2022년도 **AI보안연구회 단기강좌**

Privacy-Preserving AI

일 시 **2022.4.29** (금) 9:20~17:00

진행방식 **온라인 진행**
(등록자에 한하여 온라인 시청주소 개별공지)

주 최 한국정보보호학회

주 관 AI보안연구회, AI보안연구센터

한국정보보호학회
Korea Institute of Information Security & Cryptology

2022년도 **AI보안연구회 단기강좌**
Privacy-Preserving AI

4차 산업혁명 시대의 핵심 키워드로서 AI는 우리의 삶을 엄청나게 변혁해가고 있습니다. 이러한 눈부신 AI의 발전의 원동력에는 엄청난 양의 수집 데이터를 기반으로 학습되는 머신러닝 기법들이 있습니다. AI 서비스의 다양성이 늘어가고 머신러닝 기법이 고도화되면서 이들을 개발하는 인터넷 서비스 제공자들이 개인적이고 보안에 민감한 데이터들까지 포함해서 이전보다 더 많은 데이터를 수집하고 이용하는 경향이 강해지고 있습니다. 불행하게도 이렇게 민감한 개인 데이터를 대규모로 활용하는 과정에서 우리의 중요 정보가 악의적인 공격자에게 탈취되는 프라이버시 침해 사고의 위험성이 최근 급속도록 커지고 있습니다. 따라서, 머신러닝 모델 개발 및 서비스 과정에서 사용되는 수많은 개인정보들이 노출되어 악용되는 것을 방지하는 Privacy-Preserving AI 기술은 데이터에 기반한 오늘날 AI의 잠재력을 극대화하고 AI가 미래 우리 삶에 지속적으로 혜택을 주는 것을 가능하게 하는 Enabler라고 할 수 있으며, 산학연 전반에 걸쳐 관심을 가지고 집중해야 할 미래 기술이라고 할 수 있습니다. Privacy-Preserving AI의 이런 점증되는 중요성 및 필요성에 부응하고자 본 강좌에서는 연합학습, 동형암호, 차등 프라이버시등 관련 대표 기술 분야 국내 산학 전문가들을 연사로 초빙하여 최신 기술 동향을 소개하고자 합니다. 각 강의에서는 해당 분야의 기초 이론 및 응용 기술을 초보자들도 이해하기 쉽도록 기초부터 자세히 다루도록 설계하였으로 AI 및 보안에 관심있는 모든 분들의 많은 관심과 참석을 부탁드립니다.

행사개요

일 시 2022년 4월 29일(금) 9:20~17:00
진행방식 온라인 진행(등록자에 한하여 온라인 시청주소 개별공지)
주 최 한국정보보호학회
주 관 AI보안연구회, AI보안연구센터

조직구성

연구회위원장 백윤흥(서울대)
프로그램위원장 권태경(연세대)
프로그램위원 권태경(서울대), 김의탁(이스트시큐리티), 류승진(국가보안기술연구소), 문대성(한국전자통신연구원), 박기웅(세종대), 백남균(부산외대), 신준범(크립토랩), 윤명근(국민대), 정수환(숭실대), 조학수(윈스), 최광희(한국인터넷진흥원), 최대선(숭실대), 한명묵(가천대)

시간	연사	제목
9:20 - 9:30		강좌안내
9:30 - 10:20	**송용수** 교수 (서울대)	**동형암호 기술 소개** (Introduction to Homomorphic Encryption)
10:20 - 11:10	**김한준** 교수 (연세대)	**동형암호 컴파일러 기술** (Introduction to Homomorphic Encryption Compiler Optimization)
11:10 - 12:00	**심규석** 회장/교수 (한국정보과학회/서울대)	**프라이버시 보호 기술** (Privacy Preservation Techniques)
13:30-14:20	**배호** 교수 (이화여대)	**생성모델 기반의 프라이버시 보호 기술** (Differentially Private GAN with Class Perturbations)
14:20-15:10	**강병훈** 교수 (카이스트)	**인공지능 시대의 신뢰 기밀 컴퓨팅 개요** (Intro to. Confidential Computing in the Age of AI)
15:10-16:00	**오현영** 교수 (가천대)	**프라이버시 보존 AI를 위한 동형암호와 신뢰실행환경 기술** (Homomorphic Encryption and Trusted Execution Environment for Privacy-Preserving AI)
16:00-16:50	**신준범** CTO (크립토랩)	**데이터 활용 및 보호를 위한 동형암호 장점 및 응용 분야** (Advantages and Applications of Homomorphic Encryption for Data Utilization and Protection)

등록비 및 등록방법

4월 27일(수) 오후 5시까지
등 록 비 일반 : 150,000 원, 학생 : 100,000 원
등록방법 학회 홈페이지 (www.kiisc.or.kr) 접속 > 학회행사 > “2022년도 AI보안연구회 단기강좌” > 사전등록 바로가기 > 등록 정보 작성 후 결제 방법 선택하시어 결제

등록송금처

예 금 주 한국정보보호학회
계좌번호 754201-04-135583 (국민은행)
학생의 경우 kiisc@kiisc.or.kr 로 학생증 사본 송부 바랍니다.
신용카드결제시 세금결산서 발급이 불가합니다.
입금명은 **[연구회명 첫 2글자+등록자 성함]**으로 기재해 주시길 바랍니다.
예) 2022년도 AI보안연구회 단기강좌 등록 홍길동 > **[AI홍길동] 기재**

문의처 한국정보보호학회 **전 화** 02-564-9333(내선 5) **이메일** kiisc@kiisc.or.kr