

AI-RAN 기반 제로트러스트 보안 적용 방안

December 16, 2025

AiNA 산업융합위원회

유동호, (주)넷큐브 대표이사

NIST SP 800-207 (Zero Trust Architecture, 2020년 8월)

1. 모든 데이터와 서비스는 보호해야 할 자원(Resource)이다

네트워크 내부·외부 위치와 관계없이 모든 데이터, 장비, 애플리케이션, 서비스는 보호대상으로 간주한다.

2. 네트워크 위치에 관계없이 모든 통신은 보호되어야 한다

사내망도 신뢰하지 않으며, 모든 연결은 암호화·인증·무결성 검증이 이루어져야 한다.

3. 접근 권한은 세션 단위로 최소화하여 부여한다

사용자·기기·서비스의 접근 권한은 지속적 권한이 아니라, 요청할 때마다 세션별로 필요한 최소 권한만 허용한다.

4. 접근 결정은 동적 정책(Dynamic Policy)에 의해 이루어진다

사용자 ID, 디바이스 상태, 위치, 애플리케이션, 데이터 민감도, 위협 정보 등 "실시간 맥락(Context)"을 기반으로 정책을 평가해 접근을 허용/차단한다.

5. 모든 기기와 자산의 보안 상태는 지속적으로 파악·평가한다

엔드포인트·IoT·서버 등 모든 자산의 보안 상태(무결성, 패치 여부, 위험도)를 지속적으로 확인한다.

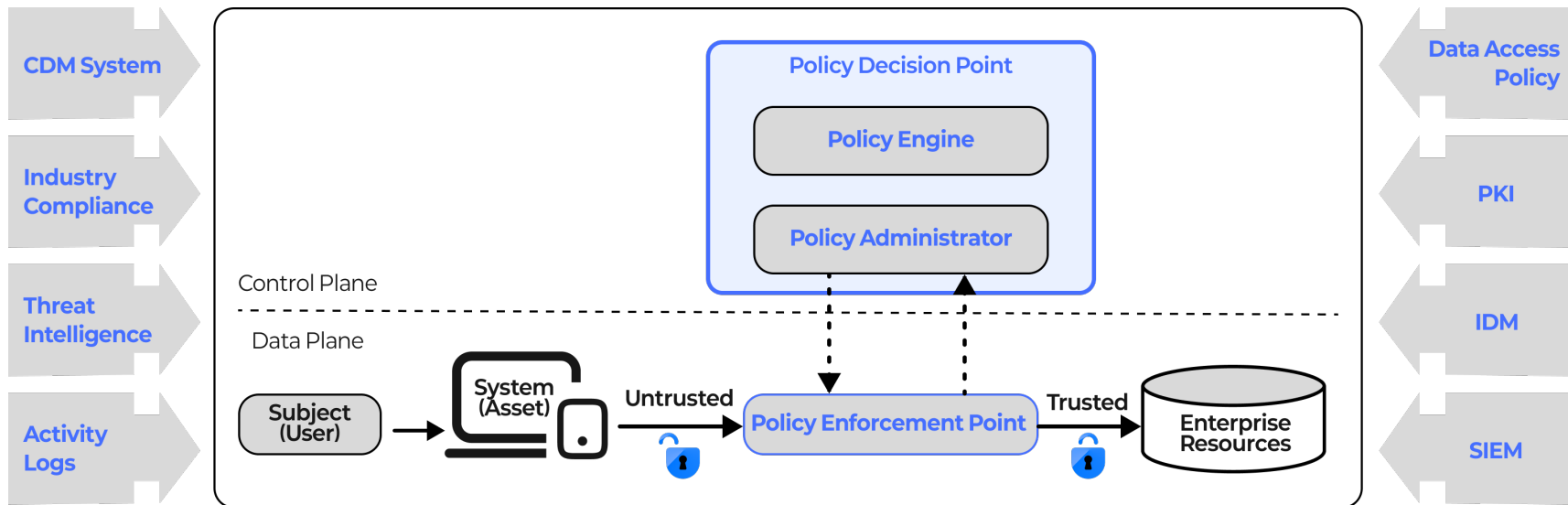
6. 모든 자원 접근은 인증과 인가가 지속적으로 검증되어야 한다

초기 인증으로 끝나는 것이 아니라, 세션 중에도 변화된 상황(리스크 상승·위치 변경·기기 이상 등)을 반영해 인증/인가를 다시 수행한다.

7. 자산, 네트워크, 트래픽 상태 정보를 최대한 수집·분석한다

로그, 트래픽, 자산 상태, 위협 정보를 지속적으로 수집·분석하여 보안 정책 개선, 이상 탐지, 자동화된 대응에 활용한다.

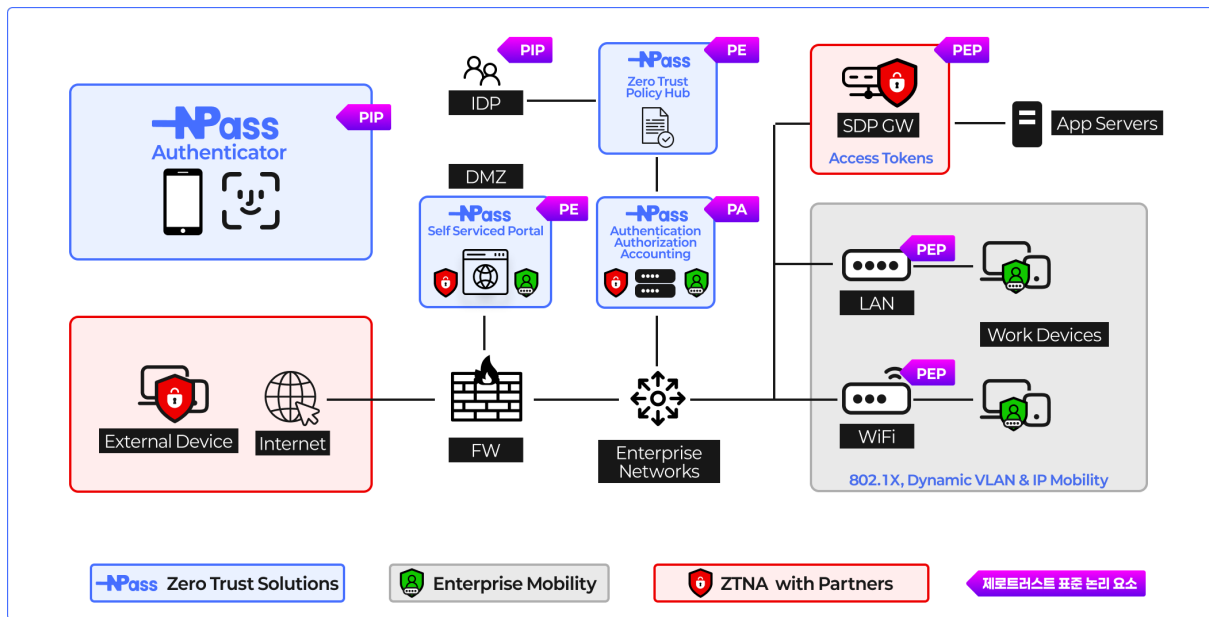
NIST SP 800-207 표준 아키텍처



- NIST 아키텍처는 OASIS xACML, IETF RFC3198 등을 참조모델로 클라우드와 같은 범용적인 컴퓨팅 환경을 고려하여 수립됨

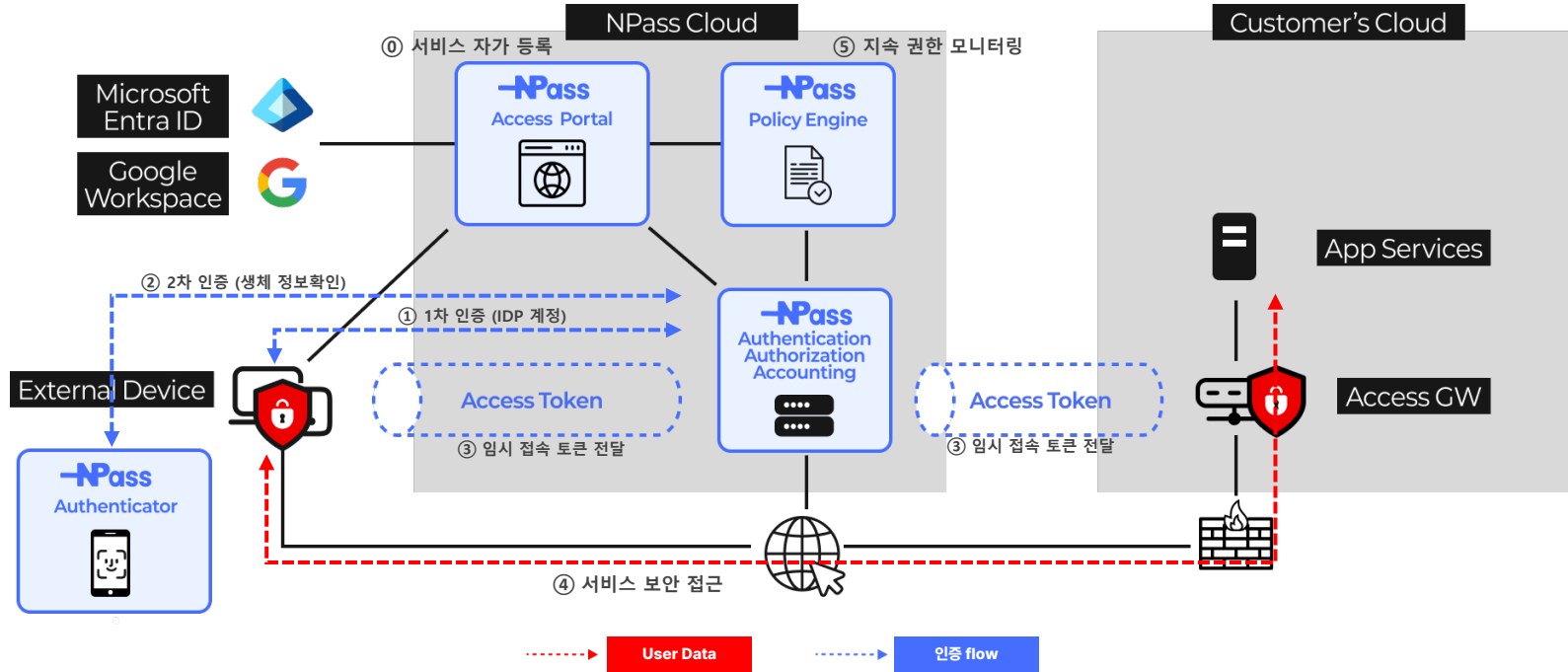
- 사용자와 시스템으로 부터 기업 리소스로의 모든 접근은 잠정적으로 비신뢰 하며, PDP의 판단에 따라 PEP에서 신뢰 상태로 전환 하게됨

NPass 제로트러스트 아키텍처



- 정통부 제로트러스트 가이드라인 2.0 아키텍처 준수
- PDP 및 일부 PIP(MFA, ICAM) 기능 제공
- ZTNA를 위한 다양한 PEP 연동 운영 기능 제공

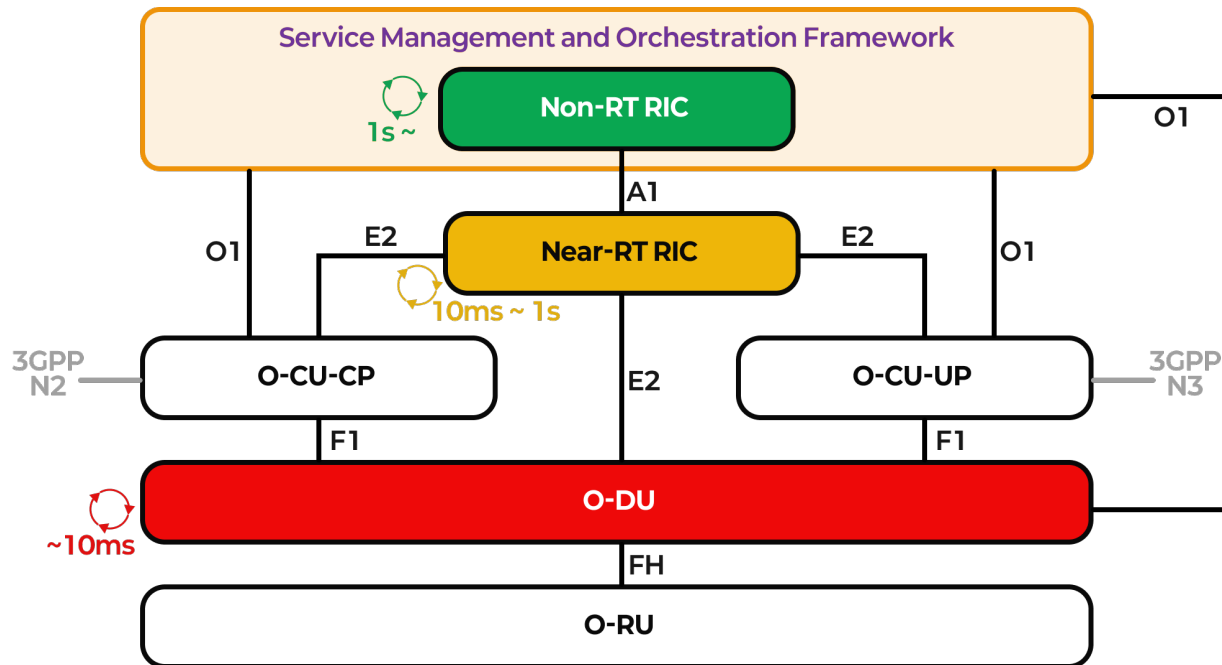
NPass ZTNA 동작 절차



- 상용 IDP 연계를 통한 임직원 DB 실시간 동기화
- Self Service Portal 을 통한 자율 운영 기능 제공

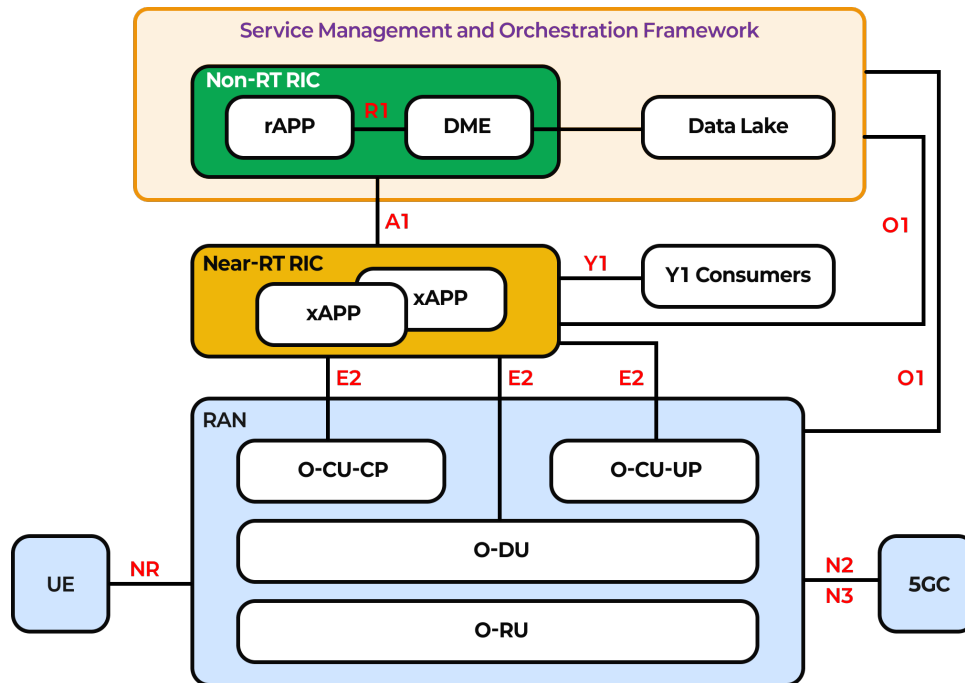
- 1차/2차 인증 성공 후 임시 Access Token 발행

O-RAN Alliance WG1 Architecture Description



- O-RAN Alliance는 3GPP와 호환성을 유지하며, RAN 내부 아키텍처 상세 표준화 제공
- AI/ML 기반 어플리케이션 플랫폼인 RIC 제공
- Non-RT RIC 은 rAPP, Near-RT RIC은 xAPP 표준 어플리케이션 인터페이스 규격 제공

RIC 및 인터페이스 노드



- RAN에서 각 UE의 Control Plane 및 User Plane 데이터는 O1/E2 인터페이스를 통해 xAPP 및 rAPP 으로 전달
- xAPP/rAPP은 O1, R1 및 DME를 통해 학습/추론에 필요한 데이터를 Data Lake에 저장
- xAPP/rAPP은 Data Lake에 수집된 데이터를 통해 학습 (Offline)
- xAPP/rAPP의 학습된 모델은 UE 및 5GC로 부터 제공되는 데이터를 추론하고 RAN을 제어 (Online)
- xAPP은 외부 Domain의 데이터를 통해 학습 및 추론 가능 (Y1)

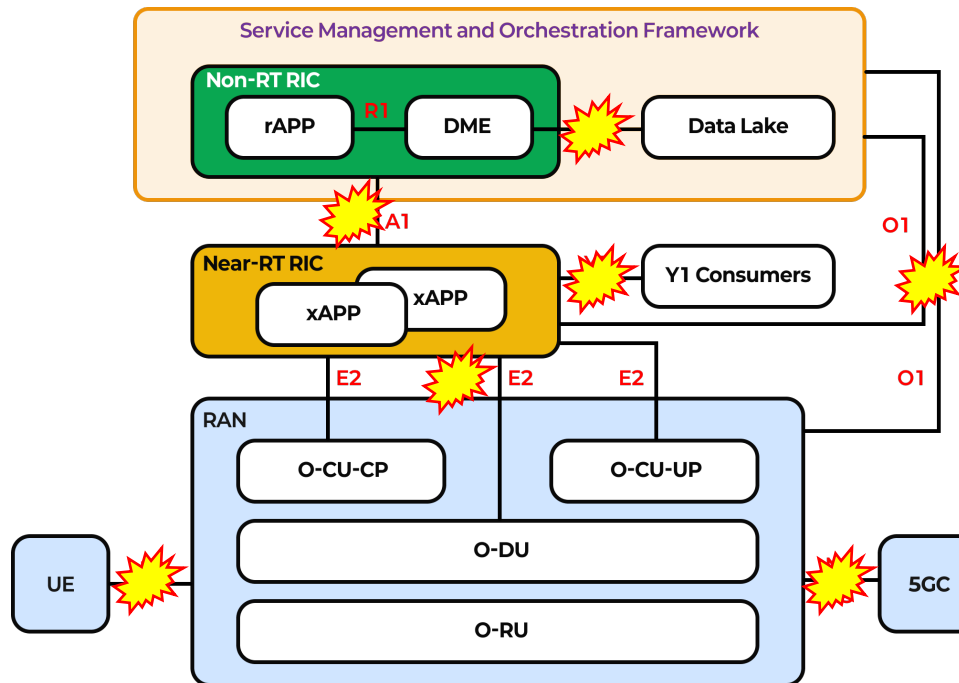
RIC 및 학습/추론 데이터 I/F 및 Flow

수집 경로	데이터 수집	용도	데이터 소스
RAN → O1 → Data Lake	Performance Data - Throughput, Packet Loss, Delay, etc	트래픽 예측, 슬라이싱 최적화 모델 학습	O-DU, O-CU
	Trace Data - 각 UE의 상세 세션 기록	Anomaly Detection, 위치 기반 분석 모델 학습	O-DU, O-CU
	Fault Management Data - 에러 기록, 알람 이력	장애예측, 자동 복구 모델 학습	O-DU, O-CU
RAN → E2 → Near-RT RIC → Data Lake	Radio Quality - 단말별 RSRP/RSRQ/SINR - CQI(Channel Quality Indicator) - Beam Index	UE별 Measurement Report 추출, 위치 추정 및 핸드오버 결정	O-DU
	Traffic & Load - PRB Usage (주파수자원 블록 사용률) - Throughput 및 Buffer 상태	망혼잡도 판단, DDoS공격 감지	O-DU
	Session & ID - UE ID, QoS Flow ID(QFI), 각 S-NSSAI 접속 정보	각 주체 및 시스템 식별, 사용자와 인가된 슬라이스 여부 검증	O-CU
	Signaling - RRC attempts 횟수, 성공율 - 핸드오버 시도, 성공율 - Radio Link Failure	Signaling Storm 공격 탐지, 비정상 접속 패턴 분석	O-CU
Near-RT RIC → A1 → Non-RT RIC	Feedback Data - 상태, 결과	모델 성능 평가 및 정책 수정	Near-RT RIC

RIC 및 제어 데이터 I/F 및 Flow

I/F	Controller	Target	Timing	제어내용
A1	Non-RT RIC(in SMO)	Near-RT RIC	Non-Real Time(> 1초)	<ul style="list-style-type: none"> • Policy: QoS 목표, 차단 등급 • Model: AI 모델 배포/갱신 • Scope: 특정 슬라이스/UE 그룹
E2	Near-RT RIC	E2 Nodes(O-CU, O-DU)	Near-Real Time(10ms ~ 1초)	<ul style="list-style-type: none"> • RRM: 핸드오버, 빔포밍, 스케줄링 • Suspend/Drop: 베어러 해제 • Scope: 개별 UE/Bearer 단위
O1	SMO(OAM/Non-RT RIC)	All Managed Elements (Near-RT RIC, O-CU/DU/RU)	Non-Real Time(설정/배포 시점)	<ul style="list-style-type: none"> • FCAPS: 장비 On/Off, 초기 설정 • Software: 펌웨어/xApp 배포 • Scope: 장비/시스템 전체

O-RAN 각 노드 간 인터페이스 공격 가능성 등장



- 전통적인 UE-RAN, RAN-5GC 구간 외에 새로운 공격 표면의 등장
- AI/ML 을 활용하여 기존 3GPP I/F의 Anomaly 를 Detect 및 제어

- 제로트러스트 모델 도입 필요성

AI-RAN 기반 제로트러스트 보안 플랫폼 개발 환경

RIC 플랫폼

- Near-RT RIC 및 xAPP Manager : O-RAN Software Community (OSC)

O-RAN

- gNB: srsRAN, UERANSIM, SDR (USRP B210)
- Commercial O-RAN: Pegatron 5G

5G Core

- Proprietary (Release 16)

AI/ML Model

- TCNs
- Explainable AI(XAI) 독자 모델 기반 (해외 대학 협력)

ZeroTrust PDP

- NPass PE/PA (자사 솔루션)

Legacy Security Platform

- TrendMicro MNS (Mobile Network Security) IDS

AI/ML 모델 연구 현황

모델 선정 기준

- 경량형 모델 (CPU 기반 동작)
- Time Series 처리에 최적화 (Signaling 메시지 및 Log 기반 추론)

주요 고려 모델

- LSTM(Long Short-Term Memory), GRU(Gated Recurrent Unit), LightLog, TCNs (Temporal Convolutional Networks)

자체 개발 모델 (진행 중)

- XAI (Explainable AI)
- 이벤트 기반 예측모델 및 심볼릭 회귀 (Symbolic Regression) 기술 활용

이데일리

실시간뉴스 [종합]원보가 대령에너지, VFP 사업 기대...후대통령 '분산에너지' 산업에 필수 >



AI검색

속보

IT·과학

모바일

방송통신

IT·인터넷

게임

과학일반

넷큐브-AI Metrica, 5G/6G 단말 이벤트 예측 AI모델 공동 개발 성공

설명가능한 AI(XAI) 기술로 네트워크 운영 패러다임 전환 예고

등록 2025-06-09 오후 4:23:43
수정 2025-06-09 오후 4:23:43

기 가

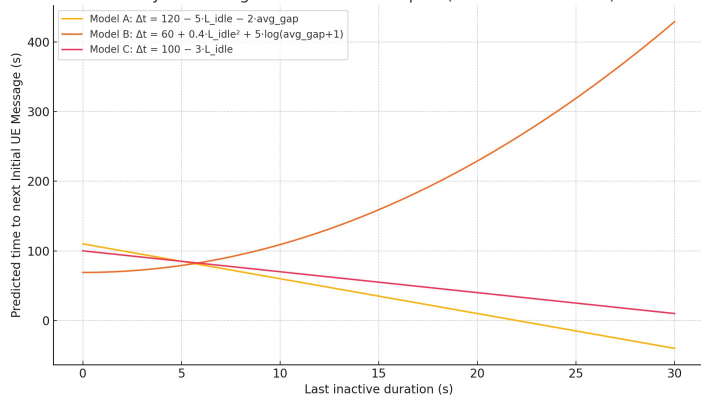


이윤정 기자

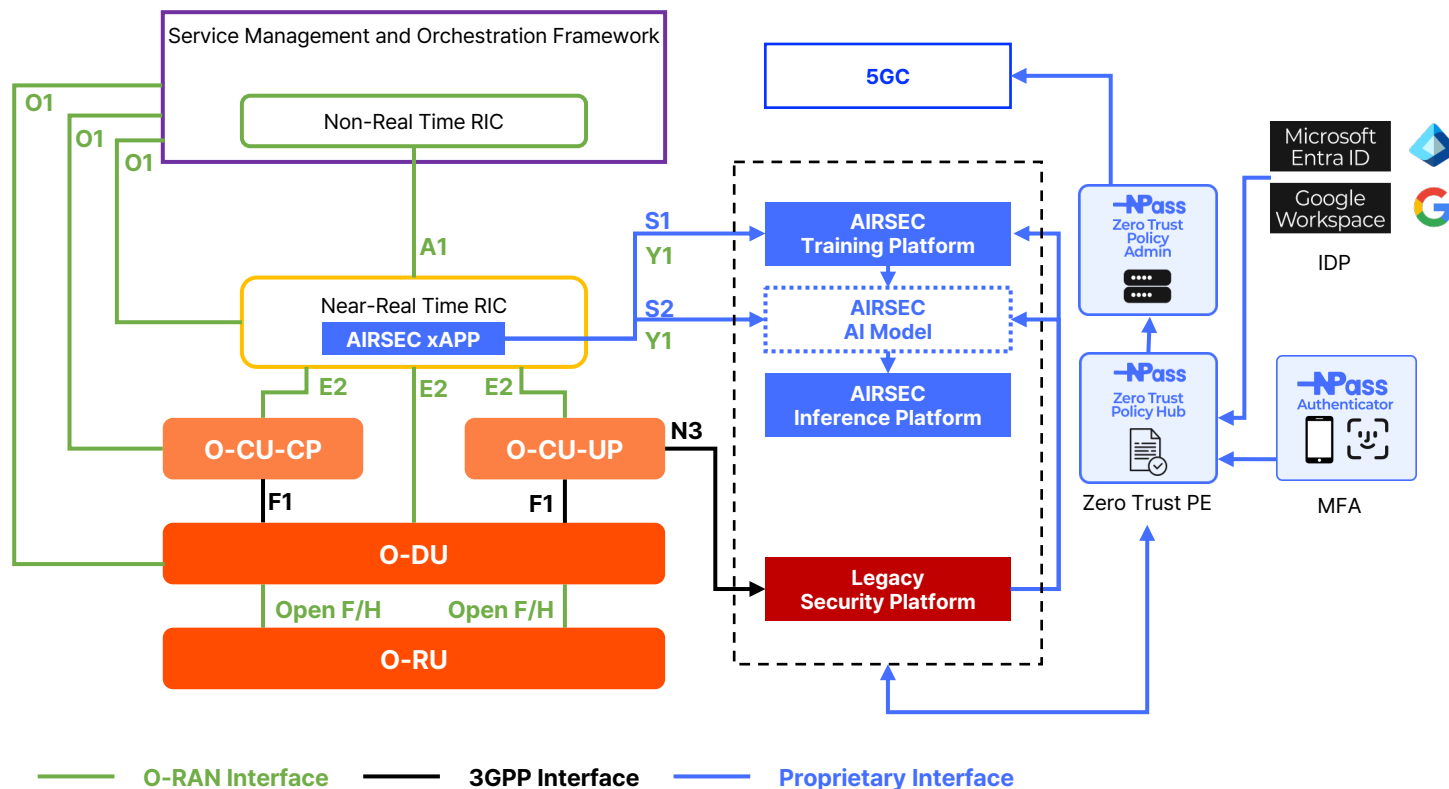
NETCUBE

[이데일리 이윤정 기자] 국내 5G 솔루션 기업 넷큐브는 미국 AI/ML 전문 기업 시 메트리카(Metrica), 동양대 김호림 교수와 공동으로 5G 네트워크에서 이동통신 단말의 접속 패턴을 예측하는 AI 모델 개발에 성공했다고 9일 밝혔다.

Symbolic Regression Model Examples (fixed other features)



AI-RAN 기반 제로트러스트 적용 플랫폼





Thank You