안면 현존성 검증과 가상 인터페이스 제어를 연동한 제로트러스트 VPN 접속 제어 구조

장수안[1], 양지용[1], 김근중[2], 이근호[3*]
[1]백석대학교 컴퓨터공학부 학생, [2](주)에스케어 대표이사, [3]백석대학교 컴퓨터공학부 교수

A Zero Trust VPN Access Control Architecture Linking Face Presence Verification to Virtual Interface Control

Su-An Jang[1], Ji-Yong Yang[1], Geun-Joong Kim[2], Keun-Ho Lee[3*]
[1]Student, Division of Computer Engineering, Baek-Seok University
[2]CEO, ESCARE Co., Ltd.
[3]Professor, Division of Computer Engineering, Baek-Seok University

요 약 원격근무 환경의 VPN은 접속 시점의 인증 이후 사용자 부재를 입력 비활동으로 추정하므로, 인가 사용자가 단말을 떠나거나 제3자로 교체되어도 타임아웃이 만료될 때까지 내부망 접근이 유지되는 노출 구간이 발생한다. 본 논문은 인증 이후 세션의 위협을 여섯 가지로 모델링하여 설계 요구사항을 도출하고, 단말 카메라 기반 안면 현존성·생동성 판별 결과를 제로트러스트 정책결정지점(PDP)의 연속 입력으로, 정책시행지점(PEP)을 세션별 VPN 가상 인터페이스의 생성·중지·소멸 수명주기로 두는 접속 제어 구조를 설계한다. 신뢰도 갱신, 상태 전이, 노출 구간의 상한과 오잠금률을 수식으로 정식화하고, 자세 변화의 발생률과 지속시간을 가정한 시뮬레이션으로 설계 변수를 분석하였다. 가정한 조건에서 자세 강인 현존 판별은 유예 시간 2.2초로 오잠금률을 시간당 0.1회 이하로 유지하면서 이탈 시 노출 구간을 2.9초 이내로, 신원 확인 기한 240초로 교체 시 노출 구간을 약 4분 이내로 제한하였으나, 정면 얼굴만 검출하면 유예 시간 5초에서도 오잠금률이 시간당 2.6회였다. 이는 비활동 타임아웃(15분~1시간)과 전체 세션 타임아웃(12~24시간)에 의존하는 기존 구조보다 노출 구간을 크게 줄이는 설계 조건과 방향을 제시한다.

주제어 : 제로트러스트, 지속 인증, 안면 현존성, VPN 접속 제어, 노출 구간, 위협 모델

Abstract Conventional VPNs authenticate users only at connection time and afterwards infer absence from input inactivity, so an unattended or handed-over endpoint keeps network access until a timeout expires. This paper models six post-authentication session threats, derives design requirements, and designs a zero trust architecture in which face presence and liveness evidence from the endpoint camera is a continuous input to the policy decision point (PDP), while the policy enforcement point (PEP) is bound to the create-suspend-revoke lifecycle of a per-session VPN virtual interface. We formalize trust updates, state transitions, exposure-window bounds, and false-lock rates, and analyze the design parameters by simulation with assumed rates and durations of posture changes. Under these assumptions, pose-tolerant presence detection with a 2.2 s grace period keeps false locks below 0.1 per hour while bounding exposure to 2.9 s when the user leaves, and a 240 s identity-confirmation deadline bounds exposure to about 4 minutes when the user is substituted, whereas frontal-only detection still causes 2.6 false locks per hour at a 5 s grace period. These results provide design conditions for reducing post-authentication exposure far below the inactivity and session timeouts of conventional VPNs.

Key Words : Zero Trust; Continuous Authentication; Face Presence; VPN Access Control; Exposure Window; Threat Model

본 논문은 2026년도 정부(중소벤처기업부)의 재원으로 중소기업기술정보진흥원의 민관공동기술사업화(R&D) 지원을 받아 수행된 것임 (RS-2026-25534656)
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2026년 09월 30일 수정일 2026년 10월 16일 심사완료일 2026년 10월 20일
www.kci.go.kr

1. 서론

VPN(Virtual Private Network)은 접속 시점에 한 번 인증한 뒤 터널이 유지되는 동안 단말을 계속 신뢰한다. 제로트러스트는 암묵적 신뢰 없이 자원 접근을 세션 단위로 결정할 것을 요구하며[1,2], 국내에서도 가이드라인 2.0이 제시되었다[3]. 그러나 NIST SP 800-63B-4는 재인증의 목적을 사용자의 현존 확인으로 규정하면서도 기본 수단으로 전체 세션 타임아웃(AAL2 24시간, AAL3 12시간 이하)과 비활동 타임아웃(AAL2 1시간, AAL3 15분 이하)을 두며[4], 국내 기준도 이와 같다[5]. 입력 비활동을 부재의 대리지표로 쓰므로 사용자가 떠나거나 교체된 뒤에도 타임아웃 만료까지 노출 구간(exposure window)이 남고, 제3자가 입력을 이어가면 비활동 타임아웃은 발생하지 않는다.

생체 지속 인증 연구[6,7]는 세션 중 신원을 재확인하되 운영체제 수준의 잠금에 머물러 네트워크 권한의 회수와 결합되지 않았다. 화면 잠금은 잠긴 화면 뒤의 원격 제어 도구가 열린 터널을 쓰는 것을 막지 못하며, OpenID CAEP 1.0은 세션 회수 이벤트를 전달하나 물리적 현존의 신호원은 정의하지 않는다[8]. 본 논문은 현존·신원을 분리한 안면 판별을 PDP의 입력으로, PEP를 세션별 VPN 가상 인터페이스의 수명주기로 두는 구조를 수식으로 정의하고, 노출 구간과 오잠금률을 시뮬레이션으로 분석하여 설계 조건을 도출한다.

2. 관련연구

2.1 제로트러스트 아키텍처와 원격 접속

NIST SP 800-207은 정책엔진·정책관리자로 구성된 PDP와 PEP, 판단 근거인 데이터 소스를 정의하고 세션 단위 접근과 자산 상태의 지속 감시를 원칙으로 제시하며[1], 국내 가이드라인은 데이터 소스를 정책정보지점(PIP)으로 구분한다[3]. Zohaib 등[9]의 ZT-VPN은 접속 이후의 통제를 세션 시간 제한에 의존한다. 비교는 〈Table 1〉과 같다.

〈Table 1〉 Comparison of existing approaches and the proposed architecture

Approach	In-session identity	Presence signal	Enforced at
Legacy VPN	Login only	None (idle timeout)	Static tunnel
ZT-VPN [9]	At connection	None (time-bound)	VPN tunnel
Continuous auth. [6,7]	Continuous biometric	Yes	OS/app lock
Proposed	Continuous face + liveness	Yes (webcam)	Per-session vNIC

2.2 지속 인증과 안면 위변조 탐지

Sim 등[6]은 얼굴·지문의 멀티모달 지속 검증을, Niinuma 등[7]은 소프트 생체 특징으로 이탈과 복귀를 추적하는 방법을 제안하였고, Baig 등[10]은 재전송 공격과 개인정보 노출을 과제로 지적하였다. 제시 공격 탐지 단서로는 EAR(눈 종횡비)로 검출한 깜빡임[11]과 출력물·화면의 질감[12]이 있으며, 최근에는 심층 학습 기반 탐지의 미지 공격 일반화가 핵심 과제로 정리되었고[13], 딥페이크 탐지 기준도 제시되었다[14]. 탐지 성능은 ISO/IEC 30107-3의 APCER·BPCER로 보고한다[15].

3. 위협 모델 및 설계 요구사항

3.1 시스템 및 공격자 가정

단말에는 기관이 배포한 에이전트와 카메라, TPM이 있고, 사용자는 ID/PW·OTP와 안면 검증으로 초기 인증을 마쳤으며 탐지 회피에 협조하지 않는다. 공격자는 방치 단말에 접근한 제3자, 단말을 넘겨받은 자, 우회 경로를 여는 행위자, 사용자가 비운 동안 터널을 쓰는 원격 제어 도구이다. 가상 카메라 주입과 사용자 권한의 에이전트 변조는 범위에 포함하고, 커널 수준 공격은 TPM 기반 단말 증명으로 탐지되는 범위까지 다룬다.

3.2 위협과 요구사항

현존·신원·생동성·경로·세션·단말 상태가 깨지는 경우를 검토하여 〈Table 2〉의 위협을 정리하였다. T1·T2는 비활동 타임아웃이 대응하지 못하고, T3는 안면 신호 도입으로 생기며, T4는 우회 경로, T5는 차단 후 남는 세션 상태, T6는 세션 중 단말 상태 악화의 문제이다. R1은 재인증의 현존 확인 목적[4]에, R6은 지속 모니터링 원칙[1]에 대응한다.

www.kci.go.kr

〈Table 2〉 Post-authentication threats, requirements, and countermeasures

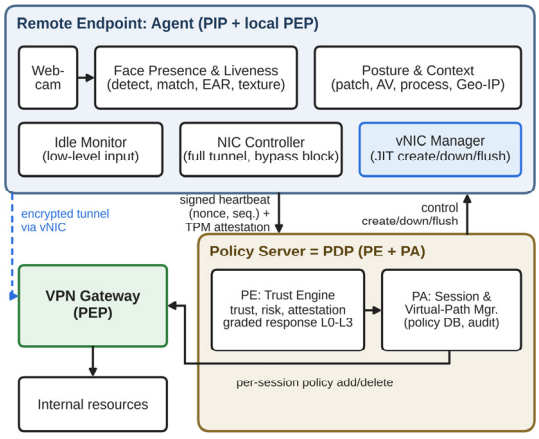
Threat	Requirement	Legacy VPN	Proposed control
T1 Leave	R1 Bounded cut-off	Idle timeout (15-60 min)	Grace period, vNIC down
T2 Swap	R2 Identity change	Overall limit (12-24 h)	Matching, ID deadline
T3 Spoof	R3 Liveness	No face check	Blink + texture
T4 Bypass	R4 vNIC path only	Client-dependent	Full tunnel, extra NICs off
T5 Residue	R5 Erase on revoke	Until session ends	Flushed at L3
T6 Posture	R6 Re-evaluation	Product-dependent	Device risk in trust

Legacy bounds follow the NIST SP 800-63B-4 recommendations [4].

4. 제안 구조

4.1 전체 구조

구조는 [Fig. 1]과 같이 에이전트, 정책 서버, VPN 게이트웨이로 이루어진다. 에이전트는 판별·상태 수집·가상 인터페이스(vNIC) 관리를 맡는 데이터 소스(PIP)이자 단말 측 PEP이다. 신뢰 엔진(PE)과 세션·가상경로 관리자(PA)가 PDP를 이룬다. 에이전트는 TPM의 키로 서명하고 PDP가 발급한 논스와 순번을 포함한 하트비트를 보내며, PDP는 TPM 원격 증명으로 부팅 기록과 에이전트를 주기적으로 검증하여 실패하거나 하트비트가 끊기면 세션을 L1으로 둔다.



[Fig. 1] Architecture of the proposed scheme mapped to ZTA components

4.2 안면 현존성 및 생동성 판별

에이전트는 주기 Δ마다 경량 CNN 얼굴·상반신 검출로 자세에 강인하게 현존을 판단하고, 정면 샘플에서만 등록 템플릿과의 유사도 s를 계산하며, 입력은 장치 정보로 확인한 물리 카메라로 한정한다. 생동 양성(l=1)은 판별 창 W 안에서 EAR 깜박임이 관측되고 질감 실물 점수 c가 τc 이상일 때이고, c〈τc가 연속 Ks회이면 위변조로 판정하며, 깜빡임 부재만으로는 위변조로 보지 않는다. 성능 목표는 NIST SP 800-63B-4의 IAPAR 0.07 미만으로 둔다[4].

현존은 신원과 분리하여, 현존 미검출이 연속 k= ⌈ g/Δ ⌉ 회이면 부재로 본다(g: 유예 시간). 신원은 생동 양성 정면 대조로 확인된 시각 tid로부터 기한 Tid 안에 다시 확인되어야 하므로, 생동 단서 없는 벽 사진은 기한 만료로 L1이 된다. 생동 양성 얼굴의 유사도가 θs 미만으로 연속 j회이면 미등록 사용자로 보아 L1을 거쳐 L2로 보내고, 카메라를 쓸 수 없으면 L1이 된다.

4.3 연속 신뢰 평가와 단계적 대응

안면 신뢰도 Tf는 생동 양성 정면 샘플 n에서만 식 (1)로 갱신하고, 단말 위험도 Rc는 패치·백신·접속 국가 등의 항목 상태 vi∈[0,1]의 가중합이며, 세션 신뢰도 S는 식 (2), L1 전환 조건은 식 (3)이다(r: 연속 미검출 수, θL: 잠금 임계값).

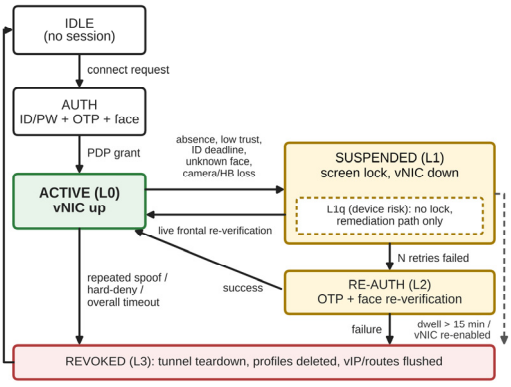
$$Tf[n] = \alpha\ sn + (1 - \alpha)\ Tf[n-1],\quad 0 < \alpha \le 1 \quad (1)$$

$$S(t) = Tf(t)(1 - Rc(t)),\quad Rc(t) = \Sigma i\ wivi(t) \quad (2)$$

$$L0 \rightarrow L1 \ \Leftrightarrow\ r \ge k \vee S < \theta L \vee t - tid > Tid \quad (3)$$

L1에서는 화면을 잠그고 vNIC를 중지하며 Tf를 0으로 초기화하여 신뢰도의 승계를 막고, 생동 양성 정면 샘플에서 S ≥ θR(=θL+η)가 연속 m회일 때만 복귀시켜 잠금 반복을 막는다. 재인식 실패가 N=5회[4]를 넘거나 미등록 사용자이면 L2에서 OTP로 재검증하고, L1 체류가 15분을 넘거나 vNIC가 재활성화되면 L3로 종료한다. 단말 위험이 원인이면 하위 상태 L1q에서 조치 서버만 허용하며, L0에서는 생동 양성 현존을 세션 활동으로 보되 전체 세션 타임아웃은 유지한다([Fig. 2], 〈Table 3〉).

www.kci.go.kr



[Fig. 2] Session and virtual-interface lifecycle

〈Table 3〉 Design parameters (*: initial values for the PoC)

Symbol	Value	Symbol	Value
Δ	0.2 s	$g(k)$	2.2 s (11)
d	0.5 s	T_{id}	240 s
W	10 s*	α	0.3*
θ_L / θ_R	0.6 / 0.7*	m, j, K_s	3*
T_{hb} / d_{gw}	3 s / 0.5 s	T_{dwell}	15 min

4.4 온디맨드 가상 인터페이스 수명주기

PA는 PDP가 허용할 때만 게이트웨이에 세션 정책을, 에이전트에 허용 자원으로만 향하는 vNIC를 설치한다. [16]은 정책을 휘발성으로 관리하나 수명이 접속·해제에 묶여 있는 반면, 제안 구조는 이를 세션 중 판정에 따른 중지(L1)·복구(L0)·소멸(L3)에 결합한다. L1에서는 에이전트가 vNIC와 터널 밖 통신을 먼저 차단하고 PA가 게이트웨이 정책을 일시 차단하며, L3에서는 세션 키·가상 IP·경로를 폐기한다. 분할 터널링은 강제 전체 터널과 방화벽으로 막는다.

5. 노출 구간과 오잠금 분석

5.1 노출 구간의 상한

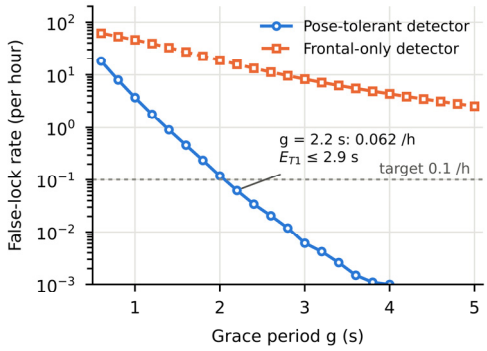
노출 구간 E는 사용자가 떠나거나 교체된 시점부터 내부망 접근이 차단되기까지의 시간으로, 기존 방식에서는 이탈 시 15분~1시간, 교체 시 12~24시간에 이른다[4]. 제안 구조에서는 이탈 시 k번째 미검출에서, 교체 시 신원 기한에서 차단되므로 식 (4)가 성립한다(d: 처리·차단 지연). 에이전트가 강제 종료되면 하트비트 타임아웃 Thb 후 게이트웨이가 차단하여 E ≤ Thb + dgw이다. 현존 오검출이 지속되면 이탈 시에도 기한이 상한이 되므로 최악 노출은 Tid가 결정하며, 이 상한은 에이전트·카메라의 무결성을 전제한다.

$$ET1 \le g + \Delta + d, \quad ET2 \le Tid + d \qquad (4)$$

5.2 오잠금률 모델과 시뮬레이션

수 초간 이어지는 자세 변화 사건 j(고개 돌림, 휴대전화 확인, 손 가림)가 시간당 λ_j회 발생하면 유예 시간에 의한 오잠금률은 식 (5)의 첫 항으로 근사되어 지속시간 Dj의 꼬리에 좌우되고, 기한에 의한 오잠금률은 생동 양성 정면 대조가 분당 μ회일 때 둘째 항이다(Tid: 분).

$$FLRE \approx \Sigma_j \lambda_j P(D_j > g),$$
$$FLRid = 60\ \mu\ \exp(-\mu\ Tid) \qquad (5)$$



[Fig. 3] Simulated false-lock rate versus grace period

사건별 발생률과 로그정규 지속시간(고개 돌림 30회/h·중앙값 1.5초, 휴대전화 6회/h·6초, 손 가림 12회/h·2초), 사건 중 미검출 확률(정면 검출 0.90~0.95, 자세 강인 검출 0.2~0.5)을 가정하고 Δ=0.2초의 미검출 계열을 각각 10,000시간 생성하였다. [Fig. 3]과 같이 정면 검출은 유예 5초에서도 시간당 2.6회의 오잠금이 났으나, 자세 강인 검출은 2.2초에서 0.062회로 목표 0.1회를 만족하여 이탈 시 상한 2.9초를 얻었다. 오검출이 샘플의 5%에 끼면 이 노출은 평균 3.5초(99백분위 8.6초)로 늘었다. μ=2에서 Tid가 60초, 240초이면 기한 오잠금은 시간당 16.2회, 0.040회이므로 Tid=240초에서 교체 시 상한은 약 4분이다. 이는 기존보다 이탈 시 310배, 교체 시 180배 이상 짧으며, 가정값 기반이므로 실측 검증이 필요하다.

www.kci.go.kr

5.3 보안성 분석 및 한계

사용자 권한의 에이전트 변조는 서명 하트비트와 원격 증명으로 탐지되나, 커널 수준 공격자는 다음 증명 전까지 신호를 위조할 수 있어 그동안 식 (4)가 보장되지 않는다. 재생·딥페이크 공격의 APCER·BPCER 실측[15]과 드라이버 수준 주입에 대한 센서 인증이 필요하며, 동석자 조작과 듀얼 모니터 환경은 다루지 않았다. 원본 영상은 단말 메모리에서만 처리하고, 생체정보 별도 동의를 전제로 하고 이석 기록의 근태 감시 전용을 제한해야 한다.

6. 결론

본 논문은 현존·신원을 분리한 안면 판별을 PDP 입력으로, PEP를 세션별 vNIC 수명주기로 두는 구조를 설계하고 노출 구간과 오잠금률을 수식과 시뮬레이션으로 분석하였다. 가정한 조건에서 유예 시간 2.2초와 신원 기한 240초로 오잠금률을 시간당 0.1회 이하로 유지하며 이탈 시 2.9초, 교체 시 약 4분의 노출 상한을 얻었고, 연속 미검출을 줄이는 현존 판별이 핵심 설계 조건임을 도출하였다. 향후 PoC에서는 업무 중 현존·생동 판정과 입력 로그로 자세 변화의 발생률·지속시간을 추정해 유예 시간, 신원 확인 기한, 처리·차단 지연을 정하고 별도 기간의 데이터로 오잠금률과 노출 구간을 검증하며, CAEP 연동[8]을 추진한다.

REFERENCES

[1] S.Rose, O.Borchert, S.Mitchell and S.Connelly, Zero Trust Architecture, NIST Special Publication 800-207, NIST, 2020.

[2] N.F.Syed, S.W.Shah, A.Shaghaghi, A.Anwar, Z.Baig and R.Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," IEEE Access, Vol.10, pp.57143-57179, 2022.

[3] Ministry of Science and ICT and Korea Internet & Security Agency, Zero Trust Guideline 2.0, 2024.

[4] D.Temoshok, J.L.Fenton, Y.Y.Choong, N.Lefkovitz, A.Regenscheid, R.Galluzzo and J.P.Richer, Digital Identity Guidelines: Authentication and Authenticator Management, NIST Special Publication 800-63B-4, NIST, 2025.

[5] Personal Information Protection Commission, Standards for Ensuring the Safety of Personal Information, PIPC Notice No.2023-6, 2023.

[6] T.Sim, S.Zhang, R.Janakiraman and S.Kumar, "Continuous Verification Using Multimodal Biometrics," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.29, No.4, pp.687-700, 2007.

[7] K.Niinuma, U.Park and A.K.Jain, "Soft Biometric Traits for Continuous User Authentication," IEEE Transactions on Information Forensics and Security, Vol.5, No.4, pp.771-780, 2010.

[8] T.Cappalli and A.Tulshibagwale, OpenID Continuous Access Evaluation Profile 1.0, OpenID Foundation, 2025.

[9] S.M.Zohaib, S.M.Sajjad, Z.Iqbal, M.Yousaf, M.Haseeb and Z.Muhammad, "Zero Trust VPN (ZT-VPN): A Systematic Literature Review and Cybersecurity Framework for Hybrid and Remote Work," Information, Vol.15, No.11, 734, 2024.

[10] A.F.Baig and S.Eskeland, "Security, Privacy, and Usability in Continuous Authentication: A Survey," Sensors, Vol.21, No.17, 5967, 2021.

[11] T.Soukupová and J.Čech, "Real-Time Eye Blink Detection Using Facial Landmarks," in Proceedings of the 21st Computer Vision Winter Workshop, Rimske Toplice, 2016.

[12] J.Määttä, A.Hadid and M.Pietikäinen, "Face Spoofing Detection from Single Images Using Micro-Texture Analysis," in Proceedings of the International Joint Conference on Biometrics, Washington, DC, pp.1-7, 2011.

[13] Z.Yu, Y.Qin, X.Li, C.Zhao, Z.Lei and G.Zhao, "Deep Learning for Face Anti-Spoofing: A Survey," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.45, No.5, pp.5609-5631, 2023.

[14] A.Rössler, D.Cozzolino, L.Verdoliva, C.Riess, J.Thies and M.Nießner, "FaceForensics++: Learning to Detect Manipulated Facial Images," in Proceedings of the IEEE/CVF International Conference on Computer Vision, Seoul, pp.1-11, 2019.

[15] ISO/IEC 30107-3:2023, Biometric Presentation Attack Detection - Part 3: Testing and Reporting, Geneva: ISO, 2023.

[16] ESCARE Co., Ltd., "Method, Apparatus, System and Computer-Readable Storage Medium for Processing VPN Connection," Korean Patent No.10-2486480, 2023.

www.kci.go.kr

장 수 안(Su-An Jang) [준회원]



■ 2023년 3월 ~ 현재 : 백석대학교 컴퓨터공학부

〈관심분야〉
시스템 해킹, 취약점 분석, AI 보안

양 지 용(Ji-Yong Yang) [준회원]



■ 2023년 3월 ~ 현재 : 백석대학교 컴퓨터공학부

〈관심분야〉
시스템 해킹, 취약점 분석

김 근 중(Geun-Joong Kim) [정회원]



■ 1995년 2월 : 순천향대학교 전자공학과 학사졸업
■ 2008년 1월 : ㈜펜타시스템 미들웨어 기술총괄 부장
■ 2012년 7월 : (주)에스케어 설립 및 대표이사 취임
■ 2013년 3월 : (주)에스케어 연구개발부 연구소장
■ 2024년 1월 : (주)에스케어 연구개발본부 본부장

〈관심분야〉
사물인터넷, 정보보호, AI보안

이 근 호(Keun-Ho Lee) [종신회원]



■ 2006년 8월 : 고려대학교 컴퓨터학과(이학박사)
■ 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 기술전략팀 과장
■ 2010년 3월 ~ 현재 : 백석대학교 컴퓨터공학부 교수

〈관심분야〉
융합보안, 블록체인, 개인정보보호, 이동통신 보안

www.kci.go.kr