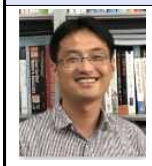
연구자 기초자료

주관기관	부산대학교 PUSAN NATIONAL UNIVERSITY	수행기관	BizBRIDGE

연구자 정보

이름	소속	전공분야	전화번호	이메일
 최윤호	정보의생명공학대학 정보컴퓨터공학부	컴퓨터 및 네트워크 보안, AI 보안, 블록체인 보안	051-510-2781	yhchoi@pusan.ac.kr

□ 주요 연구자 연구분야 및 경력

연구실 (위치)	연구분야(Keyword)
소프트웨어 및 시스템보안 연구실 (Software & System Security Laboratory)	○ Research Area ① Information Security • Network Security (V2X, SDN/NFV, Internet of Things(IoT) security, Fintech Security, etc.) • Computer Security (Malware (Worm, Virus, Botnets, Deep Packet Inspection(DPI), etc.) • Main Research Topics: Anomaly detection/prevention, Block Chain ② Algorithm • Machine learning (Ensemble algorithm, deep neural network architecture for anomaly detection) for anomaly detection • Privacy Preserving Machine Learning (PPDM, PPDL) • String/Regex Pattern Matching ③ Software Develepment • Bone age Estimation • Value Estimation of Real Estate • Mobile/Server Applications * 홈페이지: https://sec.pusan.ac.kr/sec/index.do
경력	• (현) 부산대학교 정보컴퓨터공학부 정교수 • (현) 부산대학교 클라우드 보안 센터장 • (현) 정보보호특성화 교육.연구 기획단 단장 • (현) 조달청 평가위원 • (현) 부산항만공사, 한국예탁결재원 정보보호자문위원 • (현) 한국인터넷정보학회, 한국창업학회 이사, 편집위원 • (현) 한국통신학회, 한국정보보호학회 이사 • (현) 한국연구재단 국책연구본부 전문위원(정보보안) • (전) 경기대학교 융합보안학과 조교수(2012~2014) • (전) 삼성전자 통신연구소/네트워크사업부 책임연구원(2010~2011) • (전) 미국 펜실베니아주립대학교 박사후 연구원 (2009) • (전) 서울대학교 전기컴퓨터공학부 공학박사 (2008)

전공분야	클라우드 보안, 제로트러스트, 프라이버시, PPDL(Privacy Preserving Deep Learning), AI 보안, 이상탐지(Anomaly Detection), 블록체인, 스마트 제어, 스마트 공장
전문역량	• 정보보안(이상탐지,AI보안)및 프라이버시 보호 연구 및 교육 경력 20년 이상 • 지능형 이상탐지 시스템,지능형 침입탐지 시스템를 위한 인공지능 기술 • 데이터 프라이버시 보호 원천기술(익명성, DP, HE 등), 프라이버시 보호를 위한 보안 프로토콜 최적화 및 플랫폼 구현 방안 등 프라이버시 보존 기술 • 적대적 예제 생성 및 방어 기법을 포함한 AI보안기술 • 진행형 IoT·스마트팩토리 플랫폼 구축
논문/특허	• JCR랭킹 상위 5%,10%이내 논문을 포함한 국외 학술지(SCIE)40여편 • BK인정 우수 학술대회 논문을 포함한 국외 학술대회 논문 15편 • 국내 특허 출원 25건 및 등록 13건, 국외(미국) 특허 3건 출원 및 2건 등록 • 최근 5년간 평균 2,000만원/년 기술이전 • 삼성전자 논문경진대회(금상),한국정보과학회 학술대회 우수논문상 등 • 부산대학교 정보컴퓨터공학부 연구우수 교수상 수상 (2020년,2023년)

□ 대상 특허 도출

○ 부산대학교 산학협력단이 출원한 특허 중 최윤호우 교수가 발명자로 있는 30건의 특허가 확인되었음

발명 특허	등록	공개	소멸	취하	거절
30건	18건	8건	1건	2건	1건

<표> 분석특허 행정상태별 분류

○ 특허 리스트 (등록 및 공개 건 발췌)

No	명칭	출원번호 (출원일)	등록번호 (등록일)	비고
1	다중 작업장 및 작업장 수행 능력 기반의 연속적 생산 계획 전역 최적화 스케줄링 방법 및 장치	10-2024-0105182 (2024.08.07)	10-2762820 (2025.01.31)	미국출원
2	차분 프라이버시를 이용하여 라벨링 데이터를 생성하고 학습하기 위한 딥러닝 학습 방법 및 시스템	10-2023-0191098 (2023.12.26)	10-2705570 (2024.09.06)	
3	프라이버시 보존 이미지 생성과 강력한 분류를 위한 자기주권적 접근 방법 및 장치	10-2023-0168409 (2023.11.28)	10-2799114 (2025.04.17)	
4	Tainted path extraction 및 auto generated rule기법을 활용한 스마트 컨트랙트 취약점 탐지 방법 및 장치	10-2023-0143794 (2023.10.25)	공개	
5	웹쉘 맞춤 textrank 알고리즘을 이용한 난독화된 php 웹쉘 탐지 방법 및 장치	10-2023-0142084 (2023.10.23)	공개	
6	고속 및 광역 반사 필름에 대한 인공지능 기반 불량 탐지 비전 시스템 및 방법	10-2023-0141400 (2023.10.20)	공개	PCT출원
7	고속 및 광역 반사 필름에 대한 멀티 프로세싱 기반의 불량 이미지 수집 장치 및 방법	10-2023-0141423 (2023.10.20)	공개	PCT출원
8	스마트 컨트랙트 데이터의 전처리 방법, gan 모델 학습 방법 및 스마트 컨트랙트 데이터 생성을 위한 gan 프레임워크	10-2023-0140709 (2023.10.19)	공개	공동출원 (한국전력공사)
9	프라이버시 보존 딥러닝을 위한 차분 프라이버시 기반 이미지 데이터 비식별화 처리 방법 및 장치	10-2023-0140514 (2023.10.19)	10-2807779 (2025.05.09)	
10	전송 과정 중 데이터 유출 상황에서의 데이터	10-2023-0140446	공개	

	프라이버시를 보존하기 위한 프라이버시 보존 딥러닝 서비스 방법 및 장치	(2023.10.19)		
11	변형 인셉션 모델의 스마트 컨트랙트 취약점 코드 분류 시스템, 스마트 컨트랙트 취약점 코드 분류 장치, 및 스마트 컨트랙트 취약점 코드 분류 방법	10-2022-0179672 (2022.12.20)	공개	공동출원 (한국전력공사)
12	광역 재귀 반사 필름의 불량 탐지를 위한 인공지능 비전 시스템 및 방법	10-2022-0133393 (2022.10.17)	공개	
13	프라이버시 보존 기계학습을 위한 작업 적응형 차분 프라이버시 생성 방법 및 장치	10-2022-0131326 (2022.10.13)	10-2743137 (2024.12.11)	
14	블록체인 클라이언트 취약점 탐지 방법 및 취약점 탐지 장치	10-2022-0097394 (2022.08.04)	10-2643690 (2024.02.28)	
15	다중 작업장 및 작업장 수행 능력 기반의 연속적 생산 계획 전역 최적화 스케줄링 방법 및 장치	10-2021-0142572 (2021.10.25)	거절	
16	검열 공격 방지를 위한 위임 지분 증명 기반 pbft(practical byzantine fault tolerance) 합의 기법	10-2021-0127148 (2021.09.27)	취하	
17	모발 이식 수술 결과 예측을 위한 생성적 적대 신경망 (gan) 기반 관심 영역 이미지 변환 기법	10-2021-0125305 (2021.09.17)	취하	
18	적대적 사례에 강인한 심층 신경망 모델을 위한 입력 장치 및 방법	10-2020-0112229 (2020.09.03)	10-2598909 (2023.11.01)	
19	실시간 아크 용접 결함 탐지/분류 방법 및 장치	10-2020-0050149 (2020.04.24)	10-2306269 (2021.09.23)	
20	블록체인 기반의 트랜잭션 처리 방법 및 트랜잭션 처리 시스템	10-2020-0044806 (2020.04.13)	10-2303364 (2021.09.13)	
21	차량 사고의 오판율 개선 방법 및 오판율 개선 장치	10-2019-0096648 (2019.08.08)	10-2141313 (2020.07.29)	
22	딥러닝을 위한 이미지 처리 방법 및 이미지 처리 시스템	10-2019-0086463 (2019.07.17)	10-2234097 (2021.03.25)	미국등록
23	다중 센서 데이터 수집을 위한 센서 인터페이스 설정 및 센싱 스케줄링 방법 및 그 장치	10-2019-0079087 (2019.07.02)	10-2145556 (2020.08.11)	
24	혼합문자 자동인식을 위한 문자 및 서적 생성 시스템 및 방법 그리고 이를 이용한 검색 시스템 및 방법	10-2019-0034627 (2019.03.26)	10-2125056 (2020.06.15)	

25	한글 형태소 분석 기반 회원가입 정보 자동 수집 및 개인정보 영향 평가 시스템 및 방법	10-2018-0163542 (2018.12.17)	10-2183192 (2020.11.19)	
26	웨어러블 디바이스 통신 지원 장치 및 방법	10-2017-0174064 (2017.12.18)	10-2026375 (2019.09.23)	
27	하천에서의 홍수범람 대응 관리 방법 및 하천에서의 홍수범람 대응 관리 시스템	10-2017-0164424 (2017.12.01)	10-2009574 (2019.08.05)	소멸
28	하천 수질 정보 제공 방법 및 하천 수질 정보 제공 시스템	10-2017-0016169 (2017.02.06)	10-1864528 (2018.05.29)	
29	고속의 naf 변환 장치 및 고속의 naf 변환 방법	10-2016-0154192 (2016.11.18)	10-1817879 (2018.01.05)	
30	이중 로그인 탐지 방법 및 이중 로그인 탐지 시스템	10-2016-0003719 (2016.01.12)	10-1817414 (2018.01.04)	

□ 학술지 및 학술대회 발표 논문

○ 학술지 리스트: 63건 중 15건 발췌(2022년 이후)

No	명칭	저널명	발표년도
1	CGGNet: Compiler-Guided Generation Network for Smart Contract Data Augmentation	IEEE Access	2024
2	Human-Unrecognizable Differential Private Noised Image Generation Method	Sensor24	2024
3	DP Patch: ROI-based Approach of Privacy-Preserving Image Processing with Robust Classification	IEEE Access	2024
4	Two-Fold Differentially Private Mechanism for Big Data Analysis	한국통신학회논문지	2024
5	Study on Evaluation Method of Task-Specific Adaptive Differential Privacy Mechanism in Federated Learning Environment	정보보호학회논문지	2024
6	Instance-Agnostic and Practical Clean Label Backdoor Attack Method for Deep Learning Based Face Recognition Models	IEEE Access	2023
7	Is Homomorphic Encryption-Based Deep Learning Secure Enough?	Sensors	2023
8	Bypassing Heaven's Gate Technique Using Black-Box Testing	Sensors	2023
9	PIHA: Detection method using perceptual image hashing against query-based adversarial attacks	Elsevier	2023
10	Task-Specific Adaptive Differential Privacy Method for Structured Data	Sensors	2023
11	A Study on Prevention and Automatic Recovery of Blockchain Networks Against Persistent Censorship Attacks	IEEE Access	2022
12	Clustering Approach for Detecting Multiple Types of Adversarial Examples	Sensors	2022
13	ARGAN: Adversarially Robust Generative Adversarial Networks for Deep Neural Networks against Adversarial Examples	IEEE Access	2022
14	CodeNet: Code-Targeted Convolutional Neural Network Architecture for Smart Contract Vulnerability Detection	IEEE Access	2022
15	Semantics-preserving Reinforcement Learning Attack Against Graph Neural Networks for Malware Detection	IEEE Access	2022

□ 대상 연구과제 실적

- 연구과제 리스트 68건 확인 (2020년 이후 과제 발췌)

No	사업명 (지원부처)	연구 과제명	주관기관 (연구책임자)	총 연구기간
1	집단연구지원(R&D) _기초연구실 개척형 [과학기술정보통신부]	프라이버시 친화적 재현데이터셋 생성 및 분산 분리학습 방안	부산대학교 (최윤호)	2023 ~2025
2	정보통신방송혁신인재양성(R&D) _연구지원 [과학기술정보통신부]	제로트러스트 클라우드 보안 신기술 연구 및 혁신인재 양성	부산대학교 (최윤호)	2023 ~2030
3	정보통신방송혁신인재양성(R&D) _연구지원 [과학기술정보통신부]	엣지클라우드 데이터프라이버시 강화를 위한 신기술 연구 및 혁신인재 양성	고려대학교세종 산학협력단 (최두호)	2022 ~2029
4	정보통신방송혁신인재양성(R&D) _연구지원 [과학기술정보통신부]	블록체인 기반 및 플랫폼 분야 핵심기술 개발 및 미래 혁신인재 양성	부산대학교 (김호원)	2020 ~2027
5	산학연협력활성화지원(R&D) _대학기술경영촉진 [과학기술정보통신부]	AI 기반 스마트팩토리 작업 자동화 기술사업화 추진을 위한 IP고도화 및 상용화	부산대학교 (최윤호)	2024 ~2025
6	이공학학술연구기반구축(R&D) _지역대학우수과학자지원사업 [교육부]	프라이버시 보전 연합 학습과 차분 프라이버시 기반 딥러닝 모델 성능 향상 기법	부산대학교 (최윤호)	2022 ~2024
7	정보통신방송혁신인재양성(R&D) _교육훈련 [과학기술정보통신부]	융합보안대학원(부산대학교)	부산대학교 (김호원)	2022 ~2024
8	정보통신방송혁신인재양성 _교육훈련 [과학기술정보통신부]	IoT 및 지능정보 기반 동남권 제조 IT 기술 혁신 및 인재양성	부산대학교 (정상화)	2019 ~2022
9	의료데이터 보호·활용 기술개발 _의료데이터 프라이버시 보존 컴퓨팅 기술개발 [보건복지부]	eXplainable AI(XAI)를 활용한 Differential Privacy 기반 프라이버시 보존 의료데이터 분석 모델 성능 향상 방안 연구	부산대학교 (황재준)	2021 ~2023
10	개인기초연구(과기정통부)(R&D) _기본연구 [과학기술정보통신부]	다중 레이블 Adversarial Attack 분류를 위한 클러스터링 모델	부산대학교 (최윤호)	2021
11	이공학학술연구기반구축(R&D) _지역대학우수과학자지원사업(1년~5년) [교육부]	악성 코드 Context Anomaly 탐지를 위한 Deep Adversarial Learning 알고리즘	부산대학교 (최윤호)	2018 ~2021

12	의료데이터 보호·활용 기술개발 _의료데이터 프라이버시 보존 컴퓨팅 기술개발 [보건복지부]	완전동형암호 프라이버시 보존 딥러닝을 이용한 DICOM 기반 의료데이터 개인정보 보호 및 활용 기술 개발	부산대학교 (황재준)	2019 ~2021
13	과학문화전시서비스 역량강화지원(R&D) _과학문화전시서비스 역량강화지원사업 [과학기술정보통신부]	스마트 과학관 운영을 위한 관람객 궤적 빅데이터 기반 인공지능 시스템	부산대학교 (권준호)	2018 ~2021
14	정보통신방송혁신인재양성 _교육훈련 [과학기술정보통신부]	융합보안핵심인재양성사업	한국인터넷진흥원 (윤승한)	2020 ~2021

□ 언론보도

○ 부산대 과기부 '2023 기초연구실' 8개 과제 선정(23.06.27)
(https://www.veritas-a.com/news/articleView.html?idxno=462889)

[베리타스알파=나동욱 기자] 부산대는 과학기술정보통신부와 한국연구재단이 지원하는 '2023년도 집단연구지원사업 기초연구실(BRL, Basic Research Lab)'에 최종 8개 과제가 선정됐다고 27일 밝혔다.

'기초연구실 지원사업'은 특정 연구주제를 중심으로 소규모 기초연구 그룹을 육성해 국가 기초연구 역량을 강화하고자 정부가 추진하는 사업이다.

심화/융합/개척형으로 지원하며, 올해 부산대 8개 과제(개척형 3개, 심화형 5개)를 포함해 총 114개 과제가 선정됐다. 선정된 연구실에는 2023년 6월부터 향후 3년간 연간 5억 원 이내 총 13억7500만원의 연구비가 투입된다.

올해 부산대 기초연구실(연구책임자)은 '개척형'에 ▲ 프라이버시 친화적 재현데이터셋 생성 및 분산 분리학습 방안(최윤호 정보컴퓨터공학과 교수) ▲ 작물 반수체 유도/기작규명 기초연구실(김유진 생명환경화학과 교수) ▲ 유무기 할라이드 페로브스카이트 구조동역학 연구실(장준경 나노에너지공학과 교수)이 선정됐다.

또 '심화형'에도 ▲ W-밴드 광자 레이더 시스템 집적화 원천 기술 연구(김상길 전자공학과 교수) ▲ 다기능 upconversion nanoparticle 기반 3차원 근적외선 뇌자극 시스템 연구실(신화경 한의과학과 교수) ▲ 전기활성 4D 모핑 변색기술 연구실(박종승 응용화학공학부 교수) ▲ BIM기반 설계단계별 그린빌딩계획 통합 의사결정지원시스템 개발(윤성환 건설융합학부 교수) ▲ 위상 포논을 활용한 다중 간격 위상 기초연구(박성균 물리학과 교수) 등 총 8곳이 선정됐다.