

2023년도 IT21

Global Conference
Industrial Survival Strategy for Next
Generation Information Technology



www.kips.or.kr/it21

INTELLIGENT
ARTIFICIAL
CORE

차세대통신과
자율이동체

블록체인과 NFT

AI와 보안

자율로봇지능과
플랫폼 기술

Human-
centric data
analytics

software
safety

인간중심 AI (Human Centric AI)로 여는 디지털 융합 세상

차세대통신과 자율이동체
블록체인과 NFT
AI와 보안
자율로봇지능과 플랫폼 기술
Human-centric data analytics
과학기술과 AI 활용 / software safety

2023.9.14(목) ~ 9.15(금)
삼성동 섬유센터 17층 스카이뷰
(온·오프라인 병행)



2023. 9. 14(목) - 9. 15(금) 섬유센터 17층 스카이뷰(온·오프라인 병행)

초대의 말씀

우리나라 ICT 산업 발전을 위해 산업계, 학계, 연구소 등에서 땀 흘리고 노력하시는 모든 분들의 건강과 행운을 기원합니다.

우리 학회에서는 1996년부터 매년 미래의 정보통신 기술의 흐름을 조망하고 국가의 ICT 기술 및 산업 경쟁력 확보를 목적으로 IT21 글로벌 컨퍼런스를 개최해 오고 있습니다. 금년에는 제28회 행사를 오는 9월 14일(목)부터 9월 15일(금)까지 온·오프라인 병행 컨퍼런스로 개최하고자 합니다.

스물여덟 번째를 맞는 금년도 행사는 주제를 “Human Centric AI로 여는 디지털 융합 세상”으로 정하고 산·학·연·관에서 초청한 최고의 연사들이 최신의 각종 기술 및 정책 방향을 발표함으로써 이에 대한 흐름을 파악하고 대비할 수 있도록 계획하였습니다.

본 행사를 통해 향후 인공지능 기술 발전 동향과 나아갈 방향을 제시하고 이러한 기술이 생활 속에서 활용되는 다양한 데이터 분석 기술, 자율로봇지능 및 플랫폼 기술, 블록체인과 NFT 기술, 차세대 통신 및 지능형 보안 기술, 인공지능과 소프트웨어 안전 기술에 대한 정보 공유의 장을 마련하고자 합니다. 또한 미래를 위한 인공지능 기술이 어떻게 발전하고 어떠한 산업에 적용되고 활용 및 융합될 수 있는지 그리고 정부가 어떤 정책 방향을 제시할 것인지에 대한 이슈를 함께 고민하고자 합니다. 특히 본 행사는 인공지능 기술이 생활 속에 스며들 정도로 급격히 변화하고 있는 SW와 ICT 기술에 대한 이해와 분석 뿐만 아니라 SW와 ICT 산업 발전 및 비전을 제시하는 중요한 역할을 담당할 것으로 생각됩니다.

끝으로 이번 행사에 귀중한 시간을 내어 발표해 주시는 여러 연사분과 본 행사 준비를 위해 노고를 아끼지 않으신 각 위원장과 위원님들, 그리고 본 행사를 지원해 주신 정부, 출연연구소, 기업 및 언론사 등 모든 분께 진심으로 머리 숙여 깊은 감사를 드립니다.

부디 IT21 글로벌 컨퍼런스가 회원 여러분들의 미래 연구 및 업무에 많은 도움이 되고 국가 산업과 경제를 이끌어갈 수 있는 디지털 융합 시대의 대표 기술을 선도하는 데 큰 역할을 담당하게 되길 기대합니다. 감사합니다.



2023년 9월

(사)한국정보처리학회 회장 문 남 미



2023. 9. 14(목) - 9. 15(금) 섬유센터 17층 스카이뷰(온·오프라인 병행)

● **대 회 장** 문남미(한국정보처리학회 회장, 호서대학교)

● **공동조직위원장**

위 원 장	방승찬(ETRI) 황종성(NIA)	신희동(KETI) 이재영(KLID)	이원태(KISA)	김재수(KISTI)
-------	-----------------------	------------------------	-----------	------------

● **프로그램위원회**

위 원 장	길준민(제주대학교)			
부위원장	김영갑(세종대학교) 이덕규(서원대학교)	박진호(동국대학교) 이은서(안동대학교)	윤주상(동의대학교) 임동혁(광운대학교)	이기용(숙명여자대학교)

● **운영위원장** 이덕규(서원대학교)

● **홍보위원장** 강정호(배화여자대학교)

부위원장	권태윤(네이버시스템) 신병석(인하대학교)	권혁준(순천향대학교) 유성철(쌍용정보통신)	김병욱(강릉원주대학교) 정화영(경희대학교)	박지수(전주대학교)
위 원	곽정희(한국정보기술) 김미현(와이어블) 김은영(투와이시스템) 서봉상(올포랜드) 양영욱(한신대학교) 이재진(네이버시스템) 전한수(세림TSG) 최석우(대보정보통신)	권구주(배화여자대학교) 김성길(우주텔레콤) 김은환(송실대학교) 서영석(영남대학교) 이대원(서경대학교) 이종혁(대구카톨릭대학교) 정경진(진인프라) 허준호(한국해양대학교)	김남진(LGCNS) 김세종(에스제이정보통신) 김현우(배화여자대학교) 성연식(동국대학교) 이 연(인하대학교) 임종범(평택대학교) 정재화(방송통신대학교) 황광일(인천대학교)	김도현(부산카톨릭대학교) 김윤철(트라콤) 박진호(동국대학교) 안진현(제주대학교) 이은석(유한대학교) 장항배(중앙대학교) 최 민(충북대학교)



2023. 9. 14(목) - 9. 15(금) 섬유센터 17층 스카이뷰(온·오프라인 병행)

1일차 / 9월 14일(목)

시간	프로그램		
09:30 ~	등 록		
10:00~10:40	Keynote Speech 1 사회 : 길준민 교수(제주대학교)	Deep Learning Based Inference of Private Information Using Embedded Sensors in Smart Devices Prof. Yingshu Li (Georgia State University)	
10:40~10:50	휴 식		
10:50~11:30	Keynote Speech 2 사회 : 길준민 교수(제주대학교)	데이터 분석의 미래: 일상 속으로 데이터기반 치매조기예측 기술 전홍우 센터장(한국과학기술정보연구원)	
11:30~12:10	개회식 사회 : 유진호 교수(상명대학교)	개회사 : 문남미 학회장(한국정보처리학회, 호서대학교 교수) 환영사 : 과학기술정보통신부 축 사 : 국회 과학기술정보방송통신위원회 격려사 : 방승찬 원장(ETRI), 신화동 원장(KETI), 이원태 원장(KISA), 김재수 원장(KISTI), 황종성 원장(NIA), 이재영 원장(KLID)	
12:20~13:20	중 식		
세션명 시간	Session 1 차세대통신과 자율이동체	Session 2 블록체인과 NFT	Session 3 AI와 보안
	사회 : 문종철 박사(국가보안기술연구소)	사회 : 임동혁 교수(광운대학교)	사회 : 김영갑 교수(세종대학교)
13:20~14:00	5G 특화망 보안 기술 박종근 실장 (ETRI)	NFT 기술의 최신 산업 동향 김탄휴 디렉터 (GRAFOLIO)	인공지능(AI) 보안관계 현황과 이슈 박원형 교수 (성신여자대학교)
14:00~14:40	독립형 5G 네트워크를 위한 1차 인증 프로토콜의 순방향 비밀성 지원 기술 동향: EAP-AKA'-FS를 중심으로 유일선 교수 (국민대학교)	블록체인 기술과 금융의 만남, STO (Security Token Offering) 권혁준 교수 (순천향대학교)	피싱 탐지 자동화와 대응 전략 허 규 실장 (네이버)
14:40~15:20	뉴 스페이스 및 양자 시대 핵심 보안 기술 이봉수 책임연구원 (국가보안기술연구소)	유틸리티 토큰 기반의 비즈니스 김태경 교수 (경희대학교)	지능형 영상보안 기술 현황 및 이슈 김동철 책임연구원 (한국전자기술연구원)
15:20~15:30	휴 식		
세션명 시간	차세대통신과 자율이동체	블록체인과 NFT	AI와 보안
	사회 : 이덕규 교수(서원대학교)	사회 : 김태경 교수(경희대학교)	사회 : 서영덕 교수(인하대학교)
15:30~16:10	자율자동차 센서 보안 최원석 교수 (고려대학교)	ChatGPT와 블록체인 : New 패러다임간 상호작용 이용구 CTO (피어테크)	초거대 AI에 의한 사이버 위협과 우리의 대응 전략 김병재 책임연구원 (한국인터넷진흥원)
16:10~16:50	자율주행차 보안위협 및 보안대응 방안 장재동 선임 (한국인터넷진흥원)	블록체인(주요 성과 및 과제) 및 NFT(안전한 이용표준안) 유주열 팀장 (한국인터넷진흥원)	머신러닝 기반 교육기관 사이버위협 분석체계 운영 현황 및 이슈 윤성준 부장, 정진명 책임연구원 (한국교육학술정보원)
16:50~17:30	Cybersecurity in Automotive : Current Trends and Regulations 우사무엘 교수 (단국대학교)	블록체인 서비스 전망 최선미 연구원 (한국전자통신연구원)	AI 모델의 복제 공격과 방어 기법 이상근 교수 (고려대학교)

※ 본 일정은 프로그램 기획상 변경될 수 있습니다.



2023. 9. 14(목) - 9. 15(금) 섬유센터 17층 스카이뷰(온·오프라인 병행)

2일차 / 9월 15일(금)

시간	프 로 그 램		
10:00~12:00	등 록		
10:20~11:00	Keynote Speech 3 사회 : 김준민 교수 (제주대학교)	초거대 언어모델의 윤리와 안전성 (Ethics and Safety of Large Language Models) 이화란 리더(NAVER AI Lab)	
11:00~11:10	휴 식		
11:10~11:50	Keynote Speech 4 사회 : 김준민 교수 (제주대학교)	사람에게 필요한 인공지능 기술의 발전방향 민옥기 소장(한국전자통신연구원)	
11:50~13:00	중 식		
세션명 시간	Session 4 자율로봇지능과 플랫폼 기술	Session 5 Human-Centric Data Analytics	Session 6 과학기술과 AI 활용
	사회 : 윤주상 교수(동의대학교)	사회 : 이기용 교수(숙명여대)	사회 : 최명석 단장(KISTI)
13:00~13:40	일상 작업을 돕는 로봇 AI 학습 방법 최중현 교수 (연세대학교)	Human centric AI in KETI 신사임 센터장 (한국전자기술연구원)	과학기술 문헌 분석을 위한 사전학습 언어모델 개발 사례 이승우 팀장 (KISTI)
13:40~14:20	Reactive Robot Control을 위한 거대언어모델 활용 : 반사신경지능과 안전지능 정병진 선임연구원 (한국전자기술연구원)	딥러닝을 활용한 이상 탐지 이동하 교수 (연세대학교)	맞춤형 시각지능 개발을 위한 학습데이터와 모델 개발 지원 서비스 이 용 팀장 (KISTI)
14:20~15:00	파운데이션 모델의 로봇 적용 장민수 책임연구원 (한국전자통신연구원)	자기 정규화 계층이 있는 단순 컨벌루션 신경망에 기반한 연령 및 성별 예측 권준호 교수 (부산대학교)	코로나19 대응을 위한 인공지능 기술개발 사례 안인성 팀장 (KISTI)
15:00~15:10	휴 식		
세션명 시간	자율로봇지능과 플랫폼 기술	Human-Centric Data Analytics	Software Safety
	사회 : 윤주상 교수(동의대학교)	사회 : 이기용 교수(숙명여자대학교)	사회 : 이은서 교수(안동대학교)
15:10~15:50	자율주차로봇시스템 김봉석 책임연구원 (한국전자기술연구원)	심전도(ECG) 데이터의 프라이버시 보호 분석 정연돈 교수 (고려대학교)	4차 산업혁명시대 소프트웨어 안전: 현재와 나아가야 할 방향 민상윤 대표 (솔루션링크)
15:50~16:30	로봇 자율주행을 위한 SLAM 및 AI 김곤우 교수 (충북대학교)	디지털 병리에서의 인공지능 활용 동향 곽태영 CTO (딥바이오)	거대 인공지능 기술은 SW 개발을 어떻게 변화할 것인가? - 자동 코딩 기술과 SW 신뢰성 김태호 책임연구원 (한국전자통신연구원)
16:30~17:10	에지-클라우드 기반 로보틱스 시스템 설계 및 구현 구세환 책임연구원 (LG전자)	생성형 AI 이슈와 보안 최대선 교수 (숭실대학교)	원자력 안전 소프트웨어 및 블록체인 합의 알고리즘 대상 정형 검증 적용 사례 지은경 교수 (KAIST)

※ 본 일정은 프로그램 기획상 변경될 수 있습니다.



2023. 9. 14(목) - 9. 15(금) 섬유센터 17층 스카이뷰(온·오프라인 병행)

Keynote Speech

Keynote Speech 1

9월 14일(목) 10:00~10:40
사회 : 길준민 교수(제주대학교)



Prof. Yingshu Li
Georgia State
University

Deep Learning Based Inference of Private Information Using Embedded Sensors in Smart Devices

Smart mobile devices and mobile apps have been rolling out at swift speeds over the last decade, turning these devices into convenient and general-purpose computing platforms. Sensory data collected from smart devices are important resources to nourish mobile services, and they are regarded as innocuous information that can be obtained without user permissions. However, such seemingly innocuous information could cause serious privacy issues. In this talk, we first demonstrate that users' tap positions on the screens of smart devices can be identified based on the collected sensory data by employing some deep learning techniques. Then we show that tap stream profiles can be collected, so that a lot of private information can be accurately inferred.

Keynote Speech 3

9월 15일(금) 10:20~11:00
사회 : 길준민 교수(제주대학교)



이화란 리더
NAVER AI Lab,
NAVER Cloud

초거대 언어모델의 윤리와 안전성 (Ethics and Safety of Large Language Models)

Coincidence with the astounding performance of recent large language models (LLMs), potential risks and their social impacts have been addressed. In this talk, I will give brief introduction of the ethical problems such as toxicity, social bias/stereotypes, human-values including ethics and moral norms. Then I will introduce two new datasets: SQuARE and KoSBi. In SQuARE, we consider sensitive questions that LLMs could raise negative social impacts depending on their responses on the questions, and introduce acceptable responses. In KoSBi, we propose a Korean Social Bias dataset that reflects Korean-specific culture and society.

Keynote Speech 2

9월 14일(목) 10:50~11:30
사회 : 길준민 교수(제주대학교)



전홍우 센터장
KISTI
미래기술분석센터

데이터 분석의 미래: 일상 속으로 데이터 기반 치매조기예측 기술

세계적으로 치매발병이 급증하고 있고, 아직 치료제는 없다. 병원에서 처방받는 약은 치매 진행 속도를 늦추는 것이지만, 이 또한 적절한 시기인 치매 초기부터의 복용이 필요하다. KISTI는 다양한 데이터를 기반으로 인공지능 기술을 접목하여 그 적절한 시기를 예측하는 연구를 진행하였고, 대한민국 노인인구 10%에 해당하는 사람들의 10년간의 병력기록, 치매관련 논문, 그리고 개인의 생활패턴을 통합 분석하여 치매를 조기에 예측하는 체제를 구축하였다. 본 발표에서는 인공지능 기술 기반 치매조기예측 기술과 관련하여 다양한 토픽별 모델링, 위험인자 등에 대한 실험 결과를 공유한다.

Keynote Speech 4

9월 15일(금) 11:10~11:50
사회 : 길준민 교수(제주대학교)



민육기 소장
한국전자통신연구원
초지능창의연구소

사람에게 필요한 인공지능 기술의 발전방향

현재 인공지능 기술의 중심은 ChatGPT로 대표되는 생성형 인공지능 기술에 있다. 세상의 모든 지식과 인간의 고유영역으로만 생각했던 창작의 분야까지 생성형인공지능 기술은 놀라운 결과를 쏟아내고 있다. 이는 분명 인공지능 기술의 혁신이며, 다양한 도메인 적용되어 해당분야의 혁신을 견인할 수 있는 동력임에는 분명하다.

그러나, 우리는 이러한 생성형 인공지능 기술로 만족할 수 있는지를 짚어보고자 한다. 사람이 필요로 하는 인공지능 기술은 어떤 것일까? 누군가는 ChatGPT가 이미 인공지능일반지능(AGI)라고 하는데 정말 그런 것인지, 산업 일선에서 또는 개인은 어떤 인공지능 기술을 필요로 하는 것인지 살펴보고자 한다. 산업체와 개인이 원하는 인공지능의 모습에 비추어 현재 기술은 어떤 약점이 있고, 어떤 한계가 있는지에 대해서도 논의해보고자 한다. 또한, 향후 인공지능 기술 발전을 위해서 연구자 입장에서 어떤 인공지능 기술을 준비해야 하는지에 대해서도 짚어본다.



2023. 9. 14(목) - 9. 15(금) 섬유센터 17층 스카이뷰(온·오프라인 병행)

Session 1 차세대통신과 자율이동체

Session 1-1

9월 14일(목) 13:20~14:00

사회 : 문준철 박사(국가보안기술연구원)

5G 특화망 보안 기술



박종근 실장
한국전자통신연구원

과학기술정보통신부의 5G 특화망(이음5G) 활성화 정책을 바탕으로 2021년 네이비클라우드가 최초로 5G 특화망을 도입한 이후, 현재 20여개 이상의 기관에서 5G 특화망을 구축하는 등 다양한 산업 영역에서의 5G 특화망 도입 및 구축이 빠르게 확산되고 있다. 그러나, 안전한 디지털 대전환을 위해서는 5G 특화망에 대한 보안모델을 정립하고 5G 특화망에서의 보안위협을 분석하고 대응하는 노력이 요구된다. 더욱이 5G 특화망 서비스는 5G 특화망 주파수를 지정받아 자사 전용의 5G 특화망을 구축하는 방식과, 주파수를 할당받은 기간통신사업자로부터 5G 특화망 구축 서비스를 제공받는 방식으로 크게 구분할 수 있으며, 특히 후자의 기간통신사업자의 서비스를 이용하는 방식이 더 큰 비중을 차지할 것으로 전망됨에 따라 구축 유형별로 보안성을 강화하기 위한 차별화된 대응방안도 필요하다. 본 발표에서는 최근 빠르게 확산되고 있는 5G 특화망 서비스를 소개하고, 5G 특화망의 활성화를 위해 고려해야 할 보안 이슈와 대응 방안에 대해 간략히 살펴보기로 한다.

Session 1-4

9월 14일(목) 15:30~16:10

사회 : 이덕규 교수(서원대학교)

자율자동차 센서 보안



최원석 조교수
고려대학교

현재 운전자의 운전 편의성을 제공하기 위한 단순한 형태의 '자율주행보조기술'뿐만 아니라 '완전자율주행기술'을 위한 관련 연구가 전 세계적으로 활발하게 진행되고 있다. 특히, 2022년 후반기부터 제한된 조건에서는 운전자의 전방주시가 필요하지 않는 상태에서 자율주행이 가능한 Lv3 자율주행 자동차가 출시되었다. Lv5의 완전 자율주행기술은 운전자의 운전 편의성을 향상시켜주는 것에 그치지 않고 물류, 국방 등 다양한 서비스 영역에서 활용 가치가 매우 높을 것이다. 완전자율주행기술이 가능하기 위해서는 자율주행 알고리즘에 대한 연구뿐만 아니라 통신 및 센서에 대한 기술 향상이 절대적으로 필요하다. 전통적으로 네트워크 및 통신에 대한 연구는 많은 관심을 갖은 것 같고 비교하여, 센서보안에 대한 연구 분야는 아직까지 많이 알려지지 않은 상태이다. 본 발표에서는 악의적인 신호를 주입하여 센서가 오동작하게 만드는 Fault Injection Attack에 관한 연구 동향에서 대하여 설명하고, 향후 자율주행자동차가 Fault Injection Attack에 대하여 어떻게 대응하여야 할지 이야기 하고자 한다.

Session 1-2

9월 14일(목) 14:00~14:40

사회 : 문준철 박사(국가보안기술연구원)

독립형 5G 네트워크를 위한 1차 인증 프로토콜의 순방향 비밀성 지원 기술 동향: EAP-AKA'-FS를 중심으로



유일선 교수
국민대학교
정보보안기술연구소

독립형 5G 보안의 핵심인 1차 인증 프로토콜에는 5G AKA와 EAP-AKA'이 표준으로 포함된다. 5G AKA와 EAP-AKA'은 이동단말과 5G 코어망 사이의 공유 비밀키를 통해 대칭키 기반의 상호인증과 기밀성을 제공하며, 이들의 보안 강도는 이동단말과 5G망 사이의 신뢰구축 및 유무선 구간 제어 메시지와 무선 구간 사용자 데이터 보호를 고려할 때, 적절하다고 인식되었다. 그러나, 6G로 진화하는 이동통신 기술의 발전과 다양한 이동통신 융합 어플리케이션의 출시 등으로 인해 보안 강화에 대한 요구가 높아지고 있다. 특히, 이동통신 융합 어플리케이션의 인증 및 기밀화를 위해 1차 인증시 이동단말과 코어망 사이에 구축된 자격증명을 재사용하는 3GPP의 Authentication and Key Management for Applications (AKMA)의 제안 및 표준화로 인해 1차 인증 프로토콜의 순방향 비밀성(Forward Secrecy) 지원이 필요한 실정이다. 이러한 배경에 따라 5G AKA와 EAP-AKA'에 순방향 비밀성을 지원하는 연구가 활발히 진행되고 있다. 무엇보다, IETF에서는 EAP-AKA'의 순방향 비밀성 지원 프로토콜인 EAP-AKA'-FS를 표준화 하고 있다. 본 강연에서는 EAP-AKA'-FS를 중심으로 독립형 5G 네트워크를 위한 1차 인증 프로토콜의 순방향 비밀성 지원 기술을 다룰 예정이다.

Session 1-5

9월 14일(목) 16:10~16:50

사회 : 이덕규 교수(서원대학교)

자율주행차 보안위협 및 보안대응 방안



장재동 선임연구원
한국인터넷진흥원

자율주행차는 커넥티비티 기술 및 센서 기술의 발전과 함께 급격하게 성장하고 있다. 구글을 비롯하여 GM, Ford 등 글로벌 차량 제조사들이 활발하게 자율주행차를 개발하고 있고 현대자동차 또한 CES에서 자율주행차를 선보이는 등 자율주행차가 더 이상 먼 미래의 얘기가 아니라 우리 손에 쥐어진 현실의 기술이 되었다. 이에 따라, 무인서플, 주차, 배송 등 자율주행차를 활용한 서비스 모델이 활발하게 개발되고 있는데, 이런 서비스들은 자동차, 인프라, 통신, 전자, ICT 등이 융합되어 시너지를 발휘하고 있다. 하지만, 이런 융합으로 인하여 기존 ICT 환경에서 발생했던 사이버 공격들이 자동차 환경으로 전이되고 있다. 자동차의 안전은 운전자와 승객 더 나아가 도로 위에 존재하는 모든 사람들의 안전과 직결되므로 자동차를 대상으로 수행되는 사이버 공격들에 대한 방어 태세를 완비해야 한다. 본 발표에서는 자율주행 서비스/차량/인프라 및 UN 차량 사이버보안 규정(UN Regulation No.155, 156)의 보안 요구사항을 기반으로 자율주행차의 보안위협과 대응방안에 대해 소개하고자 한다.

Session 1-3

9월 14일(목) 14:40~15:20

사회 : 문준철 박사(국가보안기술연구원)

뉴 스페이스 및 양자시대 핵심 보안 기술



이봉수 책임연구원
국가보안기술연구소

대한민국은 한국형 발사체 개발 성과를 바탕으로 도전적인 우주탐사 사업 추진, 다양한 인공위성 개발과 활용, 민간의 우주개발 역량 강화를 통해 세계 7대 우주 강국으로 도약을 준비하고 있다. 하지만, 우주자산의 통신 특성으로 재밍, 도청, 해킹 및 변조 등 타 통신 대비 다양한 보안 위협이 존재한다. 미국, 유럽 등 주요 선진국에서는 우주안보 강화와 사이버 보안 중요성을 강조하고 있으며, 특히 중국은 위성에 양자암호통신 기술을 적용하여 안전한 위성통신분야를 선도하고 있다. 또한 양자 시대가 도래하고 있다. 양자컴퓨터 발전에 따른 현대암호의 위협에 대응하기 위해서 전 세계는 양자내성암호로의 전환을 준비하고 있으며, 국내는 지난 7월12일 '양자내성 암호 전환 마스터 플랜'을 통해 2035년까지 전환을 목표로 하였다. 이번 발표에는 뉴 스페이스 및 양자 시대 보안 위협에 대해서 살펴보고, 이러한 보안 위협에 대응할 수 있는 핵심 보안 기술에 대해서 설명한다.

Session 1-6

9월 14일(목) 16:50~17:30

사회 : 이덕규 교수(서원대학교)

Cybersecurity in Automotive: Current Trends and Regulations



우사무엘 교수
단국대학교

글로벌 컨설팅회사 PwC에서는 최신 자동차 개발 트렌드를 분석한 후, 미래 자동차의 발전 방향을 "EASCY"라는 단어로 정의하였다. EASCY는 electrified, autonomous, shared, connected 그리고 yearly updated의 약자를 뜻하며, 자동차가 5G와 같은 외부 네트워크와 항상 연결되어 있는 IoT(Internet of Things) Device로 진화하였음을 시사한다. 자동차가 IoT 디바이스로 인식됨과 동시에 전통적인 IT 환경에서의 사이버 공격들이 자동차 환경으로 유입되고 있다. 이에 따라 UN (United Nations)에서는 자동차 사이버보안 관련 규정을 채택하여 안전한 자동차 환경구축을 강제하고 있다. 본 강연에서는 자율주행차의 사이버보안 기술 동향을 해킹 및 보안 기술 개발 현황과 국제 규제 및 표준화 이슈를 중심으로 살펴보고, 우리는 무엇을 준비해야 하는지 설명한다.



2023. 9. 14(목) - 9. 15(금) 섬유센터 17층 스카이뷰(온·오프라인 병행)

Session 2 블록체인과 NFT

Session 2-1

9월 14일(목) 13:20~14:00
사회 : 임동혁 교수(광운대학교)



김탄휴 전라다메터
GRAFOLIO
PTE. LTD.

NFT 기술의 최신 산업 동향

이 발표는 NFT 기술의 최신 산업 동향에 대한 자리이면서, 과거와 현재의 시장 상황을 살펴보고 앞으로 나아갈 방향을 탐색하기 위한 자리입니다. 과거, NFT 기술은 상대적으로 새로운 개념이었고, 초기에는 주로 예술 작품과 디지털 콘텐츠 분야에서 주목받았습니다. 예술가들은 자신의 작품을 NFT로 발행하여 소유권을 인증하고 거래를 진행하는 새로운 모델을 경험했습니다. 이러한 관심을 토대로 발전한 NFT 산업은 현재 예술과 엔터테인먼트 분야뿐만 아니라 게임, 스포츠, 부동산 등 다양한 산업분야로 확장되었습니다. NFT 기술은 소유권 확인과 거래의 투명성을 제공하여 산업 전반에 혁신을 가져왔습니다. 그러나 NFT 기술의 인가와 함께 환경적 이슈와 법적 쟁점도 부각되고 있습니다. 이 발표는 앞으로 우리가 NFT 기술의 가능성과 도전에 대해 더 깊이 이해할 수 있는 지표가 될 것입니다. 지속 가능한 개발과 에너지 효율성에 대한 연구와 노력, 규제와 법적 문제에 대한 논의와 해결방안 모색 등 NFT 기술이 불려올 미래에 대한 대비에 도움이 될 것입니다.

Session 2-4

9월 14일(목) 15:30~16:10
사회 : 김태경 교수(경희대학교)



이용구 CTO
피어테크

ChatGPT와 블록체인: New 패러다임간 상호작용

"ChatGPT와 블록체인: New 패러다임간 상호작용"이라는 주제로, 이 강연은 AI와 블록체인 기술의 융합 가능성, 최신 연구 동향, 산업 변화, 그리고 이 두 기술이 융합될 경우 소프트웨어 산업에 미치는 영향에 대해 다룹니다. 또한 이러한 융합이 개인 데이터 보호, 학습 시스템 개선, 미래 사회 변화 등에 어떤 영향을 미칠 수 있는지에 대한 통찰을 제공합니다.

Session 2-2

9월 14일(목) 14:00~14:40
사회 : 임동혁 교수(광운대학교)



권혁준 교수
순천대학교
경제금융학과

블록체인 기술과 금융의 만남, STO (Security Token Offering)

블록체인 기술은 분산원장기술과 토큰 이코노미로 양 축으로 발전해 왔다. 기술의 발전에 따라 여러 비즈니스 모델이 생겨났으며, 세상의 파급효과 또한 크다. 기술이 금융을 만났을 때 미래는 어떻게 전개 될 것인가. 이제 당국도 기술에 의한 금융혁신을 준비하고 금융위험 여러 국가 금융기관에서는 기술에 의한 금융재편과 국가 간의 금융경쟁을 준비하고 있다. 토큰증권(Security Token), 제도권 진입: 2월, 금융당국은 토큰증권의 가이드라인을 발표했다. 디지털자산의 증권 여부 판단원칙 제시와 토큰증권의 발행 유통 규율 체계 정비 방안 등을 포함하여 시사점은 두 가지다. ① STO의 제도권 편입이다. 현재 국내는 다양한 STO 중, 자산 유통화에 초점을 맞춘 조각투자자 처중하고 있다. 이제 조각투자 플랫폼은 증권성이 인정됨에 따라 투자계약증권이 이행해야 하는 의무를 충족해야 한다. ② 메인넷의 중앙화 또는 개별화에 대한 시스템 구성이다. 본 연구는 STO의 이해와 금융당국의 가이드 라인 그에 따른 규제샌드박스 그리고 어떠한 블록체인 시스템이 STO에 적합할 것인지에 대한 고찰을 해본다.

Session 2-5

9월 14일(목) 16:10~16:50
사회 : 김태경 교수(경희대학교)



유주열 팀장
한국인터넷진흥원
블록체인정책팀

블록체인(주요 성과 및 과제) 및 NFT(안전한 이용표준안)

블록체인 기술은 중앙의 중개 기관이나 사전 신뢰가 없는 환경에서 거래 당사자 간 직접 거래를 가능하게 하고, 다양한 디지털 신산업을 촉진하는 기술이다. 정부는 이러한 블록체인을 육성하기 위해 '신뢰할 수 있는 4차 산업혁명을 구현하는 블록체인 기술 발전전략(2018.6)', '초연결·비대면 신뢰 사회를 위한 블록체인 기술 확산전략(2020.6)', '웹3 시대 기반 마련을 위한 블록체인 산업 진흥전략(2022.12)' 등 세 차례의 정부전략을 발표한 바 있다. 그리고 NFT는 블록체인 기반에서 동작하는 대표적인 서비스이다. NFT는 디지털 예술, 수집품, 음악, 영상 등 디지털 파일에 소유권이 적힌 디지털 증명서(메타데이터)를 소유자가 소유하고 있음을 증명하고, 누구나 소유권 이전 경로를 알 수 있게 하는 기술이다. 본 발표에서는 이러한 블록체인의 주요성과와 현재 추진중인 주요과제, 그리고 안전한 NFT를 이용할 수 있는 표준안에 대해 소개하고자 한다.

Session 2-3

9월 14일(목) 14:40~15:20
사회 : 임동혁 교수(광운대학교)



김태경 교수
경희대학교

유틸리티 토큰 기반의 비즈니스

유럽 집행위원회(European Commission)은 2023년 4월에 가상자산시장법, MiCA(Markets in Crypto-Assets)를 통과시켰다. 이는 그 동안 뚜렷한 법적 지위를 가지고 있지 않은 상태에서 빠르게 성장해 온 암호화폐 비즈니스 생태계의 합법적 사업화의 범위를 명확하게 하려는 최초의 공식적인 시도라는 평가를 받는다. 크기는 MiCA는 암호화폐를 법정 통화의 가치를 추종하는 유형과 특정 자산의 가치를 추종하는 유형, 그리고 이에 포함되지 않고 상품 및 서비스에 대한 디지털 접근을 제공하기 위한 목적을 가지고 오로지 발행인만 수용하는 가상자산 유형으로 구분하고, 세부적으로는 증권형, 유틸리티형, 자산준거형, 그리고 전자화폐형으로 구분하여 각 유형별 발행 및 운영 방식을 세분화한다. 현물자산의 가치를 추종함으로써 투자목적이 분명한 경우에는 보다 강력한 규제를, 그렇지 않고 마케팅 수단이나 엔터테인먼트 비즈니스에 사용될 수 있는 대부분의 알트 코인(alternative coins)은 유연한 규제 방식으로 구분했다. 이는 점에서 MiCA는 투자자 보호와 암호화폐 생태계 활성화의 양 측면을 고안한 결과로 평가된다. 게임산업, 메타버스, 로열티 프로그램, NFT 거래에 대부분 가치를 이전하고 거래하는 수단으로 활용되는 유틸리티 토큰에 관한 명확한 법적 의무를 부여한 MiCA는 관련 비즈니스의 활성화와 함께 가치 공동생성(value co-creation) 기반의 비즈니스 모델 탄생을 가속화할 것으로 기대된다.

Session 2-6

9월 14일(목) 16:50~17:30
사회 : 김태경 교수(경희대학교)



최선미 책임연구원
한국전자통신연구원

블록체인 서비스 전망

블록체인 기술을 활용하는 다양한 서비스를 소개하고 전망을 논다. 블록체인은 데이터를 안전하게 공유하고 가치를 이동하며 디지털 환경에서 사람, 사물 및 조직 간 신뢰를 부여하는 기술적 대안의 하나다. 디지털 전환의 이점을 강화하며 경제 사회 전반에서 혁신 서비스를 끌어낼 잠재력 높은 기술로 평가된다. 기존에 잘 알려진 NFT, DeFi, DAO 외에도 분산스토리지 네트워크, 클라우드, 지갑, 개인정보보호, 스트리밍, AI+ 등 다양한 서비스를 준비 중이다. CBDC 도입 논의의 진전, STO 및 스테이블 코인 제도화 추진 등에 따른 금융시장의 변화도 주목할만하다. 관련 서비스들이 확산함에 따라 API 및 도구 등 생태계 확장의 기반이 되는 개발 환경 역시 개선되는 추세다. 향후 기반 기술로 블록체인은 그 파급력을 더욱 확대할 것으로 예상하며, 산업 육성 및 소비자 보호를 위한 법 제도 정비 및 기술 혁신을 통해 변화를 견인할 것이다. 다만, 거버넌스 관련 이슈, 지속 가능한 생태계 조성을 위한 활동양, 사이버보안 강화 등 현안을 역시 부상하고 있어 논의가 필요한 최근 이슈를 살펴본다.



2023. 9. 14(목) - 9. 15(금) 섬유센터 17층 스카이뷰(온·오프라인 병행)

Session 3 AI와 보안

Session 3-1

9월 14일(목) 13:20~14:00
사회: 김영갑 교수(세종대학교)



박원형 교수
성신여자대학교

인공지능(AI) 보안관계 현황과 이슈

최근, 보안관계는 SIEM에서 AI 보안관계로 이동 중이며, 이에 따른 다양한 이슈와 문제점이 있다. 특히, 암호화된 트래픽 환경에서 사이버공격이 발생하고 있는 상황으로 네트워크 행위 기반의 공격 및 악성코드 분석과 탐지가 어렵다. 해외에서는 AI/XAI 기술을 활용하여 암호화된 공격 행위를 자동 탐지하는 기술이 연구되고 개발되고 있다. 이번 발표는 현재, 우리나라의 보안관계 전문업체 현황과 실태에 대해 알아보고 보안관계 전문업체에서 개발하여 활용하고 있는 AI 보안관계 솔루션과 국가기관의 연구소에서 암호화 트래픽 환경에서 AI/XAI 보안관계의 개발 현황에 대해 알아 본다. 이를 통해, AI 보안관계의 현황과 이슈를 분석하여 AI보안관계 발전 방향에 대해 소개 한다.

Session 3-4

9월 14일(목) 15:30~16:10
사회: 서영덕 교수(인하대학교)



김병재 책임연구원
한국인터넷진흥원

초거대 AI에 의한 사이버 위협과 우리의 대응 전략

초거대 AI는 우리의 사회, 경제, 문화에 큰 변화를 가져오고 있지만, 동시에 새로운 사이버 위협을 초래하고 있습니다. 이번 발표에서는 이러한 초거대 AI에 의한 사이버 위협을 살펴보고, 이에 대응하기 위해 우리가 어떤 고민을 하고 있는지에 대해 전달드릴 예정입니다. 보안 전문가들 사이에서는 생성형 AI가 현실적인 위협이 될 수 있다는 의견이 많습니다. 이에 대해서, 이것이 정말로 우리에게 위협이 될지 알고 싶었습니다. 그래서, 실제로 악성 코드를 생성하는 등의 악용 사례를 시뮬레이션 해봤고, 그 결과를 기반으로 우리의 분석 대응 체계를 어떻게 구축해야 할지에 대해 고민해 보았습니다. 결론적으로 절대적인 정답은 없습니다. 하지만, 지금까지의 고민과 시도를 공유함으로써, 앞으로의 발전 방향에 대해 함께 고민하는 시간을 가져 보았으면 좋겠습니다.

Session 3-2

9월 14일(목) 14:00~14:40
사회: 김영갑 교수(세종대학교)



허 규 실장
NAVER

피싱 탐지 자동화와 대응 전략

사회공학적 기법을 이용한 피싱 공격은 서비스 이용자의 개인 정보 유출을 유발하고, 이를 기반으로 2차 공격으로 이어지는 경우가 되고 있다. 시간이 지날수록 고도화되고 지능화되는 공격 유형들은 이용자로 하여금 더욱 거짓 정보를 쉽게 입력하게 만든다. 네이버는 사용자가 대면하게 될 피싱 사이트들을 선제적으로 탐지하기 위해 기술적으로 많은 방법을 고민했으며, 이를 기반으로 실제 이용자들에게 노출되는 피싱 사이트들을 탐지하고 차단하고 있다. 사용자가 노출되는 사이트들의 위험성을 평가할 수 있는 Client Side Detection과 함께 대응 전략들을 이야기하고 그동안 확인된 피싱 사이트들의 사례를 소개한다. 더불어 한계가 있는 지점들을 대상으로 기업과 기관에서 공조가 필요한 부분도 말씀드리고자 한다.

Session 3-5

9월 14일(목) 16:10~16:50
사회: 서영덕 교수(인하대학교)



윤성준 부장
한국교육학술정보원

머신러닝 기반 교육기관 사이버위협 분석체계 운영 현황 및 이슈

인공지능(AI)은 이제 모든 일상생활에서 활용되는 분야이다. 사이버 위협의 복잡성과 정교함이 나날이 증가하는 가운데, 인공지능(AI)은 보안관계 분야에서 사람만으로는 분석하기 어려운 다량의 데이터를 분석하는데 활용되고 있다. 이를 통해 좀 더 효과적이고 신속하게 사이버 위협에 대한 대응하기 위한 방법들을 계속 연구하고 있다.

교육부 산하에는 초·중·고교를 비롯 대학, 공공, 행정기관 등 다양한 형태의 기관 유형을 가지고 있으며, 이러한 다수의 기관들에게서 수집되는 사이버 위협에 대한 정보를 수집·분석·대응하는 일은 매우 난이도가 높은 일이다.

본 발표에서는 대규모 사이버 위협 데이터 분석을 요구하는 환경에서의 머신러닝 활용 방법과 이를 활용한 성과 및 보안관계 분석시스템 구축 사례에 대해서 설명한다.

또한, 현재의 한계 및 문제점들을 분석하여 향후 차세대 사이버 위협 수집 체계 구축에 대한 방안을 제시하고자 한다.



정진명 책임연구원
한국교육학술정보원

Session 3-3

9월 14일(목) 14:40~15:20
사회: 김영갑 교수(세종대학교)



김동철 책임연구원
KETI

지능형 영상보안 기술 현황 및 이슈

CCTV 영상감시로 흔히 표현되는 기존의 영상보안 기술은 CCTV 영상을 단순히 모니터링하는 형태였으나, 인공지능 기술과 5G와 같은 초고속 네트워크 기술이 급격하게 성장함에 따라 자율적이고 지능화된 상황인식 기반의 영상보안 기술로 발전하고 있다. 최근에는 CCTV를 중심으로 생체인식, 출입통제, 보안용 센서, 음성, 음향 정보 등과 융합하여 기능을 확장할 뿐만 아니라 성능도 고도화되고 있다. 또한, 기존의 도심 등 인구 밀집 지역을 중심으로 보안 인프라가 구축됨에 따라 고령자·원격지의 사회안전망 약화 문제를 해결하기 위한 무선 엠티 카메라 기반 영상보안 기술도 연구되고 있다. 본 강연에서는 지능형 영상보안 기술에 대한 전반적인 현황 및 이슈 사항에 대해 살펴보고자 한다.

Session 3-6

9월 14일(목) 16:50~17:30
사회: 서영덕 교수(인하대학교)



이상근 부교수
고려대학교
정보보호대학원

AI 모델의 복제 공격과 방어 기법

인공지능(AI)이 우리 사회 각 분야에 사용되면서, AI의 신뢰성에 대한 관심이 높다. 심층신경망의 취약점 중 하나인 적대적 입력 변조의 존재가 2014년 알려진 이후, 다양한 AI의 취약점이 알려져 있다. 본 강연에서는 클라우드 등에서 MLaaS (ML-as-a-service) 형태로 동작하는 AI의 숨겨진 모델을 높은 정확도로 복제할 수 있는 AI 모델의 복제 공격에 대해 소개하고자 한다. AI 모델 복제 공격은 S/W 복제와 마찬가지로 AI 개발 및 사용 비용을 회피하거나, 또는 학습 데이터 추출, 적대적 변조 생성과 같은 2차 공격을 위한 사전 단계로서 활용될 수 있다. 본 강연에서는 AI 모델 복제 공격의 원리와 대표적인 공격 방법을 소개하고, 이에 대응하기 위한 방어 기법을 소개한다.



2023. 9. 14(목) - 9. 15(금) 섬유센터 17층 스카이뷰(온·오프라인 병행)

Session 4 자율로봇지능과 플랫폼 기술

Session 4-1

9월 15일(금) 13:00~13:40
사회 : 윤주상 교수(동의대학교)



최종현 교수
연세대학교

일상 작업을 돕는 로봇 AI 학습 방법

최근 일상 생활을 도와주는 로봇을 위한 AI를 만드는 연구가 Embodied AI 의 형태로 발전해 오고 있습니다. 최근 다양한 simulator, benchmark 데이터 셋 등의 개발로 발전 속도가 가속되고 있습니다. 그러나 여전히 충분한 성능을 내는 로봇 AI를 만들기 위해서는 필요한 데이터의 양에 못 미치는 데이터 셋들이 모멸의 underfitting을 야기한다는 견해가 많이 있습니다. 이러한 benchmark 중 저희 그룹은 테스크의 복잡도와 현실성이 높은 ALFRED 벤치 마크에 주목하여, 학습 기반의 방법 뿐 아니라 최근 각광 받고 있는 Neuro-symbolic approach 를 사용한 방법론을 폭넓게 적용하여 높은 성공률을 달성하는 시스템을 개발하였습니다. 본 talk에서는 ALFRED 벤치 마크를 중심으로 Embodied AI 연구 동향과 최신 알고리즘을 소개하고 논의하는 시간을 갖도록 하겠습니다.

Session 4-4

9월 15일(금) 15:10~15:50
사회 : 윤주상 교수(동의대학교)



김봉석 책임연구원
한국전자기술연구원

자율주차로봇 시스템

본 강연에서 발표할 자율 주차로봇 시스템은 크게 헤더형과 저상형 두 가지 시스템으로 나누어져 있으며, 두 가지의 가장 큰 특징은 헤더형은 전장이 조금 긴 대신에 저상형에 비해 전고가 낮아 낮은 차량에 대해 대응이 가능하다는 장점이 있습니다. 본 발표에서는 한국전자기술연구원 연구에서 개발한 헤더형 위주로 설명하도록 하겠습니다. 인공지능 알고리즘이 아무리 좋아도 일단, 구현이 되어야 하기 위해서는 그에 알맞은 하드웨어 또한 매우 중요하다고 생각합니다. 특히, 주차로봇 같은 경우 일반 차 밑으로 들어가서 차량을 들고 이동하여 주차를 시키는 특수한 목적을 가지고 있기 때문에 하드웨어의 중요도가 상당히 높다고 할 수 있습니다. 이에 본 발표에서는 지능구현은 이미 센서를 통해서 수집된 데이터의 학습을 통해 이루어진 것이기 때문에 좀 생소한지만 하드웨어에 대해 초점을 맞추어 설명을 하도록 하겠습니다. 헤더형 주차로봇을 개발하기 위해서는 가장 중요한 것이 전고에 맞는 모터부터 개발을 해야 합니다. 지금 상용모터 중에는 이를 만족하는 것이 없기 때문에 모터를 사양에 맞게 개발하여야 하고 또한 이동 메커니즘을 전역적으로 새로운 메커니즘으로 구성해야 합니다. 따라서 본 연구에서는 인공지능 알고리즘을 사용하기 위한 하드웨어를 구성할 때 구동부, 센싱부, 전장부(통신부)를 어떻게 구성하였는지를 설명할 예정입니다.

Session 4-1

9월 15일(금) 13:40~14:20
사회 : 윤주상 교수(동의대학교)



정병진 선임연구원
한국전자기술연구원

Reactive Robot Control을 위한 거대언어모델 활용 - 반사신경지능과 안전지능

Reactive Robot Control(반응형 로봇 제어)은 비정형 환경에서의 로봇 활용을 위해 오랫동안 연구되어온 주제이다. 기존에는 Adaptive Control, Potential Field, 등의 적응형 알고리즘 및 Semantic Segmentation 등 확장된 인식 알고리즘을 통한 비정형 환경에서의 로봇 행동 기반 플래닝이 연구되었다. 최근에는 딥러닝, 강화학습, 거대언어모델 등 머신러닝 기술의 발전에 힘입어 기존의 이동 로봇 등에 적용이 한정되었던 반응형 로봇 제어의 개념을 '높은 수준 비정형 환경에서의 이동 조작'과 같은 정교한 작업 수행에 확장 적용할 수 있는 가능성이 열리고 있다. 본 발표에서는 이러한 머신러닝 기반 반응형 로봇 제어에 대한 고찰을 공유하고, 이를 세분화한 개념인 반사신경지능 및 안전지능에 대하여 논의하고자 한다.

Session 4-5

9월 15일(금) 15:50~16:30
사회 : 윤주상 교수(동의대학교)



김곤우 교수
충북대학교

로봇 자율주행을 위한 SLAM 및 AI

최근 자율주행차, 배송로봇 등 여러 분야에서 자율주행 기술을 적용한 다양한 서비스를 개발하기 위한 노력이 증가하고 있다. 이러한 자율주행의 핵심 기술은 환경 인식, 위치 인식, 판단, 경로 계획 및 제어 기술로 구분할 수 있다. 그 중에서도 위치 인식 기술은 자율주행을 위한 핵심기술이라 할 수 있다. SLAM(Simultaneous Localization And Mapping) 기술은 '동시적 위치인식 및 지도작성' 방법으로 주변 환경 지도를 기반으로 자신의 위치를 인식하는 동시에 지도를 작성하는 기술을 의미한다. 기존 SLAM 기술은 2차원 격자 지도(grid map) 또는 3차원 점군(point cloud) 형태의 환경 지도를 작성하는 것이 일반적이었다. 하지만 정적 환경을 가정하는 SLAM 기술은 다양한 동적 객체가 존재하는 일반적인 환경에 적용하는데 한계가 존재하였다. 이를 극복하고 좀 더 복잡한 작업을 수행하기 위해 최근에는 인식한 환경에 대한 의미론적(semantic) 개념을 SLAM 프로세스에 적용하는 연구가 증가하고 있다. 본 발표에서는 SLAM 기술에 대한 개념을 알아보고 SLAM 프로세스에 적용되고 있는 AI 기술과 이를 통해 연구되고 있는 Semantic SLAM 관련 연구 동향을 알아본다.

Session 4-3

9월 15일(금) 14:20~15:00
사회 : 윤주상 교수(동의대학교)



장민수 책임연구원
한국전자통신연구원

파운데이션 모델의 로봇 적용

대형언어모델(Large Language Model)의 발전은 인공지능 분야의 각종 문제 해결 능력과 범위를 빠르게 향상 확장하고 있으며, 이는 로보틱스 분야도 예외는 아닙니다. 범용 로봇 구현에 있어 병목 지점 중 하나였던 작업 계획 문제를 대형언어모델로 손쉽게 유연하게 해결하는 방법론이 등장했습니다. 더불어, 언어는 물론이고 시각, 청각, 행동 등을 포함한 다중감각 정보를 처리할 수 있는 멀티모달 대형 언어 모델(Multimodal Large Language Models)이 등장하여 로봇과 체화 에이전트 분야의 적용 가능성을 높이고 있습니다. 본 발표에서는 대형언어모델과 사전훈련모델(Pretrained Model)을 로봇 분야의 다양한 범용 문제 해결에 어떻게 적용하려고 시도하고 있는지 여러 사례를 소개하고, 향후 이러한 기술들이 어떻게 로봇 파운데이션 모델로 발전해 나갈지 예상해 보고자 합니다.

Session 4-6

9월 15일(금) 16:30~17:10
사회 : 윤주상 교수(동의대학교)



구세완 책임연구원
LG전자

에지-클라우드 기반 로보틱스 시스템 설계 및 구현

지능형 로봇은 인공지능과 복잡한 기능을 갖는 센서, 액츄에이터를 통합한 매우 복잡한 시스템으로 진화하고 있으며, 이로 인해 독립적인 로봇이 아닌 클라우드와 엣지와의 연결성이 점차 중요해지고 있다. 이로 인해 로봇 시스템에 최소의 하드웨어만 남기고 클라우드나 엣지로 컴퓨팅 자원을 오프로딩(Offloading)하여 효율적이고 지속적으로 로봇을 진화시킬 수 있는 방법이 모색되고 있다. 한편, 클라우드 기반의 쿠버네티스 플랫폼은 로봇 서비스 애플리케이션을 마이크로서비스로 가상화하여 운영하는데 가장 강력한 도구이다. 본 발표에서는 클라우드 로보틱스 솔루션을 통해 Private 5G MEC 기반의 자율 주행 로봇을 실증한 사례와 엣지 클라우드 기반 3D 라이다 센서 솔루션을 로봇과 통합하여 운영한 경우를 통해 클라우드와 엣지에 연결된 로봇의 효율성을 소개한다.



2023. 9. 14(목) - 9. 15(금) 섬유센터 17층 스카이뷰(온·오프라인 병행)

Session 5 Human-Centric Data Analytics

Session 5-1

9월 15일(금) 13:00~13:40

사회 : 이기용 교수(숙명여자대학교)



Human centric AI in KETI

메타버스를 앞세운 혼합현실 서비스 시대의 도래를 준비하면서 실제계와 가상 세계에서 인간을 연결하기 위한 다양한 인공지능 기술들이 서비스를 준비하며 고도화되고 있다. 본 발표는 가상 휴먼 (Digital human) 기술의 상용화를 위해 필요한 인공지능 기술들을 소개하고, 한국전자기술연구원이 보유하고 있는 관련 기술 현황을 통해 기술 수준을 소개하고자 한다.

신사임 센터장
한국전자기술연구원

Session 5-2

9월 15일(금) 13:40~14:20

사회 : 이기용 교수(숙명여자대학교)



딥러닝을 활용한 이상 탐지

실세계 데이터의 광범위한 학습을 통해 구축되는 데이터 지능(Data Intelligence)은 다양한 분야에서 활발하게 연구되고 있으며, 수많은 애플리케이션에서 적극적으로 활용됨에 따라 큰 영향과 가치를 창출하고 있다. 이 강연에서는 데이터셋 내에서 비정상적인 패턴을 식별하는 이상 탐지(Anomaly detection) 작업에 대해 다룬다. 이상 탐지가 무엇인지에 대한 기본적인 개념에서부터 이상 탐지가 사용되는 다양한 시나리오를 살펴보고, 이를 실제 도메인에 적용할 때 발생하는 여러 중요한 챌린지들에 대해 설명한다. 더 나아가, 테이블, 텍스트, 시계열 데이터를 처리하기 위한 딥러닝 기반 이상 탐지 기술에 대한 최근 연구들을 소개한다.

이동호 조교수
연세대학교

Session 5-3

9월 15일(금) 14:20~15:00

사회 : 이기용 교수(숙명여자대학교)



자기 정규화 계층이 있는 단순 컨벌루션 신경망에 기반한 연령 및 성별 예측

인간의 얼굴 관련 문제를 자동화하는 것은 연구 커뮤니티의 큰 관심 주제였으며 다양한 실제 응용 분야에서 사용되고 있다. 얼굴 이미지 데이터에서 자동화된 연령, 성별 및 인종 인식을 위한 여러 머신러닝/딥러닝 모델이 존재한다. 이 연구들은 벤치마크 데이터를 사용하여 인상적인 결과를 얻었지만, 다양한 얼굴 형태가 존재하는 실제 사례에서 성능은 여전히 부족하다. 또한 얼굴 이미지에 대한 대부분의 공개 벤치마크 데이터 셋은 한 얼굴 그룹(예: 백인 또는 아시아인 얼굴)에 대해 강하게 편향된 반면 다른 인종(예: 중국 또는 라틴계)은 크게 부족하다. 머신러닝/딥러닝 모델은 나이, 성별, 인종에 따른 차이가 두드러지지 않는 성능을 보여야 한다. 기존의 모델들은 여전히 인종에 따른 편차가 두드러진 결과를 보이고 있다. 이러한 문제를 해결하기 위해, 자기 정규화 계층을 가지는 경량의 컨벌루션 신경망을 제안하였다. 이 모델은 대표 재료를 학습하여 지속적으로 높은 정확도를 얻는 자체 정규화 멀티태스킹 딥러닝 모델이다. 훈련 중 인종 편향 문제를 해결하기 위해 연령, 성별 및 인종 예측에 대한 FairFace 벤치마크를 모델에 활용하고, 입력 이미지를 연령 9개, 성별 2개, 인종 7개 등급으로 분류하였다. 모델의 공정성은 클래스에 추가 가중치를 할당하여 달성하였다. 제안한 프레임워크와 데이터 향상 및 공정성 기술을 사용하여 실험을 진행하였고, 얼굴 이미지 데이터 셋에서 연령, 성별 및 인종 예측을 동시에 진행이 가능하면서도 타 모델 대비 높은 정확도를 보임을 확인하였다.

권준호 교수
부산대학교
정보컴퓨터공학부

Session 5-4

9월 15일(금) 15:10~15:50

사회 : 이기용 교수(숙명여자대학교)



심전도(ECG) 데이터의 프라이버시 보호 분석

스마트 위치의 대중화로 디지털 헬스 서비스 시장이 최근 급속히 성장하고 있다. 더불어 인공지능 기술의 발달로 심전도(ECG: Electrocardiogram) 데이터를 통해 다양한 심장 질환을 정확하게 분석 가능한 시대가 되었다. 하지만 ECG 데이터는 생체 인증(biometrics) 수단으로 사용될 만큼 개인 식별성이 높다. 따라서 ECG 데이터의 분석 과정에서 개인이 식별되고, 그를 통해 프라이버시가 침해되는 상황을 방지할 필요성이 대두되고 있다. 본 발표는 ECG 데이터를 통해 부정맥 질환을 진단할 때, 개인 식별을 통한 프라이버시 침해가 발생하지 않도록 하는 방법을 소개한다. 구체적으로 말하면 ECG 데이터 분석의 본래 목적인 질병 진단/분류 정확성은 유지하면서, ECG 데이터를 통한 개인 식별은 불가능하게 데이터를 변조하는 인공지능 기술이다. 먼저 ECG 데이터에서 개인 식별을 위해 사용되는 어텐션 분포(attention distribution)와 질병 분류를 위해 사용되는 어텐션 분포를 독립적으로 구한다. 그리고 이들을 이용하여 분류 성능은 유지하면서 개인 식별은 방해하는 노이즈 생성 모델을 만든다. 이 노이즈 모델을 사용하여 ECG 데이터를 변조할 경우, 분류 정확도는 90% 이상으로 유지되면서 식별성은 제거되는 것을 실험 평가를 통해 확인하였다.

정연돈 교수
고려대학교
컴퓨터학과

Session 5-5

9월 15일(금) 15:50~16:30

사회 : 이기용 교수(숙명여자대학교)



디지털 병리에서의 인공지능 활용 동향

의료 분야는 임상 데이터에 근거하여 질병의 진단 및 치료 방법을 개선해나가는, 인간 중심적 데이터 분석에 기반한 분야로 볼 수 있다. 환자의 상태를 정확히 진단하는 것은 질병의 진행을 예측하고 적절한 치료 방향을 결정하는데 있어 매우 중요하다. 특히, 암 등 중증 질환의 경우 조직 병리 진단을 통해 최종 진단이 이루어지므로 조직 병리 진단의 정확성은 매우 중요하다. 최근, 진단용 조직 병리 슬라이드 전체를 스캔하여 생성한 대규모 이미지를 모니터로 판독하는 디지털 병리 진단 시스템을 도입하는 의료기관들이 증가하고 있으며, 조직 병리 이미지를 딥러닝 기반 이미지 분석 및 패턴 인식 기술로 분석하여 질병의 진단 및 예후 예측 등을 보조하는 정보를 제공하는 방법이 연구개발을 거쳐 상용화되고 있다. 또한, 적절한 치료 방향을 결정하기 위해 환자의 치료제 반응 여부 정보를 조직 병리 이미지로부터 추출하여 제공하는 방법도 연구되고 있다. 본 강연에서는 조직 병리 이미지 데이터의 생성 및 관리부터 진단 보조를 위한 인공지능 기술 및 이를 사용자에게 제공하는 시각화 방식까지 다양한 관점에서의 최신 연구개발 동향을 살펴본다.

곽태영 이사
딥바이오

Session 5-6

9월 15일(금) 16:30~17:10

사회 : 이기용 교수(숙명여자대학교)



생성형 AI 이슈와 보안

본 발표에서는 '생성형 AI'의 개념을 주요 주제로 삼고, 그로 인해 발생할 수 있는 다양한 문제들에 대한 심도 있는 이해를 제공한다. 우리는 콘텐츠의 문제, AI의 악용 및 오남용, 그리고 입력 데이터의 문제와 같이 AI의 역기능적인 이슈들을 분석한다. 이들 주제는 AI가 자동으로 생성하는 콘텐츠의 품질과 윤리적, AI의 잘못된 사용 방법, 데이터의 편향성 및 부정확성이 결과에 어떻게 영향을 미치는지 등을 포괄한다. 이어서, 보안과 관련된 이슈도 다룬다. 이 부분에서는 AI의 보안 취약성을 검토하고, AI를 이용한 보안 위협을 파악하는 동시에, AI를 활용하여 보안을 강화하는 방법을 모색한다. 본 발표를 통해 참석자들은 AI의 다양한 측면을 이해하게 되며, AI가 발생시킬 수 있는 문제를 인식하고, 그 문제에 대한 해결책을 찾는 데 도움을 받을 수 있다.

최대선 교수
송실대학교



2023. 9. 14(목) - 9. 15(금) 섬유센터 17층 스카이뷰(온·오프라인 병행)

Session 6 과학기술과 AI 활용 / Software Safety

Session 6-1

9월 15일(금) 13:00~13:40

사회 : 최명석 단장(KISTI)



이승우 팀장
한국과학기술
정보연구원

과학기술 문헌 분석을 위한 사전학습 언어모델 개발 사례

최근 챗GPT의 유명세로 인공지능 특히, 언어모델에 대한 관심 뜨겁다. 언어모델은 이해형 언어모델과 생성형 언어모델로 구분될 수 있으며, 챗GPT는 생성형 언어모델에 해당한다. 최근에는 거대화된 생성형 언어모델 연구에 집중되는 경향이 있지만, 구축 및 운영 비용을 고려했을 때, 용도에 따라 이해형 언어모델도 여전히 필요하다. 특히 범용이 아닌 특정 분야에 특화된 언어모델의 경우 더욱 그러하다. 한국과학기술정보연구원(KISTI)에서는 과학기술 문헌 정보를 분석하고 서비스하는데 활용될 수 있는 이해형 언어모델 알고리즘들이 개발되어 왔는데, KISTI에서는 그 중에서 BERT, ELECTRA, DeBERTa 알고리즘을 기반으로 과학기술 분야 한국어 언어모델들을 개발하였다. 학습을 위해 다양한 과학기술 문헌 (논문, 특허, 보고서 등) 데이터를 수집 및 가공하였으며, 학습된 모델의 평가를 위해 과학기술 문헌 분석용 평가 데이터셋도 구축하여, 범용 언어모델과의 비교 평가에 활용하였다. 구축된 모델 및 데이터는 AIDA (aida.kisti.re.kr)를 통해 공유되고 있다.

Session 6-4

9월 15일(금) 15:10~15:50

사회 : 이은서 교수(안동대학교)



민상운 대표이사
솔루션링크

4차 산업혁명시대 소프트웨어 안전 : 현재와 나아가야 할 방향

4차산업혁명 시대 소프트웨어 기반의 혁명이다. 특히, 소프트웨어에 기반한 산업융합과 신 산업 창조가 핵심이다. 소프트웨어 안전은 이러한 4차 산업혁명, 나아가 지능형 소프트웨어 시대를 성공적으로 이끄는 핵심 요소이다. 이러한 중요성에도 불구하고 소프트웨어 안전 공학 자체에 대한 인식과 연구는 아직 발전되어야 할 바가 많다. 본 세션에서는 소프트웨어 안전의 중요성, 4차 산업혁명시대의 소프트웨어 특성, 소프트웨어 안전의 정의 및 현재의 접근 등에 대해 살펴본다. 또한 안전공학의 기술이 되는 사고모델의 개념을 설명하고, 지능형 소프트웨어 시대에 감당하여야 할 소프트웨어 안전 공학의 당면과제에 대하여 살펴본다.

Session 6-1

9월 15일(금) 13:40~14:20

사회 : 최명석 단장(KISTI)



이 용 팀장
한국과학기술
정보연구원,
인공지능
데이터연구단

맞춤형 시각지능 개발을 위한 학습데이터와 모델 개발 지원 서비스

AI 기술의 급속한 발전 및 확산과 더불어 다양한 전문분야에서 AI 모델을 개발하기 위한 학습데이터에 대한 수요가 크게 증가되어 왔다. 특히, 학습데이터 부족 문제를 해결하기 위해 민간 및 학계 주도로 학습데이터가 양산되어 왔다. 하지만, 산발적으로 공유되고 있는 대규모 학습데이터에서 필요한 데이터를 찾아 활용하기에는 양적, 질적 한계가 여전히 존재한다. 본 강연에서는 AI 생태계 발전을 촉진하기 위한 학습데이터의 공유·활용의 필요성에 대해 설명한다. 특히, 범람하는 학습데이터 시대에 맞춤형 시각지능 개발을 효과적으로 지원하기 위한 서비스를 소개한다. 구체적으로, 1) 대규모 공개 학습데이터의 공동 활용을 위한 맞춤형 학습데이터 검색 기술, 2) 학습데이터 확보가 어려운 재난/안전 분야 등을 위한 이미지 생성 기술, 3) AI 비전문가도 모델을 바로 제작할 수 있는 모델 제작 기술에 기반한 맞춤형 학습데이터 및 모델 개발 지원 서비스를 소개한다.

Session 6-5

9월 15일(금) 15:50~16:30

사회 : 이은서 교수(안동대학교)



김태호 박사
ETRI

거대 인공지능 기술은 SW 개발을 어떻게 변화할 것인가? - 자동 코딩 기술과 SW 신뢰성

ChatGPT가 사람과의 대화 뿐만 아니라 코딩도 할 수 있다는 것은 SW 개발자들에게 충격을 가져왔다. SW 개발이 쉬워지고 생산성이 높아질 것 같다는 긍정적인 의견부터 SW 개발자는 더 이상 필요없으니 해고하겠다는 성급한 의견까지 표출되고 있다. 과거에는 제한적으로 활용된 SW 개발 자동화, 거대 인공지능 기술이 도입되면서 SW 개발 과정에 큰 변화를 일으킬 수 있을 것으로 보인다. 한편으로는 이렇게 자동으로 생성된 SW의 신뢰성 및 책임성에 대한 우려도 역시 존재한다. 이에 자동 코딩에 거대 인공지능 기술의 적용 가능성과 한계 및 활용 방안을 살펴보고자 한다. 그리고, AI 기술이 도입된 후의 SW 개발 과정 및 생태계의 미래 모습을 전망하고자 한다.

Session 6-3

9월 15일(금) 14:20~15:00

사회 : 최명석 단장(KISTI)



안인연 팀장
한국과학기술
정보연구원
감염병이해자일팀

코로나19 대응을 위한 인공지능 기술개발 사례

2020년 초 중국으로부터 최초 보고된 코로나19는 현재까지도 인류의 건강과 안전을 위협하며 막대한 피해를 야기하고 있음. 한국 정부는 2015년 중동지역으로부터 국내로 유입된 신종 코로나바이러스인 메르스(Middle East Respiratory Syndrome; MERS)에 대한 대응술련을 제시하기 위하여 학문분야 또는 부처 간 장벽을 허문 다양한 형태의 융합연구들을 수행해 왔음. 본 발표에서는 코로나19 대유행이라는 글로벌 재난상황에 효과적으로 대응하기 위한 연구자들의 노력과 성과물을 인공지능 기술 관점에서 소개하고자 함.

Session 6-6

9월 15일(금) 16:30~17:10

사회 : 이은서 교수(안동대학교)



지은경 교수
KAIST

원자력 안전 소프트웨어 및 블록체인 합의 알고리즘 대상 정형 검증 적용 사례

안전 중요 시스템에서 SW 비중이 높아지면서 SW로 인한 위험이 발생하지 않도록 SW 안전성을 확보하기 위한 기법의 개발 및 적용이 중요해지고 있다. 본 강연에서는 SW 안전성에 대한 자동화된 엄밀한 검증을 수행하고자 정형 검증 기법 중 모델 체킹 기법을 적용한 사례를 소개한다. 모델 체킹 기법을 원자력 안전 소프트웨어 대상 적용한 사례와 블록체인 합의 알고리즘 대상 적용한 사례를 소개하고, 기대효과 및 향후 발전방향을 논한다.