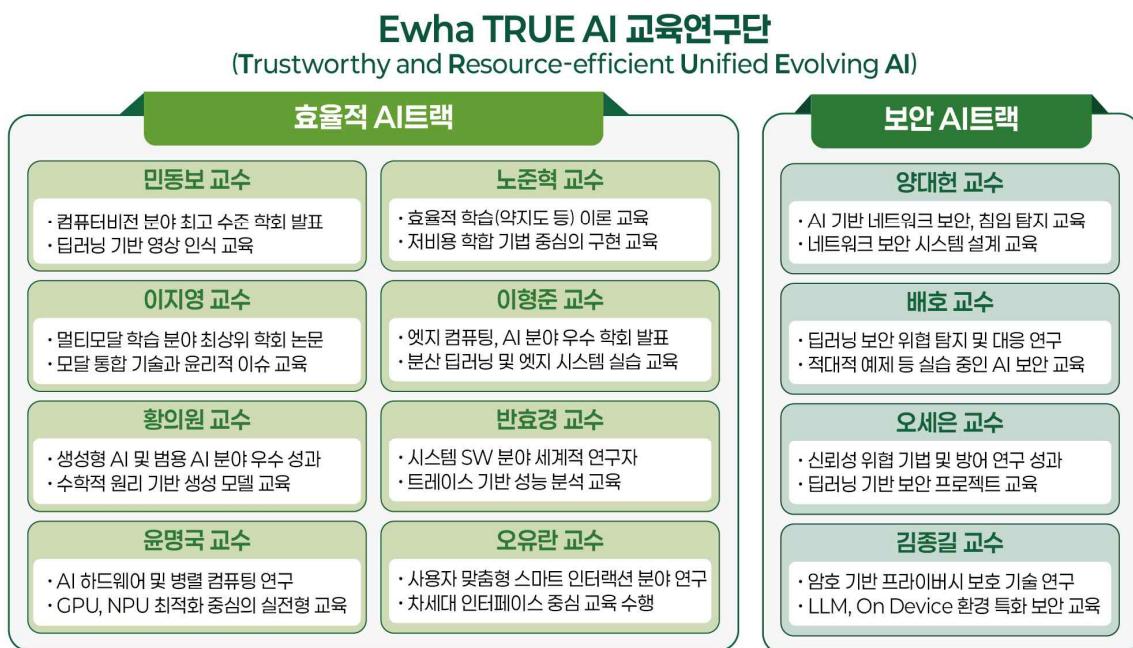
○ 신청 단위 유형의 배경 및 타당성



〈그림 1-4〉 인공지능대학 역사 및 TRUE-AI 교육연구단의 구성

- ✓ 이화여대 일반대학원 인공지능소프트웨어학부는 AI 핵심기술부터 응용·보안까지 포괄하는 단일학부 내 3개 전공(컴퓨터공학, 사이버보안, 인공지능융합)으로 구성되어 있음 (그림 1.4 참조)
 - ※ 현재 본교 인공지능대학에는 학부 기준으로 29명의 전임교수가 존재하며, 대학원 과정인 인공지능·소프트웨어학부에는 12명의 전임교수가 소속돼 있고 이들 모두 본 교육연구단에 참여함. (본교 규정상 학부에 소속을 두고 있는 이들 교수진은 대학원 과정인 인공지능·소프트웨어학부에 겸임으로 등재되어 있음)
- ✓ 각 전공은 AI 신뢰성(trustworthiness), 자원 효율성(resource-efficiency), 다양한 모델에의 융합 및 확장성(unified and evolving AI)이라는 본 교육연구단의 핵심 비전과 유기적으로 연계되어 있음
- ✓ 본 학부의 전공별 특성을 활용한 융합적 AI 교육 및 연구 수행에 최적화된 구조는 BK21 교육연구단의 단일학부형 신청 유형에 완벽하게 부합함
 - + **컴퓨터공학전공:** AI 모델 설계 및 SW/HW 최적화를 위한 교육 및 연구를 통해 자원 효율성통합적 AI구현에 기여함
 - + **사이버보안전공:** AI 기반 보안 위협 탐지 및 신뢰성(trustworthiness)문제 해결에 대한 교육 및 연구를 선도함
 - + **인공지능융합전공:** 멀티모달 도메인을 위한 AI+X 융합 역량 및 실전형 문제 해결 능력 배양을 통해 진화 가능한 AI생태계 조성에 핵심적인 역할을 수행함
- ✓ 세 전공은 대학원 모집 정원과 교육과정이 긴밀하게 연계되어 있으며, 전공 간 교차 수강, 공동 교과 운영, 융합형 프로젝트 수행 체계를 통해 자연스러운 학제 간 협력 구조를 갖추고 있음.
- ✓ 특히, 본교는 인공지능 기술의 급격한 발전과 사회적 수요 증가에 대응하기 위해 AI 분야 연구 역량 강화를 위한 학제 개편을 전략적으로 추진해왔음.
 - + 2019년 소프트웨어 중심대학 사업(학부 인력 양성)
 - + 2021년 인공지능소프트웨어학부 대학원 설립
 - + 2022년 학부 인공지능전공(3월) 및 대학원 인공지능융합전공(9월, 대학원 인력 양성) 신설
- ✓ 2023년에는 다양한 응용 분야를 연결하는 핵심 분야로서 인공지능의 위상을 강화하고 전공 간 연계 및 융합을 촉진하고자 기존 컴퓨터공학과, 사이버보안학과, 인공지능학과, 데이터사이언스학과를 통합하여 “인공지능대학”을 신설하였음
- ✓ 이는 교육과 연구의 시너지 효과를 극대화할 수 있는 구조임. 이어 2025년에는 인공지능학과와 데이터사이언스학과를 “인공지능데이터사이언스학부”로 통합하고, 세부 전공으로 인공지능 전공과 데이터사이언스 전공을 개설함으로써, AI와 데이터 분석에 모두 능숙한 융합형 인재 양성을 위한 기반을 더욱 공고히 마련하였음. 이러한 학제 개편은 본 교육연구단의 혁신적인 교육 및 연구 환경 조성에 강력한 배경이 될 것으로 판단됨
- ✓ 이는 “고신뢰 고효율 인공지능 교육연구단”의 통합적이고 진화 가능한 AI 교육 생태계 조성이라는 목표에 부합하는 기반이 됨. 이처럼 소프트웨어중심대학, 인공지능융합대학원 등 대형 국책 사업을 성공적으로 수행하며 인력 양성 및 연구 역량 강화에 대한 경험과 노하우를 축적해 왔음

○ 참여 교수진 구성의 적절성



<그림 1-5> 참여 교수진의 교육 및 연구 분야

- ✓ 본 교육연구단은 “효율적 AI 트랙”에 8명, “보안 AI 트랙”에 4명의 교수를 포함하여 총 12명의 전문 교수진으로 구성되어 있음 (그림 1-5 참조)
- ✓ AI 핵심 기술(모델 경량화, 연합 학습, 멀티모달 학습, 시스템 아키텍처 최적화)부터 신뢰성, 실시간성, 효율성, 보안성까지 포괄하는 심층적인 전문성을 보유하고 있음
- ✓ 참여 교수진은 다수의 거대 AI, 보안 AI 등 국가 R&D 과제 수행 경험과 산업체·공공기관 협업 기반 실증 경험을 바탕으로, 실전형 고급 인재 양성에 특화된 교육 역량을 보유하고 있음. 특히, AI 학회(NeurIPS, CVPR, ICLR, AAAI), 시스템 학회(ASPLOS, ISCA, ISPASS)에서의 논문 게재 및 조직 활동을 통해 연구 경쟁력을 확고히 입증하고 있음
- ✓ 다양한 전공 배경의 교수진은 팀티칭 기반의 융합형 AI 교육과정을 공동 기획 및 운영하며, TRUE-AI의 핵심 키워드인 신뢰성(Trustworthy), 효율성(Resource-efficient), 통합성(Unified), 진화성(Evolving)을 반영한 교육·연구·산학 순환 체계를 실현하고 있음

- ◆ [효율적 AI 트랙 (8명) - 자원 효율성 AI 모델 + AI 융합 연구 및 교육 담당]
 - ✓ 컴퓨터비전, 엣지 AI, 시스템 소프트웨어, 인공지능 하드웨어, 생성형 AI, 학습이론, 멀티모달 학습 등 폭넓은 연구 분야를 아우르는 8인의 전문 연구진으로 구성되어 있음
 - ✓ CVPR, ICCV, ISCA, ICML, ICLR, INFOCOM, USENIX FAST, IEEE TC 등 컴퓨터 과학 및 인공지능 분야 최상위 국제 학술대회 및 저널에 다수 논문을 게재
 - ✓ Spotlight 발표, Best Paper 수상, 산업체 공동 연구 및 특허 등 우수한 실적을 보유하고 있어 고효율 AI 기술의 학문적 기반 확립과 실용화에 모두 기여할 수 있는 역량을 갖춤
 - ✓ 참여 교수진은 각자의 전공 분야에서 실습 중심의 고도화된 교육과정을 운영하며, 컴퓨터비전특론, 엣지컴퓨팅개론, 인공지능소프트웨어, 생성형인공지능, 효율적학습특론, 멀티모달머신러닝개론 등 차세대 AI 인재 양성을 위한 핵심 교과목을 담당함
 - ✓ KOCW 인기 강의, 대기업 플랫폼 공개 강의, 국내외 산업체 연계 프로젝트 등을 통해 교육의 파급력과 접근성을 동시에 확보하고 있음

<표 1-a> 교육연구단 참여교수진의 연구 및 교육 역량: 효율적 AI 트랙

효율적 AI 트랙: 교수진 연구 및 교육 역량	
민동보 교수	<ul style="list-style-type: none"> ✓ 시각인공지능에 해당하는 컴퓨터비전 전공자로 지난 5년 동안 자율주행을 위한 3 차원 장면 이해, 모델 경량화, 거대 비전 모델의 효율적 사전학습을 연구하였음 ✓ 최근 5년간 딥러닝을 적용하여 컴퓨터비전의 여러 문제를 해결하는 연구를 수행하며 CVPR, ICCV, ECCV, NeurIPS 14편, SCI 저널 15편 (상위 3% SCI 저널 7편 포함)을 게재함 ✓ 주 담당 교과목인 “컴퓨터비전특론”은 딥러닝 기반 컴퓨터비전 기술의 핵심 개념부터 최신 연구 동향까지를 이론, 실습, 팀 프로젝트 중심으로 학습하는 심화 트랙 교과목임 ✓ 이미지 분류, 객체 탐지, 생성 모델 등 실제 연구 및 산업 응용을 위한 주제를 중심으로 구성되어, 수강생의 실전형 인공지능 개발 및 구현 역량을 강화함
이형준 교수	<ul style="list-style-type: none"> ✓ 엣지 컴퓨팅, 엣지 AI 분야에서 ECCV, PerCom, MASS, INFOCOM, SECON 등 BK21 우수학술대회 및 IEEE Internet of Things(상위 5%), IEEE Transactions on Vehicular Technology(상위 15%) 저널 등에 논문을 발표 ✓ 주 담당 교과목인 “엣지컴퓨팅개론”은 포그 네트워크 아키텍처 기반의 엣지 컴퓨팅 개념과 응용을 중심으로, 분산 자원 활용 및 프라이버시 문제 해결을 위한 핵심 기술을 학습하는 과목임 ✓ 분산 딥러닝 및 학습 가속화를 위한 최신 연구 방법을 실습과 프로젝트 중심으로 탐구함으로써, 엣지 AI 분야의 실질적 연구 역량을 함양함
반효경 교수	<ul style="list-style-type: none"> ✓ 시스템 SW분야 연구자로 IEEE TC, TKDE, TII, ACM Tos, IEEE Computer, USENIX FAST 등 저명 국제 학술지 및 학술대회에 워크로드 분석 및 시스템 자원관리 최적화 관련 100여편 이상의 논문을 게재 ✓ 국내 최초 USENIX 학회 Best paper 수상 이력을 가지고 있음 ✓ 주 담당 교과목인 “컴퓨터시스템의 성능평가와 모델링”과 “고급분산처리특론”은 차세대 AI 시스템을 위한 분산 처리 기술을 심화 학습하는 고급 교과목임 ✓ “컴퓨터시스템의 성능평가와 모델링”에서는 AI 워크로드가 시스템 자원에 미치는 영향을 트레이스 기반으로 분석하고, 이를 정량적 모델로 표현하여 논문 작성 ✓ 교육 쪽으로는 운영체제 및 오픈SW관련 교육 공개로 KOCW에 월간 인기강의 선정(50만회 이상 수강), Tizen 강의 및 Lecture Material의 삼성 타이젠 홈페이지 공개 등의 이력이 있음
윤명국 교수	<ul style="list-style-type: none"> ✓ 그래픽 처리 장치(GPU), 머신 러닝 가속기, 병렬 프로그래밍, 컴퓨터 아키텍처에 대한 인공지능 하드웨어 연구를 활발히 하고 있음 ✓ ISCA, NeurIPs, AAAI 등 CS분야 최우수 학술대회 및 다수의 SCI급 학술지에 논문을 발표하였음 ✓ 주 담당 교과목인 “인공지능 소프트웨어”는 고성능 AI 모델의 학습 및 추론을 위해 GPU, NPU 등 이기종 하드웨어에 특화된 병렬 프로그래밍 및 최적화 기법을 실습 중심으로 다루는 교과목임 ✓ CUDA, NPU 최적화, 시스템 수준 이슈 등 산업 현장에서 요구되는 핵심 기술을 폭넓게 교육함으로써, 수강생의 AI 소프트웨어 구현 및 성능 개선 역량을 강화함
황의원 교수	<ul style="list-style-type: none"> ✓ 실세계 시나리오에서 인공지능의 신뢰성을 높이고, 범용 인공지능의 기반이 되는 핵심기술을 활발히 연구하고 있음 ✓ ICML, ICLR, ECCV, IJCV 등 CS분야 최우수 학술대회 및 SCI급 학술지에 다수의 논문을 주저자로 게재하고, 최상위 연구에 기회가 주어지는 Spotlight으로 발표함 ✓ 융합연구인 생성형 AI 기반 의생명 파운데이션 모델 연구에서도 수월성 확보 ✓ “생성형인공지능”은 오토인코더, GAN, 확산 모델 등 주요 생성 모델의 수학적 구조와 학습 원리를 이론과 실습을 통해 심도 있게 학습하는 교과목임

	<ul style="list-style-type: none"> ✓ 멀티모달 대규모 언어 모델 등 최신 기술까지 아우르며, 범용 인공지능으로의 확장을 이해할 수 있도록 구성되어 차세대 AI 개발 역량을 체계적으로 강화함
노준혁 교수	<ul style="list-style-type: none"> ✓ 약지도 · 능동학습 · 도메인 적응을 아우르는 수학적 · 이론적 프레임워크 설계 및 알고리즘 연구를 수행하고 있으며, 다양한 실제 도메인에서 학습 · 적응 방법론을 적용 · 평가한 실무 경험을 가지고 있음 ✓ 워드브릭스(미국), 에스프레스토, DXR, 휴먼퍼포먼스랩, 임팩트랩스(대한민국) 등 다수 스타트업 자문을 맡고 있음 ✓ 주 담당 교과목인 “효율적 학습 특론”과 “패턴 인식 및 머신 러닝”은 AI 모델의 학습 효율성과 일반화 성능 향상을 위한 이론과 실습을 아우르는 심화형 교과목임 ✓ “효율적 학습 특론”에서는 self-/semi-/weakly-supervised learning, active learning, domain adaptation 등 실제 제약 환경에서도 고성능을 달성할 수 있는 학습 패러다임을 중심으로 최신 연구 동향과 실습 프로젝트를 병행함 ✓ “패턴 인식 및 머신 러닝”은 확률 기반 분류, 군집화, 회귀, 양상분석, 차원 축소, 기초 딥러닝까지 핵심 알고리즘을 수학적 기초와 함께 다루며, 실습 중심의 과제를 통해 인공지능 기초 역량을 체계적으로 함양함
이지영 교수	<ul style="list-style-type: none"> ✓ 멀티모달 인공지능 모델을 위한 학습 방법 개발 및 컨텐츠 생성 연구를 수행하고 있으며, CVPR, ICLR, ICCV, ECCV, AAAI 등 CS분야 최우수 학술대회 및 SCI급 저널에 다수 인공지능 논문을 게재하였음 ✓ 해외 빅테크 산업체(Microsoft, Adobe)와의 공동연구를 통한 국제 특허 등록, 공동 논문 발표, 코드 공개등을 수행함 ✓ 주 담당 교과목인 “멀티모달 머신러닝 개론”과 “음성 시스템”은 다양한 형태의 데이터를 통합적으로 처리하는 기술과, 음성 기반 인공지능 시스템 개발을 위한 핵심 이론 및 실습을 함께 다루는 심화형 교과목임 ✓ “멀티모달 머신러닝 개론”에서는 표현 학습, 정렬, 융합, 생성 등 멀티모달 처리의 기초 이론과 더불어 편향성, 프라이버시, 설명가능성 등 실제 적용상의 도전 과제를 폭넓게 탐구함 ✓ “음성 시스템”에서는 최신 음성 인식 및 합성 모델(wav2vec, HuBERT, Whisper 등)을 중심으로 음향언어 모델 구조, 디코딩 기법, 음성 기반 다운스트림 테스크 까지 실습과 이론을 병행하여 실전형 음성 AI 시스템 구축 역량을 배양함
오유란 교수	<ul style="list-style-type: none"> ✓ 인공지능 기술을 활용한 사용자맞춤형 스마트 인터랙션 관련 연구를 수행하고 있으며 ACM CHI, WWW, IUI, UbiComp, IEEE ICPR, TVCG, ISMAR 등 CS분야 최우수 /우수 학술대회 및 SCI 학술지에 다수의 논문을 게재함 ✓ 미국 구글사와의 공동연구를 통해 국제특허 등록, (주)보해미안로보틱스 이사 겸직 ✓ 주담당교과목인 “인간컴퓨터상호작용특론”은 인간-AI 상호작용의 관점에서 생성형 AI를 비롯한 차세대 인공지능기술을 활용하여 사용자 개개인에 특화된 지능형 인터페이스를 심도있게 다루는 교과목임 ✓ 음성/제스처/표정 인식등 사용자의 멀티모달 입력을 처리하는 딥러닝 모델 및 사용자의 특성 및 맥락을 반영한 개인화된 추천 시스템 등 인공지능 기술을 실전에 응용하는 법을 습득함

◆ [보안 AI 트랙 (4명) - AI 신뢰성 연구 및 교육 담당]

- ✓ AI 기반 보안 기술의 이론부터 응용까지 폭넓게 아우르는 4인의 전문 연구진으로 구성되어 있음.
- ✓ 최근 5년간 S&P, CCS, Security, NDSS, PETS, ASIACCS, ESORICS, ICLR 등 보안 및 AI 분야 최상위 국제학회에 다수의 논문을 발표하며 연구 역량을 입증함

- ✓ 침입 탐지, 암호 응용, 코드 분석, 네트워크 방어 등 다양한 영역에서 독창적 기법을 제안하며, AI의 신뢰성과 안전성을 높이는 데 기여하고 있음
- ✓ 컴퓨터보안특론, 인공지능융합보안, 딥러닝보안, AI기반IoT보안 등 AI 보안 특화 고급 교과목을 중심으로 체계적인 교육 과정을 운영하고 있음
- ✓ 실제 위협 시나리오 기반의 이론 강의와 실습, 논문 리뷰 및 프로젝트 수행을 통해 실전 대응력을 갖춘 보안 인재를 양성함

〈표 1-b〉 교육연구단 참여교수진의 연구 및 교육 역량: 보안 AI 트랙

보안 AI 트랙: 교수진 연구 및 교육 역량	
양대현 교수 (사업단장)	<ul style="list-style-type: none"> ✓ 인공지능을 위한 네트워크 기반 기술, 특히 침입탐지/방어에 대한 논문을 CCS, NDSS, Security, INFOCOM 등 BK4점에 해당하는 연구들을 수행하였음. ✓ Deep learning을 이용하여 소프트웨어의 소스코드를 분석, 저자를 식별할 수 있는 기술 등을 개발함 ✓ 주 담당 교과목인 “컴퓨터보안특론”, “시스템보안특론”, “사이버보안특론”은 네트워크와 시스템 보안 이슈를 심층적으로 다루고, AI 기반 침입 탐지 및 프라이버시 보호 기술까지 포괄하는 고급 보안 교과목임 ✓ 라우터 아키텍처와 트래픽 분석, 데이터 스케치 기반 특징 추출, 인-네트워크 방어 등 다양한 관점에서 실시간 침입 탐지 기술을 학습하며, AI 모델이 접근제어와 이상 탐지를 수행할 수 있도록 설계되는 구조를 탐구함
배호 교수	<ul style="list-style-type: none"> ✓ 박사학위 취득 이전부터 줄곧 기계학습 및 보안 분야를 연구해온 전문가로 지난 3년간 ICLR, ESORICS, RAID 등 BK21 우수학술대회 등 저명 국제 학술지에 15편의 논문을 발표하였음 ✓ 주 담당 교과목인 “인공지능융합보안”은 딥러닝 기반 AI 모델에서 발생할 수 있는 다양한 보안 위협과 이를 대응하기 위한 방어 기술을 다루는 교과목임 ✓ 적대적 예제, adversarial training, 멤버십 추론 등 최신 보안 이슈를 중심으로 AI 활용 환경에서의 데이터 보호 원리를 심도 있게 학습함
오세은 교수	<ul style="list-style-type: none"> ✓ 보안이 강화된 네트워크 시스템에서 인공지능 모델 기반 네트워크 트래픽 분석을 가능케 하는 다양한 공격방식을 보이고 이에 대한 방어기법을 제안하여 사이버 보안분야 탑컨퍼런스인 S&P, PETS에 발표하였음 ✓ 주 담당 교과목인 “딥러닝보안”은 기계학습 및 딥러닝 기법을 보안 문제 해결에 적용하는 방법을 이론과 실습을 통해 종합적으로 학습하는 교과목임 ✓ 모델 포이즈닝, 적대적 예제, 멤버십 추론 공격 등 신뢰성 위협 기법을 중심으로 실제 실험과 프로젝트를 수행하며, AI 기반 보안 솔루션의 설계 역량을 강화함
김종길 교수	<ul style="list-style-type: none"> ✓ 함수 암호 및 검색 암호를 기반으로 한 암호알고리즘과 이에 대한 응용 어플리케이션에 대한 연구를 수행 하였음. ✓ 최근 5년간 사이버보안 분야 BK21 우수학술대회인 ASIACCS (2019,2020,2021) 및 ESORICS (2019,2021)에 발표하였음 ✓ 주 담당 교과목인 “AI기반IoT보안”과 “차세대보안 특론”은 AI와 차세대 기술이 결합된 환경에서 새롭게 발생하는 보안 위협을 탐구하고, 이를 해결하기 위한 기술적, 정책적 대응 방안을 다루는 고급 보안 교과목임 ✓ “AI기반IoT보안”에서는 LLM 및 On-Device AI 도입에 따른 프롬프트 인젝션, 모델 도용, 정보 노출 등 신종 위협을 중심으로, 입력 검증, 암호화, 접근 제어 등 다양한 방어 기법과 정책 수립 방안을 학습함 ✓ “차세대보안 특론”에서는 블록체인, 랜섬웨어, 침입탐지 등 최신 보안 이슈를 기반으로 AI/ML 기반 위협 분석 기법을 실습하며, 차세대 기술 환경에 적합한 보안 솔루션을 설계할 수 있는 실전 역량을 강화함

④ 전임교수(신임교수) 충원 계획의 적절성

〈표 1-c〉 인공지능 · 소프트웨어학부의 교원 충원 실적 및 계획

인공지능소프트웨어 학부 전공	2024년	2025년	2026년 (확정)	2027년 (예정)	2028년 (예정)
컴퓨터공학	0명	1명	2명	2명 ↑	2명 ↑
사이버보안	0명	0명	1명	1명 ↑	1명 ↑
인공지능(융합)	2명	2명	2명	2명 ↑	2명 ↑

◆ 인공지능 대학 교수 충원 계획

- ✓ 본교는 인공지능 기술의 급격한 발전과 이를 둘러싼 사회적 수요 증가에 대응하기 위해, AI 분야의 연구역량을 체계적으로 강화할 수 있도록 학제 개편과 전임교원 충원을 전략적으로 추진하고 있음
- ✓ 다양한 응용 분야를 연결하는 핵심 분야로서 인공지능의 위상을 강화하고, 전공 간 연계 및 융합을 촉진하기 위해 2023년 “인공지능대학”을 신설함. 해당 단과대학은 기존 컴퓨터공학과, 사이버보안학과, 인공지능학과, 데이터사이언스학과를 통합하여 구성되었으며, 교육과 연구의 시너지 효과를 극대화할 수 있는 구조를 갖추고 있음. 이어 2025년에는 인공지능학과와 데이터사이언스학과를 “인공지능데이터사이언스학부”로 통합하고, 세부 전공으로 인공지능 전공과 데이터사이언스 전공을 개설함으로써, AI와 데이터 분석에 모두 능숙한 융합형 인재 양성을 위한 기반을 마련
- ✓ 이러한 학제 개편과 연계하여 전임교원 충원도 단계적으로 이루어지고 있음 (표 1-c 참조)
 - + 2024년: 인공지능융합 전공 2명 충원
 - + 2025년: 컴퓨터공학 1명, 인공지능융합 2명 충원
 - + 2026년 (충원 확정): 컴퓨터공학 2명, 사이버보안 1명, 인공지능융합 2명 충원 확정
 - + 2027 · 2028년 (예정): 2026년과 동일한 수준 또는 그 이상의 충원이 예정
- ✓ 본교는 「Ewha Frontier 10-10 사업」의 예산 50억 원 중 25억 원을 국내외 석학 및 우수 교원 인건비로 배정하여, 세계적 수준의 연구역량을 갖춘 전임교원을 확보하고 있음. 초빙 대상자의 연구 성과 분석을 위해, 본 사업단의 목표 및 비전에 부합하는 연구 분야를 중심으로 후보군을 구성하고, Google Scholar 및 SciVal을 활용하여 전체 인용수, 최근 5년간 인용수, h-index, 최근 5년간 h-index 등을 평가 기준으로 활용할 계획

◆ 본 사업단의 세부 연구 목표 및 참여 교수진의 연구 분야

고신뢰 고효율 인공지능 교육연구단 (TRUE-AI)



〈그림 1-6〉 신임교원 충원에 따른 교육연구단의 구성 변경

- ✓ 본 사업단은 “고신뢰 고효율 인공지능 교육연구단”이라는 명칭에 걸맞게, 자원 효율성과 인공지능 신뢰성을 동시에 달성하기 위한 이기종 협업 기반 교육·연구 체계를 구축하고자 함. 현재 12명의 교수진이 효율적 AI(8명) 및 보안 AI(4명) 트랙으로 구성되어 있으며, 각 트랙은 해당 분야의 최우수 학술대회 및 저널에 다수의 연구 실적을 보유한 교수들로 구성되어 있음
- ✓ [효율적 AI 연구 트랙]
 - + [세부 목표 1] 거대 모델을 위한 효율적 학습 연구: 민동보, 이지영, 오유란 교수 (3명)
 - + [세부 목표 2] 엣지 디바이스를 위한 효율적 학습 연구: 이형준, 노준혁, 황의원 교수 (3명)
 - + [세부 목표 3] AI 시스템의 성능 및 자원 효율성 극대화를 위한 하드웨어 아키텍처 연구: 반효경, 윤명국 교수 (2명)
- ✓ [보안 연구 트랙]
 - + [세부 목표 1] 인공지능 모델 공격 및 보호 연구: 양대현, 오세은, 교수 (2명)
 - + [세부 목표 2] 인공지능 모델의 프라이버시 침해/보호 연구: 배호, 김종길 교수 (2명)
- ✓ 3개 세부 연구 목표(거대 모델을 위한 효율적 학습, 엣지 디바이스를 위한 효율적 학습, 인공지능 모델 공격 및 보호)는 각각 1명의 전임 교원 충원이 2026년까지 확정되어 있음
- ✓ 2개 세부 연구 목표(AI 하드웨어, 프라이버시 침해/보호)는 각각 1명의 전임 교원 추가 충원을 계획 중에 있으며, 이를 통해 교육연구단 운영 기간 내에 균형 있는 전공별 인력 확충 및 연구 역량 강화가 이루어질 예정임

◆ 교육사업단 신임 교수 충원 원칙 및 계획

- ✓ 본 교육사업단은 총 5개의 세부 연구 주제(그림 1-6)를 중심으로 구성되어 있으며, 각 주제의 효과적인 수행을 위해 2026년과 2027년 2년에 걸쳐 전임 교원을 충원할 계획임
- ✓ 2026년에는 인공지능대학에서 확정된 신규 채용 인원 5명 중 3명을 ”거대 모델을 위한 효율적 학습”, ”엣지 디바이스를 위한 효율적 학습”, ”인공지능 모델 공격 및 보호” 세부 연구에 참여할 전임 교수로 임용할 예정임
- ✓ 이어 2027년에는 예정된 신규 채용 인원 5명 중 2명을 ”AI 시스템의 성능 및 자원 효율성 극대화를 위한 하드웨어 아키텍처”, ”인공지능 모델의 프라이버시 침해/보호” 세부 연구에 참여할 교수로 충원할 계획임
- ✓ 본 교육사업단은 인공지능대학과의 공동 발전을 도모하며, 다음의 원칙에 따라 신임 교원을 전략적으로 확보하고자 함
 - + [원칙 01] AI 핵심 분야의 연구역량을 보완할 수 있는 교원을 전략적으로 확보
 - + [원칙 02] 대학원 교육과 산학협력 역량을 갖춘 인재를 영입하여 지속 가능한 연구 생태계 및 실무 기반 교육 커리큘럼 확대

이러한 교수 충원 계획은 연구와 교육의 연속성과 전문성을 동시에 확보하며, 세계적 수준의 AI 교육 연구 기반을 지속적으로 확장하는 데 기여할 예정임

⑤ 대학원생 현황

〈표 1-5〉 교육연구단 참여교수 지도학생 현황

구분	신청학과명	참여 인력 구성	대학원생 수 (단위: 명, %)											
			석사			박사			석·박사통합			계		
			전체	참여	참여 비율	전체	참여	참여 비율	전체	참여	참여 비율	전체	참여	참여 비율
접수 마감일	인공지능 · 소프트웨어학부	전체	39	39	100	7	7	100	14	14	100	60	60	100
		외국인	4	4	100	2	2	100	0	0	0	6	6	100
참여교수 대 참여학생 비율			500											

〈표 1-6〉 교육연구단 참여교수 지도 외국인 학생 현황

연번	성명	국적	학사 출신 대학	공인어학성적		비고
				국어	영어	
1	OSHUNLOLA BOLUWATIFE ALIMAT	나이지리아	Cyprus International University	TOPIK(4급)		
2	Ella Djebbi	튀니지	Higher Institute of Technological studies in Communication of Tunis	TOPIK(4급)		
3	Munkhtuya Tumurchuluun	몽골	University of Mongolia		TOEIC(845)	
4	Mahlet Workneh	에티오피아	Addis Ababa University	TOPIK(5급)	TOEIC(855)	
5	Maqsudova Dilorom	타지키스탄	Technological University of Tajikistan	TOPIK(5급)		
6	Zhu Xiuyan	중국	인하대학교	TOPIK(6급)		

1.4 기대효과

○ 학문적 발전

- ♦ 교육 커리큘럼 혁신

- ✓ 산업체 수요 기반으로 구성된 실무 중심 교육과정(캡스톤디자인, 현장실습, 인턴십 포함)과 AI·보안 융합 교과목 운영은 학문과 산업의 간극을 줄이고, 실제 문제 해결을 위한 통합적 사고력을 배양할 수 있음.

- ♦ AI 및 보안 분야 연구 확장

- ✓ 생성형 AI, 멀티모달 LLM, 차분 프라이버시 기반 합성 데이터 생성, 암호 트래픽 분석 등 현재 산업에서 가장 주목받는 연구 주제를 다루며, 학제 간 융합 연구를 촉진함.

- ♦ 연구 인프라 확대와 전문인력 양성

- ✓ 다수 기업과의 산학 공동연구 프로젝트 및 기술 자문 경험을 통해 박사과정 중심의 연구 중심 대학원으로 자리매김하며, 자체 특허, 오픈소스, 국내외 특강/세미나 등을 통한 지식 확산이 활발히 이루어짐.

- ♦ 연구기반 교육 강화

- ✓ 산업체 수요 기반으로 교과목을 기획하고, 이를 실제 연구 성과와 연계함으로써 이론-실습-연구의 선순환 교육 생태계를 조성함.

○ 사회적 발전

- ♦ AI 보안 전문가 양성

- ✓ 보이스피싱 대응, 개인정보 보호, 트래픽 분석 등 사회적 현안 해결 능력을 갖춘 보안 AI 전문인력을 양성하여 국민의 삶의 질 향상에 기여함.

- ♦ 디지털 전환 가속화 기여

- ✓ 다양한 기업(현대차, LG전자, 삼성미래기술육성센터 등)과 협력하여 스마트 제조, 헬스케어, 자율주행, 홈 IoT 등 분야의 디지털 전환에 필요한 핵심 기술 개발에 참여함.

- ♦ 프라이버시 보호 역량 확산

- ✓ AI 기술의 윤리적 활용을 위한 LLM 기반 MIA 방지, 과잉 기억 문제 해결, DP 기반 합성 데이터 기술 개발 등 실질적 보호기술 연구를 통해 공공 정책 수립 및 공공데이터 개방 정책의 안전성을 높이는 데 기여함.

- ♦ 공공 교육 및 지식 공유

- ✓ KOCW, 오픈소스 공개, 공개 특강, 온라인 콘텐츠 제작 등을 통해 일반 국민 및 외부 개발자와의 지식 공유를 실현하며, AI의 공공성과 사회적 책임을 확장함.

○ 경제적 발전

- ♦ 고부가가치 산업 창출 기여

- ✓ 자율주행 시뮬레이터, 음성 LLM, 암호 트래픽 탐지 기술, 제조업 합성데이터 생성 등은 신산업 분야의 원천기술로 이어질 수 있으며, 기술 이전 및 스타트업 창업 가능성을 확보함.

- ♦ 산업체 맞춤형 인재 양성

- ✓ 네이버, 현대차, LG전자, 유니와이즈솔루션즈 등 다양한 산업체와의 인턴십·공동연구·캡스톤 설계 등 현장 밀착형 교육으로 채용 연계 효과를 창출함.

- ♦ 기술 자문 및 특허화

- ✓ 국내외 기업 대상 기술 자문(예: HyperClova-X 자문, 홈 퍼트니스 AI 앱 기술 이전), 국내·미국

특히 출원, 보안 프로토타입 구현 등 실질적 기술 상용화를 위한 준비가 활발히 진행되고 있음.

◆ 해외 기술 경쟁력 강화

- ✓ Microsoft Research, Adobe Research, KU Leuven 등과의 국제공동연구를 통해 글로벌 기술 표준화 및 경쟁력 제고가 기대됨.

● 국제화 기반 글로벌 허브화

◆ 글로벌 네트워크 확대

- ✓ Microsoft Research, Stanford 등과의 연구 협업 및 해외 대학원 인턴십 프로그램을 통해 국제적 연구 생태계 참여를 확장하고 있음.

◆ 국제 학술활동 장려

- ✓ 최우수 학술대회 참석 지원, 해외 석학 초청 세미나, 글로벌 공동 캡스톤 설계 등을 통해 학생과 연구자의 국제 경쟁력을 제고함.

◆ 국제기구 및 표준화 대응

- ✓ 프라이버시 보호 기술, AI 기반 보안 솔루션 등은 국제보안학회(IEEE S&P, CCS)와 연계되어 글로벌 규제 대응 및 정책 연계에도 파급력을 가질 수 있음.

◆ 교육-연구-국제협력 융합 모델 구축

- ✓ 교육과정 자체에 국제공동연구 결과와 사례를 반영함으로써, 이화 AI 교육연구단만의 차별화된 ‘글로벌 실전형 AI 인재 양성’ 모델을 구축하고 있음.

II. 교육역량 영역

※ 교육역량 영역부문의 항목은 기본적으로 교육연구단을 기준으로 작성하며, 세부 항목별로 특정기준이 제시된 경우 이에 준하여 신청서를 작성

II. 교육역량 영역

1. 교육과정 구성 및 운영

1.1 교육과정 구성 및 운영 계획

1.1.1 교육과정 목표 및 인재상

신뢰도 높고 효율적인 인공지능으로 발전 시킬 수 있는 기술적 역량을 기를 수 있는 교육 과정



<그림 2-1> 교육과정 목표 및 인재상

○ 교육과정 목표

인공지능 분야의 기반 기술을 갖추고 이를 사회와 기업이 요구하는 신뢰도 높고 효율적인 인공지능으로 발전시킬 수 있는 기술적 역량을 배양하는 교육 과정을 제공하고자 함. 이를 통해 양성하고자 하는 구체적인 인재상은 다음과 같음 (그림 2-1 참조)

○ 본 교육연구단의 인재상

- ◆ 신뢰도 높은 인공지능 및 효율적인 인공지능 시스템의 구축·통합 능력을 두루 갖춘 융합형 인재
 - ✓ 석·박사 과정 학생들에게 포괄적인 인공지능 기술을 교육하여 인공지능의 단순한 활용 뿐 아니라 인공지능 모델의 학습 효율성 향상을 위한 SW/HW 융합 능력과 인공지능 모델 및 서비스의 신뢰성을 확보하기 위한 인공지능 모델 보안 및 프라이버시 보호 기술 역량을 함께 갖춘 종합형 인공지능 인력으로 양성하고자 함
- ◆ 산업체 수요에 부합하고 인공지능 기술 트렌드 변화에 유연한 실무 중심 문제-기반 AI 인재
 - ✓ 참여 교수진이 협업 중인 다양한 산업체와의 산학과제 참여, 인턴십 등 실무 중심 교육을 강화하고, 학생-재직자 간 쌍방향 학습 체계를 구축함으로써, 산업체 수요에 부합하고 인공지능 기술 트렌드 및 새로운 기술의 변화에 능동적으로 대응할 수 있는 실무형 문제 해결 중심의 인재로 육성함
- ◆ 글로벌 커뮤니케이션 능력을 갖춘 국제화된 인재
 - ✓ 국제 저명 학회 논문 발표 및 참여, 해외 유수 대학과의 장단기 교류, 국제 표준 오픈 SW 개발 등 글로벌 활동을 장려하여, 세계와 소통할 수 있는 국제적 감각과 협업 능력을 갖춘 글로벌 인재로 성장할 수 있도록 함

- ◆ 최우수 학술대회/학술지 논문 게재를 통한 국내 대학원의 위상을 높이는 학자
- ✓ AI 핵심 기술, 응용 기술, 보안 기술 등 다양한 영역에서 세계 최고 수준의 최우수 학술대회 및 학술지에 논문을 게재할 수 있도록 연구 역량을 체계적으로 배양하여, 국제 경쟁력을 갖춘 학자로 성장하고 국내 대학원의 위상을 제고할 수 있도록 함

1.1.2 교육과정 구성 및 현황

○ 본 교육연구단이 속한 학부 현황

- ◆ 본 교육연구단이 소속되어 있는 인공지능·소프트웨어학부는 1981년 전자계산학과(이후 컴퓨터공학과로 명칭 변경)로 출발하여 44년의 오랜 역사와 전통을 가지고 수백 명의 대학원생을 배출하였으며, 이들은 대학, 산업체, 연구소 등에 리더로 활약하며 대한민국 인공지능, SW, 사이버보안 분야에 기여하고 있음
 - ◆ 시대적 흐름에 따라 컴퓨터공학과를 2017년 소프트웨어학부(컴퓨터공학전공+사이버보안전공)로 확대 개편하였고, 2021년에는 인공지능·소프트웨어학부(컴퓨터공학전공+사이버보안전공+인공지능융합전공)로 확대하였으며 해당 분야 인력 양성에 주력하고 있음 (그림 2-2 참조)
- * 현재 인공지능·소프트웨어학부가 속한 인공지능대학에는 총 29명의 전임교수진(학부 기준)이 소속되어 있으며, 본교 대학원에는 규정상 겸임교수로만 등록 가능하여 현재 12명만이 겸임교수로 등재되어 본 교육연구단에 참여하고 있음



<그림 2-2> 이화여자대학교 인공지능·소프트웨어학부 연혁

○ 본 교육연구단의 교육과정 현황

- ◆ 현재 인공지능·소프트웨어학부는 3개 전공인 사이버보안전공, 컴퓨터공학전공, 인공지능융합전공 각 전공별로 대학원생을 모집하고 해당 전공의 교과과정을 이수한 후 학위를 수여함
- ◆ 3개 전공은 사실상 별도의 학과 개념으로 교육과 연구, 학사 관리 등이 분리되어 있으며, 교과목 이수의 경우 타전공인정 교과목으로 수강이 허용됨
- ◆ 인공지능·소프트웨어학부의 기존 173개 교과목 중 AI 관련 주요 교과목과 AI 관련 신규 개설 예정인 5개 교과목은 아래 표 2-a와 같이 구성됨
- ◆ 효율적 AI 트랙과 보안 AI 트랙의 석사, 박사, 석박통합과정 학생은 AI 공통과목, 트랙핵심과목, 트랙선택과목, 프로젝트과목으로 구성된 이수체계를 따라 교육받도록 설계됨 (그림 2-3 참조)

〈표 2-a〉 인공지능 · 소프트웨어학부의 AI 관련 주요 교과목 (신규 개설 예정 교과목은 연두색 음영)

AI 관련 신규 개설 교과목 목표: 1차년도 2과목, 2차년도 3과목			
번호	교과목명	학수번호	교과목 개요
AI 공통 교과목			
1	인공지능시스템설계	G14341	• 인공지능 시스템 설계 및 구현 실습을 통해 개발 능력 배양
2	고급인공지능특론 I, II	G14425, G14571	• 최신 인공지능 논문 조사 및 분석을 통한 연구기반 확보 • 비판적 사고력 및 고급 분석 능력 배양
3	자연어처리특론	G14458	• 자연어처리 분야를 깊이 있게 소개하고, 자연어처리 고급연구의 기틀 확립 • 최신 연구 논문에 대한 소개
4	인공지능특론	G14523	• 딥러닝 최신 동향 소개, 딥러닝 기본 원리 및 구현 학습 • 자연어 관련 최신 동향 논문 리뷰
5	컴퓨터비전특론	G17617	• 기본 이론, 알고리즘 및 컴퓨터비전의 실습 • CNN 기초, CNN 최적화, RNN, LSTM, 생성모델, 객체 검출 소개
6	인간컴퓨터상호작용특론	G17618	• 인간과 AI 및 로봇 간의 상호작용에 대한 이해 • 차세대 AI 기술을 활용하여 사용자 및 맵락맞춤형 지능형 인터페이스 구현
7	지능형시스템기초및응용	G17848	• 머신러닝, 딥러닝 기술에 대한 이론 및 TensorFlow/PyTorch 기반 실제 구현 • 다양한 시스템 응용사례 및 프로젝트 수행을 통해 학습
8	인공지능개론	G18424	• 인공지능 기본 개념, 구현 기술 및 머신러닝 기초 학습
9	딥러닝	G18425	• 딥러닝 핵심 모델과 비전/자연어 처리 응용 학습 • 텐서플로우 기반 실습을 통한 실무 능력 향상
10	빅데이터분석과실습	G18426	• 빅데이터 분석의 기초 응용 및 실 수요형 데이터 이해 • 산업실무 응용 실습 및 실무 수업 기반의 프로그래밍 실습
11	딥러닝과영상이해	G18428	• GAN 생성모델, 객체 검출, 도메인 적응/일반화, 자기지도 학습, Transformer 등을 학습
12	딥러닝과자연어처리	G18430	• 자연언어를 다루는 딥러닝 기법에 대해서 학습 • Word2vec, GLOVE, ELMO, Bert 등 급속히 발전하는 워드임베딩 기술 학습
13	자연어처리개론	G18431	• 딥러닝을 이용한 자연어처리의 최신 동향을 소개 • 자연어처리 관련 최근의 논문들을 선별하여 세부 주제별로 학습
14	강화학습	G18432	• 강화학습에 대한 기초 및 응용에 대한 이해 • 심층 강화학습에 대한 이론적 배경과 최신 이론/응용 연구 동향 학습
15	멀티모달머신러닝개론	신규	• 강화학습에 대한 기초 및 응용에 대한 이해 • 심층 강화학습에 대한 이론적 배경과 최신 이론/응용 연구 동향 학습
16	생성형인공지능	신규	• 마스킹 기반 모델, 자기회귀모델, 확산모델 등 생성형 AI의 이론 학습 및 실습 • 멀티모달 대규모 언어 모델에 대해 학습하고 범용 인공지능과의 연결성 이해
효율적 AI 트랙 교과목			
17	컴퓨터비전	G14338	• 컴퓨터비전의 전통적인 분야를 효율적으로 처리하는 이론과 구현 설계 학습 • 이러한 연구들이 딥러닝에 기반하여 어떤 방식으로 발전하고 있는지 소개
18	고급분산처리특론	G14419	• 분산 파일 시스템, 분산 트랜잭션 처리 등 고급 기법 학습 • 실시간 시스템, 스케줄링, 보안유지 등 분산 시스템 지원 기술 학습
19	이동비쥬얼컴퓨팅	G14422	• 모바일 환경에서 시각정보기반 상호작용을 위한 영상정보의 실시간 생성 및 단순 객체화 표현기법에 대해 학습

20	분산컴퓨팅	G14538	<ul style="list-style-type: none"> 클러스터, 웹 기반 컴퓨팅 및 분산 알고리즘을 전반적으로 학습 오류 허용 기술과 분산 메모리 시스템 등 학습
21	고성능컴퓨팅	G17615	<ul style="list-style-type: none"> 슈퍼컴퓨터 및 클러스터 기반 고속 연산 기술 학습 대규모 과학 계산 및 빅데이터 분석 등 문제 해결 적용
22	엣지컴퓨팅개론	G17849	<ul style="list-style-type: none"> 엣지 컴퓨팅과 클라우드 기반의 엣지 컴퓨팅에 대한 이해 AI를 활용한 엣지 컴퓨팅 실습
23	효율적인딥러닝처리	G18407	<ul style="list-style-type: none"> 모델 양자화, 가지치기, 구조탐색 등 딥러닝 효율화 기술 학습 뉴럴 컴파일러와 하드웨어 최적화 기법 및 최신 논문 리뷰
24	인공지능융합기반시스템개론	G18455	<ul style="list-style-type: none"> 운영체제와 머신러닝 연산 플랫폼의 역할 학습
25	On-Device AI	G18456	<ul style="list-style-type: none"> 딥러닝구조 경량화, 분산 네트워크, 분산 학습 소개 TensorFlowLite, PyTorchMobile 기반의 시스템 개발
26	지능형시스템HW	G18457	<ul style="list-style-type: none"> 기본 컴퓨터 구조 및 다양한 AI 가속 하드웨어 및 시스템에 대한 원리를 학습하고 구현
27	지능형시스템SW	G18458	<ul style="list-style-type: none"> 차세대 시스템SW의 지능화 및 최적화 기술에 대한 이해 기존의 시스템SW들에 대한 최적화할 알고리즘에 대한 이해
28	컴퓨터시스템의 성능평가와 모델링	신규	<ul style="list-style-type: none"> 미래형 컴퓨터시스템에서 차세대 AI 워크로드의 실행으로 인해 달라지는 특성 학습 이를 정량적/정성적으로 분석하여 성능 평가 및 논문 작성
29	효율적학습특론	신규	<ul style="list-style-type: none"> 효율적 학습 패러다임을 중심으로 저비용 레이블 학습 기법, 동적 학습, 도메인 적응 학습 주요 학술대회의 최신 논문 리뷰와 병행하며, 실습 및 프로젝트 진행

보안 AI 트랙 교과목

30	정보보호론	G17706	<ul style="list-style-type: none"> 정보보호와 암호기술의 원리, 응용, 동향 등을 이해하기 위한 기본 지식 학습 공개키 및 비밀키 암호알고리즘, 암호 응용 프로토콜, 스테가노그래피 등 학습
31	시스템보안특론	G17709	<ul style="list-style-type: none"> 시스템보안에 관련된 다양한 하드웨어 및 소프트웨어 분야의 최신 기술 학습
32	차세대보안특론	G17710	<ul style="list-style-type: none"> 인공지능 기술을 이용한 다양한 공격 방법, 프라이버시 침해 방법 소개 이를 이용한 방어 기술과 관련된 연구결과 이해
33	컴퓨터보안특론	G17850	<ul style="list-style-type: none"> 정보보호에 관련된 암호기술, 시스템 및 네트워크 보안기술 학습 다양한 응용서비스 보호에 사용되는 기술, 법/제도, 정보통신 윤리 등 학습
34	최신암호기술특론	G17855	<ul style="list-style-type: none"> 전통적인 암호기술을 바탕으로 최신의 암호기술을 소개하고 각각의 장단점을 비교분석
35	개인정보보호	G17864	<ul style="list-style-type: none"> 개인정보를 효과적으로 보호하기 위해 보안위협요인을 분석 최신 보안기술과 연구 동향 학습
36	인공지능보안특론	G17865	<ul style="list-style-type: none"> 인공지능 보안 관련된 최근의 핵심기술과 주요연구동향에 대해 학습
37	보안개론	G18460	<ul style="list-style-type: none"> 보안 도메인의 인공지능융합에 필요한 기반지식 학습
38	AI기반IoT보안	G18461	<ul style="list-style-type: none"> AI를 활용한 IoT 로그 분석 기술 학습 및 실습
39	AI기반네트워크침입탐지	G18462	<ul style="list-style-type: none"> AI를 활용한 네트워크 패킷 및 로그 분석 기술 학습 및 실습
40	AI기반코드분석	G18463	<ul style="list-style-type: none"> AI를 활용한 SW 코드 분석 기술 학습 및 실습
41	딥러닝보안	G18813	<ul style="list-style-type: none"> 최신 딥러닝 모델들을 사용하여 네트워크 트래픽 분석, 악성코드 분석, 딥페이크 탐지, 모델전도 공격 등 다양한 사이버보안 문제를 탐색 관련 논문 발표 및 실습문제 수행을 통해 최신 딥러닝보안 연구 학습

I. 교육연구단의 구성, 비전 및 목표

혁신인재양성사업 인공지능 분야 교육연구단 사업

42	인공지능융합보안	신규	<ul style="list-style-type: none"> 딥러닝에서의 보안 문제와 AI 모델을 활용하며 발생되는 데이터보안 문제 학습 적대적 공격 및 방어, 멤버쉽 추론 등 인공지능 모델 사용 측면의 데이터 보안 기술 학습
AI 융합 및 프로젝트 교과목			
43	AI융합기반기술주제연구 I, II	G18466, G18467	<ul style="list-style-type: none"> 심화된 AI 융합 기반 기술에 관한 최신 연구에 대한 지식 학습
44	AI융합기초 I, II	G18468, G18469	<ul style="list-style-type: none"> AI 융합 프로젝트 요구사항도출, 설계, 시험, 품질 등 개발공정과 방법론 학습
45	AI융합프로젝트 I~IV	G18470, G18471, G18472, G18473	<ul style="list-style-type: none"> AI 융합 시스템 개발 프로젝트 수행
46	AI융합인턴십 I, II	G18474, G18475	<ul style="list-style-type: none"> AI 융합 시스템 개발에 필요한 지식을 산업체 인턴과정을 통하여 학습 (총42시간 이상)
47	창업연계캡스톤프로젝트	G18476	<ul style="list-style-type: none"> 기본 창업 교육과 수강생이 창업 아이디어를 제시하고 연구와 접목한 프로젝트를 진행 본교 창업보육센터와 연계하여 창업 전문가들의 멘토링 진행
48	AI융합기술이전 I~III	G18477, G18478, G18479	<ul style="list-style-type: none"> AI 융합 프로젝트 결과 기술이전 수행
49	AI융합기술상용화	G18480	<ul style="list-style-type: none"> AI 융합 프로젝트 상용화 학습
50	AI융합실무주제연구 I, II	G18481, G18482	<ul style="list-style-type: none"> AI 융합 실무에 관한 최신 연구에 대한 지식을 습득

효율적 AI 트랙	AI공통과목		트랙핵심과목	트랙선택과목	프로젝트과목	
	석사과정 (24학점)	박사과정 (36학점)	인공지능개론 딥러닝 강화학습 인공지능시스템설계 빅데이터분석과실습 자연어처리개론 멀티모달머신러닝개론	컴퓨터비전 분산컴퓨팅 효율적인딥러닝처리	지능형시스템SW 지능형시스템HW 엣지컴퓨팅개론	AI융합기반기술주제 연구 I,II AI융합기초 I,II AI융합프로젝트 I ~ IV AI융합인턴십 I,II 창업연계캡스톤 프로젝트 AI융합기술이전 I ~ III AI융합기술상용화 AI융합실무주제연구 I,II
보안 AI 트랙	석사과정 (24학점)	박사과정 (36학점)	인공지능특론 고급인공지능특론 I, II 컴퓨터비전특론 자연어처리특론 인간컴퓨터상호작용특론 딥러닝과영상이해 딥러닝과자연어처리 생성형인공지능	보안개론 딥러닝보안 인공지능융합보안	AI기반IoT보안 AI기반네트워크 침입탐지 AI기반코드분석	정보보호론 컴퓨터보안특론 차세대보안특론 인공지능보안특론
	석사과정 (24학점)	박사과정 (36학점)				개인정보보호 시스템보안특론 최신암호기술특론

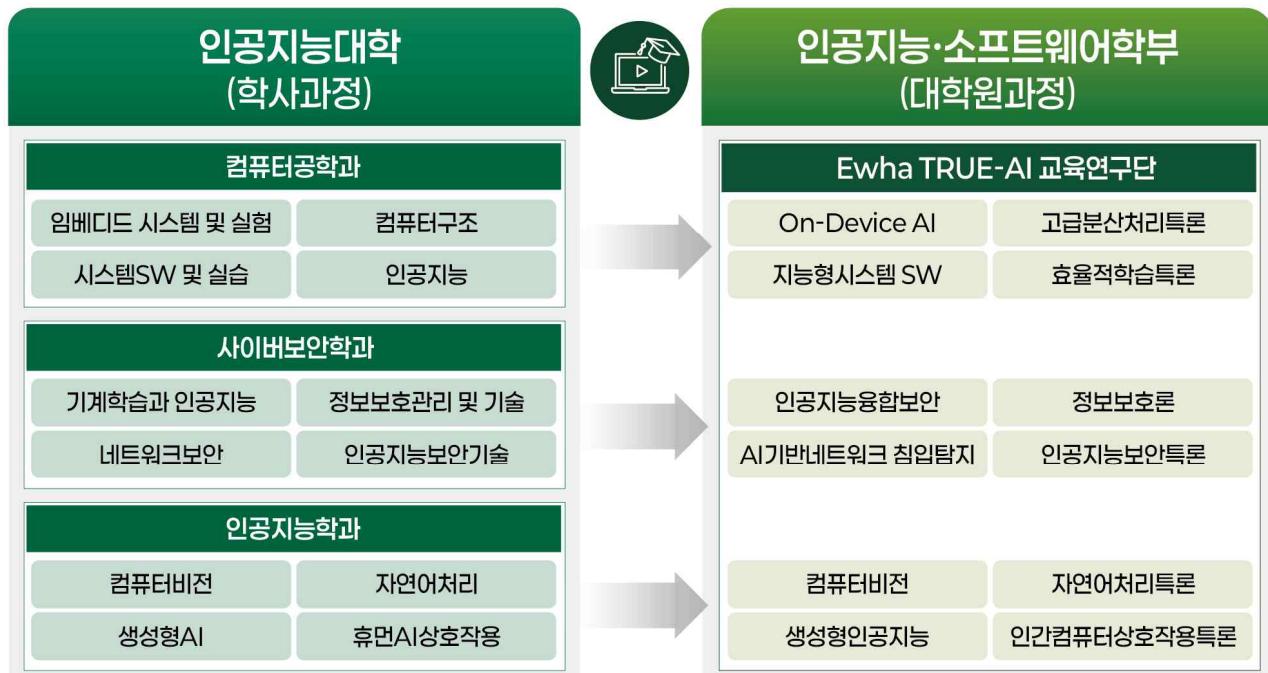
※모든 과목은 3학점이 기본임

<그림 2-3> 트랙별 교과과정의 예 (총 이수학점에 맞추어 교과목 선택 수강 가능)

1.1.3 교육과정 운영 계획

○ 교육연구단이 속한 학부와 교육연구단 교육과정의 관계

- ◆ 본 교육연구단이 속한 인공지능 · 소프트웨어학부(대학원과정)은 이화여자대학교 인공지능대학(학사과정)의 컴퓨터공학, 사이버보안, 인공지능학과 등에서 수학한 내용을 기반으로 대학원을 통해 심화된 학습을 이어가도록 설계되어 있음.
- ◆ 인공지능대학의 학사과정 전공별 교과과정 개요는 다음과 같음:
 - ✓ **컴퓨터공학과:** ICT 및 소프트웨어 산업에서 발생하는 복잡한 공학 문제를 해결하기 위한 기초 이론과 실무 중심 교육을 통해, 문제 해결력과 시스템 구현 역량을 고루 갖춘 인재를 양성함. 특히, 다양한 산업 현장에서 요구되는 시스템 설계, 데이터 처리, 알고리즘 구현, 임베디드 소프트웨어 등의 역량을 강화하고 있으며, 프로젝트 기반 수업을 통해 실질적 문제 해결 중심의 교육을 실현하고 있음.
 - 교육연구단의 '효율적 AI' 트랙과 연계하여, 자원 효율성과 연산 최적화를 고려한 AI 알고리즘 설계, 임베디드 환경에서 동작 가능한 경량화된 모델 개발, 데이터 효율 학습 등 응용 가능한 AI 기술 연구를 수행함. 또한 컴퓨터공학 기반의 이론과 구현 능력을 바탕으로 대규모 모델의 학습 효율 개선, 모델 압축 및 최적화 기법 개발에 기여함.
 - ✓ **사이버보안학과:** 사이버 공간에서의 보안 위협과 사회적 혼란이 현실화됨에 따라, 체계적인 보안 이론 교육과 실습을 병행하여 국내 보안 전문가를 양성하고 있음. 네트워크 보안, 시스템 보안, 암호 기술 등을 중심으로 한 교육과정은 다양한 침해 시나리오에 대한 대응 능력을 강화하고 있으며, 최신 보안 이슈와 연계한 교육을 통해 실무 적합성을 높이고 있음.
 - 교육연구단의 '보안 AI' 트랙과 연계하여, AI 기술을 활용한 침해 탐지, 이상행위 분석, 개인정보 보호 등 신뢰 가능한 AI 기술 개발에 기여함. 특히, 보안 데이터를 활용한 딥러닝 기반 이상 탐지, 적대적 공격(adversarial attack)에 강인한 AI 모델 설계, 설명 가능한 보안 AI(XAI for Security) 등 다중적인 보안 AI 연구를 수행할 수 있는 기반을 제공함.
 - ✓ **인공지능학과:** AI의 핵심 원리를 이해하고 다양한 도메인에 적용할 수 있는 융합형 AI 인재 양성을 목표로, 컴퓨터공학 지식뿐만 아니라 비전, 자연어처리, 로봇, 바이오 등 이기종 데이터와 도메인 지식을 결합할 수 있는 교육과정을 운영함. 다양한 프로젝트형 과제를 통해 실제 문제 해결 역량을 함양하며, 사회적 수요에 기반한 실용적인 AI 기술을 구현할 수 있는 능력을 배양함.
 - 교육연구단의 '효율적 AI'와 '보안 AI' 트랙 모두와 연계되어, 실세계 데이터의 결측, 불균형, 도메인 차이를 극복할 수 있는 멀티모달 AI 및 도메인 적용 연구를 수행할 수 있음. 특히 의료, 제조, 국방, 교육 등 실제 응용 도메인에서 AI 기술을 효과적으로 접목하고, 제한된 자원 속에서도 정확하고 신뢰성 있는 결과를 도출하는 융합형 문제 해결 연구를 뒷받침함.
- ◆ 이러한 이화여자대학교 학사 졸업생은 학석사연계 과정 또는 석 · 박사 과정 지원을 통해 인공지능 · 소프트웨어학부(대학원과정)으로 진학할 수 있으며, 학사-대학원 간 연계된 교과과정을 통해 "Trustworthy and Resource-efficient Unified Evolving AI 연구" 을 위해 3개 전공의 핵심 기술을 아우르는 교과과정을 이수하여 특화된 인재로 양성될 수 있도록 함. (그림 2-4 참조)



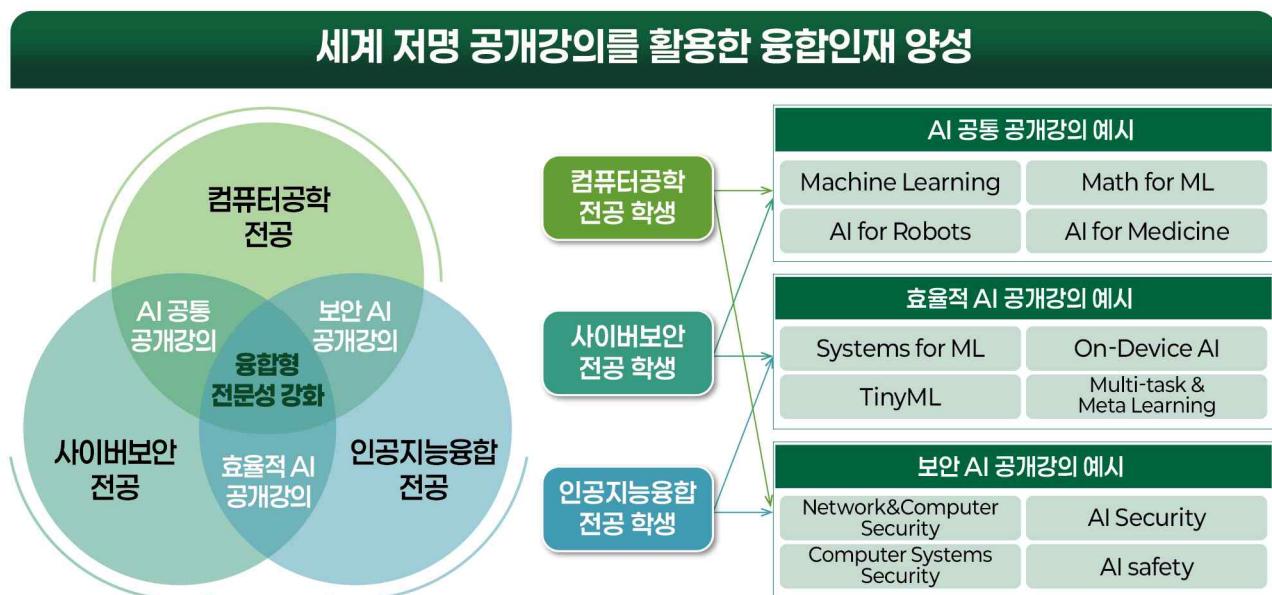
<그림 2-4> 학사-대학원 간 연계 교육체계 교과목 예시

○ 교육연구단의 교육 목표 달성을 위한 주요 계획

- 참여대학원생은 기본 역량 강화를 위해 먼저 AI공통과목을 이수하며, 이를 토대로 각 트랙의 전문성을 심화하기 위한 트랙핵심과목을 수강하도록 유도함
- 트랙선택과목을 통해 참여대학원생은 자신의 연구 관심사에 따라 다양한 응용기술을 학습함으로써 역량을 다양화할 수 있도록 함
- 프로젝트과목에서는 이를 기반으로 실제 문제 해결 능력을 키우도록 구성함. 특히, 산학협력과 연계된 실전형 프로젝트 수행을 통해 이론과 실무를 통합한 교육을 극대화함
- 모든 교과목은 참여대학원생들에게 꼭 필요한 내용들로 구성하며, 매 학기 참여교수들이 논의를 통해 최신 연구 동향과 기술 발전을 신속하게 반영할 수 있도록 하여 교육과 연구의 선순환 및 우수성이 유지될 수 있도록 함
- 지도교수의 연구 분야 외에 교육연구단의 연구목표가 달성될 수 있도록 공동지도교수를 1인 더 두는 1+1 융합연구기반 지도교수제를 시행하여 참여대학원생의 연구의 깊이와 폭을 확장할 수 있도록 지원함
- 학위 논문 작성시 오픈소스 SW 기반의 구현을 권장하여 참여대학원생의 실전 개발 능력을 함양하고, 구현 결과물 및 데이터를 GitHub, Hugging Face 등에 등록하여 전 세계 연구진과 연구자료를 공유하고 대학원생 간의 후속 주제 도출을 용이하도록 함
- 글로벌 커뮤니케이션 역량 강화를 위해 참여대학원생의 세계 유수 자매결연 대학과의 단기 연수 및 인턴쉽을 적극 지원하고 국제 학술대회 참가 시 논문발표뿐 아니라 해외 연구자와의 활발한 교류지원 방안을 마련함
- 참여 대학원생의 산업체 연구 과제 및 산업체 연구소 인턴쉽 참여 기회를 적극 제공하고 국내외 석학 및 산업체 CEO 초청 세미나를 수시 개최하여 학생들과의 직접적인 교류 방안을 마련함

1.1.4 교육연구단의 교육목표 달성을 위한 비교과 교육과정

○ 세계 저명 공개강의 수강 장려



<그림 2-5> 세계 저명 공개강의를 통해 인공지능·소프트웨어학부 내 전공 간 지식 격차를 줄이고 융합 역량을 갖춘 인재를 양성

- ◆ 컴퓨터공학전공, 사이버보안전공, 인공지능융합전공은 각각 고유한 기술적 기반과 교육 커리큘럼을 바탕으로 효율적 AI와 보안 AI 분야에서는 전문성을 갖추고 있으나, 일부 영역에서는 상대적으로 보완이 필요한 측면이 존재할 수 있음
- ◆ 특히, 세 전공이 다루는 기술 스펙트럼이 상이함에 따라, 특정 분야에 대한 이해도나 실무 역량의 깊이에서 차이가 발생할 수 있음
- ◆ 이를 해소하고 전공 간 융합형 전문 인재를 양성하기 위해, 참여 대학원생이 전 세계적으로 검증된 글로벌 공개강의를 1개 이상 필수로 수강하도록 하고, 이에 필요한 수강료를 전액 지원함
- ◆ 각 전공이 AI 공통, 효율적 AI, 보안 AI와 관련된 글로벌 저명 공개강의를 표 2-b와 같이 Coursera, Udacity, Udemy, Stanford, MIT MOOC 등에서 선별하여 수강하도록 장려하고, 수강료를 지원함
- ◆ 공개강의 수강을 통해 전공 간 격차를 보완하고 융합형 전문성을 강화하도록 유도함 (그림 2-5 참조)
 - ✓ 컴퓨터공학전공 학생은 AI 응용이나 인공지능 보안 역량을 강화하기 위해 AI 공통 및 보안 AI 공개강의를 수강할 수 있음
 - ✓ 사이버보안전공 학생은 AI 최신 모델 설계나 효율적 학습 구조에 대한 이해를 위해 AI 공통 및 효율적 AI 공개강의를 수강할 수 있음
 - ✓ 인공지능융합전공 학생은 모델 경량화, 병렬화 기술과 함께, 데이터 프라이버시 및 보안 이슈에 대한 이해도를 높이기 위해 효율적 AI 공개강의 및 보안 AI 공개강의를 수강할 수 있음

〈표 2-b〉 세계 저명 공개강의 예시

강의명	강사명 또는 제공기관	강의 내용
AI 공통 공개강의		
Machine Learning	Andrew Ng	기계학습, 강화학습, 딥러닝 학습
Deep Learning Specialization	Andrew Ng	딥러닝의 기본과 실제 적용
Math for Machine Learning	David Dye	다변수 Calculus, 선형 회귀분석, 최적화 이론 학습
Data Science Specialization	Jeff Leek	데이터 전처리, 통계학적 모델링 클러스터 분석 학습
Convolutional Neural Networks for Visual Recognition	Fei-Fei Li	Convolutional Neural Networks 이론과 물체 인식 및 개체 분할
Artificial Intelligence for Robotics	Sebastian Thrun	로보틱스에서 최신 AI 기법 학습
AI for Medicine Specialization	Pranav Rajpurkar	의료 진단 정확성을 높이기 위한 딥러닝 방법론 적용학습
Self-Driving Cars Specialization	Steven Waslander	센서, 장애물 인식, 위치 측위, 매핑, 강화 학습, 자율 주행 학습
HarvardX: CS50's Introduction to Artificial Intelligence with Python	David J. Malan	AI의 기반이 되는 개념과 알고리즘
효율적 AI 공개강의		
TinyML and Efficient Deep Learning Computing	Song Han	모델 압축, 가지치기, 양자화, NAS, 분산학습, 병렬화, 온디바이스 AI 등 효율적 딥러닝 컴퓨팅 학습
The complete Course to Build on-Device AI Applications	Kumari Ravva	다양한 기기에 적용가능한 AI 기술 학습
Generative AI Advance Fine-Tuning for LLMs	Joseph Santarcangelo	생성형 인공지능의 효율적 미세조정 기술 학습
Deep Multi-Task and Meta Learning	Chelsea Finn	인공지능의 효율적 적용을 위한 few-shot learning, meta-learning, lifelong learning 등의 기법 학습
Systems for Machine Learning	Azalia Mirhoseini	Transformer 및 LLM을 위한 효율적 학습, 미세조정, 추론 기술 학습
Applied Tiny Machine Learning (TinyML) for Scale	Vijay Janapa Reddi	데이터 수집, 인공지능 모델 개발, 모델 최적화에 이르기까지 효율적인 인공지능 모델 개발 기법 학습
보안 AI 공개강의		
Computer Systems Security	Nickolai Zeldovich	안전한 컴퓨터 시스템의 설계 및 구현
Network and Computer Security	Ronald Rivest	데이터 프라이버시 보호를 위한 암호 기법
AI Security Essentials	Francis Gorman	안전한 AI 모델, AI 인프라스트럭처 보안, AI를 이용한 침입탐지
AI Security	Starr McFarland	Responsible AI, AI security & privacy 학습
AI Security	Christopher Nett	생성형 AI를 위한 cybersecurity, ChatGPT 취약성 등 학습
Introduction to AI Safety	Max Lamparth	AI 모델의 취약성 및 해석가능성 학습

● 교내 창업 지원 프로그램을 통한 연구 내용의 사업화 지원

- ◆ 교육연구단의 연구 결과 사업화가 가능하다고 판단되는 경우 참여대학원생의 창업을 지원하기 위해 Ewha Start-up Academy 프로그램과 연계하여 체계적인 창업 커리큘럼, 각 분야 전문가의 멘토링, 스타트업 기업가 모임 및 성공 기업가와의 만남을 통한 네트워킹을 지원함
- ◆ 교내 기업가정신연계전공이 운영하는 창업 교과목들(예: 여성 CEO와 기술경영)을 수강할 수 있도록 지원하고 창업에 필요한 실무과정을 익힐 수 있는 실전 창업교과목을 수강할 수 있도록 함
- ◆ 본교의 창업지원단 및 기술사업화센터와 공조하여 실험실창업혁신단, 서울시 캠퍼스타운 프로그램 등의 지원을 통해 참여대학원생의 실험실 창업을 적극 지원함

1.1.5 본 교육연구단의 교육과정 및 학사관리 경쟁력

- 본 교육연구단이 속한 인공지능 · 소프트웨어학부의 교육과정은 컴퓨터공학전공에서 출발하여 사이버보안전공, 인공지능융합전공 등 사회 수요가 높은 영역을 새로운 전공으로 신설하고 우수한 교수진을 초빙하여 폭넓고 깊이 있는 교육과정의 경쟁력을 확보하고 있음
- 이러한 교육과정을 토대로 전공 내 가장 경쟁력 있는 핵심영역을 도출하고 우수한 교수진으로 교육 연구단을 구성하여 전공을 아우르는 대학원생 관심분야의 교차 영역을 특화시켰으며 참여대학원생이 경쟁력을 갖춘 전문적인 교과과정을 따라갈 수 있도록 함
- 본 교육연구단이 속한 인공지능 소프트웨어학부의 최근 대학원 신입생 백그라운드가 다양함을 고려하여 컴퓨터공학, 인공지능 및 사이버보안의 기초과정부터 심화과정까지 다양한 수준의 교과목을 개설하고 지도교수가 이를 가이드하고 있음
- 각종 세미나와 공개 강의, 창업 강의, 인턴쉽 강좌 등을 대학원생이 수강할 수 있도록 적극 가이드하여 기초부터 심화 과정, 그리고 이를 사업화하는 과정까지를 학생 및 분야 특성에 맞게 지원할 수 있는 다양한 방안을 제공하고 있음
- 학위 취득 요건으로 교과목 이수, 영어 자격 이수, 학술대회 및 학술지 논문발표, 종합시험, Prelim, 논문 세미나 수강, 학위논문 심사 등의 절차를 갖추어 전문성을 확보하고 있으며, 학생별 특수성을 고려해 과제 참여, 인턴쉽, 창업 등을 학점으로 인정해주는 행정적인 유연함 또한 갖추고 있음

1.1.6 교육과 연구의 선순환 구조 구축 및 연구역량의 교육적 활용 방안

- 우수한 연구결과를 도출한 데이터 및 플랫폼, 도구의 활용 방법을 교과과정 개편 주기와 무관하게 곧바로 대학원 수업에 반영할 수 있도록 사이버보안특론 I II III IV, 컴퓨터학특론 I II III IV, 인공지능 기술 주제연구 I II 등을 설정하고 참여교수들이 기술 트렌드 변화를 교육에 조기 반영할 수 있도록 함
- 교과목을 통한 프로젝트 결과물이 우수한 연구 성과로 이어질 수 있도록 자율적, 창의적인 학생 주도 프로젝트를 추진하고, 과목 담당교수와 지도교수가 공동지도를 통해 융복합 연구를 지원함
- 본 교육연구단의 우수 연구실적을 학내 SoftLunch 세미나를 통해 발표하도록 하고, 학부생 및 대학원생이 참여하도록 유도하여 분야 간 교류 및 대학원 진학을 장려하여 교육과 연구의 선순환을 도모함
- 정기적인 연구 콜로퀴엄 운영을 통해 학생(학부생+대학원생), 연구원, 교수들이 본 사업단의 연구 내용을 파악하고 학부생의 경우 연구 인턴 과정을 수행한 후 참여대학원생으로 진학할 수 있도록 지원함

1.1.7 전임교수 대학원 강의 계획

- 본 교육연구단 참여교수의 대학원 강의 계획은 표 2-c와 같음

〈표 2-c〉 전임교수 대학원 핵심 교과목 및 강의 계획

효율적 인공지능 트랙	
반효경 교수 (지능형 시스템 SW)	<ul style="list-style-type: none"> 핵심 교과목: 컴퓨터시스템의 성능평가와 모델링, 고급분산처리특론 강의 내용: ✓ 현대의 컴퓨터는 모바일과 데스크탑을 넘어 클라우드, 에지/포그 등 다양한 형태로 나타나고 있으며, 실시간 AI 응용, 미션 크리티컬 응용 등 다양한 요구조건을 가진 연산집약형 워크로드의 증가로 전통적인 컴퓨터시스템의 CPU-메모리-디스크 구조가 아닌 병렬가속기, 영속 메모리, 센서 등이 탑재되는 새로운 구조가 주목받고 있음. ✓ 컴퓨터시스템의 성능평가와 모델링 과목에서는 미래형 컴퓨터시스템에서 차세대 AI 워크로드의 실행으로 인해 달라지는 특성을 시스템 계층별 트레이스 추출 및 분석을 통해 알아보고, 수강생이 이를 정량적/정성적으로 분석하여 성능을 평가하고 논문을 작성하기까지를 담당교수와 한 학기 동안 진행하도록 지도하려 함. ✓ 고급분산처리특론 과목에서는 기존의 분산 파일 시스템, 트랜잭션 처리, 실시간 스케줄링 등 핵심 이론에 더해 연합학습(Federated Learning), 스플릿 러닝(Split Learning), 분산형 머신러닝 아키텍처 등 최신 AI 트렌드에 부합하는 기술을 심층적으로 다루고자 함. ✓ 특히 프라이버시 보호형 분산 학습, 데이터-중심 컴퓨팅 패러다임, 지능형 에지 컴퓨팅 환경에 최적화된 설계와 운영 전략을 지도하여, AI 시대에 부합하는 분산 시스템 전문가로서의 통합적 사고와 실전 역량을 기르고자 함.
민동보 교수 (컴퓨터 비전)	<ul style="list-style-type: none"> 핵심 교과목: 컴퓨터비전특론, 컴퓨터비전개론 강의 내용: ✓ 컴퓨터비전은 이미지를 인식, 처리, 이해함으로써 컴퓨터가 현실 세계를 해석하고 의사결정을 내릴 수 있도록 하는 핵심 인공지능 기술임. ✓ 본 과목은 딥러닝 기반의 컴퓨터비전 기법을 중심으로, 아래와 같은 주요 주제를 이론 및 실습을 통해 학습함: 이미지 분류, 객체 탐지 및 영상 분할, 합성곱 신경망(CNN) 아키텍처, 학습 최적화, 순환 신경망(RNN), 비지도 학습, 생성 모델, 도메인 적응. ✓ 수업은 이론 강의 + 프로그래밍 과제 + 팀 프로젝트로 구성되며, 최신 논문 기반 학습 및 구현 실습을 통해 이론과 응용 능력을 동시에 강화함. ✓ 본 과목은 AI 특화 교육과정의 심화 트랙 교과목으로서, 실제 연구 및 산업 응용을 위한 실전형 역량을 함양하는 데 중점을 둠.
이형준 교수 (엣지 컴퓨팅 및 네트워크)	<ul style="list-style-type: none"> 핵심 교과목: 엣지컴퓨팅개론 강의 내용: ✓ 본 교과목은 클라우드 컴퓨팅 환경보다 분산적인 포그 네트워크 아키텍처 상에서 엣지 디바이스들이 컴퓨팅, 저장장치 자원을 네트워크를 통해 조달하며 소비

	<p>할 수 있는 엣지 컴퓨팅의 개념과 응용에 대해서 학습함.</p> <p>✓ 더 나아가 데이터 프라이버시 문제, 엣지 디바이스에서 취득된 데이터의 네트워크 전송 부담 문제를 해결하기 위해 분산 딥러닝 학습 방법에 대해 학습하고, 효율적이면서 학습 가속화를 할 수 있는 다양한 최근 연구 방법에 대해서 학습하고, 연구 프로젝트를 수행하도록 지도할 계획임.</p>
노준혁 교수 (효율적 인공지능)	<ul style="list-style-type: none"> ◆ 핵심 교과목: 효율적 학습 특론, 패턴 인식 및 머신 러닝 ◆ 강의 내용: ✓ 효율적인 인공지능 학습은 데이터 수집 비용, 연산 자원, 도메인 변화 등 실제 환경에서 마주치는 다양한 제약 조건 하에서도 높은 성능을 달성할 수 있는 핵심 기술로 부상 중. ✓ 최근에는 labeled data를 충분히 확보하기 어려운 현실적 상황을 해결하기 위한 여러 접근들이 활발히 연구되고 있음. ✓ 효율적 학습 특론 과목은 이러한 효율적 학습(efficient learning) 패러다임을 중심으로, 특히 weakly-supervised, semi-supervised, self-supervised learning과 같은 저비용 레이블 학습 기법, active learning을 통한 데이터 효율 최적화, domain adaptation을 통한 도메인 일반화 방법론 등을 다루고자 함. ✓ 인이 과정은 이론적 배경과 함께 최근 주요 학술대회의 최신 논문 리뷰를 병행하여 진행되며, 실습 기반 과제 및 프로젝트를 통해 실전 연구 기획과 구현 능력을 함양하는 데 초점을 맞춤. ✓ 특히 "Resource-efficient AI"를 주제로 한 교육연구단의 핵심 목표와 연계되며, 학생들이 데이터, 연산, 도메인 자원 측면에서의 효율성과 실용성을 모두 고려한 차세대 AI 기술을 습득할 수 있도록 설계하고자 함. ✓ 패턴 인식 및 머신 러닝 교과목은 다양한 데이터로부터 의미 있는 패턴과 구조를 학습하고 예측하는 원리를 이해하고 구현하는 것을 목표로 함. ✓ 패턴 인식의 기본 개념, 확률론 기반 분류(classification) 및 군집화(clustering) 기법을 시작으로, 머신 러닝의 핵심 알고리즘들을 수학적 기초와 함께 심층적으로 학습함. ✓ 주요 내용으로는 <ul style="list-style-type: none"> • 베이즈 분류기, k-NN, 서포트 벡터 머신(SVM) 등 고전적 패턴 분류 기법, • 회귀, 의사 결정 트리, 앙상블 학습(Random Forest, Boosting), • 차원 축소(PCA, LDA), 커널 기법, • 기초적인 신경망 및 딥러닝 입문까지 포함되어, 머신 러닝의 실무적 활용을 위한 기반을 폭넓게 다룸. ✓ 수업은 이론 강의, 수학적 유도, 프로그래밍 실습(파이썬 기반)으로 구성되며, 실제 데이터를 다루는 과제 및 팀 프로젝트를 통해 실질적 분석 능력과 구현 역량을 동시에 강화함. ✓ 특히 본 강의는 인공지능 핵심 기초 역량을 함양하는 교과목으로, 이후 효율적 학습, 딥러닝, 컴퓨터 비전 등의 고급 과목 수강을 위한 이론적/실습적 기반을 제공함.

<p>윤명국 교수 (컴퓨터구조)</p>	<ul style="list-style-type: none"> ◆ 핵심 교과목: 인공지능 소프트웨어 ◆ 강의 내용: <ul style="list-style-type: none"> ✓ 최근 인공지능 모델은 연산량 증가와 함께 학습 및 추론에 고성능 하드웨어 (GPU, NPU 등)를 필수적으로 요구하게 되었음. ✓ 이에 따라 산업계와 학계 모두에서 AI 소프트웨어의 성능을 하드웨어 자원에 맞게 최적화하는 기술이 중요한 이슈로 부상하고 있음. ✓ 본 교과목에서는 CUDA, OpenCL 등 병렬 프로그래밍 프레임워크를 활용하여 GPU에서의 AI 연산을 최적화하는 기법을 학습하며, 더 나아가 Edge AI 및 모바일 환경에서 널리 사용되는 NPU 기반 추론 최적화 기법(예: quantization, memory tiling, operator fusion 등)을 실습 중심으로 다룰 예정임. ✓ 또한, shared memory, thread divergence 등 하드웨어 효율을 극대화하기 위한 시스템 수준 이슈도 함께 교육하여, 실제 산업 현장에서 요구되는 AI 소프트웨어 최적화 역량을 함양하고자 함.
<p>이지영 교수 (멀티모달)</p>	<ul style="list-style-type: none"> ◆ 핵심 교과목: 멀티모달 머신러닝 개론, 음성 시스템 ◆ 강의 내용: <ul style="list-style-type: none"> ✓ 멀티모달 머신러닝은 텍스트, 음성, 영상, 생체신호 등 서로 다른 형태의 데이터를 통합적으로 이해하고 처리하는 기술로, 최근 생성형 인공지능의 발전과 함께 핵심 연구 분야로 부상하고 있음. ✓ 그러나 현재 대부분의 대학원에서는 이러한 멀티모달 기술을 체계적으로 다루는 정규 교과목이 개설되어 있지 않으며, 개별 연구나 프로젝트 수준에서 제한적으로 학습되고 있는 실정임. ✓ 멀티모달 머신러닝 개론 수업에서는 멀티모달 데이터를 다루기 위한 표현 학습, 정렬(alignment), 융합(fusion), 교차 표현(cross-attention), 생성(generation) 등의 기초 이론을 딥러닝 접근법을 바탕으로 균형 있게 소개할 예정임. ✓ 또한, 멀티모달 모델의 편향 문제, 프라이버시, 안전성, 설명가능성 등 실용적 관점에서의 도전과제들을 함께 다룸으로써, 다양한 모달리티의 통합을 통해 인간 수준의 인공지능을 향해 나아가는 기술적 기반을 심도 깊게 이해하도록 함. ✓ 음성시스템 특론은 음성신호처리와 딥러닝 기반 음성 인식 및 합성 기술을 종합적으로 다루는 고급 과목으로, ASR(Automatic Speech Recognition), TTS(Text-to-Speech), 음성인식용 self-supervised learning, 음성 임베딩, 음성 기반 대화 시스템 등을 포함함. ✓ 특히 wav2vec, HuBERT, Whisper 등 최신 음성 모델의 구조와 학습 방법론을 소개하고, 음성 시스템의 성능을 결정짓는 주요 요소인 음향 모델, 언어 모델, 디코더 구조등에 대한 심층적인 이해를 도모함. ✓ 실습을 통해 음성 데이터 전처리, 특징 추출(MFCC 등), 디코딩 기법(CTC, attention-based 등), 그리고 음성 기반 downstream task(감정 인식, 화자 검증 등)에 대한 구현 경험을 쌓을 수 있도록 구성됨. ✓ 또한 음성 시스템에서의 데이터 편향, 잡음 환경 적응, 실시간 처리, 윤리적 고려 사항등에 대해서도 다루며, 실제 서비스 수준의 음성지능 시스템 구축 역량을 갖춘 인재를 양성하는 것을 목표로 함.

<p>황의원 교수 (생성형 인공지능 및 범용 인공지능)</p>	<ul style="list-style-type: none"> ◆ 핵심 교과목: 생성형인공지능 ◆ 강의 내용: <p>✓ 본 교과목은 생성형 인공지능의 핵심 이론을 이해하고, 다양한 모델들의 수학적 구조와 학습 원리를 분석하는 데 중점을 둘 계획임.</p> <p>✓ 구체적으로, 오토인코더, 생성적 적대 신경망, 플로우 기반 모델, 마스킹 기반 언어 모델, 자기회귀 모델, 확산 모델 등 대표적인 생성형 인공지능 모델들의 작동 원리를 학습하고자 함.</p> <p>✓ 아울러, 최근 주목받고 있는 멀티모달 대규모 언어 모델에 대해 학습하고, 범용 인공지능과의 연결성을 다루고자 함.</p> <p>✓ 각 모델에 대해 이론 강의와 실습을 병행하여 생성형 인공지능의 원리를 심도 있게 이해하고자 함.</p>
<p>오유란 교수 (인간컴퓨터상 호작용)</p>	<ul style="list-style-type: none"> ◆ 핵심 교과목: 인간컴퓨터상호작용특론 ◆ 강의 내용: <p>✓ 이 과목은 기본적인 인간컴퓨터상호작용 기본 이론 및 방법론을 기반으로 빠르게 발전하는 차세대 핵심기술을 응용한 인간과 AI/로봇간의 상호작용과 관련된 내용을 다룸.</p> <p>✓ 본 과목은 대학원 학생들에게 다음의 역량을 향상시킴을 목표로 함.</p> <ul style="list-style-type: none"> • 인간컴퓨터상호작용의 핵심 이론과 모델을 설명하고 이를 지능형 인터페이스 설계에 적용할 수 있음. • 차세대 AI기술을 활용하여 사용자 및 맥락맞춤형 지능형 인터페이스를 구현할 수 있음. • 구현한 인터페이스를 성능 및 사용자의 관점에서 정량적 및 정성적으로 평가할 수 있음.

보안 인공지능 트랙

<p>양대현 교수 (기계학습 기반 보안)</p>	<ul style="list-style-type: none"> ◆ 핵심 교과목: 컴퓨터보안특론, 시스템보안특론, 사이버보안특론 ◆ 강의 내용: <p>✓ 네트워크 및 시스템 분야에서 발생하고 있는 다양한 보안 이슈를 살펴보고, 이를 해결하기 위한 최신 연구 결과를 소개하고 있음.</p> <p>✓ 특히 네트워크 아키텍쳐 및 라우터 아키텍처를 살펴보고 라우터에서 침입 탐지를 위한 다양한 보안 기술을 소개함.</p> <p>✓ AI 기반 침입탐지 기술을 위한 기초가 되는 네트워크 모니터링 및 트래픽 측정 기술과 이를 이용해서 AI 모델에 사용될 특징추출이 어떻게 이루어지고 있는지를 다양한 알고리즘을 통해 소개함.</p> <p>✓ 침입탐지 인공지능 모델을 위한 실시간 플로우별 패킷 특징 추출 기술에 대해 학습함.</p> <p>✓ 플로우별 패킷 특징 추출을 위해서 근사 카운팅 알고리즘인 데이터 스케치에 대해 학습함.</p> <p>✓ AI 모델이 접근제어리스트를 관리하는 기술을 소개함.</p> <p>✓ 미래 인터넷 아키텍처의 중요한 방향 중 하나인 인-네트워크 방어(In-Network Defense)의 기본 원리를 이해하는데 필요한 기반 기술의 소개를 목표로 함.</p> <p>✓ 정량적으로 프라이버시 유출의 양을 정의하는 differential privacy 개념에 대해</p>
------------------------------------	--

	<p>소개하고 있음.</p> <ul style="list-style-type: none"> ✓ 다양한 데이터 및 함수에 대해 differential privacy를 적용하기 위한 방안을 학습 함. ✓ differential privacy를 만족하는 인공지능 모델을 만들기 위해 고안된 다양한 알고리즘 (DP-SGD 등) 및 데이터 합성 알고리즘에 대해 소개함.
배호 교수 (AI 보안 및 데이터 보안)	<ul style="list-style-type: none"> ◆ 핵심 교과목: 인공지능융합보안 ◆ 강의 내용: <ul style="list-style-type: none"> ✓ 딥러닝에서의 보안 문제와 AI모델을 활용하면서 발생되는 데이터보안 문제의 기본 개념에 대해서 소개하고 있음. ✓ 다루어질 주제로는 적대적 모델, adversarial example (공격), adversarial training (방어), 멤버십 추론 등 인공지능 모델 사용측면의 데이터 보안 기술의 소개를 목표로 함.
김종길 교수 (보안 애플리케이션)	<ul style="list-style-type: none"> ◆ 핵심 교과목: AI기반IoT보안, 차세대보안 특론 ◆ 강의 내용: <ul style="list-style-type: none"> ✓ AI기반IoT보안 과목은 인공지능 기술이 다양한 응용 기술(CPS, IoT 등)에 적용됨에 따라 발생할 수 있는 보안 이슈를 종합적으로 다루는 것을 목표로 함. ✓ 특히 최근 주목받고 있는 대규모 언어 모델(LLM) 및 On-Device AI 기술의 급속한 도입에 따라 새롭게 부각되는 보안 문제(악의적인 프롬프트 인젝션, 모델 도용, 민감 정보 노출을 방지하기 위해 입력 검증, 모델 암호화, 접근 제어 등)에 대한 이해를 바탕으로, 모델 개발부터 응용 기술에 도입에 이르기까지 전 과정에서 데이터 프라이버시, 모델 무결성, 사용자 보호를 고려한 정책 수립을 할 수 있는 능력을 확립하도록 지도하고자 함. ✓ 차세대 보안 특론 과목은 블록체인 보안, 랜섬웨어 공격, 침입탐지 시스템 등 주요 보안 문제 또는 보안 관련 기술을 소개하고, 이에 대한 최신 동향 및 연구 방향을 소개함. ✓ 특히, 차세대 기술과 관련된 보안이슈를 인공지능/기계학습 등을 활용하여 분석할 수 있고, 분석된 내용을 바탕으로 차세대 기술과 관련된 보안 이슈를 해결하기 위한 솔루션을 제시할 수 있는 역량을 기를 수 있도록 지도하려함.
오세은 교수 (인공지능 보안)	<ul style="list-style-type: none"> ◆ 핵심 교과목: 딥러닝보안 ◆ 강의 내용: <ul style="list-style-type: none"> ✓ 인공지능 알고리즘은 사이버보안 분야에서 침입 탐지, 악성코드 분석, 네트워크 이상 행위 탐지 등 다양한 목적으로 활용되고 있음. ✓ 본 과목은 기계학습과 딥러닝 모델의 핵심 원리를 이해하고, 이를 실제 보안 문제 해결에 적용할 수 있는 능력을 기르는 데 중점을 둠. ✓ 특히, 인공지능 모델의 신뢰성을 위협하는 대표적인 공격 기법인 모델 포이즌링 (Model Poisoning), 적대적 예제(Adversarial Example), 멤버십 추론 공격 (Membership Inference Attack)을 학습하며, 이러한 기법들을 실습과 프로젝트를 통해 직접 실험해봄. ✓ 이를 통해 인공지능 기반 보안 솔루션을 설계·구현하고 기존 기술을 분석·평가하는 능력을 종합적으로 향상시키는 것을 목표로 함.

2. 인력양성 계획 및 지원 방안

2.1 교육연구단의 우수 대학원생 확보 및 지원 계획

2.1.1 우수 대학원생의 확보 계획

○ 우수 대학원생 확보를 위한 파격적인 장학금 제도

- 이화여대에는 우수 대학원생 확보를 위한 다양한 대학원 장학금 제도가 마련되어 있음 (표 2-d 참조)
- BK21 장학금, 연구 인턴 장려금, 학술활동비 지원, 성과기반 장학제도 등 박사 진학을 유도하기 위한 다양한 재정적 지원을 제공하고자 함

<표 2-d> 교내 대학원 장학 제도

장학금명	장학금액
석/박사과정생 대상	
최우수이화인	대학원 수업료 전액
이화연구엑셀런스	
학·석사연계과정생	
우수이화인	대학원 수업료 1/2
우수이화과학인	
연구조교	
연구우수 장학금	
우월김활란21세기	등록금 전액 및 연구지원비(300만원/학기)
해외연구(논문집필)	US \$1,000/월 및 1회 왕복 항공료
우수연구	300만원/학기(연구지원비)
우수학술논문, 대학원융복합연구논문제재	100만원
대학원융복합프로젝트	300만원
사이언스코	1,200만원

○ 우수 대학원생 유치를 위한 프로그램 운영

- 우수 대학원생 유치를 위해 다양한 프로그램을 운영할 예정이며, 연간 신입생 기준으로 1차년도 15명 (박사·통합과정 7명), 2차년도 20명 (박사·통합과정 10명) 유치를 목표로 함 (그림 2-6 참조)

박사과정 중심의 우수 대학원생 유치를 위한 프로그램 운영

연간 대학원(박사·통합과정) 신입생 1차년도 15명 (7명), 2차년도 20명 (10명) 목표

전공 및 타 전공 학부생 대상

대학원 설명회 및
오픈랩 행사

Ewha AIH Day에서
상담부스 운영

외국인 대상

학부생/교환학생/방문학생 대상
대학원 홍보 프로그램

외국인 대학원생의 모교 및
Hub 대학 네트워크 활용

산업체 근무 여성인력 대상

동영상 및 스트리밍을 통한
원격수강 환경 구축

산학 연계 교육·연구
프로그램

<그림 2-6> 박사과정 중심의 우수 대학원생 확보 계획

- ◆ 컴퓨터공학/사이버보안/인공지능 전공 및 타 전공 학부생 대상
 - ✓ 학부생 대상으로 매 학기 초 대학원 설명회를 개최하고, 오픈 랩 행사를 통해 대학원에서의 연구 내용 및 지원 사항들, 졸업 후 진로 등의 정보를 제공하여 우수한 학부생을 유치할 수 있도록 함
 - ✓ 각 연구실별로 대학원생 멘토를 지정하여, 학부생이 대학원 진학, 연구실 생활 등에 대해 부담 없이 문의할 수 있는 소통 창구 마련
 - ✓ 교내 타전공 우수 학부생들이 인공지능 분야의 연구와 교육에 노출될 수 있도록, Ewha AI Hackathon (AIH) Day를 매년 개최하고, 참여교수의 진로 상담을 통해 대학원 진학 유도
- ◆ 외국인 학생 대상
 - ✓ 최근 K-Culture의 유행으로 전세계에서 한국으로 오는 교환학생의 수가 증대되고 있음
 - ✓ 본교에서 수학 중인 외국인 학부생/교환학생/방문생 대상으로 인공지능 대학원 프로그램 홍보 프로그램 운영하여, 연구 결과물 및 교육 내용 소개
 - ✓ 본교 대학원 외국인 졸업생의 학부 대학교 및 인적 네트워크를 통해 우수 외국인 학생 유치
 - ✓ 중국 하얼빈 공과대학, 말레이시아 쿠알라룸프르 대학, 베트남 하노이공대, Le Quy Don 대학, 파키스탄 우주기술원 등을 허브로 선별하여 우수 외국인 학생 유치 노력
- ◆ 산업체 여성 인력의 대학원 진학 유도 계획
 - ✓ 산업체 여성 인력이 대학원을 병행하며 인공지능 전문인력으로 성장할 수 있는 학습 환경 마련
 - ✓ 본 교육연구단이 개설하는 모든 대학원 강의에 대해 동영상 VOD 또는 스트리밍 서비스를 제공하고, 원격 수강을 할 수 있는 환경 구축
 - ✓ 인공지능 소프트웨어학부 홈커밍 행사에서 본 교육연구단 실적 및 산학연계 프로그램 홍보

2.1.2 우수 대학원생의 지원 계획

○ 대학원 등록금 면제

- ◆ 대학원생의 교내 연구, 실습실, 수업 조교 지원을 통한 일부 등록금 면제 혜택을 지원
- ◆ 외국인 학생 대상 EGPP (Ewha Global Partnership Program) 장학생 선정을 통한 전액 등록금 면제

○ 생활비 지원

- ◆ BK21 인건비, 대학원생 튜터링 장학금 등을 통해 생활비 지원
- ◆ 외국인 학생에 대한 EGPP 장학생 선정을 통한 일부 생활비 지원

○ 우수 장학금 지원

- ◆ 최우수 대학원 입학생에 대한 특별 장학금 지원
- ◆ 우수한 외국인 학생에 대해 입학 시 추천을 통해 이공계 특별유치 장학금 지원

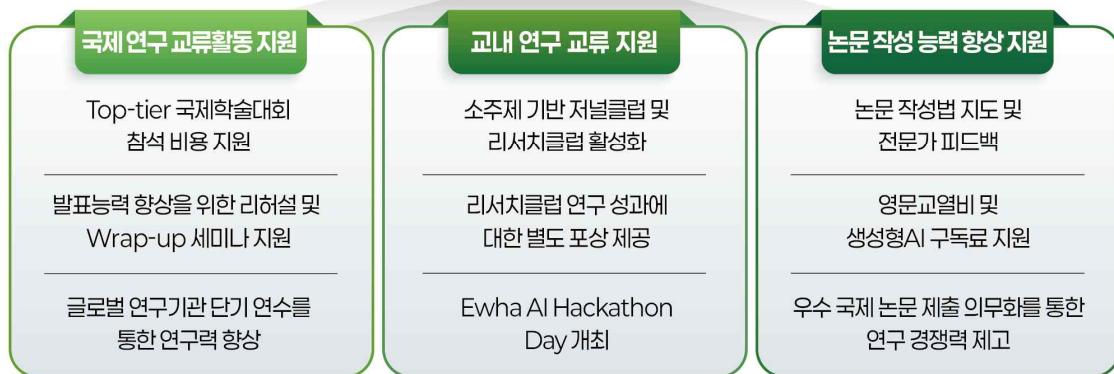
○ 우수연구결과 포상

- ◆ 참여 교수진, 산학 전문가, 글로벌 협력 자문위원 등으로 구성된 연구성과 평가위원회를 통해 논문, 특허, 기술이전 등 1년 동안 진행한 연구 결과물을 평가하여 결과에 따른 장학금 지급
- ◆ 고성과 연구자에게 주요 AI 분야 최우수 학술대회 (ICML, ICLR, KDD, ICDM, CVPR, ICCV, ECCV, NeurIPS, AAAI, NAACL, EMNLP, IJCAI, HPCA, ISCA, CCS, NDSS 등) 등록비, 출장비, 논문발표 지원 또는 국제 공동연구 파견 추천 등의 특전 부여
- ◆ 매년 사업단 연구우수팀을 선정하여 시상하고, 교내 언론, 뉴스레터 등 홍보를 통해 공식 업적 인정
- ◆ 성과에 따라 RA/TA 인건비 지원 규모 차등화

2.2 대학원생 학술활동 지원 계획

- 대학원생의 연구 수월성을 향상시키기 위하여 본 교육연구단은 국제 연구 교류 및 국내 연구 교류를 활성화하고, 논문 작성 능력을 향상시키는 지원체계를 구축하고자 함 (그림 2-7 참조)

대학원생 연구 수월성 증진을 위한 지원체계



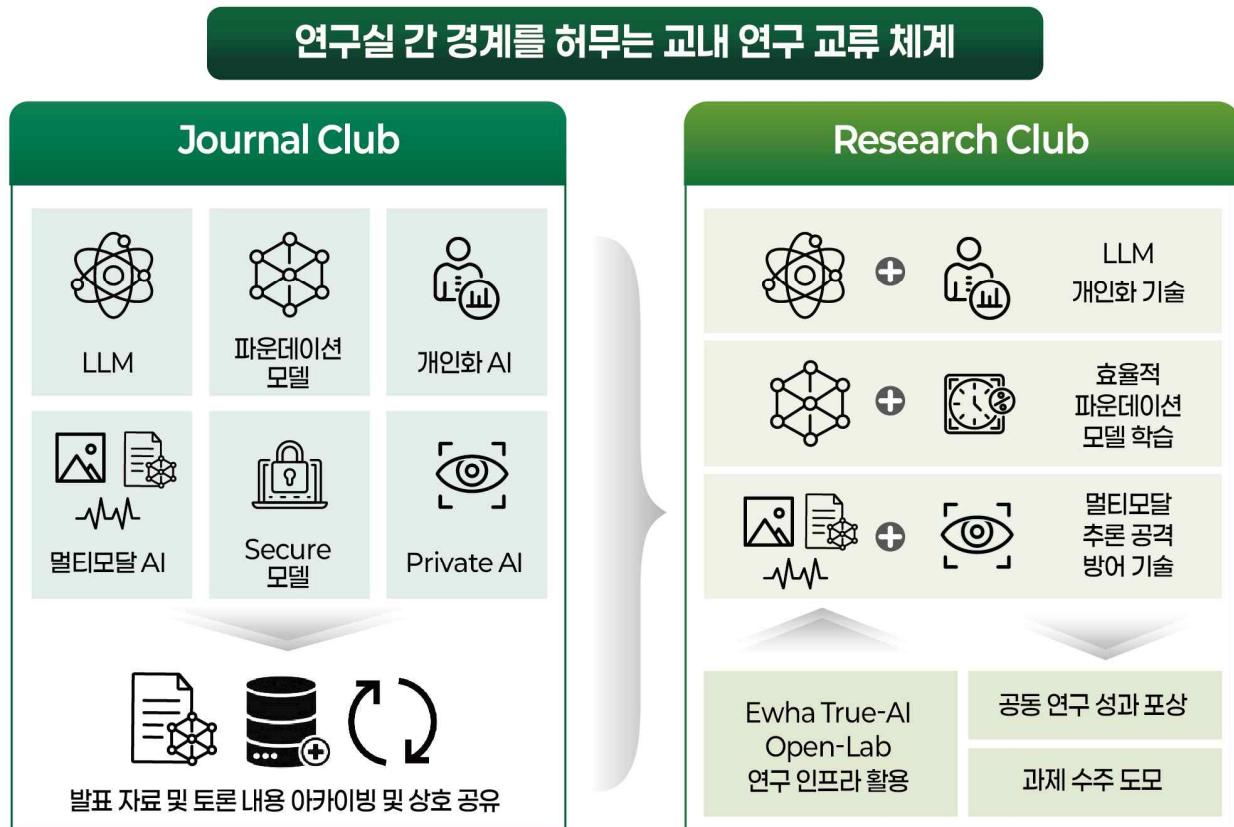
<그림 2-7> 대학원생 연구수월성 증진계획

○ 국제적 연구 교류를 통한 학술 활동 지원

- 대학원생 연구 실적 평가를 통해 최우수 학술대회 연 1회 참석 비용 지원 대학원생 선정
 - ✓ NeurIPS, ICML, ICLR 등과 같은 효율적 AI 및 IEEE S&P, ACM CCS와 같은 보안 AI 관련 분야 top-tier 국제학술대회 참석 비용을 연 1회 지원하여 연구 성과의 질적 수준을 높일 수 있도록 함
- 발표 능력 향상 지원
 - ✓ 국제학술대회 발표 리허설을 위한 회의비를 지원하여 소속 연구팀의 국제적 가시성을 제고함
 - ✓ 국제학술대회 참석 후 wrap-up 세미나 발표를 통해 국제교류 성과를 교육연구단 구성원들과 공유
- 글로벌 연구기관 단기 연수를 통한 연구 능력 향상 지원
 - ✓ 연구 실적 우수 대학원생을 선발하여 공동연구를 수행중인 해외 연구기관에 단기 연수 기회 제공
 - ✓ 관련 연구실과의 연계, 행정적 지원 및 연구에 필요한 항공료, 체재비 전액 지원

○ 교내 연구 교류를 통한 학술 활동 지원

- 연구실 간 경계를 허무는 Journal Club 및 Research Club 활성화 (그림 2-8 참조)
 - ✓ 효율적 AI 및 보안 AI를 중심으로, AI Fairness, Multimodal LLM, Tiny AI 등 다양한 세부 분야에 대한 소그룹 Journal Club 및 Research Club을 정기적으로 운영하여 연구실 간 교류를 활성화함
 - ✓ Journal Club은 참여 대학원생과 신진연구인력이 주도적으로 최신 논문을 분석하고, 발표자 및 토론자로 순환 참여함으로써 최신 기술에 대한 이해를 높이는 동시에 발표력과 토론 능력을 강화함
 - ✓ Journal Club에서 다룬 논문과 발표 및 토론 내용을 아카이빙하여 타 소그룹 간 연구 교류 활성화
 - ✓ Research Club은 각 연구자가 진행중인 연구 아이디어와 연구 진행 상황을 공유하고 토론하는 자리로, 서로 다른 연구실 및 분야 간 공동연구를 촉진하는 플랫폼으로 기능함
 - ✓ 특히, Research Club을 통해 교내 공동 연구를 수행한 논문 성과에 대해서는 별도의 포상을 제공하여 참여를 독려하고, 질 높은 연구교류 및 학술성과 창출을 유도함
 - ✓ Research Club을 통한 연구 수행 시, 코드, 데이터, 실험 공간 등의 AI 연구 인프라를 Ewha TRUE-AI Open Lab (III. 연구역량 영역 1.3.3 참조)과 연계하여 공동 활용
 - ✓ Journal Club 및 Research Club이 논문 게재 및 과제 수주 등 성과로 이어지도록 장려함



<그림 2-8> Journal Club 및 Research Club 활성화 계획

- 1년 1회 “Ewha AI Hackathon Day” Conference 개최

- ✓ 모든 참여 대학원생들이 수행하고 있는 연구의 포스터 발표를 통해 교육연구단 학술 결과 공유
- ✓ 학부생에게도 참석 동기를 부여하여, 연구 성과 홍보를 통한 우수 학부생 유치하는 계기로 활용

● 논문 작성 능력 향상 지원

- 초기 연구자를 위한 논문작성법 지도

- ✓ 본 교육연구단 소속으로 입학하는 석박사 신입생 전원을 대상으로 논문작성법 세미나/워크숍을 운영하며, 교내외 우수 연구자를 강사로 초청함

- 국제적 전문가의 연구 피드백

- ✓ 국제적 수준의 세미나 및 워크샵을 통해 지도교수 외의 전문가들의 피드백을 바탕으로 글로벌한 경쟁력을 가지는 연구 논문 작성 능력을 키우도록 함

- 국제학술지 영문교열비 및 생성형 인공지능 구독료 지원

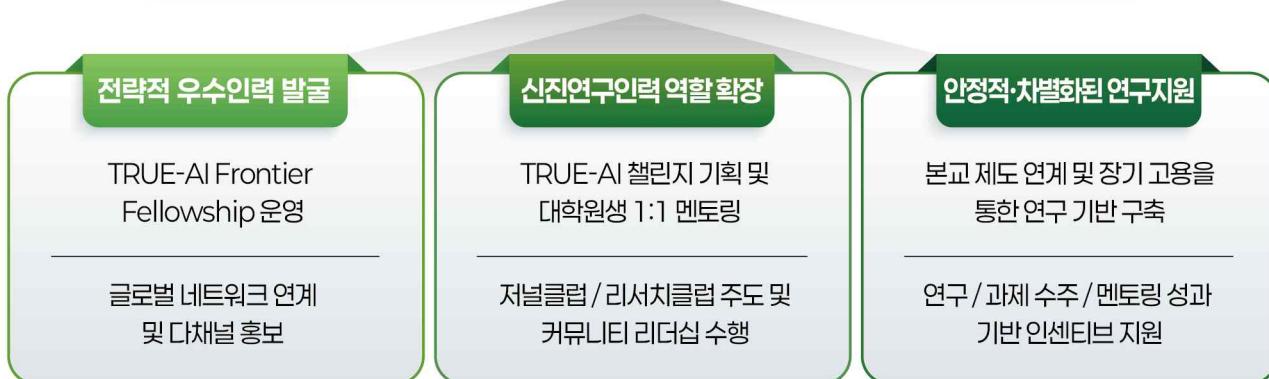
- ✓ 국제학술지 논문 채택률 제고를 위해 본교 산학협력단의 지원과 연계하여 영문교열비를 지원함
- ✓ 자료 수집, 정리, 코드작성, 영문교열 등을 보조하여 연구 생산성과 효율성을 높이기 위한 생성형 인공지능 서비스의 구독료를 지원함

- 학술지 및 국제학술대회 논문 제출 의무화

- ✓ 본 교육연구단 소속 박사과정은 IF 상위 SCI 저널 또는 BK 우수학술대회 게재, 석사과정은 국제학술대회 논문 제출을 졸업 요건으로 하여 국제 연구 경쟁력을 강화함

2.3 우수 신진연구인력 확보 및 지원 계획

우수 신진연구인력을 위한 TRUE-AI Frontier 지원체계



<그림 2-9> 우수신진연구인력 확보 및 지원 계획

○ 우수 신진연구인력 확보 및 선발 계획 (그림 2-9 참조)

◆ 신기술 분야의 우수 신진연구인력 확보 계획

- ✓ 국내 대학에서 박사학위를 취득한 신기술 분야의 우수한 외국인 신진연구인력을 매년 1~2명 박사 후 과정생 또는 계약교수로 적극 영입하여, 본 교육연구단의 연구 스펙트럼을 확장하고, 신진 연구인력의 학문적 성장을 도모함
- ✓ 효율적 AI와 보안 AI 분야의 우수 신진연구인력 확보를 위해 TRUE-AI Frontier Fellowship을 신설하여 분야별 핵심 이슈에 따라 매년 1~2개의 전략 테마를 지정하고, 해당 테마에 특화된 우수 박사인력을 국제 공개 모집함
- ✓ 예시 테마
 - 효율적 AI: “TinyML 기반 초경량 LLM 구조 설계 및 압축 기법”
 - 보안 AI: “적대적 공격 예측 탐지 및 방어를 위한 딥러닝 안전성 프레임워크”
- ✓ 연구단 웹사이트 및 국제학술대회 뿐만 아니라 LinkedIn, X, AI 커뮤니티 등에 공고하여 국내외 박사 인력풀 확대
- ✓ 후보자들은 자신의 연구와 해당 테마 간 적합성 및 기여 가능성을 강조한 전략 연구계획서를 제출
- ✓ 신진연구인력 선발은 연구 실적 및 본 교육연구단의 연구 분야와의 적합성 등을 토대로 서류 심사, 발표 심사, 면접 등의 엄중한 절차를 통해 선발함
- ✓ 선발된 신진연구인력은 연구뿐 아니라 대학원 수업 및 세미나 참여, 후속 세대 연구자 육성 등 다방면에서 본 교육연구단에 적극적으로 기여할 수 있는 인재로 성장할 수 있도록 체계적인 경력 개발 경로를 제공할 계획임

◆ 다양한 연구 네트워크를 이용한 우수 신진연구인력 확보 계획

- ✓ 본교 박사과정 졸업생 중 연구 역량이 검증된 인재를 지속적으로 관리하고, 국내외 공동 연구자 네트워크를 적극 활용하여 신진연구자를 유치할 예정임
- ✓ 특히 본 교육연구단의 참여 교수와 공동연구를 수행한 경력이 있는 연구자를 우선 고려함으로써 연구 연속성을 강화하고, 교육 및 연구 조직의 안정적 운영을 도모함
- ✓ 신진연구인력이 연구실 내에서 대학원생들과 협업을 통해 공동 논문 작성, 기술 세미나 개최, 프로젝트 기획 등을 수행하도록 하여 대학원 저학년 학생들의 연구력 배양에 기여하도록 함

○ 우수 신진연구인력 지원 및 경쟁력 확보 계획

◆ 본교의 제도 활용 및 고용 안정 지원

- ✓ 본교에서 운영 중인 전임연구인력 지원사업을 적극 활용하여, 박사후과정생(Post-doc)에게는 월 100만원, 연구교수에게는 월 150만원의 기본 인건비를 지원함
- ✓ 본 교육연구단 차원의 추가 지원을 통해, 참여 교수의 연구비 확보 여부와 관계없이 우수 신진연구인력이 안정적으로 고용될 수 있는 환경을 마련함
- ✓ 이를 통해 우수 신진연구인력의 소속감과 지속적인 연구 몰입도를 높이며, 전임교수의 연구 인프라를 강화하고 연구단 전체의 연구 경쟁력을 제고함
- ✓ 경력 단절을 방지하고 지속 가능한 연구 역량 확보를 위해 신진연구인력의 장기 고용을 권장함
- ✓ 성과 기반의 평가 체계를 마련하여, 일정 수준 이상의 연구 성과가 확인될 경우 계약 연장 및 보수 조건 개선이 가능하도록 하는 유연한 고용 운영 방식을 도입함

◆ 신진연구인력의 연구 성과 기반 경쟁력 강화 방안

- ✓ 박사후과정생 및 계약교수의 경우 본 사업 참여 교수와의 공동연구 논문 연 1편의 top-tier 국제 학술대회 논문 또는 SCI 상위 15% 논문 게재를 의무화함으로써 국제적 연구 역량을 제고
- ✓ 신진연구인력은 대학원생으로 구성된 소규모 연구팀을 이끌고, 오픈소스 기반 최신 모델들에 대해 효율성과 보안성을 벤치마킹하는 TRUE-AI Challenge를 주도함.
- ✓ 챌린지 진행 결과를 보고서, 소스코드, 시연 영상 등으로 제출하며, 연구단 내부 심사를 통해 우수 리더에게는 성과 인센티브 및 Seed 연구비를 추가로 지원하여 자율성과 창의성을 고취함

◆ 멘토링 및 커뮤니티 리더십 역할 수행

- ✓ 우수 신진연구인력과 대학원생의 1:1 멘토링을 통해 대학원생의 연구 방향, 논문 작성, 실험 설계 등에 대한 지도를 수행함
- ✓ 이를 통해 대학원생의 연구 몰입도와 성과 수준을 끌어올리는 동시에, 신진연구인력 역시 교육 및 지도 경험을 축적함
- ✓ 우수 신진연구인력이 자립적인 연구자로 성장할 수 있도록 연구과제 수주를 장려하고, 과제 수주시 일정 수준 이상의 인센티브를 제공함으로써 연구 기획 및 제안서 작성 역량 강화에 도움을 줌
- ✓ Journal Club 운영 시, 신진연구인력이 리더 역할을 맡아 세부 분야의 핵심 논문을 선정하고, 발표자 일정 조율, 발표 후 토론 유도, 자료 아카이빙까지 담당함
- ✓ 이를 통해 대학원생에게는 특정 분야에 대한 체계적인 이해와 최신 트렌드 학습 기회를 제공하고, 리더는 분야별 큐레이터로서의 전문성을 축적함
- ✓ Research Club을 마이크로랩(Micro Lab) 형태로 구성하여 신진연구인력이 직접 연구 주제를 발굴하고 대학원생들과 함께 소규모 프로젝트를 수행함
- ✓ 이 과정을 통해 연구기획력, 리더십, 팀워크, 멘토링 역량을 자연스럽게 배양할 수 있는 환경을 조성함

3. 참여교수의 교육역량

3.1 참여교수의 교육역량 대표 실적

<표 2-1> 인공지능 분야 문제해결을 위한 참여교수의 교육역량 대표실적

연번	참여교수명	연구자등록번호	세부전공분야	대학원 교육 관련 대표실적물	DOI번호/ISBN/인터넷 주소 등
	배호	11635105	기계학습및지식처리	새로운 대학원 교과목 개발 및 개설	-
1				<ul style="list-style-type: none"> • 과목명: 인공지능보안특론 • 과목 내용 <ul style="list-style-type: none"> ✓ 인공지능 보안 분야는 인공지능 등장과 함께 급격히 발전하였음 ✓ 최근 생성 모델의 발전에 따라 딥페이크와 같은 많은 공격들로 사회적 화두가 되고 있음 ✓ 대학원에서 개설되는 인공지능 보안 관련 교과목은 딥페이크의 원리 및 방어에 대한 최근 연구 결과를 소개하는 것에 초점을 맞추고 있음 ✓ 본 수업에서는 전통적인 보안 기법이 딥러닝 모델에 적용되는 방법 그리고 차이점 등에 대한 소개와 전통 보안을 접목하는 시도를 주로 소개함으로써 인공지능 보안 관련하여 처음 개설되는 수업임 	
2	반효경	10091721	인공지능시스템 및응용	새로운 대학원 교과목 개발 및 개설	-
				<ul style="list-style-type: none"> • 과목명: AI융합기반기술주제연구 I • 과목 내용 <ul style="list-style-type: none"> ✓ 현대의 AI 워크로드는 전통적인 워크로드들과 달리 여러 기능이 결합된 융합적인 성향을 띠면서 그 특성에 맞는 시스템의 최적화 과정이 필요함 ✓ 특히, 다양한 산업용 시스템에서 빅데이터, 인공지능, 실시간 워크로드 등을 처리함에 있어 복잡한 제약조건과 여러 복합 파라미터들을 동시에 최적화해야 하는 문제가 발생함 ✓ 본 강좌에서는 이러한 미래형 AI 융합 워크로드를 위한 하드웨어 및 소프트웨어 환경에서 발생하는 복잡한 최적화 문제를 진화 연산 등을 통해 해결하는 방법에 대해 살펴봄 	
3	오유란	11812138	인공지능시스템 및응용	새로운 대학원 교과목 개발 및 개설	-
				<ul style="list-style-type: none"> • 과목명: 인간컴퓨터상호작용특론 • 과목 내용 <ul style="list-style-type: none"> ✓ 이 과목은 기본적인 인간컴퓨터상호작용 기본 이론 및 방법론을 기반으로 빠르게 발전하는 차세대 핵심기술을 응용한 인간과 AI/로봇간의 상호작용과 관련된 내용을 다룸 ✓ 본 과목은 대학원 학생들에게 다음의 역량을 향상시킴을 목표로 함 <ul style="list-style-type: none"> • 인간컴퓨터상호작용의 핵심 이론과 모델을 설명하고 이를 지능형 인터페이스 설계에 적용할 수 있음 • 차세대 AI기술을 활용하여 사용자 및 맥락맞춤형 지능형 인터페이스를 구현할 수 있음 • 구현한 인터페이스를 성능 및 사용자의 관점에서 정량적 및 정성적으로 평가할 수 있음 	

	민동보	10190916	시각정보처리	새로운 대학원 교과목 개발 및 개설	
<p>◆ 과목명: 컴퓨터비전개론</p> <p>◆ 과목 내용</p> <p>✓ 컴퓨터비전 분야는 인공지능의 등장과 함께 급격히 발전하였으며, 이로 인해 대학원에서 개설되는 컴퓨터비전 관련 교과목은 딥러닝 기반 최근 연구 결과를 소개하는 것에 초점을 맞추고, 딥러닝 이전의 전통적인 컴퓨터비전에 대한 소개는 거의 진행되지 않고 있음</p> <p>✓ 그러나, 최근 연구 결과들은 전통적인 컴퓨터비전 연구 방법론을 AI 모델에 적용하여 높은 성능 향상을 보여주고 있음</p> <p>✓ 본 수업에서는 딥러닝이 적용되지 이전의 컴퓨터비전 연구에 대한 소개와 이를 딥러닝과 접목하는 시도를 주로 소개함으로써 기존 개설 교과목과는 다른 관점에서 수업을 진행함</p>					
4	참여 교수 수	7	최대 제출 건수	4	

4. 교육의 국제화 전략

4.1 교육 프로그램의 국제화 계획

4.1.1 국제화 목표 및 전략

- 본 교육연구단은 “국제공동연구 활성화를 통한 최우수 연구실적 확보 및 졸업생의 국제화 역량 증진”을 핵심 목표로 설정하고, 교육, 연구, 인력양성의 전 과정에 걸쳐 국제화를 반영한 구조적 실행 전략을 마련하고자 함
- 교육 프로그램의 국제화를 위한 추진 전략은 다음과 같음 (그림 2-10 참조)



<그림 2-10> 교육 프로그램의 국제화 전략

◆ 추진전략 1. 국제 학술 활동 및 글로벌 연구 네트워크 구축

- ✓ 연구 실적 최우수 학생에게 매년 국제 최우수 학술대회 참가비를 전액 지원함
- ✓ 국제학술대회 참가 시 세계적 연구자들과의 네트워킹을 위한 회의비를 지원함
- ✓ 형성된 글로벌 네트워크는 향후 국제 공동연구 및 연구자 교류의 발판으로 적극 활용함

◆ 추진전략 2. 해외 인턴십 및 공동연구 장려

- ✓ 해외 유수 연구기관 및 글로벌 AI 선도기업과의 협력 네트워크를 활용하여, 대학원생이 일정 기간 동안 현지에서 직접 연구에 참여할 수 있는 인턴십 또는 공동 연구 기회를 제공함
- ✓ 학생들은 국제 프로젝트를 수행하며 실전 역량과 글로벌 커뮤니케이션 능력을 강화하고, 현지 전문가와의 멘토링을 통해 연구 방향에 대한 고도화를 도모할 수 있음
- ✓ 이러한 경험은 논문 수준 향상은 물론, 해외 박사후과정 또는 해외 취업으로도 이어질 수 있음

◆ 추진전략 3. 해외 석학 및 산업 전문가 초청 프로그램 강화

- ✓ 해외 학자 및 글로벌 기업 전문가들을 정기적으로 초청하여 특강, 세미나, 워크숍 등을 운영함
- ✓ 해외 전문가 초청 시 교육연구단 예산으로 통해 교통비, 체재비, 관련 경비를 적극 지원할 예정임
- ✓ 이를 통해 학생들은 생성형 AI, 멀티모달 보안, AI 경량화 등 첨단 연구 동향과 산업계의 최신 기술을 직접 체감하고, 참여교수진은 후속 공동연구 기회를 모색할 수 있음

◆ 추진전략 4. 글로벌 산학협력 기반 교육과정 운영

- ✓ 본 교육연구단은 Microsoft Research, Adobe Research 등 글로벌 기술 선도 기업들과 협력하여 실무 중심의 프로젝트 기반 교과목을 기획하고 운영할 계획임
- ✓ 이들 기업과의 협력을 통해 생성형 AI, 멀티모달 LLM, 자율주행, 보안 인공지능 등 다양한 주제에 대해 공동 캡스톤 수업을 구성하며, 수업의 일환으로 실제 기업의 문제 해결 과제를 수행하게 함
- ✓ 또한, 기업 파트너로 구성된 글로벌 산학협의체를 통해 정기적인 수업 운영 평가 및 피드백 회의를 진행하여 교육과정의 품질과 산업적 유효성을 개선함

◆ 추진전략 5. 우수 외국인 학생 유치 전략 다각화

- ✓ 본교에 재학 중인 외국인 학부생, 교환학생 등을 대상으로 효율적 AI 및 보안 AI 분야 대학원 진학 설명회를 개최하고, 연구실 오픈랩 및 다국어 홍보자료를 활용하여 진학을 유도하고자 함
- ✓ 본교 대학원 외국인 졸업생의 모교 및 연구 네트워크를 기반으로, 'Global Ambassador' 제도를 운영하여 우수 인재를 유치하기 위한 현지 설명회, 온라인 Q&A 세션 등을 주기적으로 개최함
- ✓ 중국 하얼빈 공과대학, 말레이시아 쿠알라룸프르 대학, 베트남 하노이공대, Le Quy Don 대학, 키스탄 우주기술원 등을 허브로 선별하여 우수 외국인 학생을 유치하고자 함
- ✓ 외국인 유학생을 위한 EGPP 장학금, 연구참여기회(RA), 생활지원(비자 · 기숙사 등), 한국어 · 영어 튜터링 등 전 주기에 걸친 정착 및 성장 지원체계를 강화함

◆ 추진전략 6. 성과 기반의 지속적 피드백 체계 마련

- ✓ 모든 국제화 프로그램은 단기 실적 중심이 아닌, 중장기적인 연구 및 교육 역량 강화를 목표로 설계됨
- ✓ 국제 공동 프로젝트 결과물은 문제 중심 학습(PBL) 교과목의 실제 사례로 활용됨
- ✓ 또한 국제 교육 프로그램 평가 회의를 통해 프로그램의 효과성과 개선 사항을 주기적으로 점검함으로써, 국제화 프로그램의 질적 성장을 지속적으로 관리할 예정임

4.1.2 외국 연구소 및 대학과의 인적 교류 현황

- 현재 참여교수진은 아시아, 유럽, 미국 등 다양한 외국 연구소/대학과 활발한 인적 교류를 이어가고 있으며, 기존에 구축한 글로벌 협력 네트워크를 기반으로 향후 교류를 확대하고자 함 (표 2-e 참조)

표 2-e. 외국 연구소 및 대학과의 인적 교류 실적

담당 교수명	교류 교수명	소속 기관	교류 내용	연도
양대현	David Mohaisen	University of Central Florida (미국)	<ul style="list-style-type: none"> 공동연구를 위해 상호 기관 방문 및 Workshop 개최 ✓ 2016년~2022년 국제공동연구 (NRF Global Research Lab) 기간 동안 본교 및 UCF의 연구책임자는 매년 상호 방문 및 workshop을 개최함 ✓ 빅데이터의 measurement work을 통해 보안 관점에서의 insight를 도출하고, AI모델이 활용할 수 있는 feature measurement를 위한 알고리즘을 연구함 ◆ 보안 빅데이터 기술 연구를 위한 학생 파견 ✓ 공동 연구 기간동안 박사과정 학생 3명을 UCF에 파견하여 Dual-PhD degree를 취득하도록 함 ✓ 해당 학생들은 현재 미국 유수대학의 조교수 (Wayne State University, Loyola at Chicago) 또는 국내출연연(ETRI)의 연구원으로 재직중임 	2017~2022
	Rhongho Jang	Wayne State University (미국)	<ul style="list-style-type: none"> ◆ 공동연구 수행 ✓ AI 기반 네트워크 침입 탐지에 필요한 패킷 레벨의 고속 특징 추출을 위한 공동연구를 수행함 ✓ 매주 5년이상 거의 매주 정기 온라인 연구미팅을 진행중임 ✓ 보안분야 Top-tier conference의 다수의 논문을 공동연구의 결과로 출판함 ◆ 공동연구를 위한 본교 방문 ✓ 2023년 7월 본교에 방문하여 대면 연구 미팅을 수차례 진행함 ◆ 공동 학생 지도 ✓ 이화여자대학교의 대학원생과 Wayne State University의 대학원생을 공동 지도하며 교육에서의 국제화에도 노력하고 있음 	2020~2025
	Sanghyun Hong	Oregon State University (미국)	<ul style="list-style-type: none"> ◆ 세미나 진행 ✓ 제목: Great Haste Makes Great Waste: Exploiting and Attacking Efficient Deep Learning ✓ 효율적인 인공지능 모델의 취약점 주제의 초청 강연함 	2022
	Junsu Im	Facebook (미국)	<ul style="list-style-type: none"> ◆ 공동연구 수행 ✓ 2025년 3월 14일부터 현재까지 Log-Structured Merge Tree의 인덱싱 알고리즘을 공동연구 진행중임 ✓ 격주로 Facebook, POSTECH, 이화여대의 연구진이 온라인 미팅을 진행 ◆ 세미나 진행 ✓ 2025년 3월 14일 첫 온라인 세미나 진행: LSMTree 자료구조 및 알고리즘과 성능상의 이슈 소개 ✓ 이후 현재까지 6차례 온라인 세미나 진행함: LSMTree의 Pointquery 및 Rangequery의 성능향상을 위한 새로운 indexing scheme을 개발 중 	2025
오세은	Afsah Anwar	University of New Mexico (미국)	<ul style="list-style-type: none"> ◆ 공동연구 수행 ✓ ML 기반의 멜웨어 탐지 공동연구를 수행함 ✓ 연구 결과를 2022년 RAID, IEEE TDSC 등에 출판함 	2024
	Marc Juarez	University of Edinburgh (영국)	<ul style="list-style-type: none"> ◆ 세미나 진행 ✓ 2024년 5월 7일에 Machine Learning For Traffic Analysis를 주제로 세미나를 개최함 ✓ 기계학습 및 딥러닝 모델에 Tor 네트워크 트래픽 분석에 활용되어 온 	2024

민동보			<p>대표적 연구들을 소개함</p> <ul style="list-style-type: none"> ✓ 세미나 후 Tor 네트워크 상관관계 분석 모델 개발에 연구 협력을 위한 방안을 논의함 	
	Limin Jia	Carnegie Mellon University (미국)	<ul style="list-style-type: none"> ◆ 세미나 진행 ✓ 2024년 12월 18일에 Automatically synthesizing exploits for code injection attacks in Node.js packages 주제로 세미나를 개최함 ✓ 자바스크립트 코드 삽입 취약점에 대해 자동 익스플로잇을 생성해 766개 NPM 패키지에서 검증연구 소개함 ✓ 세미나 후 코드 합성 및 멀웨어 분석 연구에 LLM 사용 가능성 공동연구를 위한 프로젝트 논의함 	2024
	Yuchi Huo	Zhejiang University (중국)	<ul style="list-style-type: none"> ◆ 공동연구 수행 ✓ 약지도학습 환경에서 객체 분할을 위한 새로운 방식을 공동 연구함 ✓ 비정기적 온라인 미팅을 통해 아이디어 도출 및 논문 작성 검토 ✓ 공동연구 성과가 IEEE Trans. on Circuits and Systems for Video Technology 2024에 출판됨 ✓ 약지도학습 기법을 AI 모델의 적응 능력 개선에 적용할 수 있음 	2023-2024
	Yuchi Huo	Zhejiang University (중국)	<ul style="list-style-type: none"> ◆ 공동연구 수행 ✓ 물체의 경계정보를 적응적으로 활용한 객체 분할 방식을 공동 연구함 ✓ 비정기적 온라인 미팅을 통해 아이디어 도출 및 논문 작성 검토 ✓ 공동연구 성과가 IEEE Trans. on Multimedia 2023에 출판됨 ✓ 객체 분할 방식을 자율주행을 위한 AI 모델에 적용 예정 	2022-2023
	Pascal Frossard	EPFL (스위스)	<ul style="list-style-type: none"> ◆ 공동연구 수행 ✓ 3차원 정보 추정의 신뢰도를 추정하는 기법을 공동 연구함 ✓ 비정기 온라인 미팅을 통해 아이디어 개발 및 실험 설계 논의함 ✓ 공동연구 성과가 TPAMI 2023에 출판됨 ✓ 신뢰도 추정 기법을 AI 모델의 예측 신뢰도 측정으로 확장할 수 있음 	2021-2023
	Matteo Poggi	University of Bologna (이탈리아)	<ul style="list-style-type: none"> ◆ 공동연구 수행 ✓ 3차원 정보 추정의 신뢰도 추정 기법에 대한 서베이 논문을 공동 작성함 ✓ 비정기 온라인 미팅을 통해 아이디어 개발 및 실험 설계 논의함 ✓ 공동연구 성과가 TPAMI 2022에 출판됨 ✓ AI 모델의 예측 신뢰도 측정 연구로 확장할 수 있음 	2020-2022
	Stephen Lin	Microsoft Research Asia (중국)	<ul style="list-style-type: none"> ◆ 공동연구 수행 ✓ 다양한 종류의 영상 정합을 위한 새로운 표현자를 공동 연구함 ✓ 비정기 온라인 미팅을 통해 아이디어 개발 및 실험 설계 논의함 ✓ 공동연구 성과가 TPAMI 2021에 게재됨 ✓ 멀티모달 영상 데이터 기반 AI 모델로 확장 가능함 	2019-2021
	Kwang Moo Yi, Sungmin Cha	UBC (캐나다), NYU (미국)	<ul style="list-style-type: none"> ◆ 공동연구 수행 ✓ 거대 비전 모델의 효율적인 사전학습 연구를 공동으로 진행함 ✓ 격주로 온라인 미팅을 통해 아이디어 개발, 실험 설계, 논문 작성 등을 진행함 ✓ 공동연구 성과가 ECCV 2024에서 발표됨 ✓ 거대 멀티모달 AI 모델의 효율적 학습에 적용할 수 있음 	2023-2024
	Sangryul Jeon	University of Michigan (미국)	<ul style="list-style-type: none"> ◆ 공동연구 수행 ✓ 강화학습을 위한 효율적 시각 데이터 처리 기법을 공동 연구함 ✓ 비정기 미팅을 통해 아이디어 도출 및 실험 설계를 진행함 ✓ 공동연구 성과가 CVPR 2023에서 발표됨 ✓ 로봇 제어를 위한 AI 모델에 확장 가능함 	2022-2023
	Sangryul Jeon	University of Michigan (미국)	<ul style="list-style-type: none"> ◆ 공동연구 수행 ✓ 영상 정합을 위한 Nerf 기반 효율적인 AI 모델을 공동 연구함 ✓ 격주로 온라인 미팅을 통해 아이디어 개발, 실험 설계, 논문 작성 등을 진행함 ✓ 공동연구 성과가 NeurIPS 2022에서 발표됨 ✓ 3차원 공간 인식 AI 모델로 확장 가능함 	2021-2022

	Stephen Lin	Microsoft Research Asia (중국)	<ul style="list-style-type: none"> ◆ 공동연구 수행 ✓ 영상 정합을 위한 재귀적 AI 모델을 공동 연구함 ✓ 비정기적 온라인 미팅을 통해 아이디어 개발, 실험 설계를 진행함 ✓ 공동연구 성과가 NeurIPS 2020에서 발표됨 ✓ 재귀적 AI 모델에 사용된 방법론은 효율적 AI 학습에 적용할 수 있음 	2019-2020
	Kwang Moo Yi	University of British Columbia (캐나다)	<ul style="list-style-type: none"> ◆ 학생 과제 ✓ 통합과정 최혜송 학생이 2024년 7-8월 (2개월) 동안 UBC에 방문하여 공동연구를 수행함 ✓ 현지 대학원생과의 협업을 통해 생성형 AI 학습 기반 효율적 사전학습에 대한 논의를 심화하였고, 이를 기반으로 논문 투고 예정 	2024
반효경	Kang G. Shin	University of Michigan (미국)	<ul style="list-style-type: none"> ◆ 기관 학술 교류 ✓ 미시간대 Kang G. Shin 석좌교수의 본교 Ewha Global Fellow 선정 ✓ 본교 임베디드SW연구센터와 미시간대 RTCL의 기관 상호 학술 교류 ✓ 실시간 임베디드 분야의 연구인력 교류 및 공동연구 수행 	2022-2024
이지영	Daniel McDuff	Microsoft (미국)	<ul style="list-style-type: none"> ◆ 세미나 참여 ✓ 2020년에 온라인으로 개최된 Microsoft AI Breakthrough 워크샵에 참여하여 포스터 발표를 진행함 ✓ 세미나를 통해 공동연구 관심사를 도출 후, 협력방안을 논의함 ◆ 공동연구 수행 ✓ 자율주행 인과추론 기반 시뮬레이션 공동연구 진행 ✓ 매주 온라인 미팅을 통한 실험 진행상황 및 연구 진행방향을 공유함 ✓ 공동연구 성과가 CLeaR 2022 학회에서 발표됨 	2020-2021
	Justin Salamon	Adobe (미국)	<ul style="list-style-type: none"> ◆ 공동연구 수행 (해외 인턴십) ✓ 사용자 맞춤 오디오비주얼 이벤트 감지 시스템에 관한 공동연구를 진행함 ✓ 매주 온라인 미팅을 통한 실험 진행상황 및 연구 진행방향을 공유함 ✓ 이를 통해 개발한 'Automatic recognition of visual and audio-visual cues' 기술을 미국 특허로 등록함 	2021
	Gyeongsik Moon	Meta (미국)	<ul style="list-style-type: none"> ◆ 공동연구 수행 ✓ 3D Human mesh 생성 기술에 대한 공동연구를 진행함 ✓ 비정기적 온라인 미팅을 통한 실험 진행상황 및 연구 방향을 논의함 ✓ 공동연구 성과가 CVPR 워크숍에서 발표됨 	2023
	Changjae Oh	Queen Mary University of London (영국)	<ul style="list-style-type: none"> ◆ 공동연구 수행 ✓ 비디오 예측 모델 기반 데이터 이상탐지에 대한 공동연구를 진행함 ✓ 연구방향 발굴 및 문제해결에 대한 비정기적 온라인 미팅을 진행함 ✓ 공동연구 성과가 BMVC 학회에서 발표됨 	2020-2021
	Jiasen Lu	Allen Institute for AI (미국)	<ul style="list-style-type: none"> ◆ 공동세미나 진행 ✓ 멀티모달 통합 모델 관련 연구 세미나를 매달 온라인으로 진행함 ✓ MLLM, 옴니모달 모델, Unified IO와 같은 거대 멀티모달 모델에 대한 최근 연구동향을 교류함 ✓ 또한 연구중인 주제의 한계점, 문제를 공유하고 피드백을 통해 각각의 전문성을 바탕으로 한 논의를 진행함 	2022-2023
	Christian Wolf, Diane Larlus	NAVER LABS EUROPE (프랑스)	<ul style="list-style-type: none"> ◆ 학술교류 ✓ ICCV 2023, ICML 2024 학회 기간동안 참여한 각 기관의 연구자들과 단체 연구 교류회를 진행함 ✓ Round table meeting 방식으로 각자의 관심사 및 연구주제 (3D, Robotics, Vision, Generation model, Multimodal representation learning)에 관한 연구 토론을 진행함 ✓ 이를 통해 비슷한 관심사를 가진 연구자들과 새로운 연구 네트워크를 형성하며 지속적인 교류를 계획함 	2023-2024
이형준	Omprakash Gnawali	University of Houston	<ul style="list-style-type: none"> ◆ 공동연구 수행 ✓ 2020년 IEEE Access 공동 논문 실적으로 현재까지 효율적인 AI 네트워크 	2018~2024

		(미국)	구조에 대해 공동연구 진행 중임 ◆ 세미나 진행 ✓ 2018년 본교 컴퓨터공학과에 방문하여 첫 대면 세미나를 진행한 이후, 2023년 5월, 2024년 12월 방문하여 공동 연구 계획 미팅 진행하였음	
	Ji, Bo	Virginia Tech University (미국)	◆ 공동연구 수행 ✓ 효율적인 AI 아키텍처 및 강화학습 기법에 관련하여 공동 연구 수행 계획을 가지고 있음 ✓ 이형준 교수 텁 지도학생과 면담을 통해 개별 연구주제 및 내용에 대해 피드백을 주고받았으며, 이를 대학원생 교류로 확장할 기반을 마련함 ◆ 세미나 진행 ✓ 2024년 7월 Ewha Fellow 자격으로 이화여대를 방문하여 석학 초빙 세미나를 진행하였음 ✓ 강화학습에 필요한 효율적인 의사결정 방식에 대해 발표하였고, 많은 연구진들의 참석으로 연구협력 방안을 논의하게 되었음	2024
황의원	Aviral Shrivastava	Arizona State University (미국)	◆ 공동연구 수행 ✓ 소프트오류가 존재하는 환경에서 out-of-distribution을 탐지하는 딥러닝 기술에 대한 공동연구를 수행함 ✓ 매주 1회 온라인 미팅을 통해 공동연구 아이디어를 도출하고 실험 설계 및 추진 방안을 논의함 ✓ 연구성과가 BK21 CS분야 우수학술대회인 CODES+ISSS 2025에 게재 승인됨 ✓ 향후 실제계에서 발견한 Edge AI 연구로 확장할 수 있음	2023~2025
	Tom Yeh	University of Colorado Boulder (미국)	◆ 세미나 진행 ✓ 2023년 7월 26일에 fNIRS를 사용한 연구 방법을 주제로 세미나를 개최함 ✓ fNIRS를 위한 Preprocessing, task design and application, data processing using Nirs Toolbox에 대해 강연함 ✓ 세미나 후 뇌파 기반의 감정 인식 및 감정 기반 지능형 인터페이스 설계 연구와 관련된 연구협력 방안을 논의함	2023
	Augusto Esteves	Instituto Superior Técnico (포르투갈)	◆ 공동연구 수행 ✓ 매주 1회 온라인 미팅을 통해 사용자의 터치스크린 입력에 대한 수학적 모델을 기반으로 난독증을 진단하는 예측모델에 대한 공동연구를 진행함 ✓ 공동연구 성과가 Springer Lecture Notes in Computer Science에 게재됨 ✓ 향후 사용자 맞춤형 스마트 인터랙션 연구로 확장할 수 있음	2020
오유란	João Guerriero	University of Lisbon (포르투갈)	◆ 공동연구 수행 ✓ 매주 1회 온라인 미팅을 통해 가상현실에서의 동적/정적 객체의 움직임에 대한 정보 전달용 맞춤형 비시각 피드백 공동연구를 진행함 ✓ 공동연구 성과가 IEEE Transactions on Visualization and Computer Graphics에 게재됨 (IF=6.5) ✓ 향후 사용자 맞춤형 피드백 모달리티 증강 및 화장 연구로 확장할 수 있음	2023
	Dragan Ahmetovic	University of Milan (이탈리아)	◆ 공동연구 수행 ✓ 매주 1회 온라인 미팅을 통해 SLAM 기반의 3차원 객체 스캐닝을 위한 비시각적 피드백 연구를 진행함 ✓ 공동연구 성과가 BK21 CS분야 최우수 학술대회인 CHI 2020에 게재됨 ✓ 향후 3차원 공간상의 초경량 실시간 hand guidance 연구로 확장할 수 있음 ◆ 워크샵 공동 개최 ✓ 2021 IEEE International Conference on Pervasive Computing and Communications (PerCom)에 워크샵 공동 개최 ✓ 2021년 3월 22일 MPAT (Mobile and Pervasive Assistive Technologies)를 주제로 워크샵 진행	2021
	Gary Hsieh	University of Washington (미국)	◆ 공동연구 수행 ✓ 주 1회 온라인 미팅을 통해 대화 기반의 거대 언어 모델의 폐르소나 설정에 따른 사용자 경험에 대한 연구를 진행함 (현재 논문 심사중) ✓ 향후 개인화된 LLM 에이전트 설계 최적화에 대한 연구로 확장할 수 있음	2023

4.1.3 외국 연구소 및 대학과의 인적 교류 계획

- 외국 연구소 및 대학과의 인적 교류를 활성화하기 위한 구체적인 참여교수별 계획은 표 2-f와 같음

표 2-f. 외국 연구소 및 대학과의 인적 교류 계획

담당교수명	인적 교류 계획
양대현	✓ Wayne State University의 장룡호 교수와의 공동 워크샵 개최 예정
김종길	✓ Yong Yu 교수 연구진이 (중국, Shaanxi Normal University, China) Trustworthiness on AI and Blockchain을 주제로 인력 교류를 포함한 공동 연구 수행을 위한 MOU 체결
배호	✓ 미국 Arizona State University의 안길준 교수와의 협력과제를 통해 지속적인 협력연구 및 인적 교류를 수행할 계획임 (2024.07 ~ 2026.12)
민동보	<ul style="list-style-type: none"> ✓ Prof. Kwang Moo Yi(UBC, 캐나다)와 생성형 AI 모델 관련 공동연구를 위해 본교 대학원생의 방문연구를 수행할 예정임 ✓ Prof. Changjae Oh(Queen Mary University of London, 영국)와 Robitics 관련 공동연구 수행을 위해 2025년에 온라인 연구미팅을 진행하고, 연구가 심화되면 단기 방문을 통한 대학원생 교류를 추진할 예정임 ✓ Prof. Hansung Kim(University of Southampton, 영국)와 3차원 비전 분야의 공동연구 수행을 위해 2026년에 온라인 연구미팅을 진행하고, 초기 결과를 바탕으로 심도 있는 연구를 위해 대학원생의 단기 방문을 추진할 예정임
반효경	✓ University of Michigan의 Kang Shin 석좌교수 Ewha Global Fellow 재선정(2024-2026) 및 본교 임베디드SW센터와 미시간대 RTCL과의 교류 지속
윤명국	✓ UC Merced의 Hyeran Jeon 교수와 LLM에 최적화 UVM 기술 개발 국제공동연구 계획 및 대학원생 교류 계획
이지영	<ul style="list-style-type: none"> ✓ 싱가포르 NTU의 Anupam Chattopadhyay 교수와 멀티모달 기반 가짜 영상 탐지 모델 개발 공동연구를 수행할 계획임 ✓ 호주 UNSW의 Hamid Alinejad-Rokny 교수와 멀티모달 바이오 LLM 효율적 학습 방법에 대한 공동연구를 수행할 계획임 ✓ 미국 CMU의 Jun-Yan Zhu 교수와 사용자 맞춤형 멀티모달 생성 모델 개발 국제 공동 연구 계획 ✓ 미국 Google의 Dr. Daniel McDuff와 효율적 MLLM 인과추론 네트워크 학습 방법 개발 국제공동연구 계획 및 대학원생 교류 계획 ✓ 미국 Adobe의 Dr. Justin Salamon과 오디오비주얼 모델 경량화 기술 개발 국제공동연구 계획 및 대학원생 교류 계획
이형준	<ul style="list-style-type: none"> ✓ Ji, Bo 교수(미국 Virginia Tech)가 2024년 본교 방문 및 세미나 진행 이후 지속적인 교류협력을 통해서 공동 연구 및 대학원생 교류 노력을 이어가고 있음 ✓ IEEE Indonesia 지부에서 ‘Introduction to Federated Learning’이라는 주제로 Webinar 진행 (2025년 6월) 후 Indonesia 여러 대학들과 교류 계획 ✓ Wonjae Lee 교수(미국 Duke University)가 2026년 Duke University 방문 계획을 통해 국제 공동 연구 및 대학원생 교류 계획
황의원	✓ 미국 Arizona State University와의 Trustworthy AI를 주제로 공동연구 수행을 위해 월 1회 이상 온라인 연구미팅을 진행하고, 단기방문을 통한 대학원생 교류를 추진할 계획임
오유란	<ul style="list-style-type: none"> ✓ 미국 University of Colorado Boulder의 Tom Yeh 교수와의 협력 과제를 통해 공동연구 및 인적 교류 수행 예정 ✓ 이탈리아 University of Milan의 Dragan Ahmetovic 교수 본교 방문연구 계획

4.2 대학원생 국제공동연구 계획

○ 대학원생 국제공동연구 추진전략 (그림 2-11 참조)



<그림 2-11> 대학원생 국제공동연구 추진전략

◆ 추진전략 1. 국제공동연구 주제 발굴 및 협력 기반 구축

- ✓ 본 교육연구단의 주제에 알맞은 고효율 AI, 고신뢰 AI를 중심으로, 로보틱스, 바이오 AI 등 융합기술 분야까지 확장하여 상호 관심사에 기반한 공동연구 주제를 기획함
- ✓ 공동연구를 위한 컨택, 세미나, 온라인 미팅 등을 통해 연구 방향성과 협업 가능성을 사전 조율함
- ✓ 장기적 협력을 위한 MOU 체결 등을 통해 대학원생 교류와 과제 연계 가능성을 제도적으로 확보하고, 이를 토대로 자연스럽게 대학원생의 국제공동연구로 확장함

◆ 추진전략 2. 방문연구 및 현지 협력 강화

- ✓ 연구 주제에 따라 2~3개월 단위의 방문연구를 추진하여, 대학원생이 직접 해외 현지 연구실의 교수 및 대학원생들과 공동으로 실험 및 프로토타이핑을 수행할 수 있도록 필요한 경비를 지원함
- ✓ 방문연구는 연구성과 도출을 목표로 하여, 현지 전문가로부터 밀도 높은 멘토링을 받도록 함
- ✓ 복수의 대학원생이 순차적으로 방문하거나, 특정 기간 동안 팀 단위로 협업을 수행하기도 함

◆ 추진전략 3. 정기적 교류 프로그램 운영 및 공동연구 성과 창출

- ✓ 연구 성과 공유를 위한 온라인 세미나, 워크숍 등을 정례적으로 개최하여 양 연구실 간의 소통을 유지하고, 연구 아이디어의 발전을 도모함
- ✓ 현지 방문 이전 및 이후에 상호 방문 세미나 또는 발표회를 통해 연구의 맥락을 깊이있게 공유하고, 공동연구로 연결될 수 있도록 유도함
- ✓ 공동연구 결과는 top-tier 국제학술대회 및 최고권위지를 중심으로 한 논문 발표를 목표로 하며, 필요시 해외 학회 발표 및 출장 경비를 지원함

◆ 추진전략 4. 대학원생의 글로벌 연구역량 강화와 연구실 내 확산

- ✓ 해외 방문을 통해 확보한 기술과 경험을 귀국 후 세미나, 논문 스터디, 후속 프로젝트 제안 등으로 환류되어 교육연구단 전체의 수준 향상에 기여함
- ✓ 공동연구에 참여한 대학원생은 후속 참여자에게 노하우를 전수할 수 있도록 연락 시스템을 구축하고, 국제 협력의 경험을 기반으로 학위논문 작성과 취업 시 경쟁력을 갖추도록 함
- ✓ 대학원생 주도의 글로벌 프로젝트 기획, 공동 논문 저술, 공동 특허출원 등의 성과 창출을 장려함

○ 대학원생의 해외 연구실 공동연구 및 장·단기 연수를 위한 구체적인 참여교수별 계획 (표 2-g 참조)

<표 2-g> 대학원생 국제공동연구 계획

담당교수명	국제공동연구 계획
양대현	<ul style="list-style-type: none"> ✓ 지도학생인 김시안(Sian Kim) 박사과정이 Rhongho Jang (USA/Wayne State University)와 공동연구 수행 예정 ✓ Top-Tier 학회를 목표로, In-network AI-based self-driving router 설계를 위해, AI 모델에게 실시간 트래픽 특징을 추출하여 제공해주는 feature extractor의 연구/개발 진행 중 ✓ 현재 공동 연구 진행중인 Wayne State University의 장룡호 교수와의 협업을 위하여, 한 달 가량 Wayne State University를 방문하여 연구 아이디어와 진행 방향에 대해 논의하는 워크샵을 개최할 계획임
김종길	<ul style="list-style-type: none"> ✓ 한중협력 연구사업(한국연구재단)의 일환으로 중국 산시성(Shaanxi) Shaanxi Normal University의 Prof. Yong Yu와의 협력연구를 진행 계획 (2023.08 ~ 2025.07) ✓ 해당 과제는 두 연구실 간의 활발한 연구교류를 목적으로 하고 있으며, 김종길 교수와 지도학생은 과제 기간 (2023.08 ~ 2025.07) 중 4회 중국 Shaanxi Normal University를 방문하였으며 하며 상호연구 결과를 논의하고, 연구를 진행하였음 ✓ 해당 과제 종료 후에도 지속적인 공동 협력 연구를 위해 “Trustworthiness on AI and Blockchain”이라는 주제의 MOU를 통해 향후 2년간 학생 교류를 포함한 공동 연구를 진행 하기로 협의함
배호	<ul style="list-style-type: none"> ✓ 정보보호 핵심원천기술개발사업(정보통신기획평가원)의 일환으로 미국 Arizona State University의 안길준 교수와의 협력연구를 진행 계획 (2024.07 ~ 2026.12) ✓ 해당 과제는 AI 기반 자동화된 취약점 탐지 및 안전한 코드 생성 기술 개발을 목적으로, 국내-해외 공동 연구개발을 수행하고자 함 ✓ 현재 공동 연구 진행 중인 안길준 교수는 ASU의 CTF(Center for Cybersecurity and Trusted Foundations)의 설립 이사 겸 책임 자문을 맡고 있으며 해당 기관은 미국과 세계가 직면한 사이버 보안 문제를 다루기 위해 설립된 기관으로, ASU를 중심으로 한 글로벌 연구 네트워크에 접근하여 다양한 국제 협력을 도모할 계획임
오세은	<ul style="list-style-type: none"> ✓ 미국 Rochester Institute of Technology의 Matthew Wright 교수와 Genuine Tor 트래픽 수집 및 종단간 상관관계 분석을 위한 국제공동연구를 수행할 예정임 ✓ 글로벌기초연구실(한국연구재단)과 연계하여 RIT와 이화여대 연구실 간 대학원생 상호 방문연구를 추진할 계획임
오세은	<ul style="list-style-type: none"> ✓ 미국 University of Texas at El Paso의 Mohammad Saidur Rahman 교수와 평생 학습 기반 멀웨어 분석을 위한 국제공동연구를 수행할 예정임 ✓ 지도학생인 홍세연, 박정민, 전혜승 학생이 3개월간 UTEP에 방문하여 방문연구를 진행 ✓ 이외에도 참여 대학원생들이 코드 생성 방법론, 보안 네트워크 트래픽 분석 등

	보안 인공지능을 위한 다양한 국제 연구협력과 교류를 추진할 예정임
오세은	<ul style="list-style-type: none"> ✓ 영국 University of Edinburgh의 Prof. Marc Juarez 교수와 Genuine Tor 트래픽 수집 및 종단간 상관관계 분석을 위한 국제공동연구를 수행할 예정임 ✓ 글로벌기초연구실(한국연구재단)과 연계하여 Univ. of Edinburgh와 이화여대 연구실 간 대학원생 상호 방문연구를 추진할 계획임
민동보	<ul style="list-style-type: none"> ✓ 영국 Queen Mary University of London의 Changjae Oh 교수와 Vision-Language-Action(VLA) 기반 로봇 제어를 위한 국제공동연구를 수행할 예정임 ✓ 특히, VLA 기반 로봇 제어를 시뮬레이션을 통해 검증한 이후, 실세계 로봇을 이용한 실증을 위해 해당 분야 전문가인 Prof. Changjae Oh와의 공동연구를 수행하려고 함 ✓ 이를 위해 Prof. Changjae Oh의 협력 하에 대학원생 단기 방문연구(2-3개월)을 여러 차례 추진할 예정임
민동보	<ul style="list-style-type: none"> ✓ 영국 University of Southampton의 Hansung Kim 교수와 멀티모달 센서를 이용한 3차원 비전 분야의 공동연구 수행할 예정임 ✓ 멀티모달 센서를 동시에 활용한 AI 모델을 개발하고, 이를 실세계 환경에서 검증하는 작업을 위해 해당 분야 전문가인 Prof. Hansung Kim과의 공동연구를 수행하려고 함 ✓ 이를 위해 Prof. Hansung Kim의 협력 하에 대학원생 단기 방문연구(2-3개월)을 여러 차례 추진할 예정임
이지영	<ul style="list-style-type: none"> ✓ 싱가포르 Nanyang Technological University의 Anupam Chattopadhyay 교수와 Deepfake 탐지를 위한 멀티모달 모델 공동연구를 진행할 계획임 ✓ 각각의 전문성 (NTU-deepfake detection, 이화여대 Multimodal AI Lab - audiovisual fusion)을 바탕으로 국내-해외 공동 과제 수주도 추진하려함 ✓ 또한 Anupam Chattopadhyay 교수와 협력 하에 서로간의 기관에 단기 방문연구를 추진하여 오프라인 협력도 도모할 계획임
이지영	<ul style="list-style-type: none"> ✓ 호주 UNSW의 Hamid Alinejad-Rokny 교수와 멀티모달(심전도, 자연어) 기반 LLM 학습에 관한 공동연구를 진행할 계획임 ✓ 이를 통해 심장질환을 예방하는 바이오 LLM 모델을 구축하고, 관련된 국내-해외 공동 과제 수주도 추진하려함 ✓ 또한 Hamid 교수와 협력 하에 단기 방문연구 및 워크샵 공동개최등 지속적인 연구교류를 도모할 계획임
황의원	<ul style="list-style-type: none"> ✓ 미국 Arizona State University의 Aviral Shrivastava 교수와 Trustworthy AI 및 Efficient AI 분야에서 공동연구를 지속할 예정이며, 본교 대학원생이 이에 참여하여 공동연구 수행과 국제적 연구역량 강화를 동시에 도모하고자 함 ✓ 특히, Trustworthy AI 연구를 확장하여 Shrivastava 교수 연구실과 본교 대학원생이 공동으로 적대적 공격뿐만 아니라 out-of-distribution 데이터에 대해서도 강건하게 탐지할 수 있는 기법을 개발할 계획임 ✓ 이를 위해 Shrivastava 교수 연구실의 협력 하에 본교 대학원생이 ASU에 2-3개 월간 단기 방문하여 현지 교수 및 대학원생과 국제공동연구를 추진할 예정임

III. 연구역량 영역

※ 연구역량 영역부문의 항목은 기본적으로 교육연구단을 기준으로 작성하며, 세부 항목별로 특정기준이 제시된 경우 이에 준하여 신청서를 작성

III. 연구역량 영역

III. 연구역량 영역

1. 참여교수 연구역량

1.1 중앙정부 및 해외기관 연구비

1.2 연구업적물

③ 연구의 수월성을 대표하는 연구업적물 (최근 10년)

<표 3-4> 최근 10년간 참여교수의 인공지능 분야 대표연구업적물

연번	대표연구업적물 설명
1	<p>□ 논문제목: A Scalable and Dynamic ACL System for In-Network Defense</p> <ul style="list-style-type: none"> • 참여교수: 양대현 교수 (교신저자) • 학술대회명/게재년: ACM Conference on Computer and Communications Security (ACM CCS), 2022년 <p>□ 연구업적물의 우수성</p> <ul style="list-style-type: none"> • BK21 우수국제학술대회 목록에 IF=4로 지정된 사이버 보안 분야 Top-tier 학술대회인 CCS에 발표되었음 • 2025년 7월 현재 Google Scholar 기준 21회 인용되었음 <p>□ 연구 요약</p> <ul style="list-style-type: none"> • AI 모델을 활용하여 보안 정책을 자동 생성하고 네트워크 환경 변화에 따라 실시간으로 적용 가능함. • 프로그래머블 스위치를 활용하여 실시간으로 트래픽 특징을 추출하고 보안 기능을 수행. • 네트워크 트래픽 증가에 따라 ACL 정책 규모가 커지고 있는 상황에서, TCAM 사용량을 줄이면서도 고성능 필터링을 유지하는 설계를 제안함. • 정적 ACL의 한계를 극복하고, 상황 기반 동적 ACL을 통해 자율적이고 유연한 네트워크 방어를 구현함. <p>그림. 제안하는 보안 프레임워크 개요</p> <ul style="list-style-type: none"> • 다양한 트래픽 조건 및 위협 환경에서도 안정적인 동작을 보이며, 대규모 네트워크 환경에 적합한 확장성과 자원 효율성을 실현. <p>□ 본 교육연구팀 비전, 목표와의 연관성</p>

- 네트워크를 통한 공격을 사전에 탐지하고 차단할 수 있는 자율적 방어 시스템을 제안하여 사용자 데이터 보호와 프라이버시 향상에 기여함.
- 트래픽 상황에 따라 자동으로 보안 정책을 조정하는 구조는 향후 AI 기반 보안 자동화 및 실시간 대응 기술 개발의 기반이 될 수 있음.
- 보안이라는 특수 도메인에 국한되지 않고, AI가 복잡한 제약 조건과 실시간 처리 요구를 동반하는 다양한 시스템 환경에 적용될 수 있는 가능성을 제시함.

□ 논문제목: KNN Local Attention for Image Restoration

- 참여교수: 민동보 교수 (교신저자)
- 학술대회명/게재년: IEEE Computer Vision and Pattern Recognition (CVPR), 2022년

□ 연구업적물의 우수성

- BK21 우수국제학술대회 목록 IF=4로 지정된 컴퓨터비전 분야 Top-tier 학술대회인 CVPR에 발표되었음.
- 2025년 7월 현재 Google Scholar 기준 78회 인용되었음.

□ 연구 요약

- 전역적 주목 작업을 CNN 또는 Transformer와 통합하려는 시도들이 영상 복원 작업에서 놀라운 성능을 달성함.
- 그림 (a)와 같이 전역적 유사성은 지역성이 부족하고 계산 복잡도가 높다는 문제가 있으며, 그림 (b)의 국부적 주목 메커니즘은 컨볼루션과 유사한 연산자를 사용하여 국부성의 귀납적 편향을 도입함으로써 이러한 문제를 완화할 수 있음.

2

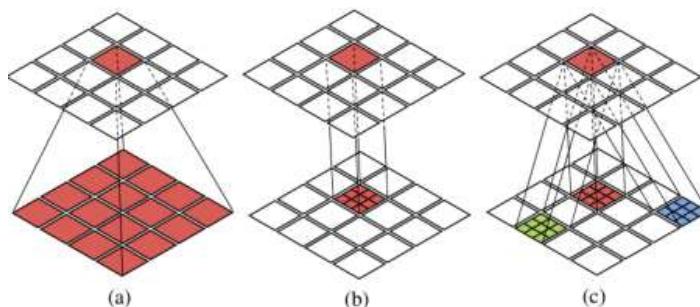


그림. 제안하는 k-NN 주목 메커니즘과 기존 기술 비교

- 그러나 인접한 위치에만 초점을 맞추면 영상 복원을 위한 수용 영역이 부족하여 성능 개선에 한계가 있으며, 본 논문에서는 이러한 한계를 해결하는 k-NN Image Transformer(KiT)라는 영상 복원을 위한 새로운 주목 메커니즘을 그림 (c)와 같이 제안함.
- 아래 그림과 같이 k개의 유사한 패치를 탐색한 후, 쌍별 국부 주목 메커니즘을 유사한 패치에만 적용함으로서 낮은 복잡도를 유지하면서도 영상 전체 영역을 수용 영역으로 고려할 수 있음.

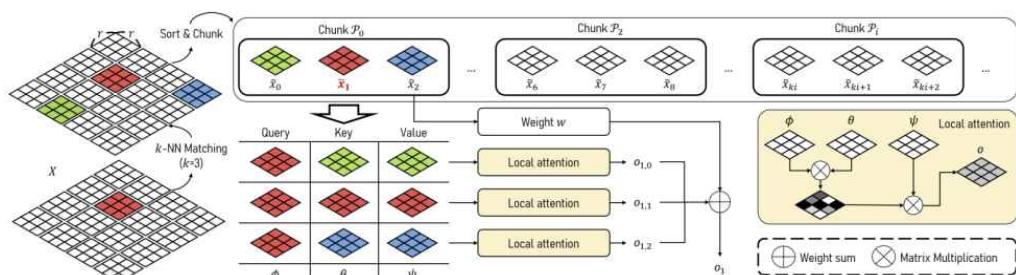


그림. 제안하는 k-NN Image Transformer 프레임워크

- 제안 방법은 영상 노이즈 제거, 디블러링 및 디레이닝 벤치마크에 대한 최신 복원 방식보다 높은 성능을 도출함.

본 교육연구팀 비전, 목표와의 연관성

- 제안한 새로운 Attention 매커니즘은 k-NN 연산을 접목하여 Transformer의 높은 계산복잡도를 크게 감소시키며, 이는 거대 모델의 효율적인 학습에 핵심 기술로 사용될 수 있음.

논문제목: Warped-Compaction: Maximizing GPU Register File Bandwidth Utilization via Operand Compaction

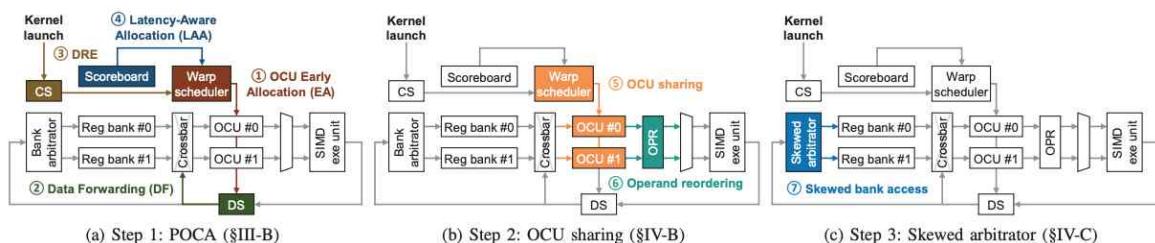
- 참여교수: 윤명국 교수 (교신저자)
- 학술대회명/개재년: The 31st International IEEE Symposium on High Performance Computer Architecture (HPCA), 2025년

연구업적물의 우수성

- BK21 우수국제학술대회 목록에 IF=4로 지정된 컴퓨터 구조 분야 Top-tier 학술대회인 HPCA에 2025년 발표되었음
- 미국 University of Illinois Urbana-Champaign의 Nam Sung Kim 교수, 연세대학교 정이품교수와 국제공동연구한 성과

연구 요약

- AI 모델의 대규모 병렬 연산 처리에 필수적인 GPU는 연산자 공급을 위한 대용량 레지스터 파일(RF)을 필요로 함.
- 최신 GPU는 RF 뱅크 수가 제한적이며, 단순한 뱅크 분배 방식에 의해 RF 대역폭의 약 3분의 1이 비활성 상태로 낭비되고 있음.
- 기존 제안된 기법은 RF 접근 수를 줄이는 데 효과적이나, 남은 대역폭을 적극적으로 활용하지 못함.
- 제안된 Warped-Compaction 아키텍처는 하드웨어 비용 증가 없이 RF 대역폭 활용도를 높이며, 기존 대비 성능과 에너지 효율 모두 우수한 개선 효과를 보임.



그럼. 제안하는 Warped-Compaction 아키텍처 개요

본 교육연구팀 비전, 목표와의 연관성

- AI 모델 학습 및 추론에서 요구되는 고성능·저전력 연산 환경을 실현하는 데 기여할 수 있는 GPU 마이크로아키텍처 수준의 해결책을 제시함.

1.3 교육연구단의 연구역량 향상 계획

1.3.1 대표연구업적물의 질적 우수성 향상 방안

◆ 목표: 교수 1인당 피인용지수 향상

- ✓ Times Higher Education(THE) 세계대학평가의 핵심 지표 중 하나인 '연구 영향력(Research Influence)' 항목은 논문 평균 피인용 수(Citation Impact)를 기준으로 산출되며, 이는 곧 질적으로 우수한 연구성과의 계제율과 직접적으로 연관되어 있음.
- ✓ 단순한 논문 수가 아닌, 국제적으로 주목 받는 고임팩트 논문 발표가 연구경쟁력의 핵심이 됨.
- ✓ 탑티어 논문 다수 배출 → 우수 학생의 관심과 지원 유도 → 유능한 학생 선발 → 다시 우수한 연구성과 창출로 이어지는 선순환 구조.
- ✓ 특히 AI 분야는 "학생=공동연구자"이므로 고임팩트 논문 생산 과정 자체가 학생 교육의 핵심 커리큘럼역할 수행.
- ✓ 이에 따라 본 사업단은 참여 교수들의 국제적 학술 영향력 제고 및 질적 연구성과 창출을 위한 표 3-a와 같은 목표와 추진계획을 수립하며, 본 사업 참여기간을 넘어 장기적인 5년 목표를 통해 인공지능소프트웨어학부 연구업적물의 우수한 질적 성장을 도모함.

<표 3-a> 연구업적물 질적 우수성 향상 정량적 장기 목표 (기준: Google Scholar)

항목	2020-2025 (최근 5년)	연도별목표				
		2026 (BK21 1차년도)	2027 (BK21 2차년도)	2028	2029	2030
최근 5년 논문 1편당 환산보정 피인용지수	37.7	41.5	45.6	50.2	55.2	60.8
최근 5년 사업단 참여교수 1인당 환산보정 피인용지수	1055.8	1161.4	1277.5	1405.3	1545.8	1700.4
H-index 20 이상 사업단 참여교수 수	33%	38%	45%	-	-	-
H-index 15 이상 사업단 참여교수(신임) 수	40%	47%	55%	-	-	-

*참여교수 수 = N

$$\text{*논문 1편당 환산보정 피인용지수} = \left(\sum_{n=1}^N (\text{교수별 피인용지수}/\text{교수별 논문편수}) \right) / N$$

$$\text{*참여교수 1인당 환산보정 피인용지수} = \left(\sum_{n=1}^N \text{교수별 피인용지수} \right) / N$$

◆ 추진전략 1. 세계 최상위 학술대회 중심 연구성과 기획 및 투고 지원

- ✓ 급변하는 컴퓨터공학 및 인공지능 분야의 특성 상, 영향력 있는 우수한 연구 결과 도출을 위하여 세계 최상위 학술대회에서의 논문 발표 실적을 양적, 질적 향상 시키는 것을 목표로 함.
- ✓ 질적 우수성 향상을 위하여 논문 인용지수를 성과에 반영 및 출업 요건 반영 내규 개편 계획.
- ✓ 연구논문 작성법 및 연구 윤리에 대한 세미나 정기 운영 (1학기 중 1회).
- ✓ AI 대학원 학생들이 국내외 학회 발표, 산학연 협력 발표, 세미나 등에 자신있게 참여할 수 있도록

록 발표력 향상을 위한 실질적인 훈련과 피드백을 제공하는 발표 클리닉 프로그램 운영.



<그림 3-1> 각 세부연구 분야별 연구 목표 및 목표 최우수(Top-tier) 국제 학술대회

◆ 추진전략 2. 내부 공동 연구 및 상호 피드백 시스템 구축

- ✓ 최우수학회 제출 2주 전 관련연구자 단체 리뷰세션을 진행하여, 연구의 완성도와 깊이를 향상시킴.
- ✓ 사업단 내 교수간 공동 연구 시스템을 강화하며, 공동 코드/데이터베이스/GPU 자원 공유 플랫폼을 구축 및 활성화 (세부 계획 1.3.3 참조)
- ✓ 세부 관심 연구주제에 대하여 융합 연구 성과 창출을 위하여 지속적으로 관심 연구분야를 공유 하며, 최신 연구 동향을 공부하는 저널/리서치 클럽을 운영할 예정.
- ✓ 특히, 신진 연구자(신임교원, 박사후연구원, 박사과정생)를 대상으로 한 고품질 연구 설계 멘토링 체계화를 통해 전반적인 업적 수준을 균질하게 끌어올릴 예정.

◆ 추진전략 3. 국내외 공동연구 및 인적교류 지원 시스템 강화

- ✓ AI 분야는 기술 발전 속도가 매우 빠르고 글로벌 연구 경쟁이 치열하기 때문에, 국제 공동연구를 통해 최신 연구 동향을 빠르게 반영하고, 차별화된 공동성과를 창출하는 것이 필수적임.
- ✓ Horizon Europe, NSF 등 국제 다기관 공동 과제 수주 및 컨소시엄 참여 또한 목표로 함.
- ✓ 국내외 석학, 우수 연구자 및 산업체 인사 초청 세미나를 매년 10회 이상 개최하고, 교수들에게는 외부 연구자들과의 교류 및 공동연구를 위한 출발점으로 활용.
- ✓ 국제 유명 석학 초청시, 내부 심사를 통해 비행기, 숙소, 경비를 사업단 예산으로 적극 지원.
- ✓ 영문 이력서 및 연구계획서 작성 세미나 정기 운영.
- ✓ 원활한 원격 협업을 위하여 협업 툴 (GitHub, HuggingFace, WandB, DVC 등) 교육 세미나 진행.
- ✓ EWHA G-AI Research (교환연구원) 프로그램을 신설하며, 표3-b의 연구성과평가위원회의 평가기준을 통해 매학기 일정 인원 선발 및 해외 공동연구 경비 (비행기, 숙소, 경비) 차등 제공.

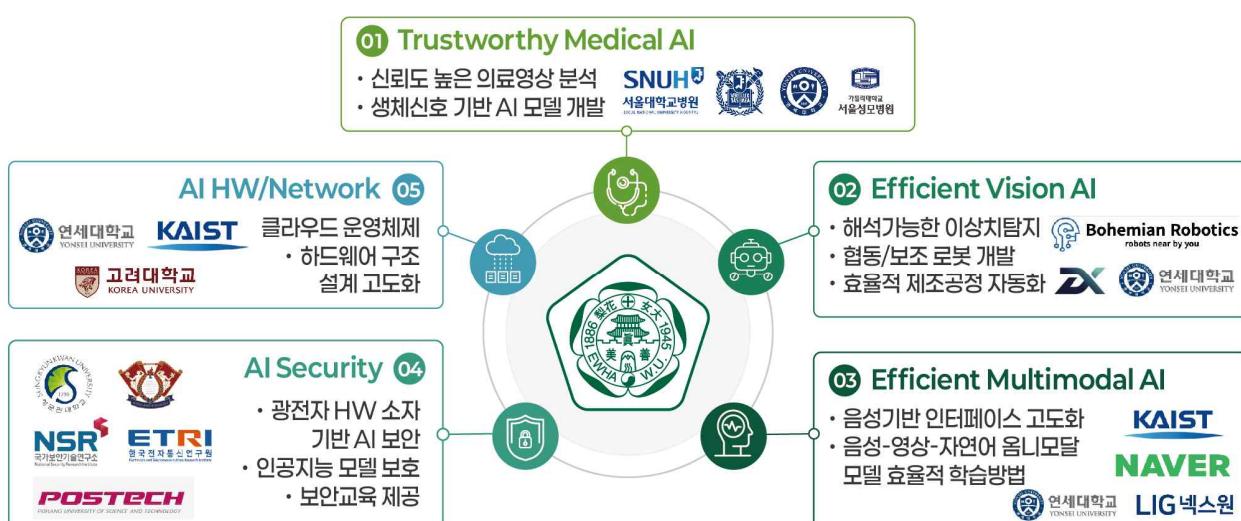
<표 3-b> EWHA G-AI Research 프로그램 선별평가 기준

평가항목	세부내용	배점
연구의 창의성	기존 연구들과 비교하여 연구의 주제 및 접근방법이 얼마나 창의적인가?	25
연구의 필요성	연구의 필요성 및 중요성이 잘 기술되었는가?	25
연구계획의 구체성 및 적합성	연구 계획이 구체적으로 서술이 되어있고 일정 내 구현가능한가?	25
연구성과의 활용 및 기대효과	연구목적이 달성될 경우 AI 관련 분야의 발전에 학문적/기술적으로 얼마나 영향을 미칠 것인가?	25

◆ 추진전략 4. 연구 성과 평가위원회 구성 및 우수 연구자 보상 강화

- ✓ 연구성과 평가위원회는 논문, 특히, 기술이전 등 1년 동안 진행한 연구 결과물을 평가 하며, 참여 교수진, 산학 전문가, 글로벌 협력 자문위원 등으로 구성.
- ✓ 특히, 양적 성장 뿐 아니라 질적 수준 향상(인용지수, 오픈소스 공개 및 홍보, 연구의 창의성과 필요성, 학술활동, 산학협력 등)을 평가하여 결과에 따른 장학금 계상 및 지급.
- ✓ 고성과 연구자에게 주요 AI 분야 최우수 학술대회 (ICML, ICLR, KDD, ICDM, CVPR, ICCV, NeurIPS, AAAI, EMNLP, HPCA, ISCA, CCS, NDSS 등) 등록비, 출장비, 논문발표지원을 우선 제공하며, 학술대회 참석 후 최근 기술동향에 대한 Wrap-up 발표를 진행.
- ✓ 매년 평가위원회는 우수 연구학생을 예산 내 정원으로 선발하여, 해외 학회 동행 기회 또는 국제 공동연구 파견 추천등의 특전 부여.
- ✓ 연 1회 ‘사업단 연구우수팀’ 선정 및 홈페이지, 뉴스레터 홍보 및 시상을 통해 공식 업적 인증.
- ✓ 성과에 따라 RA/TA 인건비 지원 규모 차등화.
- ✓ 우수연구자에게 학생 지원 배정 우선권, 외부연구원 채용 시 우선 추천권, 공동지도 인정 부여.

1.3.2 국내 공동연구 협력 체계



<그림 3-2> 각 세부연구 분야별 국내 공동연구 협력목표 및 협력기관

◆ 전문 분야 기반 공동연구 협력

- ✓ 사업단에 참여하는 교수진의 연구 전문 분야(예: 멀티모달 AI, 의료 AI, AI 하드웨어, AI 보안, AI 시스템/네트워크 등)에 따라 관련 역량을 보유한 국내 대학, 정부출연연구기관, 병원, 산업체와 공동연구 추진.
 - ✓ 정부 주관의 대형 R&D 사업(예: NRF, IITP, 보건의료연구원 등)에 공동 참여할 수 있는 다기관 컨소시엄을 구성하는 등, 참여 교수들이 실질적인 연구 협력 체계를 적극적으로 구축.
 - ✓ 원활한 컨소시엄 구성 및 대형 R&D 수주 지원을 위하여 준비에 필요한 경비(씨드머니)를 교내 재원으로 부담 예정이며, 연구비 규모에 따라 차등 지급.
- ◆ 교육 연계 협력 및 학생 교류

- ✓ 협력기관과의 공동 교육 프로그램(예: 여름학교, 학점교류, 공동강의, 공동지도 석박사 프로그램)을 운영하고, 연구단 소속 학생들이 타 기관의 프로젝트에 참여할 수 있도록 인턴십, 단기 파견 등 인재 교류도 함께 추진함.
- ✓ 예: KIST와 이화여자대학교는 2025년 7월 14일 연구협력 및 인재양성을 위한 MoU 체결 (그림 3-3 참조). 특히, AI·로봇 분야 협력을 약속하며, 공동 학생지도과정과 임무중심 공동연구 체계 구축 중.



<그림 3-3> KIST (한국과학기술연구원) - 이화여자대학교 업무협약 체결식

◆ 정기적 연구교류 및 공동세미나 개최

- ✓ 국내 협력기관과 분기별 정기 워크숍 및 기술세미나를 개최를 연 2회 이상을 목표로 하여 연구 진간 기술 공유 및 협력 방향 논의를 정례화하며, 공동 성과 도출로 이어질 수 있도록 지원함.

1.3.3 내부 공동연구 협력 체계 강화

코드/데이터/실험환경 공유를 통한 Ewha TRUE-AI Open Lab

코드 공유 체계 운영	데이터 공유 및 공동 구축 체계	공동 실험 환경 운영
공동 GitHub Repository 운영을 통한 코드베이스 공유	데이터 수집 계획 공유 및 증복수집 최소화	공유 GPU 서버 운영 (현재 A6000 8대 서버 x 15대 운영)
공동 HuggingFace Repository 운영을 통한 성과 공유 및 홍보	메타정보(수집 조건, 정제 방식, 활용 예시 등)를 함께 관리	공동 실험실 (Open Lab) 공간 지원

<그림 3-4> 내부 협력 체계 운영 계획

◆ 코드 공유 체계 운영을 통한 기본 연구역량 향상 및 외부 성과 홍보

- ✓ GitHub 레포지토리를 통한 코드베이스들을 내부적으로 공유하여, 융합 연구의 효율성 향상 목표.
- ✓ 사업단 공동 HuggingFace 레포지토리 운영을 통한 오픈소스 공개 및 성과 홍보.
- ✓ 연구의 실용성/응용성을 높여 연구의 질적 향상 도모.

◆ 학습 데이터셋 및 평가 벤치마크 공유를 통한 연구체계 구축

- ✓ 고품질 학습데이터 대규모 확보는 AI 연구의 확장성과 효율성을 높이는 데 필수적임에도 불구하고, 각 연구실별로 독립적인 서버에 확보하며 불필요한 메모리 낭비가 심함.
- ✓ 인공지능 학습 데이터셋을 공유하는 플랫폼을 사용하여, 데이터 중복 수집을 줄이고, 연구 효율성을 극대화하며 이를 통한 연구 준비 시간 단축 및 새로운 연구 주제 접근성 향상 기대.

◆ 공동 실험환경 공유를 통한 대학원생 연구역량 향상

- ✓ 내부 자원의 경계 없는 개방과 활용을 통해, 참여 교수 간 실시간 연구 공유 및 문제 해결이 가능한 협력적 연구 생태계를 구축하도록 공유 GPU 클러스터를 운영 (2025년 7월 기준 A6000x8 15 대 운영 중)하고 있으며, 공동 과제 수주를 통해 추가 확보할 계획.
- ✓ 공동 실험실 (오픈랩) 운영을 통해 연구자들이 자율적으로 모이고 문제 중심의 융합연구를 실현 할 수 있는 환경을 제공하는 것을 목표로, 현재 ECC B220-1/2 호실에서 운영 중인 오픈랩 공간을 사업단에서 추가 확보할 계획임.
- ✓ 정기적인 연구 콜로퀴엄 운영(연 2회)과 리서치클럽, 저널클럽 등을 통해 세부 관심주제에 따른 새로운 마이크로공동연구팀을 결성하고, 이를 통한 연구 성과에 대해서는 별도의 포상을 제공함.

1.3.4 인공지능 연구역량 강화를 위한 적극적 학제 개편

◆ 융합 인재 배양

- ✓ AI와 데이터 분석에 관한 기술적 이해를 갖춘 인력 배양을 위해, 2025년 인공지능데이터사이언스학부로 인공지능학과와 데이터사이언스학과를 통합하는 등 본 사업단은 융합 인재 교육을 위한 적극적인 학제 개편 의지가 있음.
- ✓ 교차전공학점 이수과목 확대 (현재 17과목, 사업 종료시까지 25과목 목표)를 통해 융합 능력을 갖춘 인재를 배양. (예: 컴퓨터공학전공에서 개설되는 컴퓨터 핵심교과목을 인공지능전공 학생들이 수강할 시에 전공학점 이수로 인정)

◆ 공동지도교수제 운영 및 활성화

- ✓ 두 전공의 교수진으로 구성된 공동지도교수제를 통해 SW분야에서의 인공지능 융합연구를 활성화함. 이를 통해 인공지능에 관심있는 대학원생의 보다 활발한 전공 선택을 유도하고 융합형 인재 육성에 도움이 될 것으로 기대함.

1.3.5 우수 인공지능 전임 교원 및 연구 인력 확보 계획

◆ 전임 교원 확보 계획

- ✓ 인공지능대학 인공지능소프트웨어학부는 2023년 인공지능대학 신설 후, 현재까지 인공지능분야 전임교원 15명을 신규 채용하였으며, 2026년 3월 5명 추가 신규임용(확정)을 목표로 로봇틱스, EdgeAI, 머신러닝, 소프트웨어공학, 인공지능보안, 빅데이터 관련 교원을 채용할 예정이며 본교의 연구경쟁력을 지속적으로 향상시킬 계획임.

◆ 우수신진연구인력(박사후과정 연구원/연구교수) 선발 및 지원 계획

- ✓ 연구 능력이 뛰어난 사업단 소속 우수신진연구인력을 선발하며, 본 사업 참여 교수 및 대학원생과의 공동연구를 통한 연 1편의 top-tier 국제 학술대회 논문 게재를 의무화 함.
- ✓ 우수 해외 연구인력 유치를 위해 현지 거주자의 경우 정착지원을 위한 최대 USD 1,800까지의 왕복항공료를 대학 대응자금으로 지원함.

2. 연구의 국제화 현황 및 계획

2.1 참여교수의 국제적 학술활동 참여 실적 및 현황

<표 3-c> 학술지 편집위원 참여 실적

참여 교수	학술지 및 직책	기간
양대현	ETRI Journal, Section Editor	2017-현재
민동보	IEEE Trans. on Circuits and Systems for Video Technology, Editor	2022-2024
반효경	Applied Science, Editor	2024-현재
이형준	ICT Express, Editor	2015-현재

<표 3-d> 국제학술대회 및 국제워크숍 위원장 및 좌장 참여 실적

참여 교수	학술대회 및 직책	기간
양대현	THE 25TH WORLD CONFERENCE ON INFORMATION SECURITY APPLICATIONS	2024
김종길	ACISP (Australasian Conference on Information Security and Privacy), Publication Co-Chairs	2021
윤명국	IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS)	2025
이형준	ICOIN (International Conference on Information Networking), publication chair	2021-2023
오유란	ACM CHI conference on Human Factors in Computing Systems	2021
	IEEE 19th International Conference on Pervasive Computing and Communications (PerCom) MPAT, Workshop chair	2021
	The 24th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS), Global Outreach Chair	2022
	The ACM Symposium on User Interface Software and Technology (UIST), Treasurer	2025

<표 3-e> 국제 수상 내역

참여 교수	수상내역	수상년도
양대현	2020 IEEE Systems Journal Best Paper Award (less than 1% selection rate)	2020
김종길	ACM ASIACCS 2020, Best Paper Award	2020
노준혁	CVPR 2020 LID (Learning from Imperfect Data) Challenge - 트랙 3(WSOL) 우승	2020
	CVPR 2020 LID (Learning from Imperfect Data) Challenge - 트랙 1(WSSS) 준우승	2020
반효경	IEEE AEECA 2024, Best Paper Award	2024
	과학기술우수논문상, 세계한인과학기술인대회, 과총	2023
오유란	ACM IUI 2023, Best Paper Award	2023

〈표 3-f〉 국제학술대회 프로그램 위원 참여 실적

참여 교수	학술대회	기간
양대현	IEEE ICDCS (IEEE International Conference on Distributed Computing Systems)	2021-2023
	IEEE DSC (IEEE Conference on Dependable and Secure Computing)	2021
	Asia Joint Conference on Information Security (AsiaJCIS) PC member	2024-2025
	IEEE Global Blockchain Conference PC member	2025
김종길	International Conference on Quantum Communications, Networking, and Computing (QCNC)	2024
	ACISP (Australasian Conference on Information Security and Privacy)	2024
오세은	IEEE DSC (IEEE Conference on Dependable and Secure Computing)	2025
노준혁	AAAI (AAAI Conference on Artificial Intelligence)	2021-2025
	IJCAI (International Joint Conference on Artificial Intelligence)	2024-2025
민동보	AAAI (AAAI Conference on Artificial Intelligence)	2022-2025
반효경	IEEE NVMSA (Non-Volatile Memory Systems and Applications Symposium)	2020-2021
	ICOIN (International Conference on Information Networking)	2020-2021
	ICUFN (International Conference on Ubiquitous and Future Networks)	2020-2021
	ICAIIC (International Conference on Artificial Intelligence in Information and Communication)	2020-2021
윤명국	IEEE/ACM MICRO (International Symposium on Microarchitecture)	2025
이지영	AAAI (AAAI Conference on Artificial Intelligence)	2024-2025
	CIKM (The Conference on Information and Knowledge Management)	2025
이형준	IEEE ICC (IEEE International Conference on Communications)	2024
	IEEE WCNC (IEEE Wireless Communications and Networking Conference)	2025
	ICCE (International Conference on Consumer Electronics)	2023-2025
오유란	ACM CHI (Conference on Human Factors in Computing Systems)	2021, 2023 2025

2.2 참여교수의 국제공동연구 실적 및 계획

<표 3-5> 최근 5년간 참여교수 국제공동연구 실적

연번	공동연구 참여자		상대국/ 소속기관	국제공동연구 실적	DOI 번호/ISBN 등 관련 인터넷 link 주소
	교육연구단 참여교수	국외 공동연구자			
1	양대현	RhongHo Jang	미국/Wayne State University	Kim, S., Mirnajafizadeh, S. M. M., Kim, B., Jang, R., & Nyang, D. (2025, February). SketchFeature: High-Quality Per-Flow Feature Extractor Towards Security-Aware Data Plane. In Proc. of ISOC NDSS.	https://www.ndss-symposium.org/wp-content/uploads/2025-1071-paper.pdf
2	양대현	David Mohaisen; RhongHo Jang	미국/University of Central Florida; 미국/Wayne State University	Kim, S., Jung, C., Jang, R., Mohaisen, D., & Nyang, D. H. (2023). A robust counting sketch for data plane intrusion detection. In 30th Annual Network and Distributed System Security Symposium, NDSS 2023. The Internet Society.	https://www.ndss-symposium.org/wp-content/uploads/2023/02/ndss2023_s102_paper.pdf
3	민동보	Kwang Moo Yi	캐나다/The University of British Columbia	Salience-Based Adaptive Masking: Revisiting Token Dynamics for Enhanced Pre-training, ECCV 2024	https://www.ecva.net/papers/eccv_2024/papers_ECCV/papers/10063.pdf
4	민동보	Stephen Lin	중국/Microsoft Research Asia	Dense Cross-Modal Correspondence Estimation with the Deep Self-Correlation Descriptor, IEEE Trans. on Pattern Analysis and Machine Intelligence (TPAMI), vol. 43, no. 7, pp. 2345–2359, July 2021	https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8955799
5	윤명국	Nam Sung Kim	미국/UIUC	Warped-Compaction: Maximizing GPU Register File Bandwidth Utilization via Operand Compaction, HPCA 2025	https://ieeexplore.ieee.org/document/10946777
6	윤명국	Babak Falsafi	스위스/EPFL	Avant-Garde: Empowering GPUs with Scaled Numeric Formats, ISCA 2025	https://dl.acm.org/doi/full/10.1145/3695053.3731100
7	오유란	Dragan Ahmetovic	이탈리아/University of Milan	Touch Screen Exploration of Visual Artwork for Blind People. ACM WWW 2021	https://dl.acm.org/doi/abs/10.1145/3442381.3449871
참여교수 수		7		최대 제출 건수	7

○ 국제 공동연구 계획



<그림 3-5> 이화여자대학교 인공지능소프트웨어학부 국제연구협력기관

- ◆ 본 연구과제의 참여 연구진은 그림 3-5와 같이 AI 분야에서 다양한 국제 공동연구를 진행하고 있음. 미국, 영국, 중국, 등 다양한 국가(8개국, 30개 국제 협력기관)와의 국제 공동연구를 통해, 연구의 다양성을 높이고 국제적으로 경쟁력 있는 연구를 진행하기 위해 노력하고 있음. 상세 계획은 아래와 같음.
- ◆ 해외 파견 학생 체재비 및 항공료 지원, 공동 워크숍/세미나 운영비에 대한 지원 예정.
- ◆ 국제학회 연계 해외 연구자 초청 계획
 - NeurIPS, IJMLC, ACL, CVPR, ICLR 등 AI 분야 최우수 국제학회가 최근 한국에서 정기적으로 개최 또는 유치되고 있음.
 - 예, 2025년 정보과학회 최우수학술대회인 MECCAI 가 한국 대전에서 9월 개최 될 예정임.
 - 예, 2026년 정보과학회 최우수학술대회인 ICML이 한국 서울에서 7월 개최 될 예정임.
 - 이를 기회로 삼아 해외 석학 및 공동연구자들을 국내로 초청, 학생 및 교내 연구진과의 실질적인 교류의 장으로 확장하고자 함.
 - 해외 석학 강연, 교내 연구실 투어, 학생 포스터 세션, 공동 논문 미팅 등으로 구성.

<표 3-g> 국제 공동연구 해외 파트너 및 연구 내용

참여 교수	해외 파트너	소속	국제 공동연구 계획 상세 내용
양대현	Prof. Rhongho Jang	미국, Wayne State Univ.	AI 모델 경량화를 위한 새로운 텐서 표현법 개발
	Prof. Rhongho Jang	미국, Wayne State Univ.	LSM 기반 파일 시스템의 성능 최적화 기법 개발
김종길	Prof. Yong Yu	중국, Shaanxi Normal University	Trustworthiness on AI and Blockchain

배호	Prof. 안길준	미국 Arizona State University	AI 기반 자동화된 취약점 탐지 및 안전한 코드 생성 기술
오세은	Prof. Mohammad Saidur Rahman	미국, University of Texas at El Paso	평생학습 기반 멜웨어 분석
	Prof. Marc Juarez	영국, University of Edinburgh	Genuine Tor 트래픽 상관관계 분석을 가능하게 하는 모델 개발
	Prof. Matthew Wright	미국, Rochester Institute of Technology	Genuine Tor 트래픽 수집 및 종단간 상관관계 분석
노준혁	Dr. Wonho Bae	미국, Apple	능동학습 방법론 개발
	Dr. Jing Wang	캐나다, University of Alberta	소스프리(Source-free) 도메인 적응 방법론 개발
	Dr. Jiahong Chen	미국, Amazon	소스프리(Source-free) 도메인 적응 방법론 개발
	Dr. Mingyu Kim	캐나다, UBC	테스트타임(Test-time) 적응 방법론 개발
	Dr. Johanna Schwartz	미국, LLNL	능동학습 방법론의 산업 분야 적용
민동보	Prof. Kwang Moo Yi	캐나다, UBC	생성형 모델 기반 효율적 사전학습 연구
	Prof. Changjae Oh	영국, Queen Mary University of London	Robot control using vision language action
	Prof. Hansung Kim	영국, University of Southampton	멀티모달 AI 기반 3차원 공간 재구성
윤명국	Prof. Hyeran Jeon	미국, UC Merced	UVM 기술을 활용한 대규모 LLM 모델 학습 기술 개발
이지영	Prof. Jun-Yan Zhu	미국, Carnegie Mellon University	사용자 맞춤형 멀티모달 생성 모델 개발
	Dr. Daniel McDuff	미국, Google	효율적 MLLM 인과추론 네트워크 학습 방법 개발
	Dr. Justin Salamon	미국, Adobe	오디오비주얼 모델 경량화 기술 개발
	Prof. Anupam Chattopadhyay	싱가포르, NTU	Deepfake 탐지를 위한 멀티모달 모델
	Prof. Hamid Alinejad-Rokny	호주, UNSW	멀티모달 바이오 기반 LLM 학습
이형준	Prof. Bo Ji	미국 Virginia Tech	멀티 모달 연합 학습 모델 개발
	Prof. Wonjae Lee	미국 Duke University	알츠하이머 환자 맞춤형 치료 예측을 위한 패턴 인식 및 인과관계 분석
황의원	Prof. Aviral Shrivastava	미국, Arizona State University	적대적 공격 및 이상치 탐지 기술 개발

〈표 3-h〉 국제 공동연구 목표, 협력 방식 및 기대 성과물

참여 교수	연구 목표	협력 방식	기대 성과물
양대현	AI 모델 경량화를 위한 새로운 텐서 표현법 개발	공동 학생 연구자 지도 및 학생 연구자 해외 파견	- 국제 공동 논문 2건 이상
	LSM 기반 파일 시스템의 성능 최적화 기법 개발	공동 학생 연구자 지도 및 학생 연구자 해외 파견	- 국제 공동 논문 1건 이상
김종길	AI 분야에서 신뢰성을 확보할 수 있는 기법연구	최신 기술 공유 및 학생 교류, 공동 연구 수행	- 국제 공동 논문 1건 이상
배호	AI 기반 자동화된 취약점 탐지 및 안전한 코드 생성 기술 연구	공동 과제 수행	- 국제 공동 논문 1건 이상
오세은	보다 효율적인 Generative Replay 방법론 개발	공동 학생 연구자 지도 및 공동 세미나 개최	- 국제 공동 논문 3건 이상
	비쌍별 상관관계 분석 모델 개발	공동 학생 연구자 지도 및 최신 기술 공유	- 국제 공동 논문 1건 이상
노준혁	제학된 학습 조건하 AI 학습 방법론 개발	학생 공동 지도, 공동 연구, 공동 세미나 개최	- 국제 공동 논문 3건 이상
민동보	생성형 모델 기반 효율적 사전학습 연구	학생 공동 지도 및 최신 기술 공유	- 국제 공동 논문 1건 이상
윤명국	UVM 기술을 활용한 대규모 LLM 모델 학습 기술 개발	공동 학생 연구 지도	- 국제 공동 논문 1건 이상
이지영	사용자 맞춤형 MLLM 효율적 추가학습 방법 개발	공동 학생 연구자 지도 및 최신 기술 공유	- 국제 공동 논문 1건 이상
	안전한 오디오비주얼 인식 모델 개발	공동 학생 연구자 지도	- 국제 공동 논문 1건 이상
이형준	멀티 모달 연합 학습 모델 개발	대학원생 교류 및 공동 논문 발표	- 국제 공동 논문 1건 이상
	알츠하이머 환자 맞춤형 치료 예측을 위한 패턴 인식 및 인과관계 분석	대학원생 교류 및 공동 논문 발표	- 국제 공동 논문 1건 이상
황의원	신뢰가능한 인공지능을 위한 적대적 공격 및 이상치 감지 기법 개발	최신 기술 교류 및 학생 단기 파견	- 국제 공동 논문 1건 이상 - 국내 특허 1건 이상 출원

2.3 외국 대학 및 연구기관과의 연구자 교류 실적 및 계획



<그림 3-6> 해외 연구자 교류 실적 및 계획 요약

<표 3-i> 외국 대학 및 연구기관과의 연구자 교류 실적

연번	참여 교수	해외 파트너 (해외 기관)	연구 주제	기간	교류 종류
효율적인 AI 학습 방법론 관련 해외 공동 연구 실적					
1	노준혁	Prof. Danica J. Sutherland (캐나다, University of British Columbia)	준/약지도 학습 방법론	2021-2022	공동연구
2	노준혁	Prof. Danica J. Sutherland (캐나다, University of British Columbia)	능동학습 방법론	2022-2025	공동연구
3	노준혁	Dr. Johanna Schwartz (미국, Lawrence Livermore National Laboratory)	능동학습 방법론의 산업분야 적용	2023-2025	공동연구
4	노준혁	Dr. Jing Wang (캐나다, University of Alberta)	도메인 적용 방법론	2024-2025	공동연구
5	노준혁	Dr. Jiahong Chen (미국, Amazon)	도메인 적용 방법론	2024-2025	공동연구
6	노준혁	Dr. Mingyu Kim (캐나다, University of British Columbia)	테스트타임 적용 방법론	2025	공동연구
7	민동보	Prof. Kwang Moo Yi (캐나다, University of British Columbia)	거대 비전 모델의 효율적인 사전학습	2025	공동연구
8	이지영	Dr. Justin Salamon (미국, Adobe)	퓨砂浆 러닝 기반 오디오비주얼 사용자 맞춤화 학습 방법	2021	공동연구

AI 시스템의 성능 및 자원 효율성 극대화를 위한 하드웨어 아키텍처 관련 해외 공동 연구 실적

9	윤명국	Prof. Nam Sung Kim (미국, University of Illinois Urbana-Champaign)	GPU Register File 에너지 효율을 위한 연구	2024-2025	공동연구
10	윤명국	Prof. Babak Falsafi (스위스, Federal Institute of Technology in Lausanne)	Block Floating Point 연산 지원을 위한 GPU 하드웨어 구조	2025	공동연구
11	이형준	Prof. Ji Bo (미국, Virginia Tech)	강화학습 Exploration-Exploitation trade-off 연구	2024	초청장연
12	이형준	Dr. JinYi Yoon (미국, Virginia Tech)	엣지 디바이스간의 선택적 지식 전이 구조 연구	2024-2025	공동연구
13	이형준	Prof. Omprakash Gnawali (미국, University of Houston)	UAV를 이용한 효율적 데이터 전달 연구	2020	공동연구

효율적인 거대 AI 및 Edge AI 모델 응용 관련 해외 공동 연구 실적

14	이지영	Prof. Jun-Yan Zhu (미국, Carnegie Mellon University)	사용자 맞춤화 텍스트 기반 이미지 생성 모델 변형	2023	공동연구
15	이지영	Dr. Daniel McDuff (미국, Microsoft)	인과추론 가능한 자율주행 시뮬레이션	2020-2021	공동연구
16	이지영	Dr. Gyeongsik Moon (미국, Meta Reality Labs)	3D Human mesh 생성	2023	공동연구
17	이지영	Prof. Changjae Oh (영국, Queen Mary University of London)	비디오 예측 모델 기반 데이터 이상탐지	2020-2021	공동연구
18	황의원	Prof. Aviral Shrivastava (미국, Arizona State University)	딥러닝 모델의 소프트 오류 탐지 기법 연구	2024-2025	공동연구
19	오유란	Prof. Augusto Esteves (포르투갈, Instituto Superior Técnico, University of Lisbon)	터치스크린에서의 사용자입력 예측 모델링	2020-2021	공동연구

AI 공격 보호 및 프라이버시 보호 AI 관련 해외 공동 연구 실적

20	양대현	Prof. Mohammed	Code 분석 기술	2022	공동연구,
----	-----	----------------	------------	------	-------

		Abuhamad (미국, Loyola University Chicago)			해외파견
21	양대현	Prof. David Mohaisen (미국, University of Central Florida)	보안 빅데이터 기술	2022	공동연구, 해외파견
22	양대현	Prof. Rhonho Jang (미국, Wayne State University)	인-네트워크 보안 실현을 위한 트래픽 분석 기술	2023-2024	공동연구
23	김종길	Prof. Yong Yu (중국, Shaanxi Normal University)	블록체인 상의 악의적인 사용자 추적을 위한 Accountable 전자서명에 관한 연구	2023-현재	과제수주, 공동연구, 해외파견
24	오세은	Prof. Matthew Wright (미국, Rochester Institute of Technology)	Genuine Tor 트래픽 수집 및 종단간 상관관계 분석	2023	공동연구
25	오세은	Prof. Nicholas Hopper (미국, University of Minnesota)	웹사이트 평거프린팅 방어기법	2022-2024	공동연구
26	오세은	Prof. Mohammad Saidur Rahman (미국, University of Texas at El Paso)	맬웨어 분석	2025	공동연구
27	오세은	Prof. Marc Juarez (영국, University of Edinburgh)	Machine Learning For Traffic Analysis	2024	초청장연
28	오세은	Prof. Limin Jia (미국, Carnegie Mellon University)	Automatically synthesizing exploits for code injection attacks in Node.js packages	2024	초청장연
29	황의원	Prof. Aviral Shrivastava (미국, Arizona State University)	절대적 공격 방어기법 연구	2023-2024	공동연구

<표 3-j> 외국 대학 및 연구기관과의 연구자 교류 계획

연번	참여 교수	해외 파트너 (해외 기관)	연구 주제	교류 기간	교류 종류
30	양대현	Prof. Rhongho Jang (미국, Wayne State University)	AI 모델 경량화를 위한 새로운 텐서 표현법, LSM 기반 파일 시스템 최적화 기법	2025-2027	해외파견, 워크샵개최 , 공동연구

31	김종길	Prof. Yong Yu (중국, Shaanxi Normal University)	Trustworthiness on AI and Blockchain	2023-현재	과제 수주, 공동연구
32	오세은	Prof. Matthew Wright (미국, Rochester Institute of Technology)	Genuine Tor 트래픽 수집 및 종단간 상관관계 분석	2022-현재	공동연구
33	오세은	Prof. Mohammad Saidur Rahman (미국, University of Texas at El Paso)	평생학습 기반 멀웨어분석	2023-현재	공동연구
34	오세은	Prof. Marc Juarez (영국, University of Edinburgh)	Genuine Tor 트래픽 수집 및 종단간 상관관계 분석	2025-현재	공동연구
35	민동보	Prof. Changjae Oh (영국, Queen Mary University of London)	Robot control using vision language action	2025-2027	공동연구
36	민동보	Prof. Hansung Kim (영국, University of Southampton)	멀티모달 AI 기반 3차원 공간 재구성	2025-2027	공동연구
37	이지영	Prof. Anupam Chattopadhyay (싱가포르, NTU)	Deepfake 탐지를 위한 멀티모달 모델	2025-현재	공동연구
38	이지영	Prof. Hamid Alinejad-Rokny (호주, UNSW)	멀티모달 바이오 기반 LLM 학습	2025-현재	공동연구
39	이형준	Prof. Omprakash Gnawali (미국, University of Houston)	엣지 AI 분산 딥러닝 분야	2023-현재	공동연구
40	이형준	IEEE Indonesia 지부 (인도네시아)	‘Introduction to Federated Learning’ 웹세미나 진행(2025년 6월) 후 인도네시아 대학들과 연구자 교류 계획	2025-현재	웹세미나 진행, 공동연구
41	황의원	Prof. Aviral Shrivastava (미국, Arizona State University)	신뢰 가능한 인공지능을 위한 통합적 이상치 탐지 연구	2025-현재	해외파견, 공동연구

IV. 산학협력 영역

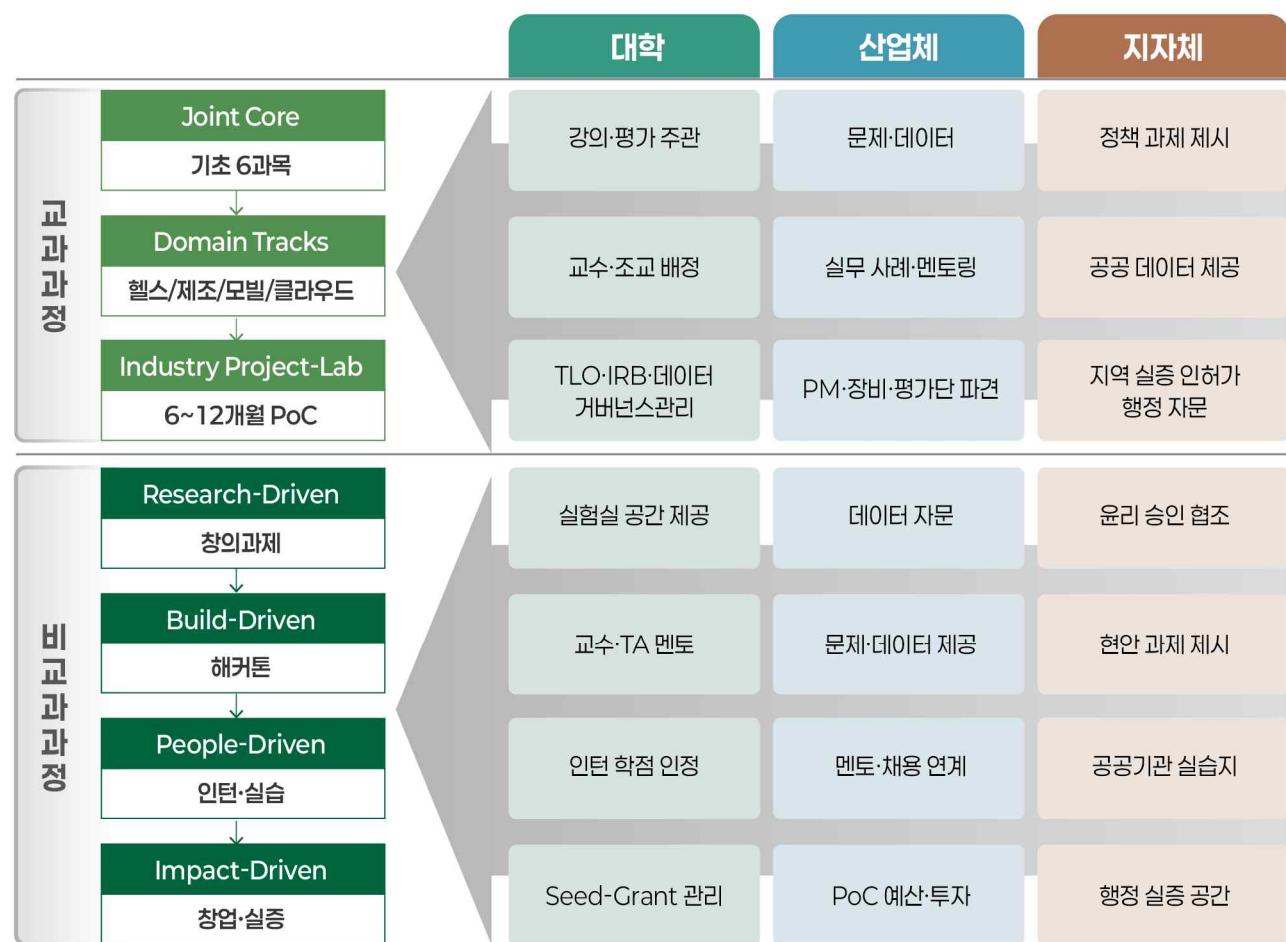
* 산학협력 영역부문의 항목은 기본적으로 교육연구단을 기준으로 작성하며, 세부 항목별로 특정기준이 제시된 경우 이에 준하여 신청서를 작성

IV. 산학협력 영역

1. 산학공동 교육과정

1.1 산학공동 교육과정 구성 및 운영 계획

산학공동 교육과정은 “교과↔비교과↔현장실증”이 톱니바퀴처럼 맞물리는 삼중 구조로 설계. 학생은 강의실에서 개념을 배우고, 비교과 프로그램에서 문제를 정의·탐색해 보며, 마지막으로 산업체·지자체가 제공한 실제 데이터와 장비를 활용해 6~12개월짜리 PoC(Proof-of-Concept)를 완주하는 것을 목표로 함. 이 과정에서 산업 전문가가 강사·멘토·평가자로 상시 참여해 ‘이론-실무’ 간 간극을 최소화하고자 함.



<그림 4-1> TRUE-AI 교육연구단 교과·비교과 통합 플로우와 3자(대학-산업체-지자체) 참여 구조

○ 교과 프로그램

- 현장 AI 문제를 풀 수 있는 인재를 키우려면 ‘개념→도메인→ 실증’ 이 단계적으로 축적되어야 하기에, 전체 교과과정(약 60 여 과목) 중 기초 공통, 전공 심화, 응용 세 레이어를 설정하고 그 가운데 Joint Core(공통 기초 6과목) · Domain Tracks(각 트랙 핵심 · 선택 4과목) · Industry Project-Lab(프로젝트 과목)을 ‘대표 러닝 패스’로 추려 운영. 즉 Joint Core는 전체 교과과정의 기초 영역에서 개념·윤리를 다지고, Domain Tracks는 심화 영역에서 헬스케어·제조 등 특화 과목을 뚫어 역량을 쌓으며, 마지막 Project-Lab은 응용 영역의 프로젝트 과목군과 엮여 실제 데이터를 다루는 PoC까지 완주하게 함으로써, 방대한 전체 커리큘럼을 기본-심화-실증의 한 흐름으로 체계화하는 것이 이 프로그램의 운영 동기이자 목표가 됨.

◆ Joint Core 모듈

- ✓ 트랙 구분과 무관하게 AI 공통 교과목으로부터 모든 학생이 초·중기(1~2 학년) 필수로 수강하는 과목들 위주로 TRUE-AI 4대 가치(T·R·U·E)를 균형 있게 커버하도록 편성.
- ✓ 모든 Joint Core 과목에는 대학 교수와 산업체 실무자가 공동 강사로 등재되며, 평가 점수의 20% 이상을 산업 쪽이 직접 채점해 지식의 실전 타당성을 검증.
- ✓ 예를 들어, ‘빅데이터분석과실습’에서는 KT AI2XL 데이터 엔지니어가 2시간 특강으로 5G SOC 로그 전처리 및 Spark ML 튜닝 사례를 소개하고, 학기말 팀 프로젝트의 처리량·지연(latency) 지표를 산업 관점에서 20% 배점으로 직접 평가. 이렇게 Joint Core 단계에서는 산업체가 사례 특강 + 평가 역할에 집중하여, 학생들이 핵심 개념을 안정적으로 습득한 뒤 다음 단계인 Domain Track 으로 자연스럽게 넘어가도록 설계.

〈표 4-a〉 Joint Core 모듈 예시

과목코드	과목명	참여 산업체 예시
G14337	인공지능개론	NVIDIA - “GPU 아키텍처와 딥러닝 연산” 특강
G18460	AI윤리와 사회적 영향	서울시 AI센터 - AI 윤리 정책 세션
G14338	머신러닝개론	AlibabaCloud - AutoML·PAI 워크숍
G18426	빅데이터분석과실습	KT AI2XL - 5G 로그 샘플·Spark 튜닝 팀
G18425	딥러닝	LG전자 - 로봇청소기 이미지 활용 CNN 세미나
G18432	강화학습	현대자동차 - 주행 시뮬·RL 적용 사례

◆ Domain Track 모듈

- ✓ 산업 수요가 뚜렷한 네 개 트랙(헬스케어·스마트제조·모빌리티·클라우드/통신)을 선택 과목 뮤음으로 제공. 효율적 AI/보안 AI 상위 트랙의 핵심·선택 과목 교과를 사용하며, 도메인별로 산업 데이터/실험 장비/규제·윤리 이슈가 명확한 과목을 배치.
- ✓ 여기서는 기업이 제공한 실제 데이터셋을 문제·과제 두 축에서 동시에 활용. 예를 들어, 헬스케어 트랙에서는 Samsung Medison 초음파 영상의 익명화·정체를 학생이 직접 수행해 모델 학습 파이프라인을 구성.
- ✓ 트랙별 교·강사는 기업 실무자·의료기관 임상의·지자체 담당자까지 포함해 “AI-도메인-규제” 시각을 한꺼번에 전달.

〈표 4-b〉 Domain Track 모듈 예시

트랙	과목(코드)	현장 데이터·문제	규제·윤리 관점 포함 사례
헬스케어AI (효율적 AI)	효율적인 딥러닝처리 (G18407)	Samsung Medison 초음파 영상 → 모델 양자화·가지치기로 Tiny-ML 병변 검출	의료기기SW 심사 가이드 (식약처)
스마트제조AI (효율적 AI)	On-Device AI (G18456)	LG전자 생산 라인 센서 로그 → 경량화 모델·분산 학습	제조 데이터 국외 이전 규정
모빌리티AI (보안 AI)	AI기반네트워크 침입탐지 (G18462)	현대차 V2X 패킷·주행 로그 → AI IDS·RL 기반 위협 예측	자동차 사이버보안 ISO/SAE 21434
클라우드/통신AI (보안 AI)	프라이버시보존 합성데이터특론 (G18463)	NaverCloud LLM 학습 로그 → DP-GAN 합성 데이터 생성	전기통신사업법·개인정보 국외 이전 조항

◆ Industry Project-Lab

- ✓ 교과 마지막 스텝은 6~12개 월짜리 캡스톤이자 PoC 실증 코스: AI융합프로젝트 1·2(G18470/71).
- ✓ 학생·교수·기업 PM이 한 팀을 이루어 수행.
- ✓ Demo-Day에는 VC·지자체 정책 담당자도 초청해 기술 사업화·지역문제 실증의 진입로 확보.

<표 4-c> Industry Project-Lab 절차 예시

단계	기간	활동 내용	산학 참여
문제정의 워크숍	2주	기업 · 학생 협동 디자인 쟁킹	기업 PM · 교수
데이터 확보 · 베이스라인	10주	원천 데이터 전처리, 베이스라인 모델 구축	기업 데이터 엔지니어
중간검증	2주	KPI 초기 달성을 점검, 피봇 여부 결정	산학 평가단
모델 고도화	12주	하이퍼파라미터 튜닝, MLOps 파이프라인	기업 DevOps
Demo-Day	2주	VC · 지자체 앞 데모 및 피칭	투자 심사역 · 공무원
IP 검토	2주	특허 · 논문 · 기술이전 루트 결정	대학 TLO · 기업 법무

● 비교과 프로그램

◆ Research-Driven Stage

- ✓ 창의자율과제는 학생이 흥미 있는 문제를 자유롭게 정의하고 6개월간 작은 연구팀을 꾸려 실험.
- ✓ 교내 교수뿐 아니라 해당 주제와 연관된 산업 멘토를 매칭해 논문 준비 · 데이터 윤리 심사를 동시에 경험하도록 함.

◆ Build-Driven Stage

- ✓ 해커톤 · 캡스톤 세션은 산업체 · 공공기관이 직접 문제를 내고 데이터를 제공.
- ✓ 36시간 연속 해커톤으로 프로토타입을 뽑아 보고, 캡스톤에서는 산업용 평가 지표로 재검증.
- ✓ 우수팀은 기업 PoC 예산 또는 지자체 실증 예산으로 후속 지원을 수혜.

◆ People-Driven Stage

- ✓ 인턴십 · 현장실습은 매 학기 정규 교과 일정과 겹치지 않도록 모듈형(9주 · 144h 이상)으로 편성.
- ✓ 취업 연계를 염두에 두고 기업 PM이 사전에 직무 요구 역량을 공지하고, 학생은 그것을 과연 전 한 학기 동안 맞춤형 세미나 · 과제를 통해 준비.

◆ Impact-Driven Stage

- ✓ 실험실 단위의 연구 성과가 사업화 가능성이 보이면 대학 Seed Grant와 기업 매칭펀드를 뮤어 “창업 탐색 팀”을 구성.
- ✓ 서대문구청 · 서울시 AI센터 등 지자체와 협력해 공공 문제를 해결하는 팀에게는 행정실증 공간과 정책 피드백을 제공.

● 운영 체계와 품질 보증

- ◆ 산학공동 교육협의체가 8주 단위로 모든 교과 · 비교과 모듈을 리뷰. 이 협의체에는 교수, 산업 CTO, 지자체 융합정책 담당자를 균형 있게 포함.
- ◆ 실험 · 데이터 윤리, IP 관리, 보안 인증은 품질 · 윤리 TF가 전담. 모든 참가자는 NDA · IPP(50:50 공동 소유)를 서명해야 하며, 의료 · 개인 데이터 사용 시 IRB Fast-Track을 거침.
- ◆ Demo-Day · 수강 만족도 · 산출물의 산업 활용도 등 핵심 KPI를 시각 대시보드로 제공해 심사위원, 기업, 학생 모두가 진척을 한눈에 볼 수 있도록 할 예정.

● 기대효과

- ◆ 본 교육과정은 “교과에서 배우고 → 비교과에서 문제를 정의해 보고 → Project-Lab에서 실현해 보고 → Demo-Day에서 시장 · 정책 피드백을 받는” 완결형 문제 해결 루프를 설정.
- ◆ 학생 관점 : 전공 4년 내에 “모델 설계→엣지 배포→규제 대응” 까지 경험, 졸업 즉시 현장 투입.
- ◆ 산업체 관점 : 베이스라인을 넘어 현장에서 바로 활용할 PoC + 예비 인력 확보.
- ◆ 지역사회 관점 : 교통 · 치안 · 보건 등 공공 데이터를 AI 서비스로 전환하는 데모 프로젝트 확보.
- ◆ 대학 관점 : 교육 품질 데이터를 KPI로 관리해 커리큘럼을 매 학기 개선, “Evolving AI Curriculum” 자체 확립.

2. 참여교수 산학협력 역량

2.1 국내 및 해외 산업체, 지자체 연구비

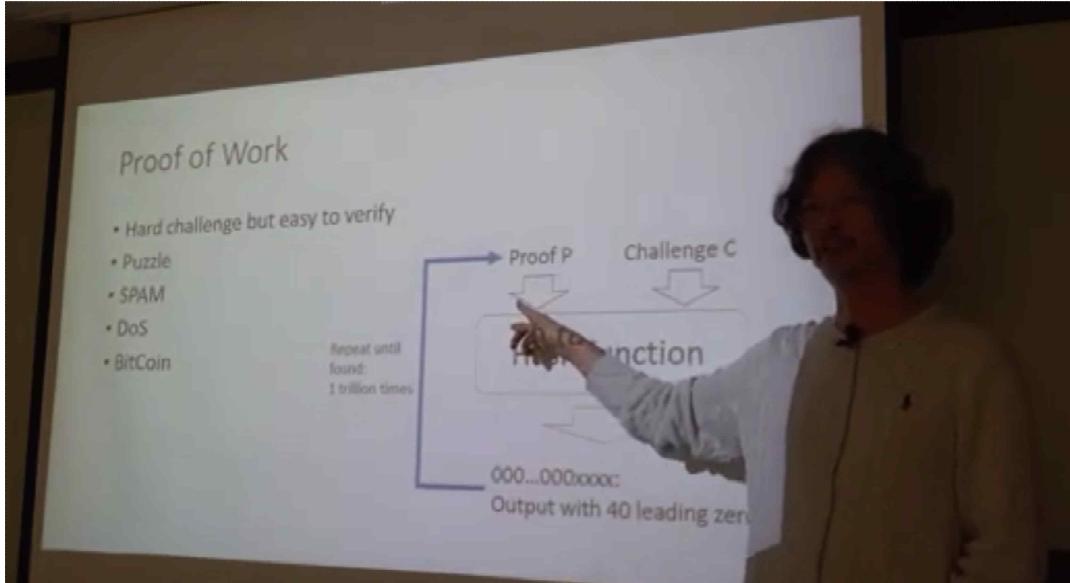
2.2 특허, 기술이전, 창업 실적의 우수성

2.3 산학협력을 통한 (지역)산업문제 해결 실적의 우수성

<표 4-3> 최근 5년간 참여교수 (지역)산업문제 해결 대표실적

연번	참여교수명	연구자등록번호	세부전공분야	(지역)산업문제
	실적의 적합성과 우수성			
	양대현	10190916	인공지능시스템및응용	기업현안 해결
실적명: 하나금융그룹 수석 고문 교수				
1. 실적의 우수성 <ul style="list-style-type: none"> 2016-2022 년 하나금융TI 수석고문으로 블록체인 · AI 보안 기술 자문 → 금융 분석 · 예측 · 보안 모델 고도화 사내벤처 C&D Factory 조직 · 보안 아키텍처 설계 자문, IT Communication Day 기조강연(참석자 100-150명) 연구원 채용 심층 면접 · 멘토링 등 우수 인재 확보 기여, 월간 보안 자문 보고서로 그룹 보안 역량 강화 2. 본 과제와의 연관성 <ul style="list-style-type: none"> 금융권의 신뢰 가능한 통합형 AI 보안 경험은 TRUE-AI의 Joint Core ‘AI 윤리 · 보안’ 및 Domain Track ‘클라우드/통신 AI’ 실증 과제와 직결 				
	배호	11635105	기계학습및지식처리	기업현안 해결
실적명: 자유로운 데이터 이동을 위한 보안 연구				
1. 실적의 우수성 <ul style="list-style-type: none"> 국내 대기업인 LG 이노텍과 공동으로 진행한 과제로 같은 계열사 내에 자유로운 데이터 이동을 목적으로 한 AI 모델 개발이 목적이었음 계열사 내에 데이터를 보호하면서 이동을 하려면 데이터의 변환 모델이 필요하였음 이를 개발하기 위해 차등정보보호를 적용하여 데이터를 보호하면서 반출이 가능한 모델을 개발함 2. 본 과제와의 연관성 <ul style="list-style-type: none"> 차등정보보호 기술을 활용하여 오류 개발한 모델은 인공지능 AI보안을 세부 연구분야로 하는 본 교육 사업팀의 연구 목표와 밀접하게 연관됨 				
	반효경	10091721	인공지능시스템및응용	일자리창출
실적명: “청년 TLO 육성사업” 및 “IP 마켓플레이스 in 이화” 개최				
1. 실적의 우수성 <ul style="list-style-type: none"> 2019-2021 년 총괄책임자로 23 억 원 수주, 이공계 미취업 졸업생 200명 6개월 채용 → TLO 전문가 양성 맞춤형 교육 · 컨설팅으로 S 등급(최우수) 달성, 다수 특허 기술이전 · 창업 촉진 교내 최초 IP 마켓플레이스 개최 → 우수 특허 100건 발표, 수요기업 · TLO 직접 매칭 2. 본 과제와의 연관성 <ul style="list-style-type: none"> 기술이전 · 창업 파이프라인 구축 경험은 Industry Project-Lab Demo-Day 성과 확산 및 학생 창업 · 취업 연계 모델로 활용 가능 				

	이형준	11091991	인공지능시스템및응용	산학협력 프로그램 운영
실적명: 인공지능대학원 사업 운영				
1. 실적의 우수성 <ul style="list-style-type: none"> IITP 인공지능융합대학원 사업 책임교수로서, 산학연계 공동 연구 추진 및 재학생 인턴십, 재직자 교육 프로그램, 세미나 운영을 통해, 긴밀한 산학협력 프로그램을 다양하게 운영해 오고 있음 산업에서 필요한 기술, 문제 해결을 대학원생들과 연계하여 창의자율과제를 수행토록 하고, 산업체 인력을 지도교수로 함께 공동 지도하는 대학원생을 위한 교과 프로그램 설계 및 운영 산업에서 필요한 기술 및 연구 개발 능력을 함양하기 위해 재직자 프로그램 및 세미나를 운영하여 교육시켜 산업체 인력을 위한 양성 프로그램 운영 2. 본 과제와의 연관성 <ul style="list-style-type: none"> 인공지능융합대학원 사업을 통해 확보된 인공지능혁신인재양성 프로그램과 연계하여 본 BK 사업의 대학원생을 고도의 인공지능 연구 및 교육 프로그램 수혜를 받게 함으로써 기여할 수 있음 				
4	이형준	11091991	인공지능시스템및응용	창업 · 기술사업화
실적명: 실험실창업혁신단 사업 수주 및 운영				
1. 실적의 우수성 <ul style="list-style-type: none"> 과기정통부 실험실창업혁신단 사업 책임자: AI 특허 사업화 · 창업 탐색 프로그램 · 공유 실험 공간 구축 교내 AI 기술 Market-Fit 검증→시제품 제작→투자 연계 전주기 지원 경험 보유 2. 본 과제와의 연관성 <ul style="list-style-type: none"> 창업 인큐베이팅 노하우는 TRUE-AI Impact-Driven Stage(Seed-Grant × 기업 매칭펀드) 운영 모델과 직접 호환, 학생 · 기업 공동 창업 촉진 				
참여교수 수		7	최대 제출 건수	7

연번	교육연구단 참여교수 (지역)산업문제 해결 대표실적 설명
1	<p>실적명: 하나금융그룹 수석 고문 교수 참여교수: 양대현</p> <p>실적내용</p> <ul style="list-style-type: none"> • 2016년부터 2022년까지 하나 금융 그룹 산하의 (주)하나금융티아이 수석고문으로 블록체인 및 인공지능 관련 연구 자문을 수행하여, 금융 및 IT 분야에서 기업의 기술적 문제들을 해결 • 하나 금융그룹의 디지털 혁신 그룹인 하나TI에 금융 분석, 예측, 보안 관련해서 다양한 인공지능 연구 기술 자문을 3년 동안 수행 • 이를 통해 산업체의 인공지능 및 보안 관련 애로사항을 많은 부분 해결해 주었으며, 기술 부문 뿐 아니라 연구원 채용에도 관여하여 우수 인재 채용에도 기여 • 하나 그룹 내 사내벤처(C&D Factory) 추진을 위한 조직 구성 자문 및 보안 기술 분야 구성 자문 • 100 ~ 150명의 하나금융그룹 IT 담당 직원들이 참석하는 최신 IT기술(인공지능, 빅데이터, 블록체인, IoT, Open Banking API 등) 공동세미나인 하나금융그룹 IT Communication Day에 강연자로 블록체인 관련 강연 • 하나금융그룹 사원 대상으로 다양한 인공지능 보안 기술, 랜섬웨어 현황 분석 및 인공지능 기술을 이용한 방어 기법 강연 • 하나금융융합기술원 연구원 채용 면접 참여해서 기술 심층 면접을 진행해 회사의 인재 채용에 기여 • 매월 하나 금융 보안 자문 결과를 보고서로 작성해 하나 금융 그룹의 보안 역량을 강화 

실적명: 자유로운 데이터 이동을 위한 보안 연구

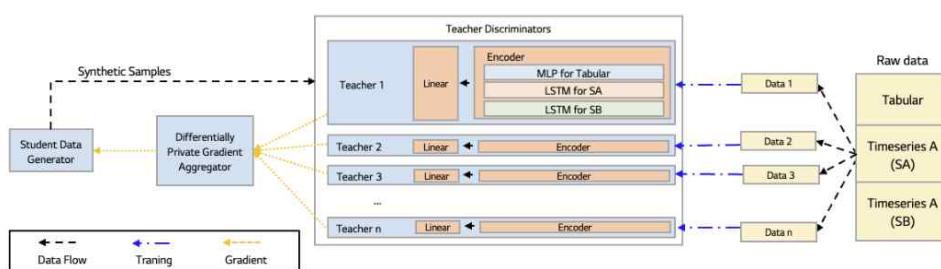
참여교수: 배호

실적내용

- 2022. 4 ~ 2023. 5 LG이노텍과 “데이터 보호 기반 AI 학습 모델 개발” 공동 수행, 계열사 간 자유로운 데이터 이동·공유가 가능한 AI 모델 구현이 궁극 목표
- 연구 골격: Federated Learning(FL) + Differential Privacy(DP) 융합

1. Federated Learning 파트

- 다양한 단말 간 협업 학습을 지원하는 네트워크·프로토콜 아키텍처 설계
통신 비용 절감·이종(Non-IID) 데이터 대응을 위한 FedClassAvg 알고리즘 제안
 - ✓ 전송 주기 최적화·가중치 압축 적용 → 모델 파라미터 전송량 10× 감소
 - ✓ 실험 결과, 기존 FedAvg 대비 MSE 5.26% 개선 (예측 정확도 상승)
- Edge 디바이스-서버 간 동적 학습률·배치 크기 조절 기법 포함 → 실시간성 확보



2

2. Differential Privacy 파트

- DP 적용 G-PATE + Transformer 재생성 모델 설계 (교사-학생 구조)
 - ✓ Tabular·Time-Series 모두 대응, $\epsilon \leq 3.0$ 수준에서 개인정보 보호 보장
 - ✓ teacher gradient → Transformer student generator 전달 → 재생성 데이터 품질 향상
- DP-GAN 대비 MAPE 120% 이상 성능 향상, 원본과 유사한 통계·유용성 확보
- 재생성 데이터 기반 모델을 실제 데이터로 검증 시 기존 성능의 90% 이상 유지

PATE-GAN (Baseline)			G-PATE + Transformer (Ours)		
Epsilon	# of teachers	Test MAPE (%)	Epsilon	# of teachers	Test MAPE (%)
0.3	10	738	0.3	500	617.3

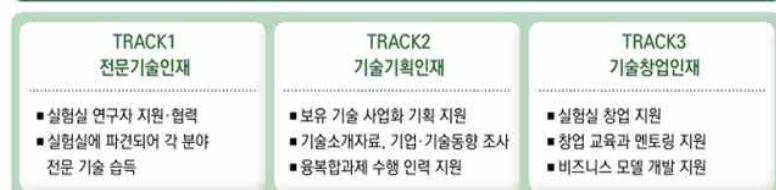
- LG이노텍 AOI 불량·공정 로그 실데이터로 학습 → F1 +4.7p(기존 대비)
- 데이터 반출 없이 고성능 모델 학습 가능 → 민감 정보 제조 라인 디지털 전환 촉진
- 계열사 간 데이터 이동 규제·보안 이슈 해결, 확장성 있는 SaaS 솔루션 모델 제시
- FL·DP 두 핵심 기술의 현장 실증 성공 → 기업·기관 데이터 주체가 정보 유출 위험 없이 AI 성능 확보
- 지역 산업(제조·의료 등)에서 민감 정보 기반 AI 서비스 가속화 → 디지털 경제 성장 발판

실적명: “청년 TLO 육성사업” 및 “IP 마켓플레이스 in 이화”개최
참여교수: 반효경

실적내용

- 2019 - 2021 년 과학기술일자리진흥원 “청년 TLO(Technology Licensing Officer) 육성사업” 총괄책임자로 23 억 원 사업비 수주, 이공계 미취업 졸업생(대학원 포함) 200명 6개월 간 채용·교육·멘토링 → 기술사업화 전문 인력 대규모 양성
- 사업 운영 전 과정(모집·선발·트랙 설계·평가)을 총괄, 기술이전·창업·취업 성과를 종합적으로 관리하여 최종평가 S 등급(최우수) 달성
- 참여 인력별로 전공 및 성향을 파악하기 위한 심층 인터뷰를 한 후 분석 결과를 토대로 전문기술인재, 기술기획인재, 기술창업인재 세 트랙으로 배치하고 맞춤형 교육 및 컨설팅을 통해 지식재산, 기술마케팅 및 기술이전, 창업 및 엑셀러레이팅 등의 역량을 강화함으로써 다수의 취·창업 성과를 거둠

청년 TLO 기술사업화 유형별 인재 양성 시스템 구축



3

- “IP 마켓플레이스 in 이화” 최초 기획·개최, 대학 우수특허 100건 선별 → 발명자 직접 PT(구두 20건)·포스터 80건 발표
- 행사 참가자: 수요기업·VC·특허사무소·창업보육센터 관계자 등
- 청년 TLO 연구원들이 행사 기획·매칭·후속 협상 전 과정에 참여하여 실전 기술증개 경험 확보, 산학협력 인재로 성장
- 산학협력단장으로서 대학 IP 포트폴리오 재정비·시장성 평가 체계 구축, 발명자 인센티브·성과금 제도 개선 → 교원·학생 특허 출원 건수 증가



실적명: 인공지능대학원 사업 운영

참여교수: 이형준

실적내용

- IITP 인공지능융합혁신인재양성사업(인공지능융합대학원) 사업 책임 교수로서 산학연계 공동연구, 재학생 인턴십, 재직자 교육 프로그램, 세미나, 산학협력포럼 등을 운영하며 산업체 문제 해결 역량을 갖춘 연구 인력을 양성하고 있음
- 산업 현안 기반 창의자율과제 수행을 통해 대학원생이 기업이 요구하는 기술·문제를 직접 해결하도록 유도하고, 특히 출원·SW 등록·논문 발표를 졸업요건에 포함하여 산업체 수요에 부합하는 인공지능융합인재 배출을 목표로 함
- 산업체 인력을 지도교수로 공동 참여시키는 교과·비교과 프로그램을 설계·운영하여, 학생들이 학문적 지도와 동시에 실무 지도를 받을 수 있도록 지원하고 있음
- 재직자 대상 맞춤형 교육 프로그램과 세미나를 정례화하여, 산업체 인력이 최신 AI 기술·연구개발 능력을 함양하도록 돋고 있으며, 이를 통해 학계-산업계가 함께 시너지를 창출하는 대학원 전공 체계를 구축하고 있음

비전

AI for A Better World, 보다 더 나은 세상을 위한 AI

핵심가치

GO-EWHA

- Global** 글로벌 기업과 함께하는 AI융합 연구 선도
- Open** 모델 · 데이터셋 · 벤치마크 공개를 통한 AI 혁신 기여
- Education with convergence** 다양한 분야와 융합하는 AI 기술 교육
- With diversity** 다양성의 시대를 선도하는 AI 인재 양성
- Harmonized** 기업과 대학이 조화를 이루는 AI 생태계 조성
- AI for All** 모두를 위한 AI 융합 교육 및 연구 제공

4

추진전략

모두를 위한 AI 교육 제공

다양한 분야의 학생 및
재직자에게 수준별
커리큘럼 제공

문제 해결형 AI 융합 인재 양성

AI-의료 · 바이오,
AI 융합 기반 기술
분야의 산업체 현안 문제
해결형 인재 양성

AI 융합 산학 생태계 구축

NVIDIA, MS, Boeing 등
31개 국내외 기업체와의
AI 산학 생태계 구축

AI 기초 교과목 운영

AI 기술 기초 교육과정을 폭넓게 제공하여 비전공자 · 재직자들의 AI 진입 장벽 완화

연구분야

AI-의료 · 바이오 융합

EWHA MEDI-CLUSTER
(이화의료원)

AI 기반 융합 기술

산학협력 교과목 운영

산업체 인턴 및 공동 연구를 통한 산업체 현안 문제 해결형 AI 인재 양성

대학원 운영

산학 · 공공 운영위원회

교육 · 연구 · 융합 운영위원회

글로벌 인턴 · 창업 위원회
(위원장: 윤송이 석좌명예교수)

신촌 협의회

대학원 운영 협업

AI · 소프트웨어
온라인 교육 개발 협업

산학 · 해외 교류 협업

목표 및 기대효과

AI 관련 우수 학술대회 및
저널에 논문 50편 게재글로벌 역량을 갖춘 AI
여성인재 140명혁신적 AI 벤처 창업
졸업생 취업률 100%

실적명: 실험실창업혁신단 수주 및 운영

참여교수: 이형준

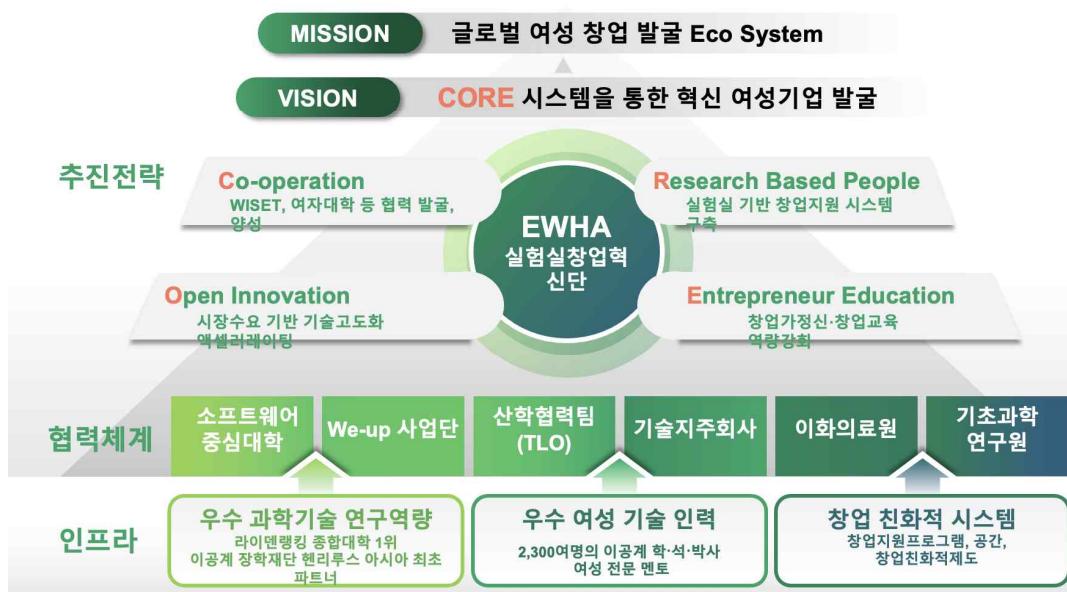
실적내용

- 과학기술정보통신부 '실험실창업혁신단' 사업을 사업책임자로 수주
- 이화여대 인공지능 기술의 기술사업화·창업 탐색 지원을 위해
 - ✓ 교과·비교과 창업 교육 프로그램 설계
 - ✓ 전용 창업 실험공간 구축 및 운영
- 컨소시엄 대학: 고려대·성균관대·KAIST·GIST·포항공대·UNIST + 이화여대
- 사업 규모: 5년(2 + 3년), 연 평균 12억 원, 최대 60억 원 지원
- 주요 성과
 - ✓ 창업팀 90여 개 발굴
 - ✓ 시장탐색교육기관과 협력해 실전 창업 교육·실시간 멘토링 진행
 - ✓ 창업 아이템 고도화 및 사업화 전략 수립 지원
- 특화 전략 - CORE 시스템을 통한 혁신 여성기업 발굴
 - ✓ 여성 맞춤형 창업 경험·노하우 전수
 - ✓ 여성 창업 전문가 멘토단 운영
 - ✓ 기술창업 교육, 단계별 사업화 지원, 여성기술창업 인포럼 등 프로그램 운영
- 결과적으로 이화여대 AI 기술 기반 창업 기술 발굴·창업 기업 배출의 기반을 마련

5

이화여대 제안 내용

사업추진 목표 및 비전



3. 산학 간 인적/물적 교류

3.1 산학 간 인적/물적 교류 실적과 계획

3.1.1 산학 간 인적/물적 교류 실적

○ 양대현 교수

- ◆ 협력기관/기업 : 하나금융그룹 하나금융융합기술원
- ◆ 기간 : 2016 ~ 2022
- ◆ 교류 형태 : 인공지능 보안 분야 자문 교수로 6년 이상 활동
- ◆ 핵심 실적
 - ✓ 인공지능 보안 분야 전문 인력 채용 자문
 - ✓ 하나금융그룹 핵심 서비스의 인공지능 보안 분야 자문
 - ✓ 블록체인과 인공지능의 금융 서비스 연구 및 자문

○ 반효경 교수

- ◆ 협력기관/기업 : KOCW, 삼성 타이젠
- ◆ 기간 : — (공개강의 · 오픈소스 활동 지속 중)
- ◆ 교류 형태 : 공개강의 제공, 강의자료 · 소스코드 · 데이터 오픈
- ◆ 핵심 실적
 - ✓ 운영체제·시스템 SW 강의 누적 조회 95만+ 회, 월간 인기 강의 선정 경험
 - ✓ IoT 플랫폼 타이젠 강의자료 공개 → 개발자 학습용으로 활용
 - ✓ 안드로이드·리눅스 등 오픈 SW 프로젝트·데이터 공개 → 학문 개방화·재교육 기여

○ 배호 교수

- ◆ 협력기관/기업 : 큐빅
- ◆ 기간 : — (연구 진행 중)
- ◆ 교류 형태 : 생성형 AI 합성데이터 연구
- ◆ 핵심 실적
 - ✓ 기업 간 민감정보 유출 방지를 위한 합성데이터 생성 모델 개발 연구 수행
 - ✓ 데이터 통계적 속성 유지·보호를 동시에 달성하는 기술 검증 중

○ 김종길 교수

- ◆ 협력기관/기업 : 사이버안전훈련센터(CSTEC)
- ◆ 기간 : 2023 ~ 2025
- ◆ 교류 형태 : 재직자 대상 보안 교육 · 특강
- ◆ 핵심 실적
 - ✓ 랜섬웨어 대응 교육 5회 ('23 2회, '24 2회, '25 1회) : 강의 + 실습(1일/4 시간)
 - ✓ ChatGPT 보안위협 특강 2회 ('24, '25 각 1회) : 1.5 ~ 2 시간 과정
 - ✓ 국가기관 · 공기업 정보보호 담당자 역량 강화

○ 이형준 교수

- ◆ 협력기관/기업 : 대성산업, (주)유니와이즈솔루션즈, 삼성미래기술육성센터
- ◆ 기간 : 2018 ~ 현재
- ◆ 교류 형태 : 기업 자문, 기술이전, 산학연 공동연구
- ◆ 핵심 실적
 - ✓ 대성산업 사외이사·감사위원 ('22~) → AI 전환 전략 지원
 - ✓ (주)유니와이즈솔루션즈에 홈 피트니스 AI 앱 3종 국내 특허·프로토타입 기술이전 추진('23)
 - ✓ 삼성미래기술육성과제('18-'22) "Hybrid HW-SW 기반 학습면역 보안 IoT 아키텍처" 수행 → Physical Unclonable Function (PUF) 기반 보안 프로토타입 구현

○ 민동보 교수

- ◆ 협력기관/기업 : LG전자, 현대자동차
- ◆ 기간 : 2021 ~ 2025
- ◆ 교류 형태 : 산업체 공동 연구과제(3건)
- ◆ 핵심 실적
 - ✓ 로봇청소기 On-device AI 고도화 ('24.10-'25.10)
 - ✓ 로봇청소기 주행 오류 탐색 자기지도 학습 ('23.04-'24.04)
 - ✓ 차량 물 유입 검출 AI 업그레이드 ('21.04-'22.09)

○ 이지영 교수

- ◆ 협력기관/기업 : Microsoft Research, Adobe Research, 네이버 클라우드, LIG 넥스원
- ◆ 기간 : 2020 ~ 현재
- ◆ 교류 형태 : 국제공동연구, 기술 자문, 산학 프로젝트
- ◆ 핵심 실적
 - ✓ CausalCity 자율주행 시뮬레이터 공동 개발 ('20-'21) → 오픈소스 공개
 - ✓ 음성/영상 구간 탐지 기술 ('21) → 미국 특허 출원
 - ✓ HyperClova-X 음성 LLM 구축 자문 ('24)
 - ✓ 멀티모달 LLM 경량화 연구 ('25.08~) · 보이스피싱 대응 탐지 기술 연구 ('25.06~) – 오픈소스 공개 예정

○ 황의원 교수

- ◆ 협력기관/기업 : 네이버, 서울대학교병원, 서울대학교, KAIST, 현대자동차
- ◆ 기간 : 2024 ~ 현재
- ◆ 교류 형태 : 대형 컨소시엄 연구, 산업체 기술 자문
- ◆ 핵심 실적
 - ✓ 단일세포 파운데이션 모델 개발('24-'26) : scRNA-seq → scATAC-seq 멀티모달 확장
 - ✓ 현대자동차 생성형 AI 개인화 기술 세미나·리포팅 ('24.09-11)

○ 노준혁 교수

- ◆ 협력기관/기업 : Wordbricks Inc.(US), 휴먼퍼포먼스랩, 에스프레스토, DXR, 스포터, 비엠스마일, 서울 대병원 · 울산대병원 · 서울성모병원 · 이대서울/목동병원

- ◆ 기간 : 2023 ~ 현재
- ◆ 교류 형태 : 기술 자문, 공동 연구, 인턴 · 인재 교류
- ◆ 핵심 실적
 - ✓ GetGPT 노코드 플랫폼 기술 자문 ('23~)
 - ✓ 피로도 예측 인솔 AI 모델 연구 (휴면폐포먼스랩, '24.11~)
 - ✓ 화면보호기 이상행위 감지 알고리즘 고도화 (에스프레스토, '24.03-08)
 - ✓ 제조 합성데이터 생성 연구 (DXR, '24.07~) → 대학원생 2명 인턴 참여
 - ✓ 한식 조리 로봇 비전 AI 모델 공동 개발 (스포터, '24.08~)
 - ✓ IoT-펫 헬스케어 AI 공동 연구 (비엠스마일, '24.11~)
 - ✓ 의료 AI 공동 연구 및 학생 파견 - 서울대·울산대·서울성모·이대병원 등 (지속)

3.1.2 산학 간 인적/물적 교류 계획

○ 인적 교류 전략

- ◆ 본 연구단은 “사람이 움직여야 지식이 진화한다”는 원칙 아래, 대학과 산업체 · 지자체가 사람을 공유하는 다층적 메커니즘을 설계.
- ◆ **산학 공동 멘토링: 듀얼-멘토(교수 + 산업) 지도 체계**
 - ✓ 석·박사 과정 학생 한 명에게 학교 지도교수와 산업체 책임연구자가 함께 ‘공동 지도교수’로 지정.
 - ✓ 산업 멘토는 데이터 보안, MLOps, 현장 관제 시스템 등 현실 제약을 꾸준히 알려 주고, 대학 교수는 이론적 엄밀성과 연구 윤리를 책임.
 - ✓ 결과적으로 학생 논문은 학문적 기여를 갖추는 동시에 기업 내부 리뷰를 통과할 수 있는 형태로 완성.
- ◆ **양방향 인력 순환: 인턴↔Visiting-Engineer 순환 파이프라인**
 - ✓ 연구단은 학기마다 산업체-파견 인턴십을 열어 학생이 9주 이상 현장을 경험하도록 함.
 - ✓ 반대로 기업에서는 재직자들이 “Visiting Engineer”라는 이름으로 랩실에 들어와 6~12주 동안 최신 논문 재현, 데이터 라벨링 자동화, 테스트 스크립트 작성 등을 수행.
 - ✓ 이렇게 서로의 조직에 몸을 담아 보는 경험은 “대학은 현실을 알지 못한다”거나 “산업은 연구를 경시한다”는 고정관념을 깨뜨리고 학습 속도를 획기적으로 높여줄 것.
- ◆ **겸임교수 · 초빙교원 제도**
 - ✓ 대규모 LLM을 운영해 본 클라우드 아키텍트, 5G 보안 SOC를 설계한 통신 보안 전문가, 의료영상 PACS를 구축한 의료 AI 리더와 같이 “현업에서 이미 검증된 전문가”를 겸임교수로 위촉.
 - ✓ 이들은 정규 과목의 일정 부분을 맡아 사례 기반 강의 · 실습을 진행하고, 캡스톤 디자인이나 해커톤에서 평가위원 역할까지 수행.
 - ✓ 겸임 기간 동안 교수들은 주기적으로 산업체를 방문해 워크샵을 열고, 현장의 애로사항과 연구자의 문제의식을 동시에 리프레시.
- ◆ **글로벌 교류: 해외 허브형 Talent Exchange**
 - ✓ 연구단은 미주 · 아시아 · 실리콘 IP 생태계를 각각 대표하는 세 거점 기업과 인재 순환 프로그램을 운영하고자 함.
 - + 미국 실리콘밸리에서는 Wordbricks Inc.가 보유한 노코드 자동화 플랫폼(GetGPT) 공동 개발팀에 학생을 파견하고, 역으로 Wordbricks의 시니어 엔지니어를 “CTO-in-Residence” 형태로 초청해 다국적 협업 문화를 전파.

- + 반도체 · AI 시스템 분야에서는 NVIDIA Global Headquarters와 연계해 Jetson Educator 프로그램을 공동 운영. 연구단 교수 · 연구원은 미국 사무소에서 엣지-AI 커리큘럼을 공동 설계하고, NVIDIA DLI 강사진은 매년 이화 캠퍼스에 방문해 최신 GPU 아키텍처 워크숍을 진행.
- + 클라우드 서비스 · 멀티모달 LLM 분야에서는 Alibaba Cloud와 협력해 Asia-Pacific AI Fellowship 트랙을 마련. 상하이 AI 센터에서 글로벌 데이터 거버넌스 사례를 학습하고, 귀국 후 연구단 랩 실에서 중국 출 엔지니어와 공동 세미나를 이어 가며 동아시아 시장 특성에 맞는 모델 현지화 방안을 테스트.
- ✓ 이 세 갈래 교류는 “학생 파견 - 해외 멘토 초청 - 공동 커리큘럼 개발”이라는 동일한 프레임으로 설계돼 있어, 참여 인원이 어느 허브로 가든 돌아와 곧바로 수업 · Project-Lab에 교차 적용할 수 있는 구조적 호환성을 확보.

○ 물적 교류 전략

- ◆ 사람이 움직이려면 데이터 · 장비 · 인프라와 같은 자원도 함께 움직여야 하며, 아래와 같은 물적 교류를 계획.
- ◆ 데이터 · 문제 공유 플랫폼: Ewha Data Trust Hub
 - ✓ 연구단은 ‘Ewha Data Trust Hub’를 중심으로 협력 기업 · 지자체로부터 받은 로그, 영상, 센서, 단일세포 시퀀싱 데이터를 집적.
 - ✓ 각 데이터셋은 학습에 앞서 GDPR · PIPA 요구사항과 IRB 심의를 통과한 뒤 메타정보(취득 방식, 라벨 품질, 위험 등급)를 달고 내부 카탈로그에 등록.
 - ✓ 학생과 연구원은 허가된 프로젝트 범위에서 데이터 · 문제 시트를 내려 받아 바로 실험을 시작할 수 있도록 함.
- ◆ 공동 테스트베드
 - ✓ 연구단 GPU 클러스터, Jetson 엣지 장치, 측정 센서, 5G Edge GPU 팜 등 하드웨어 자산을 협력 기업이 예약제로 사용하도록 개방하고, 반대로 기업이 보유한 실물 로봇 플랫폼 · 클라우드 GPU 인스턴스도 수업 · 프로젝트 단계에서 활용할 수 있게 협의.
 - ✓ 이를 통해 연구자와 학생은 “논문상의 모델”이 실제 기기에서 얼마나 빠르고 안정적으로 동작하는지 수시로 측정하고, 기업은 재무적 부담 없이 다양한 알고리즘을 시험할 수 있도록 함.
- ◆ 파일럿 실증(PoC) 프로그램
 - ✓ 산업체 또는 지자체가 “구체적 성능 기준치”를 제시하면, 연구단은 소규모 팀을 꾸려 6~12개월 짜리 실증 프로젝트를 진행. 예를 들어 KT의 경우 “5G 보안 로그를 활용해 위협 탐지 F1 스코어를 기존 대비 15% 이상 끌어올릴 것”이라는 명확한 목표를 제시하고, 연구단은 이를 교과(통신 · 클라우드 AI 트랙)와 연결된 프로젝트-랩 과제로 등록.
 - ✓ 성능 목표를 달성하면 기업은 PoC 코드를 직접 서비스 환경에 이식하고, 연구단은 논문화 또는 특히 출원을 추진.
- ◆ 현물 · 현금 매칭 투자: Seed Grant × 기업 매칭펀드 창업 스프링보드
 - ✓ 대학이 마련한 Seed Grant(프로토타입 제작 · 법률 컨설팅 · 시장조사 지원)와 기업이 약정한 현물(HW · SW) · 현금(프로젝트 인센티브)을 짹지어 학생-기업 공동 창업팀을 지원.
 - ✓ 이 모델은 “캠퍼스 기술→산업 현장→지역사회 서비스”라는 가치사슬을 끊김 없이 이어 주는 연결 고리로 작동.

○ 대표 기업 - 교류 내용 요약 표

지역	기업·기관	과거 협력 실적 (2020-2024)	향후 협력 계획 (2025-2027)
해외	NVIDIA	• Language 모델 연구 및 인턴 파견	• GPUCluster(A100) · JetsonOrin 40대 무상 대여 • CUDA 촉진화 재직자 교육 연 50명
	Alibaba Cloud		• 클라우드 크레딧 제공
	Wordbricks	• GetGPT 노코드 플랫폼 기술 자문	• GetGPT v2 공동 개발 · 해외 파견 1명 • 미국 시장 PoC → 기술이전 1건
국내	삼성메디슨	• 의료영상데이터 제공 및 합성데이터 프라이버시 공동연구 및 인턴 파견	• 초음파 · MRI1PB 추가 기타 • 합성데이터 Metric 오픈소스 · 공동 특허 1건
	LG전자	• 로봇청소기 On-deviceAI 공동과제 2건 • 초청 세미나	• Project-Lab 2기 연속 수행(경량화 2단계) • Edge-AI Workshop 연 1회 / 인턴 파견
	현대자동차	• 물 유입 겹출 AI 업그레이드 공동과제	• AIX 컨설팅 PoC 2건 • 모빌리티 AI 트랙 현장실습, 인턴 파견
	KT AI2XL	• 초청 세미나	• Bootcamp 연 1회(재직자 100명) 유지 • SOC-기반 캡스톤 과목 신설
	NaverCloud	• HyperClova-X 음성 LLM 구축 연구	• 멀티모달 LLM 경량화 공동 연구 • VoiceLLM 보안 벤치마크 & 리더보드
	DXR	• 제조 합성 이미지 · 영상 데이터 생성 연구 및 인턴 파견	• 스마트제조 AI 트랙 데이터 확장 • Project-Lab 1건 + 특허 공동출원
	서울시AI센터		• “AIforSeoul” 지역문제 PoC 연 1건
	큐브세븐틴	• On-device 양자화 연구 인턴 파견	• 경량 모델 공동 논문 1편 계획
	프리미어ICT	• 컴퓨터비전 실무 인턴 파견	• Edge-Cloud Orchestration PoC 참여
	텔레피스	• 저전력 AI HW 개선 인턴 파견	• 공동 칩 시뮬레이션 연구 예정
국내	파수(Fasoo)	• 온디바이스 NN 양자화 인턴 파견	• AI-DRM 보안 모듈 공동 개발
	소셜엔비즈	• 병렬컴퓨터 구조 연구 인턴 파견	• GPU-CPU 협업 스케줄러 PoC
	세명장교	• On-device AI 연구 인턴 파견	• 건설 현장 안전 · AI 예측 시스템 시험
	유니유니	• 최신 CV 동향 연구 인턴 파견	• 온라인 세미나 · 공개 튜토리얼 공동 개최
	토탈체장	• 차세대 메모리-기반 시스템SW 인턴 파견	• 공정 제어 AI 모듈 데모 계획
	큐빅·하이	• 치과 영상 AI 인턴 파견	• 의료영상 세그멘테이션 합동 데이터셋 제작
	NEXUS	• LLM 적합성 분석 인턴 파견	• AI-Legal QA 서비스 공동 검증
	법무법인 대륙아주	• AI · 법률 리서치 인턴 파견	• 윤리 · 규제 White-paper 공동 발간
	시큐아이 · 이니텍		• 보안 분야 공동연구

4단계 BK21 사업

교육연구단장 연구과제 참여현황

<표 1-2> 교육연구단장 연구과제 참여 현황

연번	연구과제 정보			총 연구기간 (YYYYMMDD- YYYYMMDD)	연구비 규모(천원)		국가주도 대형 연구개발사업 해당여부 (해당 시 작성)
	사업명	협약기관	연구과제명	시작일	종료일	총 연구비	
1	집단연구사업	한국연구재단	커넥티드 자율주행 자동차를 위한 SPV(Security/Privacy/Visual) 방화벽 연구	20230601	20260228	1,375,000	500,000
2	중견연구	한국연구재단	인-네트워크 보안을 위한 인공지능 기반 의 자율 운영 라우터 설계 및 구현	20230301	20280229	978,481	195,696

4단계 BK21 사업

연구비 수주실적

<표 3-1> 최근 3년간 참여교수 중앙정부 및 해외기관 대표 연구비 수주실적

<표 3-1> 최근 3년간 참여교수 중앙정부 및 해외기관 대표 연구비 수주실적

<표 3-1> 최근 3년간 참여교수 중앙정부 및 해외기관 대표 연구비 수주실적

<표 3-1> 최근 3년간 참여교수 중앙정부 및 해외기관 대표 연구비 수주실적

<표 3-1> 최근 3년간 참여교수 중앙정부 및 해외기관 대표 연구비 수주실적

<표 3-1> 최근 3년간 참여교수 중앙정부 및 해외기관 대표 연구비 수주실적

<표 3-1> 최근 3년간 참여교수 중앙정부 및 해외기관 대표 연구비 수주실적

<표 4-1> 최근 3년간 참여교수 국내 및 해외 산업체, 지자체 대표 연구비 수주실적

<표 4-1> 최근 3년간 참여교수 국내 및 해외 산업체, 지자체 대표 연구비 수주실적

4단계 BK21 사업

대표연구업적물

<표 3-2> 최근 5년간 참여교수 대표연구업적물 실적

연번	참여 교수명	연구자 등록번호	이공계열/ 인문사회계열	세부 전공분야	대표 연구 업적물 분야	업적물 종류	대표연구업적물 상세내용	키워드	
								한글	영문

대표연구업적물의 우수성

4	노준혁	11436386	이공계열	인공지능(지각 /인식)	학술대회 논문	1	Wonho Bae, Junhyug Noh, Gunhee Kim	약지도 학습	Weakly Supervised Learning
						2	Rethinking Class Activation Mapping for Weakly Supervised Object Localization	객체 위치 추정	Object Localization
						3	European Conference on Computer Vision (ECCV)	클래스 활성화 맵	Class Activation Mapping
						4	European Computer Vision Association (ECVA)	설명가능 인공지능	Explainable AI
						5			
						6	1		
						7	2020.10		
						8	10.1007/978-3-030-58555-6_37		

□ 연구목표

- 약지도 객체 위치추정(WSOL) 문제 해결을 위한 Class Activation Mapping 기반 접근을 분석함.
- 기존 CAM 기반 방법론이 가지는 구조적 한계 세 가지 식별: ① GAP의 작은 활성화 영역 채널에 대한 과도한 가중치, ② 객체 내부의 음수 활성화, ③ 최대값 기반 thresholding의 불안정성.
- 위 한계를 해결하기 위해 세 가지 단순하지만 강력한 개선 기법 제안: ① Thresholded Average Pooling, ② Negative Weight Clamping, ③ Percentile 기반 Thresholding.

우수성 및 사업단 목표와의 연관성

- CAM 기반 WSOL 파이프라인의 근본적 한계를 분석하고, TAP, NWC, PaS 세 가지 모듈 교체만으로 구조 변경 없이 CUB2002011, ImageNet1K, OpenImages30K 세 벤치마크의 Top1Loc를 최대+14.18p 개선하며 새로운 SOTA를 달성함.
- 연산 오버헤드가 거의 없고 다양한 백본과 호환돼 효율적(R)-진화형(E) AI 구현에 적합함.
- 제안한 방법론은 신뢰성(T) 확보를 위한 모델 해석 도구로도 활용 가치가 높음.
-

연번	참여 교수명	연구자 등록번호	이공계열/ 인문사회계열	세부 전공분야	대표 연구 업적물 분야	업적물 종류	대표연구업적물 상세내용	키워드	
								한글	영문
대표연구업적물의 우수성									
5	노준혁	11436386	이공계열	시각정보처리	인공지능(응용)	학술지 논문	1	Junhyug Noh, Sun Young Park, Wonho Bae, Kangil Kim, Jang-Hee Cho, Jong Soo Lee, Shin-Wook Kang, Yong-Lim Kim, Yon Su Kim, Chun Soo Lim, Jung Pyo Lee, Kyung Don Yoo	조기 사망 예측
							2	Predicting Early Mortality in Hemodialysis Patients: A Deep Learning Approach Using a Nationwide Prospective Cohort in South Korea	신대체요법
							3	Scientific reports	Renal Replacement Therapy
							4	14(1), 29658	Clinical Risk Modeling
							5	2045-2322	Hemodialysis
							6	1	혈액투석
							7	2024.11	
							8	10.1038/s41598-024-80900-6	

□ 연구목표

- 한국 HD 코호트 데이터를 바탕으로 신대체요법 초기 환자의 조기 사망률을 예측하는 딥러닝 기반 모델을 제안함.
 - 사망에 이르기까지 시간의 흐름에 따른 심혈관 사건의 발생률과 패턴을 분석함.
 - 표준 통계모델(로지스틱, 라쏘, 릿지)뿐 아니라 딥러닝 모델을 활용해 생존률 예측 정확도 비교 및 향상을 확인함.
 - 다양한 임상적, 생화학적 특성(약 80개 변수)을 조합하여 조기 사망 고위험군을 정밀 예측함.

우수성 및 사업단 목표와의 연관성

- 대규모 전국 단위 코호트(약 6,000명 이상)를 기반으로 한 딥러닝 모델 개발 및 검증함.
 - 단일 시점의 예측이 아닌, 치료 초기의 시간 가변적 이벤트 데이터를 반영해 모델의 현실성을 높임.
 - 다변량 기반 위험인자 해석을 통해 XAI 기반의 해석 가능성도 확보함.

연번	참여 교수명	연구자 등록번호	이공계열/인문사회계열	세부 전공분야	대표 연구업적물 분야	업적물 종류	대표연구업적물 상세내용	키워드		
								한글	영문	
대표연구업적물의 우수성										
14	배호	11635105	이공계열	기계학습및지식처리	정보보안	학술대회 논문	1	Dahuin Jung, Dongjin Lee, Sunwon Hong, Hyemi Jang, Ho Bae, Sungroh Yoon	연속 학습	Continual learning
							2	New Insights for the Stability-Plasticity Dilemma in Online Continual Learning	안전성-유연성 딜레마	Stability-plasticity dilemma
							3	International Conference on Learning Representations (ICLR)	온라인 지속 학습	Online Continual Learning
							4	-	다중 스케일 피처 적응 네트워크	Multi-scale feature adaptation network(MuFAN)
							5	-	구조별 지식 종류 손실	Structure-wise distillation loss
							6	0		
							7	2023.05		
							8	https://doi.org/10.48550/arXiv.2302.08741		

□ 연구목표

- Continual learning(CL)은 데이터가 엄격하게 스트리밍 방식으로 제공되기 때문에 단일 데이터 포인트로부터 얻을 수 있는 훈련 신호가 제한적이어서 오프라인 계속 학습에 비해 온라인 계속 학습의 유연성이 취약함.
 - 본 논문은 CL의 안정성과 유연성 사이의 딜레마를 극복하기 위해 'multi-scale feature adaptation network (MuFAN)'라는 online CL 프레임워크를 제안하였음.
 - MuFAN은 사전 훈련된 네트워크의 다양한 수준에서 추출한 풍부한 컨텍스트 인코딩을 활용함.

우수성 및 사업단 목표와의 연관성

- 온라인 지속 학습에서 안정성과 유연성 간의 딜레마를 극복하기 위한 혁신적인 MuFAN 프레임워크를 제안하며, 뛰어난 안정성과 유연성을 동시에 유지할 수 있음을 입증함.
 - 또한, structure-wise distillation loss를 도입하고 일반적인 배치 정규화 레이어를 대체하는 'stability-plasticity normalization module'을 제안하여 MuFAN을 훈련하여 높은 유연성과 안정성을 동시에 유지함. 이에 보안 분야 최우수 학회인 RAID(IF: 24.75)에 개제되었다.

연번	참여 교수명	연구자 등록번호	이공계열/인문사회계열	세부 전공분야	대표 연구 업적물 분야	업적물 종류	대표연구업적물 상세내용	키워드	
								한글	영문
대표연구업적물의 우수성									
15	양대현	10116341	이공계열	인공지능시스템 및 응용	정보보안	학술대회 논문	1	Sian Kim, Changhun Jung, RhongHo Jang, David Mohaisen, DaeHun Nyang	스케치
							2	A Robust Counting Sketch for Data Plane Intrusion Detection	인-네트워크
							3	Network and Distributed System Security (NDSS 2023)	In-network
							4	Internet Society	트래픽 분포
							5	-	Intrusion Detection System
							6	1	
							7	2023.03	
							8	10.14722/ndss.2023.23102	

연번	참여 교수명	연구자 등록번호	이공계열/인문사회계열	세부 전공분야	대표 연구업적물 분야	업적물 종류	대표연구업적물 상세내용	키워드		
								한글	영문	
대표연구업적물의 우수성										
21	오유란	11812138	이공계열	인공지능시스템 및 응용	인공지능(지각 /인식)	학술대회 논문	1	Suhyun Kim, Semin Lee, Kyungok Kim, Uran Oh	만화	Comics
							2	Utilizing a dense video captioning technique for generating image descriptions of comics for people with visual impairments	이미지 설명	Image Description
							3	Proceedings of the 29th International Conference on Intelligent User Interfaces (IUI 2024)	고밀도 비디오 자막 생성	Dense Video Captioning
							4	Association for Computing Machinery (ACM)	People with Visual Impairments	
							5		시각장애인	
							6	1		
							7	2024.03		
							8	10.1145/3640543.3645154		

□ 연구 목표

- 기존 시각자료의 접근성 향상을 위해 수행되었던 이미지의 대체텍스트를 자동으로 생성하는 다수의 연구들을 만화에 적용할 경우, 비슷한 장면이 연어이 등장하기 때문에 동일하거나 비슷한 설명이 중복되는 문제가 있음.
 - 또한, 매 컷에 대해 각각 이미지해설을 생성할 경우, 앞뒤 맥락정보를 잃게 됨.
 - 본 연구는 dense video captioning이라는 비디오 내에서 시공간적으로 이벤트를 로컬라이징하고 이에 대한 캡션을 생성하는 기술을 활용하여 만화를 위한 이미지 해설 생성에 특화된 모델을 새롭게 제안함.

우수성 및 사업단 목표와의 연관성

- 정적인 만화의 각 장면을 여러 장의 프레임으로 변환하여 매 회당 하나의 동적인 비디오를 생성한 뒤, 비디오 캡션 생성을 위한 기술을 적용했다는 점에서 큰 차별성을 가짐.
 - 실제 시각장애인을 대상으로 사용성 평가를 했을 때, 제안하는 방법으로 생성된 설명이 정확성, 명확성, 이해 가능성, 길이, 정보성 면에서 기존 방법보다 더 향상되었음을 확인함.
 - 한국정보과학회 우수국제학술대회 중 하나인 ACM IUI에 발표되었고, Best Paper Award를 수상하였음.

연번	참여 교수명	연구자 등록번호	이공계열/인문사회계열	세부 전공분야	대표 연구 업적물 분야	업적물 종류	대표연구업적물 상세내용	키워드	
								한글	영문
대표연구업적물의 우수성									
34	황의원	11462992	이공계열	컴퓨터/인공지능	인공지능(기반 및 학습/추론)	학술대회 논문	1	Jonghyun Lee, Dahuin Jung, Saehyung Lee, Junsung Park, Juhyeon Shin, Uiwon Hwang, Sungroh Yoon	테스트 시간 적응
							2	Entropy is not Enough for Test-time Adaptation: From the Perspective of Disentangled Factors	엔트로피
							3	International Conference on Learning Representations (ICLR)	특징 분리
							4	International Conference on Learning Representations (ICLR)	Feature Disentanglement
							5		허위 상관
							6	1	Spurious Correlation
							7	2024.05	강건성
							8		Robustness

<표 3-3>최근 5년간 참여교수 대표연구업적물의 적합성

연번	참여 교수명	연구자 등록번호	이공계열/인문사회계열	세부 전공분야	대표 연구 업적물 분야	업적물 종류	대표연구업적물 상세내용	키워드	
								한글	영문
대표연구업적물의 적합성									
3	노준혁	11436386	이공계열	시각정보처리	인공지능(지각/인식)	학술대회 논문	1	Jinhwan Seo, Wonho Bae, Danica J Sutherland, Junhyug Noh, Daijin Kim	약지도 학습 Weakly Supervised Learning
							2	Object Discovery via Contrastive Learning for Weakly Supervised Object Detection	물체 검출 Object Detection
							3	European Conference on Computer Vision (ECCV)	대조 학습 Contrastive Learning
							4	European Computer Vision Association (ECVA)	자기감독학습 Self-supervised Learning
							5		표현 학습 Representation Learning
							6	1	
							7	2022.10	
							8	10.1007/978-3-031-19821-2_18	

연번	참여 교수명	연구자 등록번호	이공계열/인문사회계열	세부 전공분야	대표 연구 업적물 분야	업적물 종류	대표연구업적물 상세내용	키워드		
								한글	영문	
대표연구업적물의 적합성										
6	민동보	10190916	이공계열	시각정보처리	인공지능(지각/인식)	학술대회 논문	1	Seungmin Baek, Soyul Lee, Hayeon Jo, Hyesong Choi, and Dongbo Min	다중작업 학습	Multi-task Learning
							2	TADFormer: Task-Adaptive Dynamic Transformer for Efficient Multi-Task Learning	파라미터 효율적인 미세조정	Parameter Efficient Fine-Tuning
							3	IEEE Conference on Computer Vision and Pattern Recognition (CVPR)	작업 프롬프트	Task Prompt
							4	Institute of Electrical and Electronics Engineers (IEEE)	동적 작업 필터링	Dynamic Task Filter
							5			
							6	1		
							7	2025.06		
							8			

연번	참여 교수명	연구자 등록번호	이공계열/ 인문사회계열	세부 전공분야	대표 연구 업적물 분야	업적물 종류	대표연구업적물 상세내용	키워드																																
								한글	영문																															
	대표연구업적물의 적합성																																							
11	반효경	10091721	이공계열	인공지능시스템 및 응용	컴퓨터시스템 / 처리	학술지 논문	<table border="1"> <tr><td>1</td><td>Jeongha Lee, Soojung Lim, Hyokyung Bahn</td><td>데이터 접근 패턴</td><td>Data access pattern</td></tr> <tr><td>2</td><td>Analyzing Data Access Characteristics of AIoT Workloads for Efficient Write Buffer Management</td><td>모바일 사물 인공지능</td><td>Mobile AIoT</td></tr> <tr><td>3</td><td>IEEE Internet of Things Journal</td><td>버퍼 관리</td><td>Buffer management</td></tr> <tr><td>4</td><td>Early Access, pp. 1-14</td><td>LRU 알고리즘</td><td>LRU algorithm</td></tr> <tr><td>5</td><td>2327-4662</td><td>루프 패턴</td><td>Loop pattern</td></tr> <tr><td>6</td><td></td><td></td><td></td></tr> <tr><td>7</td><td>2025</td><td></td><td></td></tr> <tr><td>8</td><td>10.1109/JIOT.2025.3573759</td><td></td><td></td></tr> </table>	1	Jeongha Lee, Soojung Lim, Hyokyung Bahn	데이터 접근 패턴	Data access pattern	2	Analyzing Data Access Characteristics of AIoT Workloads for Efficient Write Buffer Management	모바일 사물 인공지능	Mobile AIoT	3	IEEE Internet of Things Journal	버퍼 관리	Buffer management	4	Early Access, pp. 1-14	LRU 알고리즘	LRU algorithm	5	2327-4662	루프 패턴	Loop pattern	6				7	2025			8	10.1109/JIOT.2025.3573759			
1	Jeongha Lee, Soojung Lim, Hyokyung Bahn	데이터 접근 패턴	Data access pattern																																					
2	Analyzing Data Access Characteristics of AIoT Workloads for Efficient Write Buffer Management	모바일 사물 인공지능	Mobile AIoT																																					
3	IEEE Internet of Things Journal	버퍼 관리	Buffer management																																					
4	Early Access, pp. 1-14	LRU 알고리즘	LRU algorithm																																					
5	2327-4662	루프 패턴	Loop pattern																																					
6																																								
7	2025																																							
8	10.1109/JIOT.2025.3573759																																							
							<ul style="list-style-type: none"> - 최근 모바일 GPU의 급격한 발전으로 온디바이스 딥러닝 학습 및 추론이 급부상하고 있으며, 본 논문은 이러한 상황에서 AIoT 워크로드의 특성을 규명하고 이를 효율적으로 관리하기 위한 연구를 수행하여, 본 사업단의 연구주제에 부합한다고 할 수 있음. - 특히, 연산 자원뿐 아니라 스토리지 자원의 효율적인 관리가 중요한 이슈로 떠오르는 상황에서 AIoT 워크로드의 쓰기 중심 파일 접근 특성 및 복합 루프 패턴을 분석하고 이를 효율적으로 관리하는 버퍼 정책을 통해 큰 폭의 성능 개선 효과를 얻음. 																																	

연번	참여 교수명	연구자 등록번호	이공계열/ 인문사회계열	세부 전공분야	대표 연구 업적물 분야	업적물 종류	대표연구업적물 상세내용	키워드																																	
								한글	영문																																
	대표연구업적물의 적합성																																								
13	배호	11635105	이공계열	기계학습및지 식처리	정보보안	학술대회 논문	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 5%;">1</td><td>Hyunjun Kim, Yungi Cho, Younghan Lee, Ho Bae, Yunheung Paek</td><td>클러스터링 된 연합학습</td><td>Clustered Federated Learning</td></tr> <tr> <td>2</td><td>Exploring Clustered Federated Learning's Vulnerability against Property Inference Attack</td><td>속성 추론 공격</td><td>Property Inference Attack</td></tr> <tr> <td>3</td><td>Research in Attacks, Intrusions and Defenses (RAID)</td><td>차등정보보호</td><td>Differential Privacy</td></tr> <tr> <td>4</td><td>236-249</td><td>개인 정보 누출 위험</td><td>Privacy Leakage Risk</td></tr> <tr> <td>5</td><td>9798400707650</td><td>비독립적이며 동일하게 분포되지 않은 데이터</td><td>Non-IID(Non-Independently and Identically Distributed data)</td></tr> <tr> <td>6</td><td>0</td><td></td><td></td></tr> <tr> <td>7</td><td>2023.10</td><td></td><td></td></tr> <tr> <td>8</td><td>https://doi.org/10.1145/3607199.3607218</td><td></td><td></td></tr> </table>	1	Hyunjun Kim, Yungi Cho, Younghan Lee, Ho Bae, Yunheung Paek	클러스터링 된 연합학습	Clustered Federated Learning	2	Exploring Clustered Federated Learning's Vulnerability against Property Inference Attack	속성 추론 공격	Property Inference Attack	3	Research in Attacks, Intrusions and Defenses (RAID)	차등정보보호	Differential Privacy	4	236-249	개인 정보 누출 위험	Privacy Leakage Risk	5	9798400707650	비독립적이며 동일하게 분포되지 않은 데이터	Non-IID(Non-Independently and Identically Distributed data)	6	0			7	2023.10			8	https://doi.org/10.1145/3607199.3607218				
1	Hyunjun Kim, Yungi Cho, Younghan Lee, Ho Bae, Yunheung Paek	클러스터링 된 연합학습	Clustered Federated Learning																																						
2	Exploring Clustered Federated Learning's Vulnerability against Property Inference Attack	속성 추론 공격	Property Inference Attack																																						
3	Research in Attacks, Intrusions and Defenses (RAID)	차등정보보호	Differential Privacy																																						
4	236-249	개인 정보 누출 위험	Privacy Leakage Risk																																						
5	9798400707650	비독립적이며 동일하게 분포되지 않은 데이터	Non-IID(Non-Independently and Identically Distributed data)																																						
6	0																																								
7	2023.10																																								
8	https://doi.org/10.1145/3607199.3607218																																								
							<ul style="list-style-type: none"> - 본 논문은 클러스터 연합 학습 기법의 취약점을 탐구하며, 특히 속성 추론 공격에 대한 취약성을 분석하고 있음. - 이는 분산 학습 환경에서 발생할 수 있는 정보 유출 위험을 다루고 있으며, 클러스터링을 통해 데이터의 유사성을 높이는 과정에서 발생할 수 있는 프라이버시 문제를 심층적으로 연구하였음. - BK21 본 사업단의 목표 중 하나인 사이버 보안 강화와 직접적으로 관련이 있으며, 특히 연합 학습과 같은 최신 기술의 보안성을 개선하는데 기여할 수 있다. 더불어, 차분 프라이버시를 이용한 정보 유출 방어 기법을 제안하며, 이를 통해 높은 수준의 보안성과 모델 성능 간의 균형을 달성하고자 함. 																																		

연번	참여 교수명	연구자 등록번호	이공계열/ 인문사회계열	세부 전공분야	대표 연구 업적물 분야	업적물 종류	대표연구업적물 상세내용	키워드	
								한글	영문
	대표연구업적물의 적합성								
21	오유란	11812138	이공계열	인공지능시스템 및 응용	인공지능(지각 /인식)	학술대회 논문	1	Suhyun Kim, Semin Lee, Kyungok Kim, Uran Oh	만화 Comics
							2	Utilizing a dense video captioning technique for generating image descriptions of comics for people with visual impairments	이미지 설명 Image Description
							3	Proceedings of the 29th International Conference on Intelligent User Interfaces (IUI 2024)	고밀도 비디오 자막 생성 Dense Video Captioning
							4	Association for Computing Machinery (ACM)	시각장애인 People with Visual Impairments
							5		
							6	1	
							7	2024.03	
							8	10.1145/3640543.3645154	X
							- 보안이 중요한 시나리오에서 학습 데이터를 공개하지 않고 학습된 모델만을 이용하여 도메인 적응이 가능함. - 사전지식이 부족한 실세계 데이터에 대해서도 데이터 기반의 특징 증강이 가능하며, 무한한 수의 증강을 유한한 시간에 계산 가능하도록 근사하는 이론적 기반을 제공함. - 인공지능 모델이 학습하는 특징들을 표현공간 상에서 분리함으로써 강건하고 해석 가능한 인공지능 모델 개발에 활용될 수 있음.		

4단계 BK21 사업

기타연구업적물
특허, 기술이전, 창업 실적

<표 4-2>최근 5년간 이공계열 참여교수 특허, 기술이전, 창업 실적

연번	참여교수명	연구자등록 번호	업적물 분야	실적구분	특허, 기술이전, 창업 상세내용		키워드	
							한글	영문
특허, 기술이전, 창업 실적의 우수성								
1	양대현	10116341	정보보안	특허	1	백성하, 양대현	랜섬웨어 감지 시스템	Ransomware Detection System
					2	랜섬웨어의 패턴인식과 매직 넘버를 이용한 랜섬웨어 감지 시스템	NAND 플래시 메모리 기반 SSD	NAND Flash Memory-base SSD
					3	대한민국	매직넘버	Magic Number
					4	1025727700000	파일 덮어쓰기 모니터링	File Overwrite Monitoring
					5	202309	랜섬웨어 활동 탐지	Ransomware Activity Detection
					<p>1. 특허 개요 - NAND 플래시 메모리 기반 SSD 내부에서 랜섬웨어의 활동을 탐지하여, 랜섬웨어를 방어할 수 있는 랜섬웨어의 패턴인식과 매직넘버를 이용한 랜섬웨어 감지 시스템에 관한 것</p> <p>2. 특허의 차별성 - 사용자가 백신 소프트웨어를 설치하지 않았더라도, 또한 운영 체제의 종류에 상관 없이, 랜섬웨어를 탐지하여 공격에 방어할 수 있는 기술이라는 점에서 혁신적</p>			

연번	참여교수명	연구자등록 번호	업적물 분야	실적구분	특허, 기술이전, 창업 상세내용		키워드	
							한글	영문
특허, 기술이전, 창업 실적의 우수성								
4	반효경	10091721	컴퓨터·소프트웨어 기반 융합	기술이전	1	반효경, 이도영	소셜 네트워크	SNS
					2	소셜 네트워크 서비스에서 사용자의 활동을 식별하고 표시하는 방법	스마트폰	Smartphone
					3	(주)더블에이치컴퍼레이션	상태	Status
					4	5,500,000	센서	Sensor
					5	2024.04	메신저	Messenger
					<p>1. 기술개요</p> <ul style="list-style-type: none"> - 스마트폰의 앱 동작 로그·센서 데이터를 실시간 분석해 '취침·운전·도보·영화 감상' 등 사용자의 활동 상태를 자동 추론 - 추론 결과를 SNS·메신저 상태 메시지로 연동하여 상대방에게 현재 활동 맥락(Context) 을 직관적으로 표시 <p>2. 기술의 차별성</p> <ul style="list-style-type: none"> - 사용자가 상태를 수동 갱신하지 않아도 센서·앱 히스토리 기반 자동 업데이트 제공 - 상대방이 사용자 상태를 즉시 인지해 비동기 커뮤니케이션 적절성(예: 운전 중 메시지 알림 지연) 향상 			

4단계 BK21 사업

첨부자료

[첨부 1]2025년도 신청학과 소속 전체 교수 현황

연번	연구자 등록번호	성명		직급	원소속 정보		신청학과 정보		세부전공 분야	이공계열/ 인문사회 계열	특정 분야	대표 연구업적물 제출 요구량	대표 연구업적물 분야	내국인/ 외국인	신임/ 기존	사업 참여 여부	참여 요건 확인	비고
		한글	영문		대학명	학과명	신청학과명	전임/ 겸임										
1	12961764	김종길	Jongkil Kim	부교수	이화여자대학교	사이버보안학과	인공지능소프트웨어학부	겸임	정보보호	이공계열		3	정보보안 정보보안 정보보안	내국인	신임	참여	O	
2	11436386	노준혁	Junhyung Noh	조교수	이화여자대학교	인공지능데이터사이언스학부	인공지능소프트웨어학부	겸임	시각정보처리	이공계열		3	인공지능(지각/인식) 인공지능(지각/인식) 인공지능(응용)	내국인	신임	참여	O	
3	10190916	민동보	Dongbo Min	부교수	이화여자대학교	컴퓨터공학과	인공지능소프트웨어학부	겸임	시각정보처리	이공계열		3	인공지능(지각/인식) 인공지능(기반 및 학습/추론) 인공지능(지각/인식)	내국인	기존	참여	O	
4	10091721	반효경	Hyokyung Bahn	정교수	이화여자대학교	컴퓨터공학과	인공지능소프트웨어학부	겸임	인공지능시스템및 응용	이공계열		3	컴퓨터시스템/처리 컴퓨터시스템/처리 컴퓨터시스템/처리	내국인	기존	참여	O	
5	11635105	배호	Ho Bae	조교수	이화여자대학교	사이버보안학과	인공지능소프트웨어학부	겸임	기계학습및지식처리	이공계열		3	정보보안 정보보안 정보보안	내국인	기존	참여	O	
6	10116341	양대현	DAEHWI NYAN	정교수	이화여자대학교	사이버보안학과	인공지능소프트웨어학부	겸임	인공지능시스템및 응용	이공계열		3	정보보안 정보보안 정보보안	내국인	기존	참여	O	
7	12880629	오세은	Se Eun Oh	조교수	이화여자대학교	컴퓨터공학과	인공지능소프트웨어학부	겸임	인공지능시스템및 응용	이공계열		3	인공지능(응용) 정보보안 정보보안	내국인	신임	참여	O	
8	11812138	오유란	Uran Oh	부교수	이화여자대학교	컴퓨터공학과	인공지능소프트웨어학부	겸임	인공지능시스템및 응용	이공계열		3	인공지능(지각/인식) 인공지능(응용) 인공지능(응용)	내국인	기존	참여	O	
9	11089187	윤명국	Yoon, Myung Kuk	조교수	이화여자대학교	컴퓨터공학과	인공지능소프트웨어학부	겸임	프로세서및 분산/병렬컴퓨터구조	이공계열		3	컴퓨터시스템/처리 컴퓨터시스템/처리 컴퓨터시스템/처리	내국인	기존	참여	O	

연번	연구자 등록번호	성명		직급	원소속 정보		신청학과 정보		세부전공 분야	이공계열/ 인문사회 계열	특정 분야	대표 연구업적물 제출 요구량	대표 연구업적물 분야	내국인/ 외국인	신임/ 기존	사업 참여 여부	참여 요건 확인	비고
		한글	영문		대학명	학과명	신청학과명	전임/ 겸임										
10	11564062	이지영	Jiyoun g Lee	조교 수	이화여자대학교	인공지능데 이터사이언 스학부	인공지능소 프트웨어학 부	겸임	인공지능 시스템및 응용	이공계열		3	인공지능(지각/인식) 인공지능(기반 및 학습/추론) 인공지능(지각/인식)	내국인	신임	참여	O	
11	11091991	이형준	HyungJ une Lee	정교 수	이화여자대학교	컴퓨터공 학과	인공지능소 프트웨어학 부	겸임	인공지능 시스템및 응용	이공계열		3	인공지능(기반 및 학습/추론) 인공지능(응용) 인공지능(응용)	내국인	기존	참여	O	
12	11462992	황의원	Uiwon Hwang	조교 수	이화여자대학교	컴퓨터공 학과	인공지능소 프트웨어학 부	겸임	컴퓨터 /인공지 능	이공계열		3	인공지능(기반 및 학습/추론) 인공지능(기반 및 학습/추론) 인공지능(기반 및 학습/추론)	내국인	신임	참여	O	

전체 교수 수	전체 교수 수	12	기존 교수 수 (참여교수)	전체 교수 수	7	신임교수 수 (참여교수)	전체 교수 수	5
	전임교수 수	0		전임교수 수	0		전임교수 수	0
	겸임교수 수	12		겸임교수 수	7		겸임교수 수	5
전체 참여교수 수	전체 교수 수	12	이공계열 교수 수 (참여교수)	전체 교수 수	12	인문사회계열 교수 수 (참여교수)	전체 교수 수	0
	전임교수 수	0		신임교수 수	5		신임교수 수	0
	겸임교수 수	12		기존교수 수	7		기존교수 수	0

구분	신임교수 실적 포함 여부		
			미포함
최대 제출 건수	<표 2-1> 우주 분야 문제해결을 위한 참여교수의 교육역량 대표실적	6	4
	<표 3-1> 최근 3년간 참여교수 중앙정부 및 해외기관 대표 연구비 수주실적	12	7
	<표 3-5> 최근 5년간 참여교수 국제공동연구 실적		
	<표 4-1> 최근 3년간 참여교수 국내 및 해외 산업체, 지자체 대표 연구비 수주실적		7
	<표 4-2> 최근 5년간 이공계열 참여교수 특허, 기술이전, 창업 실적	12	
	<표 4-3> 최근 5년간 참여교수 (지역)산업문제 해결 대표실적	12	7

[첨부 2] 2025년도 참여교수의 지도학생 현황

기준일	대학명	신청학과명	성명		학번	생년 (YYYY)	외국인/ 내국인	학위과정			사업 참여 여부	지도교수 성명	비고
			한글	영문				과정	재학 학기 수	수료 여부			
접수마감일	이화여자대학교	인공지능소프트웨어학부	김가영	GaYoung Kim	252AIG 01	2001	내국인	석사	1	재학	참여	양대현	
접수마감일	이화여자대학교	인공지능소프트웨어학부	김지연	JiYeon Kim	242AIG 07	2001	내국인	석사	3	재학	참여	양대현	
접수마감일	이화여자대학교	인공지능소프트웨어학부	배윤주	YunJu Bae	242AIG 30	2000	내국인	석사	2	재학	참여	양대현	
접수마감일	이화여자대학교	인공지능소프트웨어학부	최정혜	JungHye Choi	232AIG 48	1999	내국인	석사	4	수료	참여	양대현	
접수마감일	이화여자대학교	인공지능소프트웨어학부	김시안	Sian Kim	22AIG0 6	1996	내국인	박사	6	재학	참여	양대현	
접수마감일	이화여자대학교	인공지능소프트웨어학부	김연희	Yeonhee Kim	241AIG 01	1997	내국인	박사	3	재학	참여	김종길	
접수마감일	이화여자대학교	인공지능소프트웨어학부	불루마티페 알리맛	Oshunlola, Boluwatife Alimat	242AIG 25	2001	외국인	석사	2	재학	참여	김종길	
접수마감일	이화여자대학교	인공지능소프트웨어학부	엘라 드제 비	Djebbi, Ella	221AIG 03	1995	외국인	박사	6	재학	참여	김종길	
접수마감일	이화여자대학교	인공지능소프트웨어학부	김보은	Boeun Kim	232AIG 37	1999	내국인	석사	4	재학	참여	김종길	

기준일	대학명	신청학과명	성명		학번	생년 (YYYY)	외국인/ 내국인	학위과정			사업 참여 여부	지도교수 성명	비고
			한글	영문				과정	재학 학기 수	수료 여부			
접수마감일	이화여자대학교	인공지능소프트웨어학부	박지민	Jimin Park	242AIG 12	2000	내국인	석사	3	재학	참여	오세은	
접수마감일	이화여자대학교	인공지능소프트웨어학부	김보나	Bona Kim	242AIG 05	1997	내국인	석사	3	재학	참여	오세은	
접수마감일	이화여자대학교	인공지능소프트웨어학부	전혜승	Haeseung Jeon	242AIG 35	2001	내국인	석사	2	재학	참여	오세은	
접수마감일	이화여자대학교	인공지능소프트웨어학부	박정민	Jungmin Park	252AIG 06	1996	내국인	석사	1	재학	참여	오세은	
접수마감일	이화여자대학교	인공지능소프트웨어학부	홍세연	Saeyeon Hong	252AIG 20	1999	내국인	석사	1	재학	참여	오세은	
접수마감일	이화여자대학교	인공지능소프트웨어학부	한소현	Sohyun Han	252AIG 19	1997	내국인	석사	1	재학	참여	오세은	
접수마감일	이화여자대학교	인공지능소프트웨어학부	김정인	Jeongin Kim	242AIG 06	1999	내국인	석박사통 합	3	재학	참여	노준혁	
접수마감일	이화여자대학교	인공지능소프트웨어학부	정이진	Egene Chung	250AIG 07	2000	내국인	석박사통 합	1	재학	참여	노준혁	
접수마감일	이화여자대학교	인공지능소프트웨어학부	이정현	Junghyun Lee	250AIG 06	1985	내국인	석박사통 합	1	재학	참여	노준혁	

기준일	대학명	신청학과명	성명		학번	생년 (YYYY)	외국인/ 내국인	학위과정			사업 참여 여부	지도교수 성명	비고
			한글	영문				과정	재학 학기 수	수료 여부			
접수마감일	이화여자대학교	인공지능소프트웨어학부	김현서	Hyunseo Kim	242AIG 09	2001	내국인	석사	3	재학	참여	노준혁	
접수마감일	이화여자대학교	인공지능소프트웨어학부	고서연	Seoyeon Ko	242AIG 02	1999	내국인	석사	3	재학	참여	노준혁	
접수마감일	이화여자대학교	인공지능소프트웨어학부	송민경	Mingyeong Song	252AIG 11	2001	내국인	석사	1	재학	참여	노준혁	
접수마감일	이화여자대학교	인공지능소프트웨어학부	김수민	Soomin Kim	252AIG 04	1999	내국인	석사	1	재학	참여	노준혁	
접수마감일	이화여자대학교	인공지능소프트웨어학부	김정원	Jungwon Kim	240AIG 02	2000	내국인	석사	3	재학	참여	민동보	
접수마감일	이화여자대학교	인공지능소프트웨어학부	윤지원	Jiwon Yoon	242AIG 32	2001	내국인	석사	2	재학	참여	민동보	
접수마감일	이화여자대학교	인공지능소프트웨어학부	김다은	Daeun Kim	240AIG 04	2000	내국인	석박사통합	2	재학	참여	민동보	
접수마감일	이화여자대학교	인공지능소프트웨어학부	소예림	Yerim So	250AIG 03	2000	내국인	석박사통합	1	재학	참여	민동보	
접수마감일	이화여자대학교	인공지능소프트웨어학부	김지영	Jiyeong Kim	210AIG 01	1999	내국인	석박사통합	8	재학	참여	민동보	

기준일	대학명	신청학과명	성명		학번	생년 (YYYY)	외국인/ 내국인	학위과정			사업 참여 여부	지도교수 성명	비고
			한글	영문				과정	재학 학기 수	수료 여부			
접수마감일	이화여자대학교	인공지능소프트웨어학부	백승민	Seungmin Beak	240AIG 03	1999	내국인	석박사통합	3	재학	참여	민동보	
접수마감일	이화여자대학교	인공지능소프트웨어학부	고주은	Jueun Ko	230AIG 05	2000	내국인	석사	4	재학	참여	민동보	
접수마감일	이화여자대학교	인공지능소프트웨어학부	김수민	Soomin Kim	230AIG 06	2000	내국인	석사	4	재학	참여	민동보	
접수마감일	이화여자대학교	인공지능소프트웨어학부	최혜송	Hyesong Choi	202CPG 04	1997	내국인	석박사통합	9	재학	참여	민동보	
접수마감일	이화여자대학교	인공지능소프트웨어학부	박혜원	Hyewon Park	230AIG 08	1997	내국인	석사	4	재학	참여	민동보	
접수마감일	이화여자대학교	인공지능소프트웨어학부	이소율	Soyul Lee	230AIG 11	2000	내국인	석사	4	재학	참여	민동보	
접수마감일	이화여자대학교	인공지능소프트웨어학부	지현진	Hyeonjin Jee	231AIG 04	1997	내국인	박사	3	재학	참여	반효경	
접수마감일	이화여자대학교	인공지능소프트웨어학부	이정하	Jeongha Lee	220AIG 01	1996	내국인	석박사통합	7	재학	참여	반효경	
접수마감일	이화여자대학교	인공지능소프트웨어학부	권가현	Gahyeon Kwon	250AIG 01	2001	내국인	석박사통합	1	재학	참여	반효경	

기준일	대학명	신청학과명	성명		학번	생년 (YYYY)	외국인/ 내국인	학위과정			사업 참여 여부	지도교수 성명	비고
			한글	영문				과정	재학 학기 수	수료 여부			
접수마감일	이화여자대학교	인공지능소프트웨어학부	정은수	Eunsoo Jung	242AIG 21	2000	내국인	석사	3	재학	참여	윤명국	
접수마감일	이화여자대학교	인공지능소프트웨어학부	이지영	JiYeong Yi	242AIG 18	1998	내국인	석사	3	재학	참여	윤명국	
접수마감일	이화여자대학교	인공지능소프트웨어학부	이제인	Jane Rhee	242AIG 33	2001	내국인	석사	2	재학	참여	윤명국	
접수마감일	이화여자대학교	인공지능소프트웨어학부	김선우	Sunwoo Kim	242AIG 27	2001	내국인	석사	2	재학	참여	윤명국	
접수마감일	이화여자대학교	인공지능소프트웨어학부	정은비	Eunbi Jeong	242AIG 34	2002	내국인	석사	2	재학	참여	윤명국	
접수마감일	이화여자대학교	인공지능소프트웨어학부	주정현	Jeonghyeon Joo	252AIG 18	1999	내국인	석사	1	재학	참여	이지영	
접수마감일	이화여자대학교	인공지능소프트웨어학부	정홍경	Hongkyeong Jung	251AIG 03	2000	내국인	박사	1	재학	참여	이형준	
접수마감일	이화여자대학교	인공지능소프트웨어학부	뭉크투야	Tumurchuluun Munkhtuya	232AIG 02	1997	외국인	석사	4	재학	참여	이형준	
접수마감일	이화여자대학교	인공지능소프트웨어학부	마흘렛 워크네	Mahlet Workneh	232AIG 33	1997	외국인	석사	4	재학	참여	이형준	

기준일	대학명	신청학과명	성명		학번	생년 (YYYY)	외국인/ 내국인	학위과정			사업 참여 여부	지도교수 성명	비고
			한글	영문				과정	재학 학기 수	수료 여부			
접수마감일	이화여자대학교	인공지능소프트웨어학부	김수경	Sookyeong Kim	240AIG 01	1998	내국인	석사	3	재학	참여	이형준	
접수마감일	이화여자대학교	인공지능소프트웨어학부	배수현	Su-hyeon Bae	252AIG 09	1999	내국인	석사	1	재학	참여	이형준	
접수마감일	이화여자대학교	컴퓨터공학	딜로롬	Maqsudova Dilorom	232AIG 35	2001	외국인	석사	4	수료	참여	오유란	
접수마감일	이화여자대학교	인공지능융합	박혜진	HAEJIN PARK	252AIG 08	2000	내국인	석사	1	미수료	참여	오유란	
접수마감일	이화여자대학교	인공지능융합	양지선	JISEON YANG	242AIG 14	1997	내국인	석사	3	미수료	참여	오유란	
접수마감일	이화여자대학교	인공지능융합	임다희	DAHEE LIM	242AIG 20	2000	내국인	석사	3	미수료	참여	오유란	
접수마감일	이화여자대학교	인공지능융합	정미수	MISOO JUNG	232AIG 47	1998	내국인	석사	4	수료	참여	오유란	
접수마감일	이화여자대학교	인공지능융합	정주희	JOOHEE JEONG	252AIG 16	1997	내국인	석사	1	미수료	참여	오유란	
접수마감일	이화여자대학교	컴퓨터공학	허진영	JINYOUNG HUH	232AIG 49	2000	내국인	석사	4	수료	참여	오유란	

기준일	대학명	신청학과명	성명		학번	생년 (YYYY)	외국인/ 내국인	학위과정			사업 참여 여부	지도교수 성명	비고
			한글	영문				과정	재학 학기 수	수료 여부			
접수마감일	이화여자대학교	컴퓨터공학	정승아	SEUNGA CHUNG	221AIG 02	1998	내국인	박사	7	수료	참여	오유란	
접수마감일	이화여자대학교	컴퓨터공학	주수연	XIUYAN ZHU	241AIG 04	1994	외국인	박사	2	미수료	참여	오유란	
접수마감일	이화여자대학교	인공지능융합	김하연	HAYEON KIM	250AIG 02	1999	내국인	석박사통합	1	미수료	참여	오유란	
접수마감일	이화여자대학교	인공지능융합	이소현	SOHYUN LEE	250AIG 04	1998	내국인	석박사통합	1	미수료	참여	오유란	
접수마감일	이화여자대학교	컴퓨터공학	이연정	YUNJUNG LEE	202CPG 02	1995	내국인	석박사통합	11	수료	참여	오유란	
접수마감일	이화여자대학교	컴퓨터공학	조화연	HWAYEON JOH	202AIG 07	1996	내국인	석박사통합	10	수료	참여	오유란	

전체 대학원생 수(명)	석사	39	참여대학원생 수(명)	석사	39	참여비율(%)	석사	100
	박사	7		박사	7		박사	100
	석·박사통합	14		석·박사통합	14		석·박사통합	100
	계	60		계	60		전체	100
외국인 전체 대학원생 수(명)	석사	4	외국인 참여대학원생 수(명)	석사	4	외국인 참여비율(%)	석사	100
	박사	2		박사	2		박사	100
	석·박사통합	0		석·박사통합	0		석·박사통합	0
	계	6		계	6		전체	100