서울대, 2023

하반기 가우스 콜로퀴움 개최

가우스 콜로퀴움은 여러 학생들과 대중들에게 수학을 활용한 산업문제에 대하여 배우고 토론할 수 있는 자리입니다.

김 장 우 교수(서울대 전기정보공학부 [망고부스트]) | 9월 26일 (화) 17:00-17:45

MangoBoost : Academic Researcher's Road to the World-Leading Startup

Modern high-performance computer systems are deploying an increasing number of high-performance devices (e.g., GPU, SSD, NPU, NIC) per server to maximize the target application's overall performance, while minimizing the system's total cost of operation. To achieve the goal, the next-generation datacenters aim to deploy a newly-designed data processing unit (DPU) (a.k.a., IPU, xPU, smart-Xdevice) which is specially designed to orchestrate various devices in the most efficient way.
In this talk, I will first introduce key challenges in developing the next-generation servers. Next, I will explain what ideal DPUs should look like and how they should perform. Finally, I will present how the state-of-the-art DPUs provided by Mango Boost can achieve such design goals successfully.

권 태 경 교수(연세대학교 정보대학원) | 9월 26일 (화) 17:55-18:35

ChatGPT 등 생성형 AI 보안

최근 비약적인 발전을 거듭하며 눈부신 성과를 내기 시작한 생성형 AI는 대량의 데이터를 학습하여 이와 유사한 새로운 데이터를 생성하는 딥러닝 기반 인공지능 기술의 한 분야를 일컫는다.
특히 ChatGPT를 필두로 하는 트랜스포머 모델 기반 챗봇 서비스는 자연스러운 문장 생성과 질의응답 기능을 통해 이미 많은 사람들에게 친숙해지고 있다. 뿐만 아니라 그림, 사진, 영상, 음성, 음악 등 여러 분야에서 생성 모델이 속속 개발되고 활용되면서 생성형 AI는 우리의 일상과 산업, 교육 등 많은 영역에 영향을 주기 시작했다. 하지만 이러한 딥러닝 기반 생성형 AI 기술의 발전은 우리 사회에 혁신과 유익한 변화를 가져오는 한편 보안과 개인정보보호에 대한 많은 우려도 수반하게 된다.
따라서 이번 강연에서는 먼저 생성형 AI 서비스의 현재를 소개한 후 ChatGPT를 중심으로 생성형 AI 보안 위협에 대해 살펴보고 이와 관련하여 최근 발간된 보안 가이드라인을 다루도록 한다. 또한 동영상이나 음성 데이터를 조작하여 실제와 유사한 가짜 콘텐츠를 생성하는 기술로 알려진 딥페이크에 대해서 조명하여 생성형 AI의 올바른 활용과 보안을 위한 방향을 논할 예정이다.

| 장 소 | 서울대학교 129동 101호 대강당

수학기반 산업데이터해석 연구센터
Industrial & Mathematical Data Analytics Research Center