



ACK
2025
논문집

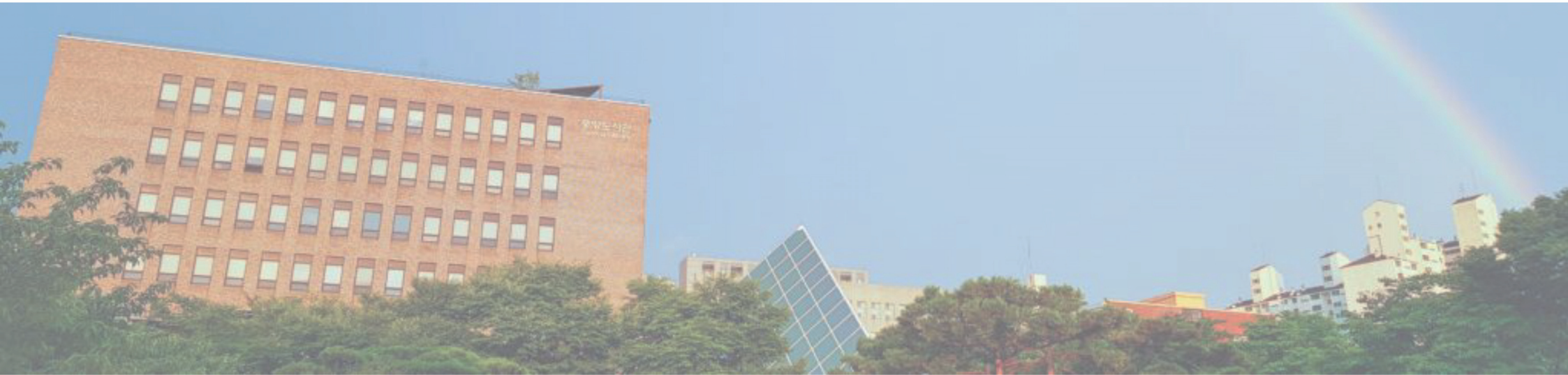
Annual Conference of KIPS 2025

신진학자 워크숍

////////////////////

데이터 프라이버시 보호를 위한 기술적 접근과 기업에서의 도전

안용대 교수(숭실대학교)



데이터 프라이버시 보호를 위한 기술적 접근과 기업에서의 도전

2025.11.07.(금)

송실대학교 IT대학 글로벌미디어학부

안용대

연사 소개

- 안용대

• 경력

- 2004.03.~2012.02. KAIST 산업및시스템공학과 졸업
- 2012.01.~2015.02. 현대중공업 조선사업기획부 근무
- 2015.03.~2021.08. 서울대학교 산업공학과 데이터마이닝 연구실 박사졸업
- 2021.09.~2022.08. 세종대학교 호텔관광대학 호텔관광경영학과 연구교수 근무
- 2020.09.~ 2025.02. 디사일로 리서치팀 근무
- 2025.03.~ 숭실대학교 글로벌미디어학부 재직

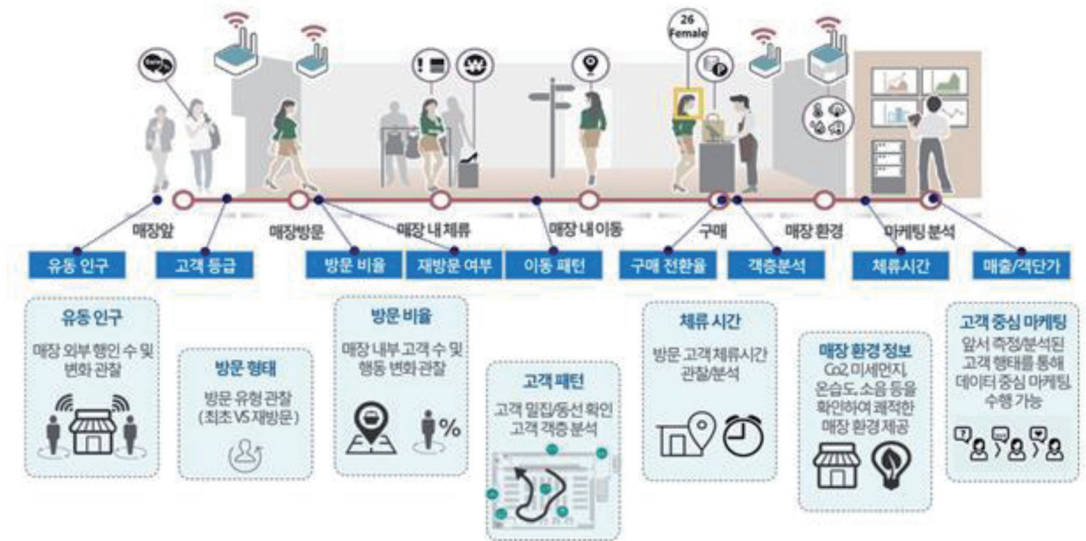
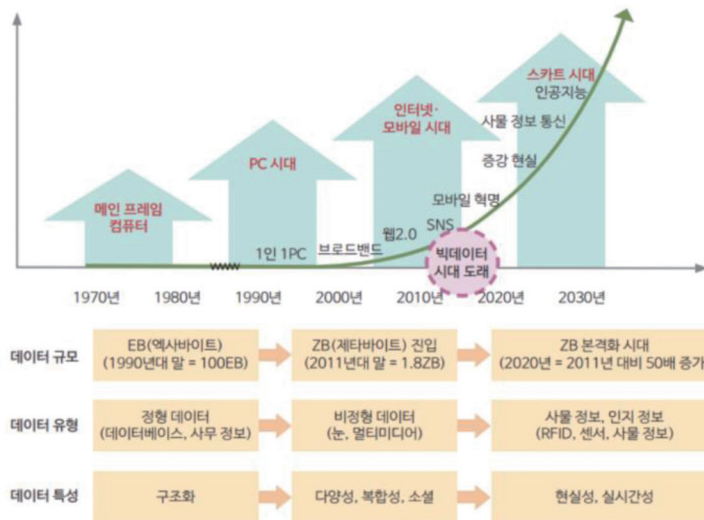


프라이버시 강화 기술의 필요성

- 프라이버시 이슈의 등장 배경

• 수집 가능한 데이터의 양과 질이 달라지고 있음

- 예전에는 공장 단위라던지, 사업체 단위로 장비 혹은 생산과 관련된 데이터가 주로 분석의 대상이었음
- 하지만, 최근에는 기술의 발전으로 개인과 관련된 민감한 데이터를 많이 수집할 수 있게 됨



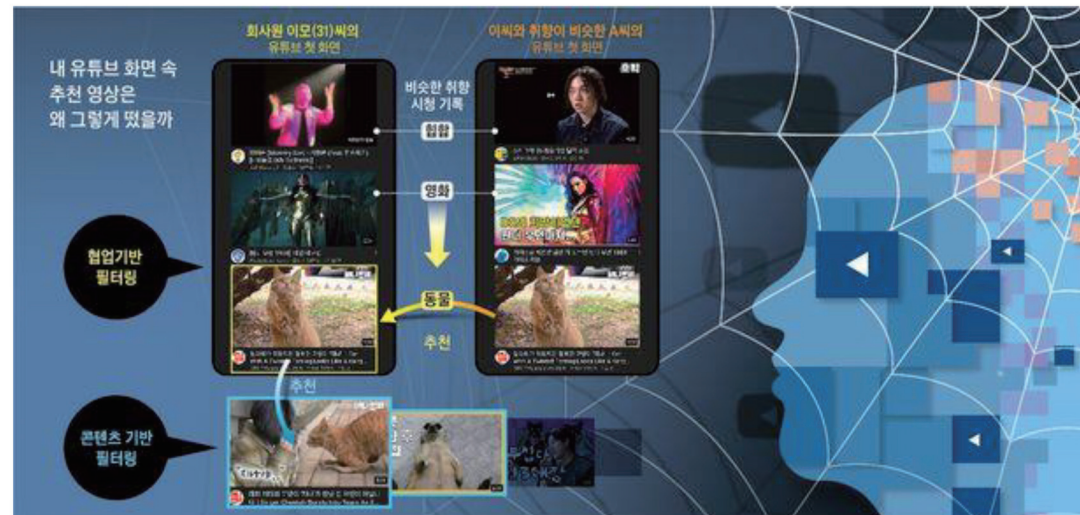
* 이미지 출처: http://banker.kfb.or.kr/webzine/mobile/section.php?idx=78&PublishDate=201809&sub_idx=1546

* 이미지 출처: <https://kolonbenits-time.com/20>

프라이버시 강화 기술의 필요성

- 프라이버시 이슈의 등장 배경

- 기업 간의 경쟁이 치열해지면서 개인 레벨의 추천이 필요한 수준의 경쟁 상황이 도래함
- 개인 레벨의 니즈를 파악하기 위해서는 당연히 개인 레벨에서 분석이 더욱 중요해짐 → 개별 고객에 대한 개인정보를 수집해야 되는 필요성이 증가하고 있음



* 이미지 출처: https://www.chosun.com/economy/tech_it/2021/01/01/IYRYZY6L45GVFB6IUkDDGDRlHY/

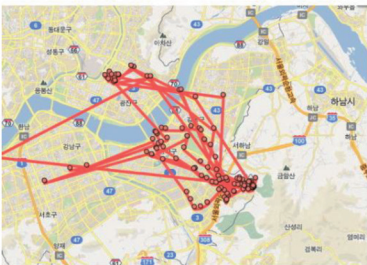
프라이버시 강화 기술의 필요성

- 데이터의 활용 vs. 프라이버시 침해

- 개인 레벨의 서비스를 제공하기 위해서는 개인 레벨의 개인정보가 반드시 필요함
- 하지만, 반대로 이로 인해서 개인정보의 노출과 유출이 발생하게 때문에 딜레마가 발생하게 됨

※개인정보예시

• 위치정보

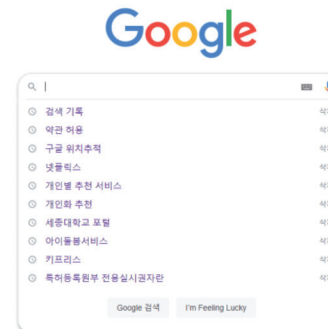


• 지인들과 찍은 사진

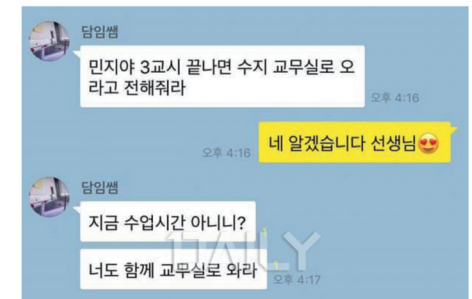


designed by freepik

• 검색기록



• 메신저대화기록



※ 지도 이미지 출처: <https://ccami.net/39>

※ 메신저 이미지 출처: <https://www.daily.co.kr/life3128152122#lifeback>

프라이버시 강화 기술의 필요성

- AI에 대한 글로벌 추세

- **AI 규제 논의**
- **글로벌 주요국들은 다양한 방법으로 AI의 신뢰성을 확보하기 위해서 전담기관을 설립하고 있음**
 - AI 안전연구소 설립을 추진하고 있음
 - AI 기술의 안정성 평가, AI 관련한 안전 및 위험 등 기술연구, 인증체계 및 표준화 마련, 글로벌 협력체계 구축 등을 수행함

인공지능 윤리 관련 주요국 동향		AI 기술 발전에 따른 부작용	
미국	- AI 윤리적, 법적, 사회적 의미 연구 - 윤리체계 구축 - 안전기준 마련	개인정보 유출	사생활 침해
중국	- 안전기준 마련	개인정보 자기 결정권 침해	불건전 정보 확산
인도	- 윤리위원회 설립 및 윤리행동강령 신설	지능정보 격차	
영국	- 데이터 윤리체계 구축 및 AI 인식 재설계		
프랑스	- AI 관련 규정 마련 - 윤리위원회 설립 및 윤리행동강령 신설		
싱가포르	- 윤리체계 구축		
유럽연합	- AI 효율적 사용 위한 규제 및 장려책 마련 - 안전인식 기술 규제 논의		
한국	- AI 이용자 보호체계 마련 추진		

그래픽: 김지영 디자인가자

생성형 AI 개발 중단 찬반 논쟁

개발 속도 조절해야



"GPT-4보다 더 강력한 AI는 인류 위험 초래, 개발을 최소 6개월 잠정 중단하자."
(미국 '실의 미래 연구소' 공개서한)

스티브 워즈니악 애플 공동창업자, 일론 머스크 테슬라 CEO, 유발 하라리 예루살렘히브리대 교수 등

"기술 개발자들도 AI가 인류 실존에 위협 인정, 그러면서도 위험을 완화할 계획 없어."
에마드 모스타크 스테빌리티AI CEO

신중론



"AI는 질병과 기후문제 해결에 도움 되지만 국가안보와 사회의 잠재적 위협 해결 역시 중요."
(과학기술자문위원회 회의)

조 바이든 미국 대통령

개발 중단하면 안 돼



"일시 중단을 요청한다고 문제가 해결 되지 않는다. 분명한 건 이 기술에 큰 이점이 있다는 것."
빌 게이츠 마이크로소프트(MS) 창업자



"AI 개발 중단은 말도 안 되는 일. 유익한 기술의 위험성을 꾸며서 사람들을 두렵게 하는 것."
안드루 메타 수석과학자

"AI 개발을 6개월간 유예하자는 건 끔찍한 아이디어"
앤드루 옴 딥러닝AI 창립자

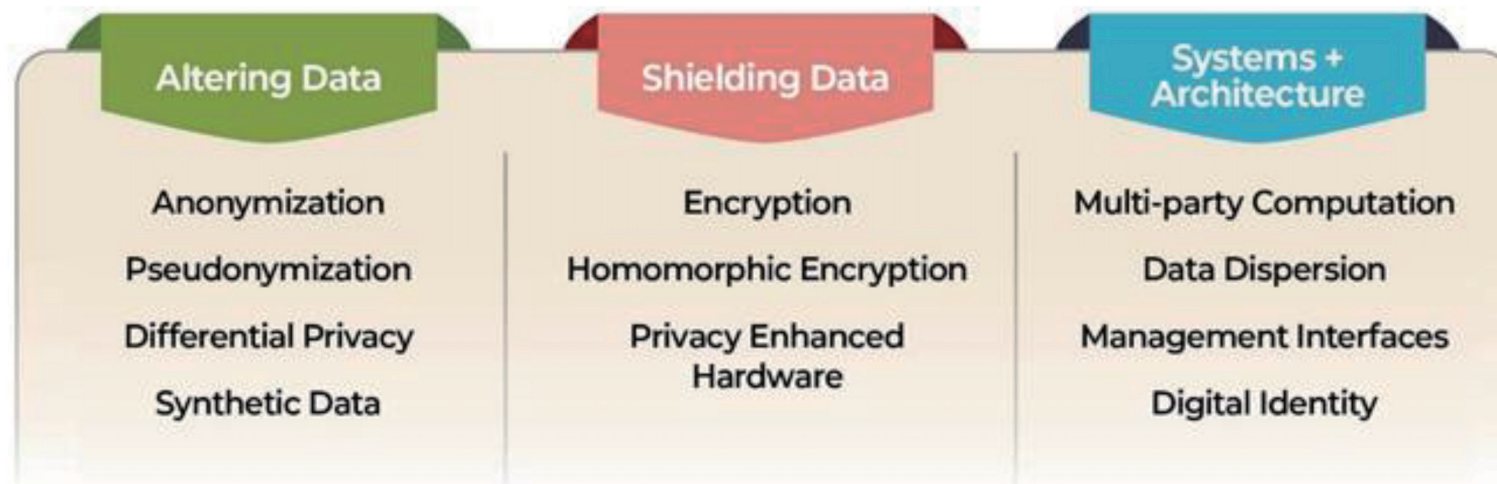
※ 이미지 출처: <https://news.mt.co.kr/mtview.php?no=2020033009593747341>

※ 이미지 출처: <https://www.donga.com/news/Economy/article/all/20230407/118723700/1>

프라이버시 강화 기술의 필요성

- 데이터 활용과 프라이버시 침해간 딜레마를 감소시키기 위한 대안

- 프라이버시 강화 기술(Privacy Enhancing Technologies, PETs)



프라이버시 강화 기술의 필요성

- 프라이버시 강화 기술(Privacy Enhancing Technologies, PETs)

- PETs는 신뢰할 수 없는 환경에서도 데이터를 안전하게 보호하면서 데이터로부터 가치를 창출할 수 있게 해주는 기술
- '데이터 보호와 활용의 충돌'이라는 문제를 해결해주는 수단으로서, 2022년 Gartner가 선정한 핵심전략 기술로 선정되었고 많은 기업에서 투자를 하고 있음

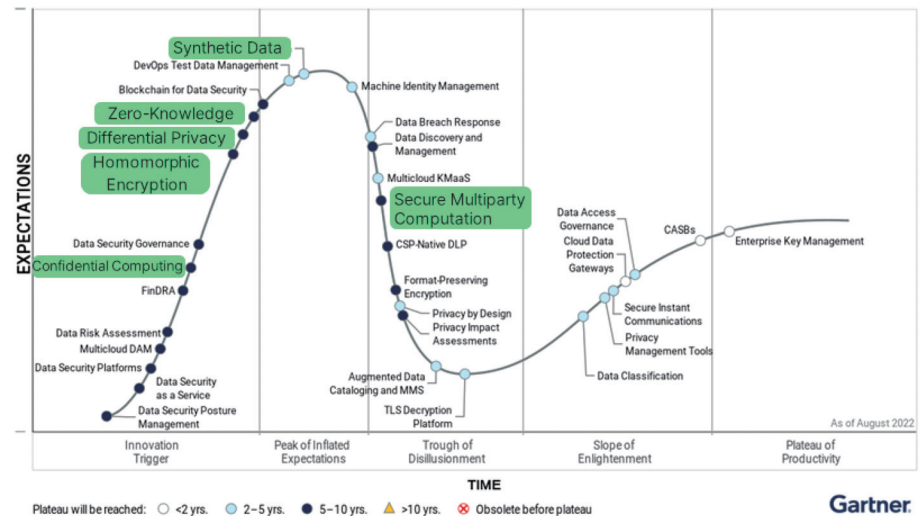
● PET 라이브러리 및 툴을 개발 중인 주요 글로벌 기업

Microsoft Research Google IBM Meta

● PET Summit North America 2022 참여 기업



● Hype Cycle for Data Security 2022



- 해당 내용은 오프라인 발표에서 말씀드리도록 하겠습니다.