

통신정보보호 연구실

- ▶ 위치: IT-1호관 704호, 705호, 706호
- ▶ 전화: 053-950-7842, 053-940-8872
- ▶ E-mail: parkyh@knu.ac.kr

- ▶ 팩스: 053-950-5505
- ▶ 홈페이지: <http://cisl.knu.ac.kr>

01

연구실구성원

- 지도교수 : 박영호 교수님
- 박사과정 : 김종현, 유성진, 이준영, 김명현, 손승환, 권덕규, 오지현, 안진수
- 석사과정 : 김보겸, 김명기

02

연구분야

본 연구실은 정보통신 네트워크 및 시스템의 신뢰성과 안전성을 보장하는 정보보호 관련 기술을 연구하고 있다.

□ 네트워크 보안 :

- 유무선이 통합된 통신환경에서 단말기 혹은 통신 서비스에 이동성 및 정보보호 서비스를 제공하는 차세대 핵심 기술 연구
- IoT 네트워크 또는 차량 네트워크에서의 안전성 증명 문제 등의 보안 이슈를 해결하고 안전한 통신을 보장하기 위한 보안기법 연구

□ 핀테크 보안 : 온라인상에서 민감한 금융 서비스를 안전하게 제공하기 위하여 핀테크에서의 사용자 확인, 거래부인 방지, 데이터의 무결성, 기밀성 확보 등을 제공하는 기술 연구

□ 양자후 보안 : 양자 컴퓨팅 환경에서 안전한 보안 알고리즘 및 보안 프로토콜 관련 보안체계 연구

□ 블록 체인 응용 보안 : 블록 체인 기법을 이용한 스마트 그리드, 차량 통신 및 IoT 관련 보안기술 연구



□ 주요 수행과제

- 무선 은닉채널 위험성 검증 연구/**정보통신기획평가원**
- 개인 데이터 안전성 보장을 위한 사용자 검증 알고리즘 연구/**한국전자통신연구원**
- 블록체인 기반 IoT 보안 알고리즘 개발/**중소기업기술정보진흥원**
- 트러스트 데이터 커넥툼 서비스에서 프라이버시 강화를 위한 사용자 중심의 인증 및 키 관리 프로토콜 연구/**한국전자통신연구원**
- 개인 데이터 중심의 데이터 책임성 보장 알고리즘 개발/**한국전자통신연구원**
- WiFi 기반 무선 은닉채널에 대한 은닉성 분석 연구/**한국전자통신연구원**
- 개인 데이터 거래 플랫폼을 위한 데이터 책임성 연구/**한국전자통신연구원**
- 엣지 컴퓨팅 기반 차량 네트워크에서의 보안 기술 개발/**연구재단**
- 차량통신을 활용한 서비스 보안성 강화 방안 분석 및 연구/**한국전자통신연구원**
- 단일도메인 온보드 보안을 위한 시스템 보안기술 분석 및 실증 연구/**한국전자통신연구원**
- 양자 컴퓨팅 환경에 안전한 보안 프로토콜 개발에 관한 연구/**연구재단**
- 차량보안플랫폼 인증모듈 시험 환경 개발/**한국전자통신연구원**
- PQ 공개키암호 기반 인증 프로로콜 및 상용 기술에 관한 연구/**국가보안연구소**

□ 연구 논문: SCI(E)

- “Robust and Efficient Authentication and Group-Proof Scheme Using Physical Unclonable Functions for Wearable Computing,” *Sensors*, Vol. 23, Issue 12, No.5747, pp. 1-26, June 2023.
- “Fog-Based Single Sign-On Authentication Protocol for Electronic Healthcare Applications,” *IEEE Internet of Things Journal*, Volume 10, No. 12, pp. 10983-10996, June 2023.
- “Design of Secure and Lightweight Authentication Scheme for UAV-Enabled Intelligent Transportation Systems using Blockchain and PUF,” *IEEE Access*, Vol. 11, pp. 60240-60253, June 2023.
- “Blockchain Integration for IoT-Enabled V2X Communications: A Comprehensive Survey, Security Issues and Challenges,” *IEEE Access*, Vol. 11, pp. 54476-54494, June 2023.
- “Designing attribute-based verifiable data storage and retrieval scheme in cloud computing environment,” *Journal of Information Security and Applications*, Vol. 75, No.103482, pp. 1-29, June 2023.
- “Blockchain-Based Data Access Control and Key Agreement System in IoT Environment,” *Sensors*, Vol. 23, Issue 11, No.5173, pp. 1-19, May 2023.
- “Private Blockchain-Based AI-Envisioned Home Monitoring Framework in IoMT-Enabled COVID-19 Environment,” *IEEE Consumer Electronics Magazine*, Vol. 12, Issue 3, pp. 62-71, May 2023.
- “Blockchain-Enabled Secure Big Data Analytics for Internet of Things Smart Applications,” *IEEE Internet of Things Journal*, Vol. 10, No. 7, pp. 6428-6443, April 2023.
- “LAKA-UAV: Lightweight authentication and key agreement scheme for cloud-assisted Unmanned Aerial Vehicle using blockchain in flying ad-hoc networks,” *Computer Networks*, Vol. 224, No. 109612, pp. 1-15, April 2023.
- “An Effective Privacy-Preserving Blockchain-Assisted Security Protocol for Cloud-Based Digital Twin Environment,” *IEEE Access*, Vol. 11, pp. 26877-26892, March 2023.
- “BPPS:Blockchain-Enabled Privacy-Preserving Scheme for Demand-Response Management in Smart Grid Environments,” *IEEE Transactions on Dependable and Secure Computing*, Vol. 20, No. 2, pp. 1719-1729, March/April 2023.
- “A Secure and Anonymous Authentication Protocol Based on Three-Factor Wireless Medical Sensor Networks,” *Electronics*, Vol. 12, Issue 6, No.1368, pp. 1-27, March 2023.

- “Provably Secure Mutual Authentication and Key Agreement Scheme Using PUF in Internet of Drones Deployments,” *Sensors*, Vol. 23, Issue 4, No.2034, pp. 1-25, February 2023.
- “A Provably Secure Mobile User Authentication Scheme for Big Data Collection in IoT-Enabled Maritime Intelligent Transportation System,” *IEEE Transactions on Intelligent Transportation Systems*, Vol. 24, No. 2, pp. 2411-2421, February 2023
- “Post-Quantum Lattice-Based Secure Reconciliation Enabled Key Agreement Protocol for IoT,” *IEEE Internet of Things Journal*, Volume 10, No. 3, pp. 2680-2692, February 2023.
- “Blockchain-Enabled Authenticated Key Agreement Scheme for Mobile Vehicles-Assisted Precision Agricultural IoT Networks,” *IEEE Transactions on Information Forensics and Security*, Vol. 18, pp. 904-919, January 2023.
- “Healthcare 5.0 Security Framework: Applications, Issues and Future Research Directions,” *IEEE Access*, Vol. 10, pp. 129429-129442, 12 December 2022.
- “A Secure Data Sharing Based on Key Aggregate Searchable Encryption in Fog-Enabled IoT Environment,” *IEEE Transactions on Network Science and Engineering*, Vol. 9, No. 6, pp. 4468-4481, November-December 2022.
- “Secure biometric-based access control scheme for future IoT-enabled cloud-assisted video surveillance system,” *Computer Communications*, Vol. 195, pp. 27-39, November 2022.
- “SLAP-IoD: Secure and Lightweight Authentication Protocol Using Physical Unclonable Functions for Internet of Drones in Smart City Environments,” *IEEE Transactions on Vehicular Technology*, Vol. 71, No. 10, pp.10374-10388, October 2022.
- “A Robust Authentication Protocol for Wireless Medical Sensor Networks Using Blockchain and Physically Unclonable Functions,” *IEEE Internet of Things Journal*, Volume 9, No. 20, pp. 20214-20228, October, 2022.
- “A Secure Personal Health Record Sharing System with Key Aggregate Dynamic Searchable Encryption,” *Electronics*, Vol. 11, Issue 19, No.3199, pp. 1-24, October 2022.
- “Uniting cyber security and machine learning: Advantages, challenges and future research,” *ICT Express*, Volume 8, Issue 3, pp. 313-321, September 2022.
- “A Secure and Anonymous User Authentication Scheme for IoT-Enabled Smart Home Environments Using PUF,” *IEEE Access*, Vol. 10, pp.101330-101346, 21 September 2022.
- “PUFTAP-IoT: PUF-Based Three-Factor Authentication Protocol in IoT Environment Focused on Sensing Devices,” *Sensors*, Vol. 22, No.7075, pp. 1-24, September 2022.
- “Blockchain-Envisioned Provably Secure Multivariate Identity-Based Multi-Signature Scheme for Internet of Vehicles Environment,” *IEEE Transactions on Vehicular Technology*, Vol. 71, No. 9, pp.9853-9867, September 2022.
- “Blockchain based energy trading scheme for vehicle-to-vehicle using decentralized identifiers,” *Applied Energy*, Vol. 322, No. 119445, pp. 1-9, September 2022.
- “Design of Secure Mutual Authentication Scheme for Metaverse Environments Using Blockchain,” *IEEE Access*, Vol. 10, pp. 98944-98958, September 2022.
- “A Secure Batch Authentication Scheme for Multiaccess Edge Computing in 5G-Enabled Intelligent Transportation System,” *IEEE Access*, Vol. 10, pp. 96224-96238, September 2022.
- “iAKA-CIoT: An Improved Authentication and Key Agreement Scheme for Cloud Enabled Internet of Things Using Physical Unclonable Function,” *Sensors*, Vol. 22, Issue 16, No.6264, pp. 1-19, August, 2022.
- “On the Design of a Privacy-Preserving Communication Scheme for Cloud-Based Digital Twin Environments Using Blockchain,” *IEEE Access*, Vol. 10, pp.75365-75375, July 2022.
- “A Secure Three-Factor Authentication Protocol for E-Governance System Based on Multi-Server Environments,” *IEEE Access*, Vol. 10, pp.74351-74365, July 2022.
- “SCS-WoT: Secure Communication Scheme for Web of Things Deployment,” *IEEE Internet of Things Journal*, Vol. 9, No. 13, pp. 10411-10423, July 2022.
- “Design of Blockchain-Based Lightweight V2I Handover Authentication Protocol for VANET,”

IEEE Transactions on Network Science and Engineering, Vol. 9, No. 3, pp. 1346-1358, May/June 2022.

- “On the Security of a Lightweight and Secure Access Authentication Scheme for Both UE and mMTC Devices in 5G Networks,” *Applied Sciences*, Vol. 12, Issue.9, No.4265, pp.1-18, April 2022.
- “Design of Secure Handover Authentication Scheme for Urban Air Mobility Environments,” *IEEE Access*, Vol. 10, pp.42529-42541, April 2022.
- “Blockchain-enabled secure communication mechanism for IoT-driven personal health records,” *Transactions on Emerging Telecommunications Technologies*, Volume 33, Issue 4, e4421, 20 pages, April 2022.
- “Blockchain-Based Robust Data Security Scheme in IoT-Enabled Smart Home,” *CMC-Computer, Materials & Continua*, Vol. 72, No. 2, pp. 3549-3570, March 2022.
- “Authenticated Key Agreement Scheme With User Anonymity and Untraceability for 5G-Enabled Softwarized Industrial Cyber-Physical Systems,” *IEEE Transactions on Intelligent Transportation Systems*, Vol. 23, No. 3, pp. 2316 - 2330, March 2022
- “Secure ECC-Based Three-Factor Mutual Authentication Protocol for Telecare Medical Information System,” *IEEE Access*, Vol. 10, pp.11511-11526, January 2022.
- “Designing Fine-Grained Access Control for Software-Defined Networks Using Private Blockchain,” *IEEE Internet of Things Journal*, Volume 9, No. 2, pp. 1542-1559, January, 2022.
- “Robust Authentication Protocol for Dynamic Charging System of Electric Vehicles,” *IEEE Transactions on Vehicular Technology*, Vol. 70, No. 11, pp.11338-11351, November 2021.
- “Blockchain-Envisioned Secure Authentication Approach in AloT: Applications, Challenges, and Future Research,” *Wireless Communications and Mobile Computing*, Volume 2021, Article ID 3866006, 19 pages, October 2021.
- “A Secure Key Aggregate Searchable Encryption with Multi Delegation in Cloud Data Sharing Service,” *Applied Sciences*, Vol.11, Issue 19, No. 8841, pp.1-20, September 2021.
- “Secure and Efficient Honey List-Based Authentication Protocol for Vehicular Ad Hoc Networks,” *IEEE Transactions on Network Science and Engineering*, Vol. 8, Issue 3, pp. 2412-2425, July-September 2021.
- “Lightweight Three-Factor Based Privacy-Preserving Authentication Scheme for IoT-Enabled Smart Homes,” *IEEE Access*, Vol. 9, pp. 126186-126197, September 2021.
- “Provably Secure Three-Factor-Based Mutual Authentication Scheme with PUF for Wireless Medical Sensor Networks,” *Sensors*, Vol. 21, Issue 18, No.6039, pp. 1-27, September 2021.
- “AI-Enabled Blockchain-Based Access Control for Malicious Attacks Detection and Mitigation in IoE,” *IEEE Consumer Electronics Magazine*, Vol. 10, No. 5, pp. 82-92, September 2021.
- “A Secure, Lightweight, and Anonymous User Authentication Protocol for IoT Environments,” *Sustainability*, Vol. 13, No 16: 9241, p.1-21, August 2021.
- “Block-CLAP: Blockchain-Assisted Certificateless Key Agreement Protocol for Internet of Vehicles in Smart Transportation,” *IEEE Transactions on Vehicular Technology*, Vol. 70, No. 8, pp. 8092-8107, August 2021.
- “Blockchain-Enabled Certificate-Based Authentication for Vehicle Accident Detection and Notification in Intelligent Transportation Systems,” *IEEE Sensors Journal*, Vol. 21, No. 14, pp. 15824-15838, July 2021.
- “iGCACS-IoD: An Improved Certificate-Enabled Generic Access Control Scheme for Internet of Drones Deployment,” *IEEE Access*, Vol. 9, pp. 87024-87048, June 2021.
- “Lightweight Failover Authentication Mechanism for IoT-Based Fog Computing Environment,” *Electronics*, Vol. 10, Issue 12, No. 1417, pp. 1-25, June 2021.
- “On the Security of a Secure and Lightweight Authentication Scheme for Next Generation IoT Infrastructure,” *IEEE Access*, Vol. 9, pp. 71856-71867, May 2021.
- “Design of Secure Decentralized Car-Sharing System Using Blockchain,” *IEEE Access*, Vol. 9,

pp. 54796-54810, April 2021.

- “Comments on “ALAM: Anonymous Lightweight Authentication Mechanism for SDN Enabled Smart Homes”,” *IEEE Access*, Vol. 9, pp. 49154-49159, March 2021.
- “On the Design of Mutual Authentication and Key Agreement Protocol in Internet of Vehicles-Enabled Intelligent Transportation System,” *IEEE Transactions on Vehicular Technology*, Vol. 70, No. 2, pp. 1736-1751, February 2021.
- “A Secure and Lightweight Authentication Protocol for IoT-Based Smart Homes,” *Sensors*, Vol. 21, Issue 4, No. 1488, pp. 1-24, February 2021.
- “WSN-SLAP: Secure and Lightweight Mutual Authentication Protocol for Wireless Sensor Networks,” *Sensors*, Vol. 21, Issue 3, No. 936, pp. 1-23, January 2021.
- “On the Design of Lightweight and Secure Mutual Authentication System for Global Roaming in Resource-limited Mobility Networks,” *IEEE Access*, Vol. 9, pp. 12879-12895, January 2021.
- 이 외 다수의 SCI(E) 논문 게재

□ 수상 실적

- 2023. 한국산업정보학회 춘계학술대회 우수논문상 선정. 한국산업정보학회
- 2023. *Sensors* 저널 2023 Best Paper 선정. *Sensors*
- 2023. 경북대학교 질적성과부분(JCR 5%) 우수연구교수 선정. 경북대학교
- 2023. *Sensors* 저널 Editor's Choice Article 선정. *Sensors*
- 2022. 한국산업정보학회 추계학술대회 최우수논문상 선정. 한국산업정보학회
- 2022. 과학기술 발전 및 지식공유 대상 장관 표창장. 과학기술정보통신부
- 2022. 첨성인 대학원생 논문 경진대회 장려상 선정. 경북대학교
- 2022. 한국산업정보학회 춘계학술대회 우수논문상 및 장려논문상 선정. 한국산업정보학회
- 2022. *Sensors* 저널 Editor's Choice Article 선정. *Sensors*
- 2021. 한국산업정보학회 추계학술대회 최우수논문상 선정. 한국산업정보학회
- 2021. 한국통신학회 하계종합학술발표회 우수논문상 선정. 한국통신학회
- 2021. 경북대학교 질적성과부분(JCR 5%) 우수연구교수 선정. 경북대학교
- 2020. 한국산업정보학회 하계학술대회 우수논문상. 한국산업정보학회
- 2019. 제1회 미래형자동차 우수 논문 콘테스트 우수상 수상. 미래형자동차 인재페스티벌
- 2019. 2018년도 멀티미디어학회논문지에 게재된 논문중 최우수논문상 수상. 한국멀티미디어학회
- 2018. 한국통신학회 하계종합학술발표회 우수논문상 선정. 한국통신학회

04

졸업생 진로 현황

교수, 공무원(국정원 등), 공공기관(한국인터넷진흥원, 금융보안원 등), 연구소(국가보안연구소, 한국전자통신연구원, 국방과학연구소 등), 기업체(삼성전자, LG전자, SK 텔레콤 등) 등에 취업