# 2023년 제4차 단기강좌 개최계획서

## ■ 행사개요

- 일　자 : 2023년 **12월 15일(금)**
- 장　소 : 실시간 온라인 개최
- 주　제 : **인공지능과 정보보안, 융합을 보다!**
- 주　최 : 사단법인 한국정보처리학회
- 참가대상 : 학부(대학원) 학생, 교수, 개발자, 연구자 등

## ■ 강좌소개

미래를 여는 인공지능과 사이버 보안의 최전선에 여러분을 초대합니다. 본 강좌에서는 인공지능과 보안의 교차점에서 발생되는 다양한 주제들에 대해서 최신 기술 동향과 사례를 중심으로 살펴봅니다. '서비스형 머신러닝에서 암호화된 영오차 처리기술', '딥페이크 기술', '생성형 AI를 활용한 금융 이상징후 탐색', '칩페이크 기술', 그리고 '사이버보안 모의훈련과 AI튜터'와 같은 주제들을 통하여 다양한 분야의 전문가들과 함께 지식을 나누시길 바랍니다. 이번 강좌를 통해 가장 혁신적인 기술 영역 중 하나인 인공지능과 사이버보안의 세계에 깊이 있는 통찰을 얻을 수 있게 되시길 바랍니다.

단기강좌 운영위원장 김 현 희

## ■ 조직구성

- 학　회　장 : 문남미 교수(호서대학교)
- 수석부회장 : 백윤흥 교수(서울대학교)
- 담당부회장 : 김현희 교수(동덕여자대학교)
- 프로그램위원장 : 도경화 교수(고려대학교)
- 프로그램위원 : 이민수 교수(서울대학교), 김미혜 교수(충북대학교), 윤혜정 교수(이화여자대학교)

## ■ 등록비

| 구분 | 사전등록 |
|---|---|
| **일 반** | 250,000원 |
| **학 생** | 150,000원 |
| ※ 참가자에게 커피쿠폰 제공 | |

## ■ 영수증 및 참가확인증 발급안내

- 참가확인증 : 유료 등록자에 한하여 아래의 사이트에서 행사일 이후부터 출력 가능합니다.
- 영수증(계산서 발행 불가) : 학회의 고유목적사업에 해당하는 행사 참가비(등록비) 항목에 대해서는 (세금)계산서 발행이 불가하고, 입금 확인 후 아래의 사이트에서 출력 가능합니다.

## ■ 전체 일정 및 강좌 내용

| 일자 | 시간 | 발표 주제 및 요약 내용 | 강사 |
|---|---|---|---|
| 12/15 (금) | 10:00~10:10 (10′) | 사회: 김현희 교수(동덕여자대학교)<br>인사말 : 문남미 회장(한국정보처리학회, 호서대학교) | |
| | 10:10~11:10 (60′) | 사회: 김현희 교수(동덕여자대학교)<br>**서비스형 머신러닝 클라우드상의 암호화된 신경망 데이터 영오차 처리기술**<br>ChatGPT를 포함해서 다양한 서비스형 머신러닝 클라우드(MLaaS)가 확산되고 있으며, 이러한 서비스를 제공하기 위해 MLaaS 상의 신경망은 민감한 개인정보를 포함한 많은 데이터를 학습과 추론에 사용하고 있다. 이 과정에서 필연적으로 개인 정보 유출의 위험이 증가하고, 이러한 유출에 대한 적절한 대책 없이는 MLaaS를 통한 미래 AI 서비스의 확장이 불가능함이 명확하다. 이에 따라 프라이버시 보장형(Privacy Preserving) 머신러닝(PPML) 기술의 개발이 급속도로 중요해지고 있는데, 지금까지 알려진 여러 PPML 기술 중, 동형암호 기술이 특히 주목받고 있다. 그러나, 이 기술은 성능 부하와 함께 AI 서비스의 질적 하락을 야기하는 암호문 연산 결과의 정확도 하락이라는 주요 단점을 가지고 있다. 현재까지 대부분의 연구는 성능 문제에 집중했으며, 정확도 하락 문제 해결에 대한 노력은 상대적으로 부족했다. 이 발표에서는 프라이버시를 보장하면서 높은 성능을 달성하는 새로운 접근 방식을 소개할 것이다. 본 접근법은 다종 동형암호 체계라는 기술을 기반으로 기밀연산을 보장하는 기존의 하드웨어 기반 신뢰실행환경(TEE)을 채용하여 높은 정확도와 성능을 동시에 달성하도록 설계되었다. 우리 기술은 CNN과 RNN 계열의 신경망에 모두에 적용 가능하며, 이를 위해 기존의 다항식 근사 방식을 넘어서는 새로운 암호문 근사 기법을 사용하여 동형암호의 정확도 문제를 효과적으로 해결했다. | **백윤흥 교수 (서울대학교)** |
| | 11:10~11:20 | 휴 식 | |
| | 11:20~12:20 (60′) | 사회: 김현희 교수(동덕여자대학교)<br>**인공지능 딥페이크 기술과 적용사례**<br>인공지능 딥러닝을 기반으로 얼굴같은 다양한 생체정보, 중요이미지 등를 생성하는 기술을 딥페이크라고 한다. 최근 딥페이크 기술을 통해 정지영상뿐만 아니라 동영상인 생체정보, 특히 얼굴을 기존 유명인 및 허상의 인물로 만드는 기술이 주목을 받고 있다. 딥페이크 기술은 긍정적 영향과 부정적 영향을 모두 가져오고 있다. 개인의 다양한 사유에 따라 비대면 온라인 시대에서 본인을 대변하는 허상의 인물을 만들기도 하고 과거에 위인 등 죽은 사람을 살아오게 만들기도 한다. 그러나 실제 인물의 모습을 추론하여 거짓 정보를 포함하게 하는데 사용되기도 하여 다양한 문제를 가져오기도 한다. 본발표에서는 인공지능 딥러닝을 활용한 딥페이크 기술(생성에서 검증까지지) 기술과 환경 그리고 인공지능 윤리문제까지 알아보고자 한다 | **도경화 교수** (고려대학교) |
| | 12:20~13:20 (60′) | 중 식 | |
| | 13:20~14:20 (60′) | 사회: 도경화 교수(고려대학교)<br>**생성형AI와 의사결정시스템으로 보는 금융 이상징후 탐색(사례포함)**<br>본 강의는 생성 형 AI 와 빅데이터 그리고 의사결정시스템과의 상호 협력 기술을 설명한다. 의사결정시스템에 대한 실질적인 사례를 통해 기업/기관에서 사용되고 있는 현황을 이해하고 빅데이터와의 결합을 공유한다. 금융감독에서의 규제사항에 대비하는 기술과 fraud detection 사례의 시나리오와 스코어모델을 설명한다.<br>기업의 needs와 기술의 결합으로 향후 모색되고 있는 의사결정,데이타분석, genAI 응용 부문에 대해서도 방향도 살펴보고자한다.<br>이를 토대로 전사적 의사결정플랫폼으로 발전하고 있는 글로벌 트랜드도 경험할 수 있다. | **유인지 대표** (코리아엑스퍼트) |
| | 14:20~14:30 | 휴 식 | |

| | | | |
|---|---|---|---|
| | | 사회: 도경화 교수(고려대학교) | |
| | 14:30~15:30<br>(60′) | **칩페이크 기술(신분증 진짜/가짜, 시연)**<br>본 강의에서는 비대면계좌 개설 과정에서 발생하는 다양한 신분증 위변조 사례를 보고 이를 인공지능이 어떻게 탐지하는지 설명하고 실습하고자 한다. 최근의 급격한 비대면 거래 증가는 예상치 못한 보안의 헛점을 드러내고 있습니다. 비대면 환경에서 타인의 신분증 사진을 도용, 개설한 계좌로 대출을 받는 등 금융 피해가 늘어 나고 있다. 이러한 위협들로 인해 보안의 중요성은 더욱 부각되고 있으며 이를 사전에 예방하는 데에 인공지능 기술이 어떻게 활용되는지를 살펴보고자 한다. | **박창현 프로**<br>(삼성SDS) |
| | 15:30~15:40 | 휴 식 | |
| | 15:40~17:50<br>(70′) | 사회: 도경화 교수(고려대학교) | |
| | | **사이버보안 모의훈련과 AI튜터 (시연포함)**<br>본 강의에서는 사이버보안 전문인력의 체계적인 양성 방안을 목표로 클라우드, 가상화기술을 이용한 모의훈련 플랫폼 소개, AI 튜터 기술을 활용한 초보자 맞춤형 실습을 시연 형식으로 진행한다. 먼저 사이버보안 모의훈련 플랫폼 "사이버이지스"를 이용한 해킹방어 실습에 대해 알아본다. 해킹방어 실습은 취약점 방어 등 기초 단계부터, 실시간 해킹 방어, 복합 방어, 공방훈련 등 보다 전문 단계까지 실습 진행을 시연을 통해 이해를 돕고자 한다. 마지막으로 AI 튜터를 이용하여 초보자의 사이버보안 교육을 효과적으로 진행하는 방안을 시연을 통해 제시하고자 한다.<br>참가자들은 본 강의를 통해 사이버보안 교육훈련 플랫폼을 이용한 효과적인 전문인력 양성방안을 이해할 수 있습다. 또한, AI 튜터링 기술을 이용하여 사이버보안에 초기 접근이 어려운 초보자들이 적응할 수 있도록 어떻게 활용할 수 있는지 살펴볼 수 있다. | **박영선 대표**<br>(두두아이티) |

* 주최 측의 사정으로 프로그램이 일부 변경될 수 있습니다.