KCA연구2023

농산물 산지 유통센터(APC) 내 이음5G망 구축을 위한 보안 기술 연구

(최종 보고서)

2023. 12. 01.

한국방송통신전파진흥원

연구수행기관 : 국민대학교 산학협력단

이 보고서는 한국방송통신전파진흥원의 재정지원으로 이루어졌으며, 보고서 내용은 연구자의 견해이며 한국방송통신전파진흥원의 공식 입장과 다를 수 있습니다.

본 결과물은 농림축산식품부의 재원으로 농림식품기술기획평가원의 신선농산물 풀필먼트(Fulfillment) 산지유통센터(APC) 구축 및 핵심 기술개발 사업의 지원을 받아 연구되었음(1545027294)

제 출 문

한국방송통신전파진흥원 귀하

본 보고서를 『**농산물 산지 유통센터(APC) 내 이음 5G망 구축을 위한 보안 기술 연구**』의 연구결과 중간보고서로 제출합니다.

2023년 12월

연구기관 : 국민대학교 산학협력단
총괄책임자 : 유일선
참여연구원 : 김보남, 김건우, 권호석

요 약

1. 제목

o **농산물 산지 유통센터(APC) 내 이음5G망 구축을 위한 보안 기술 연구**

2. 연구목적 및 추진계획

o **본 연구과제의 연구목적 및 필요성은 다음과 같음**

- 과학기술정보통신부가 이음5G 정책방안 및 공급방안을 발표하고 전용 주파수를 공급함에 따라 국내 이음5G 서비스가 시작됨
- 이음5G 서비스는 원전, 의료, 물류, 전력 등 다양한 분야에 적극 활용될 수 있으며 현재 이음5G 서비스 활성화를 위해 실증사업이 진행 중임
- 또한 정부가 농산물 산지유통센터(APC)에 대한 자동화·정보화 지원을 통해 2027년까지 스마트 APC 100개를 구축한다는 계획하에 APC내 이음5G 구축을 위한 실증사업이 진행 중임
- 성공적인 APC 내 이음5G 활성화를 위해선 보안 기술 연구가 필수적임
- 그러나 APC 내 이음5G뿐만 아니라 국내 이음5G 관련 보안 사례 동향 및 보안 요구사항 조사가 미비한 상황임
- 이에 국내 이음5G 활성화를 위한 선제조건으로 보안 기술 연구가 요구되며, 특히 농산물 유통이라는 특수 산업에 디지털 전환 및 안전한 이음5G망 구축을 위한 최적의 보안 모델 조사가 필요함

o **연구과제의 수행 시 기대성과는 다음과 같음**

- 농산물 산지 유통센터(APC) 내 이음5G망 구축은 농업 산업 분야에서 새로운 서비스 및 기회를 제공하며, 지역 경제 발전을 촉진

- 이음 5G 보안 가이드라인으로 발전하여 정책 및 개정을 위한 자료로 활용함
- 국내기업의 이음 5G 시장 활성화를 위한 기업들이 고려해야 할 요구사항이 정책으로 반영 및 활용함
- 유통과 같은 형태의 이음 5G 서비스가 제공·발굴됨으로써 국내 5G 산업생태계가 활성화되고 보안 분야에 있어 여러 파급효과를 기대할 수 있음
- 이음 5G를 활용하여 미래 신사업을 육성하고, 이를 위한 정보보호의 핵심 원천기술을 기획하기 위한 기반을 마련함

3. 연구 목표 및 추진계획

o 연구 목표 및 방법

- 본 과제에서는 농산물 산지 유통센터(APC) 내 이음5G망 구축을 위한 보안 기술 연구를 통하여 APC 내 이음5G 실증 사이트 구축 시 활용 가능한 이음5G 보안구조 및 인증, APC 내 이음5G 보안 모델을 정리한 기술 문서 2건 작성 및 국내 학술대회 논문 1편

o 본 과제에서 작성되는 기술 문서는 다음과 같은 내용을 포함

- 이음5G 적용 사례 조사
- 이음5G 보안구조 및 인증기법
- 이음5G 적용 기술 유형 및 기술별 보안 고려사항
- 농산물 산지 유통센터(APC) 내 이음5G망 구축을 위한 보안 모델 조사

o 본 과제의 최종목표 달성을 위해 제 2장 연구수행과 같은 결과를 조사하였으며 해당 결과를 기반으로 기술문서 2건 작성 및 국내 학술대회 논문 1편 완료

o **추진계획 및 실적 진도**

- 추진 일정에 따라 현재까지 (1) 이음5G 적용 사례 보안 구조 조사, (2) 이음5G 보안구조 및 인증기법 조사, (3) 이음5G 적용 기술 유형 및 기술별 보안 고려사항 (4) 농산물 산지유통센터(APC) 내 이음5G망 구축을 위한 보안 모델조사 완료
- 보안 모델 조사를 위해 천안 배 농협 APC(농산물산지유통센터) 방문 전북 고창 황토배기 영농조합(고구마 APC) 방문 완료
- 2개의 APC 답사를 기반으로 APC 내 이음5G망 구축을 위한 보안 모델 조사 완료
- APC와 농협 망 간의 VPN 사용 등 보안 기술 적용에 따른 성능 저하 개선 기술 조사 완료

4. 연구 수행내용 및 최종결과

o **본 연구과제의 수행 내용은 다음과 같음**

- **이음5G 적용 사례 및 보안구조 조사**

▶ 국내외 이음5G망 구성요소 및 보안구조 조사

- 이음5G 모델별 사업장 내 구성요소 조사
- 국내외 공공분야 이음5G망 모델별 구축 사례 조사
- 국내외 민간분야 이음5G망 모델별 구축 사례 조사

▶ 국내외 이음5G 서비스별 적용 특성 조사

- 이음5G 제조·생산 서비스 적용 특성 조사
- 이음5G 공공·인빌딩 서비스 적용 특성 조사
- 이음5G 에너지·자원 서비스 적용 특성 조사
- 이음5G 교통·수송 서비스 적용 특성 조사

- **이음5G 보안구조 및 인증기법 조사**

▶ 5G 표준 보안구조 조사

- 5G 보안 도메인
- 1차 인증, 2차 인증, AKMA

▶ 5G 인증 및 키 계층, AKMA 관련 기술 조사

- 5G 인증기법 조사(5G-AKA, EAP-AKA', AKMA)
- 키 계층 분석

- **이음5G 적용기술 유형 및 기술별 보안 고려사항 조사**

▶ **MEC 보안 위협 및 고려사항 조사**

- 가상화 인프라
- MEC 애플리케이션
- MEC 오케스트레이터(orchestrator)
- MEC 가상화 인프라 관점에서의 보안 위협 및 보안 고려사항 조사
  - 가상화 기술 비교
  - 호스트 운영체제 보안 위협과 고려사항
  - 컨테이너 런타임 보안 위협과 고려사항
  - 컨테이너 이미지 보안 위협과 고려사항

- MEC 애플리케이션 관점에서의 보안 위협 및 보안 고려사항
  - MEC 애플리케이션
  - 런타임 소프트웨어 내의 보안 위협 및 보안 고려사항 분석
  - 어플리케이션 인증 및 통신 암호
  - 어플리케이션 간 접근통제

- MEC 오케스트레이터 및 네트워크 관점 보안 위협 및 보안 고려사항
  - 컨테이너의 언바운드 네트워크 액세스
  - 언바운드 관리자 액세스

- MEC 데이터 보호 보안 고려사항
  - 데이터 자산 식별
  - 데이터 위변조 및 유출 방지
  - 개인정보 및 민감 데이터 비식별 조치
  - 저장 데이터 보호

- MEC 플랫폼 보안 고려사항
  - 가상화된 보안 솔루션 구축
  - MEC 소프트웨어 보안
  - MEC 서비스 장애관리
  - 보안 인증 획득 플랫폼 활용

- MEC 연동 구간 보안 고려사항
  - MEC 연결 API 보안
  - MEC 연동 구간 보안관제

▸ **네트워크 슬라이싱 보안 위협 및 고려사항 조사**

- 네트워크 슬라이스 내 위협 지점 및 대응기술
  - 5G 고객 단말
  - 슬라이스 서비스 인터페이스
  - 하위 슬라이스
  - 슬라이스 관리자
  - 리소스 및 네트워크 기능

- 스마트 APC 사업에 참여 중인 고창 황토배기 청정 고구마 연합의 유통센터를 2차 방문지로 선정하여 현장 답사 및 현업 관계자 미팅 진행
- 현장 사례 분석 내용
- 스마트 APC 적용방안 논의 내용

▶ **현장 방문 기반 APC 내 보안 요구 사항 및 제안 모델**

- 현장 보안 요구 사항
- APC 내 이음5G 구축모델 제안

목 차

표 목차

그림 목차

제 1 장 연구목적 및 추진계획

제 1 절 연구목적

1. 연구의 필요성

o **해당분야에 대한 기술동향 분석 및 중장기 예측**

- 국내

▶ 과학기술정보통신부가 이음5G 정책방안('21.1월) 및 공급방안('21.6월)을 발표하고 4.7㎓/28㎓ 대역 주파수를 공급함에 따라 국내 이음5G 서비스가 시작됨

▶ 국내 이음5G는 자가구축 기업 및 이음5G 사업자가 4.7㎓ 대역 전용 주파수를 할당받아 구축하여 서비스를 제공함

▶ 이음5G 서비스의 활성화를 위해 현재 원전, 의료, 물류, 전력 등 다양한 분야에 실증사업을 진행 중임

- 국외

▶ 본, 독일, 영국 등 주요 선진국들은 2019년부터 이음5G 전용 주파수를 공급함

- 일본은 5G 지역확산을 위해 28.2~28.3GHz 대역 ('19년 12월~), 4.6~4.8GHz 및 28.3~29.1GHz 대역 ('20년 12월~)을 이음5G 면허로 공급. NTT 동일본, NEC, 도쿄대학 등 45개 기관이 면허 취득함 ('21년 4월)
- 독일은 제조업체 중심으로 이음5G 수요가 있으며, 3.7~3.8GHz 대역을 지역 이음5G 면허로 공급 ('19년 11월~). 현재 보쉬, 폭스바겐 등 120개 기업 및 기관에 면허 발급함 ('21년 4월)
- 영국은 산업체의 이음5G 구축, 실내 커버리지 확대를 위해 3.8~4.2GHz 대역을 산업용 사설망 대역으로 공급함 ('19년 12월~). BT, Quickline 등 13개 면허권자에 794개 면허를 발급함

('20년 12월)

- 미국 FCC는 2020년 1월에 CBRS GAA(무면허, 무료주파수)를 상용화했고, 2020년 7월에 CBRS PAL에서 200여 개의 회사가 PAL 주파수 라이센스를 보유함

o **연구개발의 타당성 분석**

- 고령화·인구감소에 따라 이음5G의 초고속, 초연결, 초저지연을 이용하여 APC내 로봇·자동화 설비 등의 도입 기술개발·실증이 추진되고 있으며, 안전·안정적이고, 현장 친화적인 인프라 구축을 위한 이음5G 보안 기술 동향 조사 필요
- 국내 이음5G망 구축은 '22년부터 본격적으로 시작되어 관련 보안 기술 동향 및 사례 조사 미비
- 농산물 유통이라는 특수 산업에 디지털 전환에서 필요로 하는 이음5G망 구축을 위한 최적의 보안 모델을 조사가 필요

o **연구과제의 경제·사회·기술적 중요성**

- 기술(정책)적 측면
  - ▶ 5G 상용망에서 도입이 늦어진 SA 기술을 조사함으로써 이음5G에 SA 기술 도입, 운영 경우 필요한 보안 가이드라인을 제공
  - ▶ APC내 이음5G를 구축하는데 특히 고려되어야 하는 보안 요구사항을 조사
  - ▶ 운영 가이드라인을 통해 SA 기술의 이론적 안전성과 운영 시 사회공학적 요소에 의한 실질적 안전성 사이의 간극을 줄임
  - ▶ 구현 및 실증이 미성숙한 SA 기술은 표준문서를 기반으로 보안 구조와 키 계층을 조사
  - ▶ 이음5G와 연결된 다양한 어플리케이션에서 요구하는 사용자 인증을 AKMA 기술을 사용해 이음5G 인증시 어플리케이션 인증까

지 가능한 기술을 조사

▶ 이음5G망이 적용된 APC방문을 통해 구축, 운영 실태를 조사

- 사회·경제적 측면

▶ 이음5G망 보안구조 조사를 통해 이음5G망 보안 가이드라인을 만들고, 이음5G 도입을 간편화하여 도입 비용을 감소

▶ 서비스별 이음5G 적용 특성을 조사해 스마트시티, 자율주행차, 의료, 에너지, 농업 등 다양한 산업에 이음5G 적용을 촉진 시킴

▶ 농산물 산지 유통센터(APC) 내 이음5G망 구축은 농업 산업 분야에서 새로운 서비스 및 기회를 제공하며, 지역 경제 발전을 촉진

o **현 기술상태(정책)의 취약성**

- 네이버 클라우드, LG CNS 등 10개의 이음5G망 사업자가 주파수 할당 승인을 받아 자체적으로 이음망 구축사업을 추진하고 있음 그러나 이음 5G망에 특화된 보안 기술 및 장비의 부재로 자체적인 보안정책 및 보안 기술에 의존하고 있는 상황
- 5G 이음망을 위한 체계적인 보안정책 및 보안 지침 그리고 이음5G망에 특화된 보안 기술 확보가 필요
- 이음5G를 도입하는 엔드 유저에 대해 적극적인 규제 완화 정책과 홍보가 필요
- 이음5G 설치기업에 대해 주파수 사용료 전면 면제 혹은 시장에서 안정적으로 정착 전까지 면제 유예 기간을 두는 제도를 시행하고, 사후 관리 강화를 지향하는 정책 추진이 필요
- 중소 영세업자의 이음5G 도입 장려를 위해 use case의 적극적이고 지속적인 발굴과 홍보, 그리고 상세 가이드라인 제공이 필요
- 이음5G의 사용자 단말의 활용성을 위해 듀얼심 또는 eSIM(embedded Sim card) 도입은 필수이며, 이를 위한 적극적인 정책 지원이 필요

- 주요국 대비 좁은 이음5G 할당 대역폭으로 이음5G 관련 산업 경쟁력 확보를 위해 이음5G 대역폭 추가 개발 필요
- 5G 대비 1/10 저 지연성, 10배 이상의 고용량 데이터와 초연결성을 활용하기 위해 THz파 활용 기술, 망 운영의 완전 자동화, 저전력 반도체 그리고 소자 기술 등 관련 기술의 원천기술 확보 필요

o **연구과제 수행 시 기대성과**

- 기술(정책)적 측면
  - ▶ 이음5G 보안 가이드라인으로 발전하여 정책 및 개정을 위한 자료로 활용
  - ▶ 국내기업의 이음5G 시장 활성화를 위한 기업들이 고려해야 할 요구사항이 정책으로 활용 및 반영
- 산업·경제적 측면
  - ▶ 유통과 같은 형태의 이음5G 서비스가 제공・발굴됨으로써 국내 5G 산업생태계가 활성화되고 보안 분야에 있어 여러 파급효과를 기대
  - ▶ 이음5G를 활용하여 미래 신사업을 육성하고, 이를 위한 정보보호의 핵심 원천기술을 기획하기 위한 기반을 마련

제2절 연구 목표 및 추진계획

1. 연구 목표 및 방법

o **연구의 최종목표**

- 본 과제에서는 농산물 산지 유통센터(APC)내 이음5G망 구축을 위한 보안 기술 연구를 통하여 APC내 이음5G 실증 사이트 구축 시 활용 가능한 이음5G 보안구조 및 인증, APC내 이음5G 보안 모델을 정리한 기술 문서 2건 작성 및 국내 학술대회 1편 제출

o **본 과제에서 작성되는 기술 문서는 다음과 같은 내용을 포함**

- 이음5G 적용 사례 조사
- 이음5G 보안구조 및 인증기법
- 이음5G 적용기술 유형 및 기술별 보안 고려사항
- 농산물 산지 유통센터(APC) 내 이음5G망 구축을 위한 보안 모델 조사

o **본 과제의 최종목표 달성을 위해 제2장 연구수행과 같은 결과를 조사하였으며 해당 결과를 기반으로 기술문서 2건 작성 및 국내 학술대회 논문 1편 제출**

2. 추진계획 대비 실적 진도

o **추진방법**

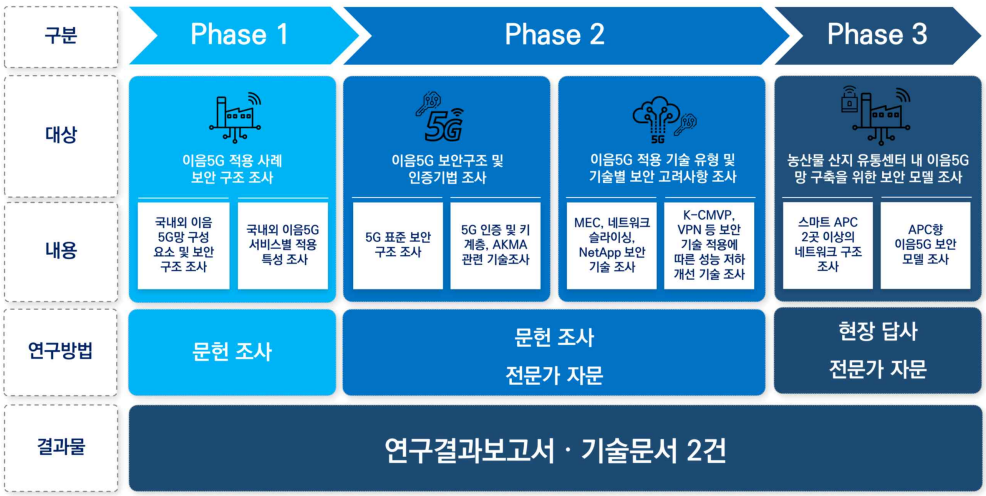
- **Phase1 : 문헌 조사 단계**
  - ▶ 국내외 이음 5G망 구성요소 및 보안구조, 서비스별 적용 특성 조사를 통해 이음 5G 보안구조 조사
- **Phase2 : 농산물 산지 유통센터(APC) 내 보안 고려사항을 위**

한 이음5G 보안 고려사항 조사

▶ 이음 5G 보안구조 및 인증기법 조사를 통한 이음 5G 내 활용 가능한 보안 고려사항 조사

- **Phase3 : 농산물 산지 유통센터(APC) 내 이음 5G 구축을 위한 보안 모델 조사**

▶ 실증 스마트 APC 네트워크 구조 조사를 기반으로 APC 향 이음 5G 보안 모델 조사



[그림 1] 연구 추진방법

o 추진계획 및 실적 진도

연구 내용	추 진 일 정 (개월)												실적진도
	1	2	3	4	5	6	7	8	9	10	11	12	
1) 이음5G 적용 사례 보안 구조 조사					■	■							100%
2) 이음5G 보안 구조 및 인증기법 조사						■	■						100%
3) 이음5G 적용 기술 유형 및 기술별 보안 고려 사항 조사								■	■				100%
4) 농산물 산지 유통센터 (APC) 내 이음5G망 구축을 위한 보안 모델 조사										■	■		100%

제 2 장 연구 수행내용 및 최종결과

제 1 절 연구수행내용

1. 이음5G 적용사례 및 보안 구조 조사

o 국내외 이음5G망 구성요소 및 보안 구조 조사

- 이음5G 모델별 사업장 내 구성요소 조사

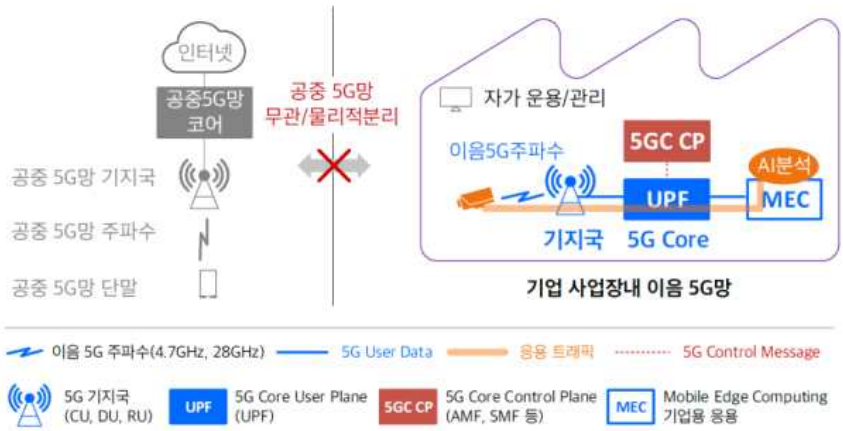
▶ 5G 이동통신 기반 제조업 고도화를 추진하는 협업체인 5G ACIA에서는 이음5G 구축방식에 따른 4가지 시나리오를 제시함

[표 1] 이음5G 모델별 사업장 내 구성요소

모델명	구축 주체	구축 구조	사업장 내 구성 요소
Ⅰ) 기업 자가구축	이용 기업	독립형	5G 단말, 기지국, 코어, MEC
Ⅱ) 이음5G 사업자 자가 구축	5G 이음5G 사업자	독립형	5G 단말, 기지국, 코어, MEC
Ⅲ) 5G Core CP 공유형		5G 코어 CP 공유형	5G 단말, 기지국, UPF, MEC
Ⅳ) 5G Core 전체 공유형		5G 코어 전체 공유형	5G 단말, 기지국

- 기업 자가구축 모델은 이음5G 인프라 및 기타 MEC 등을 모두 독립적으로 구축하여 높은 수준의 보안 및 안정성을 제공함
- 이음5G 사업자 자가구축 모델은 기업 자가구축과 유사하게 기업에 모든 장비가 존재함. 그러나 해당 장비의 구축과 유지보수를 이음5G 사업자가 담당함
- 5G Core CP 공유 모델은 5G 코어망에서 제어부를 분리하여 이음5G 사업자의 서버에 구축함
- 5G Core 전체 공유형은 5G RAN을 제외한 모든 코어 기능을 이음5G 사업자로부터 제공받음.

▶ 기업 자가구축형은 기업 또는 사업자가 소유한 무선망과 코어망을 사용하여 이음5G를 구축하는 방식. 해당 기업 또는 사업장 소속의 가입자만 접속 가능한 이음5G 서비스를 사용 가능. 기업 자가구축형 이음5G는 PLMN 식별자와 이음5G망 식별자가 결합 된 정보를 참조하여 구분. 여기서 PLMN 식별자는 이동통신망을 식별하는 정보이고, 이음5G 식별자는 글로벌하게 유일한 값 또는 PLMN 내부에서 유일한 값임. 기업 자가구축형은 [그림 3]과 같이 기업 또는 그룹 소유의 내부망을 이용하여 이음5G 서비스를 제공하며, 서비스의 특성을 고려하여 하나 또는 하나 이상의 네트워크 슬라이스로 분리하여 서비스를 제공 가능. 여기서 이음5G 운영자는 일반적으로 해당 기업 또는 이동통신 사업자일 수 있으며, 5G 장비 제조업체가 운영자인 경우도 있음



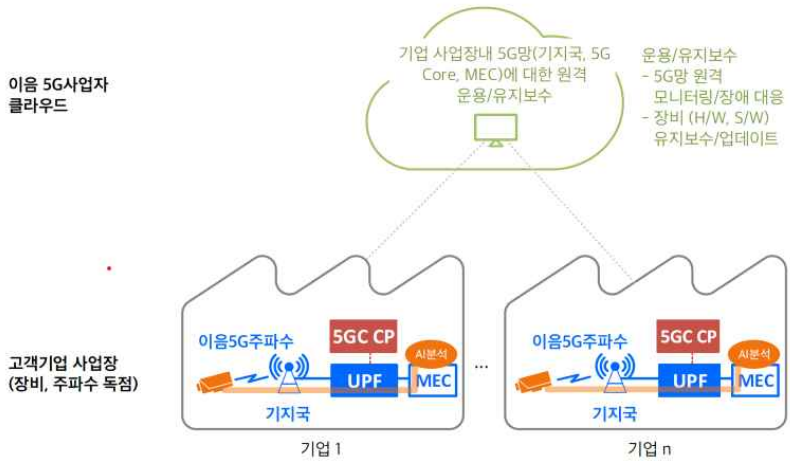
[그림 2] 기업 자가구축형 구조 예시
자료: Netmanias.com 이음5G 4가지 구축모델

- 보안 : 자가 구축된 내부망이 물리적으로 외부와 분리되어 있어 외부 침입으로부터 완벽한 데이터 보안 제공
- 초저지연 : 단말과 코어 그리고 응용 서버간 물리적인 거리가 가

까워서 네트워크 지연이 수 ms 이내이기 때문에 초저지연 응용 서비스 구현 가능

- 서비스 장애 : 이동통신사의 서비스 장애와 무관하게 독립적으로 대응
- 구축비용 : 코어망 자가구축 및 자체 유지보수에 따른 비용 다른 모델에 비해 가장 높음

▶ 이음5G 사업자 자가구축형은 이동통신사의 무선망과 이음5G의 코어망을 결합한 형태로 기업 등의 허락을 받은 단말만 이음5G 서비스를 받을 수 있음. 이음5G 사업자 자가구축형은 PLMN 식별자를 참조하여 네트워크를 선택하고 그룹 식별자를 참조하여 CAG 셀을 선택함. 여기서 그룹 식별자는 3GPP NPN 표준에서 CAG 식별자를 의미함. CAG는 CAG 셀의 식별자로서 이음5G망에 접속하는 그룹을 식별하는 정보임



[그림 3] 이음5G 사업자 자가구축형
자료: Netmanias.com 이음5G 4가지 구축모델

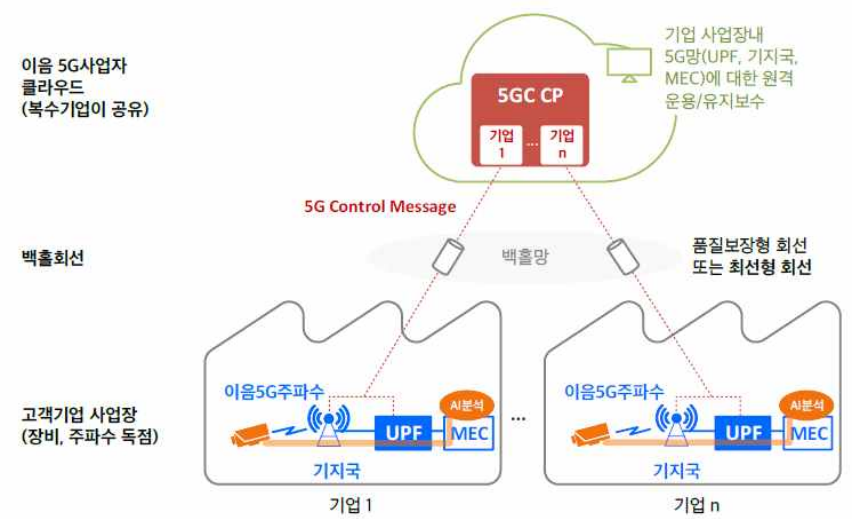
이음5G 사업자 자가구축형은 [그림 4]과 같이 구축의 주체만 다를 뿐 기업 자가구축형과 동일함. Private 슬라이스에 속한 단말들의 데이터 트래픽은 기업 내 전용 UPF로 전달되며, Public 슬

라이스에 속한 단말들의 데이터 트래픽은 이음5G 사업자 엣지 클라우드에 전달됨. 즉, 기업 내 기기 제어 데이터 등과 같은 트래픽은 기업 내에서만 머무르며, 유지보수를 위한 시그널링은 이음5G 사업자 클라우드로 전달됨. 여기서 Private 슬라이스는 이음5G 구축 기업 등에서만 사용하는 네트워크 슬라이스를 의미하며, 3GPP 표준에서 정의됨

- 보안 : 코어와 Private 데이터 트래픽에 대한 UPF가 내부에 있어 데이터 보안의 측면은 우수하나 유지보수를 위해 이음5G 사업자의 클라우드와 연결된 UPF가 있어 이를 통한 보안 위협은 일부 존재함
- 초저지연 : Private 데이터 트래픽에 대한 단말과 코어 그리고 응용 서버간 물리적인 거리가 가까워서 네트워크 지연이 수ms 이내이기 때문에 초저지연 응용서비스 구현 가능함
- 서비스 장애 : 외부 공용망과 분리되어 있어 이동통신사의 서비스 장애와는 무관하게 운영가능하며, 이음5G 사업자에 전문가의 유지보수 서비스를 받아 서비스 장애 발생 시 대응 가능함
- 구축비용 : 자가구축형과 비용 비교를 하여 기업 또는 사업장의 상황에 맞는 방향으로 선택을 함

▶ 5G Core CP 공유형은 이음5G 사업자의 코어망을 공유하는 형태로 기업 등의 허락을 받은 단말만 이음5G망 서비스를 받을 수 있음. 5G Core CP 공유형은 PLMN 식별자를 참조하여 네트워크를 선택하고 그룹 식별자를 참조하여 CAG 셀을 선택함. 여기서 그룹 식별자는 3GPP NPN 표준에서 CAG 식별자를 의미함. CAG는 CAG 셀의 식별자로서 이음5G에 접속하는 그룹을 식별하는 정보임. 5G Core CP 공유형은 [그림 5]와 같이 기업 등에 존재하는 기지국, UPF, MEC가 이음5G 사업자의 코어망과 CP가 공유됨. 내부망과 이음5G 사업자의 망 간에 기지국, UPF, MEC는 분리되며, 이음 5G 사업자의 CP를 공유함. Private 슬라이스에 속한 데이터 트래픽은 기업 내 전용 엣지 클라우드에 있는

UPF로 전달되며, Public 슬라이스에 속한 데이터 트래픽은 이동통신사 엣지 클라우드에 있는 CP로 전달됨. 즉, 기업 내 기기 제어 데이터, 센서 데이터 등과 같은 Private 데이터 트래픽은 기업 내에서만 머무르며, 기기 인증과 같이 5G 코어망과 통신이 필요한 데이터 트래픽은 외부에 있는 이음5G 사업자의 CP와 통신함



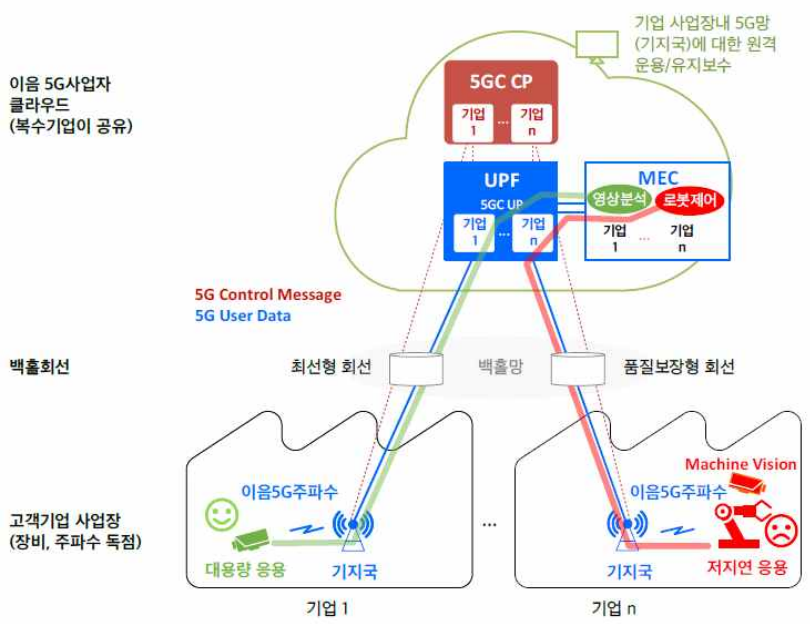
[그림 4] 5G Core CP 공유형
자료 : Netmanias.com 이음5G 4가지 구축모델

- 보안 : Private 데이터 트래픽에 대한 UPF가 내부에 있어 데이터 보안의 측면은 우수하나 기기 인증을 담당하는 코어망은 이음5G 사업자의 클라우드에 존재하여 내부 망이 외부망과 연결되어 있어 이를 통한 보안 위협은 존재함
- 초저지연 : Private 데이터 트래픽에 대한 단말과 코어 그리고 응용 서버간 물리적인 거리가 가까워서 네트워크 지연이 수ms 이내이기 때문에 초저지연 응용서비스 구현 가능함
- 서비스 장애 : 외부 공용망과 분리되어 있어 이동통신사의 서비스 장애와는 무관하게 운영가능하다. 이음5G 사업자에 전문가의 유지보수 서비스를 받아 서비스 장애 발생 시 대응 가능함. 그러나 코어가

이음5G 사업자의 클라우드에 존재하므로 해당 클라우드의 장애는 이음5G망의 장애로 이어질 가능성 있음

- 구축비용 : 코어망에 대한 비용이 절감되므로 상대적으로 저렴함. 다른 유형과 비용 비교를 하여 기업 또는 사업장의 상황에 맞는 방향으로 선택을 함

▶ 5G Core 전체 공유형은 이음5G 사업자의 코어망에 네트워크 슬라이싱을 적용하여 이음5G망 서비스를 제공함. [그림 6]은 5G Core 전체 공유형의 구조를 나타냄



[그림 5] 5G Core 전체 공유형
자료: Netmanias.com 이음5G 4가지 구축모델

이음5G 사업자 호스팅 방식은 S-NSSAI 또는 S-NSSAI와 DNN이 결합한 정보를 참조하여 선택됨. 여기서 S-NSSAI는 네트워크 슬라이스를 선택하는 정보이며, DNN은 DN을 표시하는 이름으로서 단말이 요청한 서비스 네트워크 이름을 표시함. 일반적으

로 하나의 네트워크 슬라이스는 다수의 DNN을 포함할 수 있음. 이음5G 사업자가 소유하고 운영하는 망은 할당된 주파수를 사용하므로 기본적으로 이음5G 서비스를 제공하는 절차는 동일함. 소비 기업 등이 전용으로 사용하는 Private 슬라이스를 통해 이음5G 서비스를 제공하며, 협약한 서비스의 특성을 고려하여 다수의 네트워크 슬라이스를 생성할 수 있음. 단말은 PLMN 레벨의 기본 인증과 네트워크 슬라이스 레벨의 추가 인증을 통과하면 이음5G망 서비스를 받을 수 있음

- 보안 : 기기 인증을 담당하는 코어망, 데이터 핸들링을 담당하는 UPF 모두 외부 이음5G 사업자의 클라우드에 존재하여 외부 서비스를 이용하는 부분에서의 보안 위협이 존재함
- 초저지연 : 무선 신호 구간을 제외한 데이터 트래픽을 처리하는 UPF, 인증을 담당하는 코어 등이 모두 외부 클라우드에 있어 내부망을 구축한 유형보단 네트워크 지연시간이 상대적으로 높음
- 서비스 장애 : 외부 공용망과 분리되어 있어 이동통신사의 서비스 장애와는 무관하게 운영가능함. 이음5G 사업자에 전문가의 유지보수 서비스를 받아 서비스 장애 발생 시 대응 가능함. 그러나 코어 및 UPF가 이음5G 사업자의 클라우드에 존재하므로 해당 망의 장애 여부는 이음5G 사업자의 클라우드 서버 운영 역량에 의존함
- 구축비용 : 코어망 및 UPF 대한 비용이 절감되므로 상대적으로 저렴함. 다른 유형과 비용 비교를 하여 기업 또는 사업장의 상황에 맞는 방향으로 선택을 함

▶ 살펴본 이음5G 구축방식에 따른 4가지 시나리오를 종합해보면 독립구축, 일부 공유, 전부 공유 등 3가지로 압축할 수 있는데 이때 3가지 구성방식의 특징을 살펴보면 다음과 같음

▶ 먼저 독립구축은 내부 이음5G 운용 전담인력 구성이 가능한 기업에 적합한 모델임. 기지국과 코어망, MEC를 사업장 내 별도로 구축하여 전송지연·성능 등을 향상시키고 보안성을 제공하는 사

업장 특화된 네트워크를 구축할 수 있음. 따라서 데이터 저장·관리에 민감한 사업장에 적합한 방식임

- ▶ 두 번째 일부 공유는 이음5G 사업장 내에 기지국과 코어망의 UP, MEC를 구축하는 모델임. 이동통신사 또는 이음5G 사업자 코어망의 CP를 공유하기 때문에 코어망 구축 및 운영, 유지보수 비용 부담이 완화될 수 있음
- ▶ 세 번째 전부공유는 이음5G 사업장 내 기지국만 설치하는 모델임. 이동통신사 코어망 전부를 활용하기 때문에 보안성이 떨어지지만 중소 규모의 경제성 있는 이음5G 구축이 가능함. 또한 이동통신사와의 거리에 따라 데이터 트래픽 지연이 발생할 수 있음

- **국내외 공공분야 이음5G망 모델별 구축 사례 조사**

▶ **국내 공공(한국수력원자력) - 독립형**

- 한국수력원자력은 지난 10년간 1,463건의 해킹 시도가 있었으며, 2022년 울진 대형 산불로 한울원전 근처의 상용통신망 일부 구간이 손실됨. 따라서 사이버 보안 측면에서 상용통신망과 분리된 사설망이 필요하고 재해의 영향을 받지 않는 안전한 이음5G망이 필요함

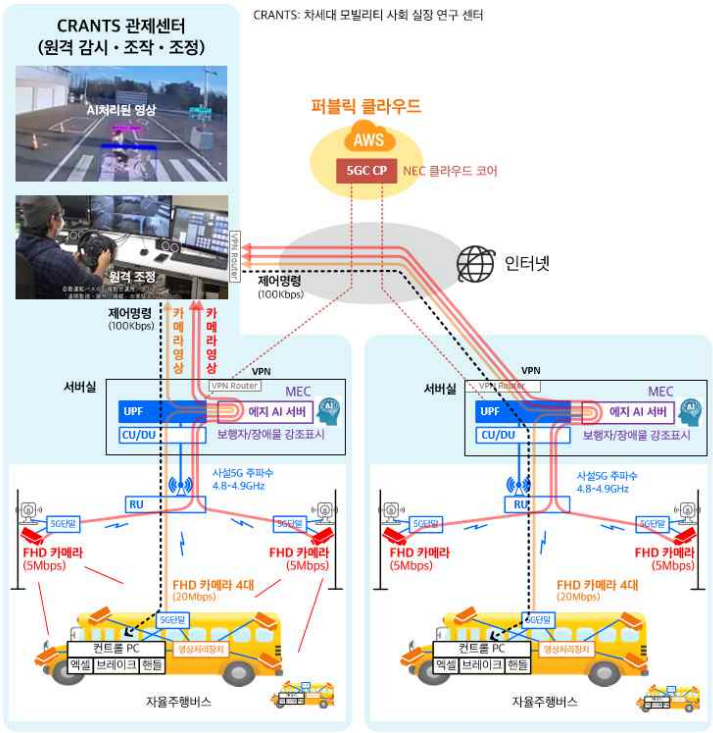
[그림 6] 한울 한전 특화망 구조도
자료: Netmanias.com
한국수력원자력 5G 특화망 구축 사례

- 이동통신망에 문제가 생겨도 이에 무관한 이음5G망을 한수원 전용 지휘 통신망으로 활용. 재난 상황에서 재해 현장 근처에 설치한 이동형 360° 카메라와 VR(3D)·AI(객체 인식)를 이용. 지휘자는 본관 통신실에서 현장에 가지 않고도 5G 특화망을 통해 라이브로 전달되어 오는 현장 상황을 관찰하면서 신속하게 재난 상황을 지휘

▶ **해외 공공(일본 마에바시시) - 5G Core CP 공유형**

- 마에바시시는 버스 운전자 부족, 인구감소로 인한 버스 수입 감소 등의 문제로 현재의 버스 노선을 유지하기 어려울 것으로 예상하여 변두리 지역에 원격 자율주행 기술 도입을 계획함. 이음5G망을 통해서 자율주행을 운영하는 동시에 사고 발생을 감지하여 직접 제어를 목표로 함. 이를 통해 운행 비용 감소, 운전자 보완, 이동 수단 확보를 목표로 함

- 관제센터에서는 차량 카메라를 통해 주변 상황을 살피고, 도로 카메라를 통해서 전체적인 상황을 감지함. 따라서 일반적으로 버스는 자율주행으로 운행하면서, 이상 상황 발생 시 감시자가 원격으로 조종함. 자율주행 버스의 FHD 카메라 영상(버스 2대, 버스 탑재 FHD 카메라 4대, FHD 카메라 1대 5Mbps, 2대 버스 합계 총40Mbps)과 전주에 설치된 FHD 카메라 영상(전주 2개, 전주당 HFD 카메라 1대, FHD 카메라 1대 5Mbps, 2개 전주 합계 총 10Mbps)이 로컬 5G망을 통해 관제센터의 AI 에지 서버로 전달되고, 관제관이 집중하도록 보행자/ 장애물을 강조 표시한 후 관제센터로 송출됨



[그림 7] 마에바사시 자율주행 버스 구조도
자료: Netmanias.com [교통] 로컬 5G 원격형 자율운행 버스 실증

- 국내외 민간분야 이음5G망 모델별 구축 사례 조사

▶ 국내 민간(삼성서울병원) - 독립형

- 기존 레지던트 대상의 수술 참관 교육 시, 인원과 장소 문제로 많은 어려움을 겪음. 더불어 집도의 또한 상황에 따라 전문의의 조언이 필요하나, 항상 함께할 수 없다는 문제가 있음
- 삼성서울병원은 KT의 계열사인 KT MOS와 함께 이음5G망을 구축하여 두 가지 문제를 한 번에 해결함. 수술 현장을 이음5G망을 통해 실시간으로 공유하여 전문가의 조언을 얻음. AR글래스, 360도 카메라 등 다양한 장비들을 통해 현장에 있지 않더라도 구체적인 상황을 파악하고, 상황에 맞는 조언이 가능함. 동시에 현장 화면을 교육에 사용함으로써 참관 교육까지 해결함

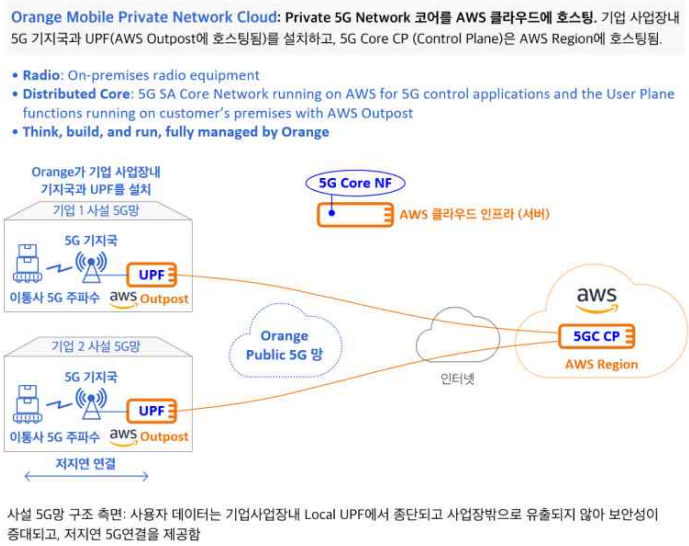
[그림 8] 삼성서울병원 이음5G 구조도

자료: Netmanias.com KT MOS의 5G 특화망 서비스 (삼성서울병원)

▶ 국외 민간(AWS인프라) - 5G Core CP 공유형

- AWS는 이통사가 AWS 클라우드 인프라를 활용하여 기업에게 이음5G망을 제공해줄 수 있게 하는 Integrated Private Wireless on AWS 프로그램이 2023년 2월 21일에 출시함. AWS는 이음5G망

구축을 희망하는 기업에 이통사를 연결해줌. 기업이 원하는 기능과 관리에 따라서 이통사는 이음5G망을 구축하고 운영함



[그림 9] AWS 인프라 구조도
자료: Netmanias.com 프랑스 Orange의 Private 5G

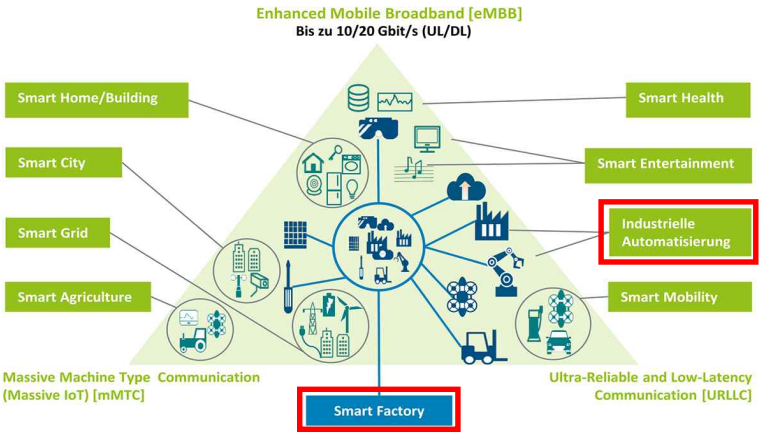
–

o **국내외 이음5G 서비스별 적용 특성 조사**

- **이음5G 제조·생산 서비스 적용 특성 조사**

▶ 이음5G 적용 특성을 분석하기 위해 5G 적용이 가능한 다양한 분야들 중 제조 및 생산 서비스 분야에 대한 이음5G의 활용 형태를 제시함. 이음5G가 가지는 3가지 특성, 초고속(eMBB), 저지연(URLLC), 초연결(mMTC) 특성을 통해 여러 가지 서비스를 제공할 수 있지만, 자동화된 제조·생산 설비에는 초고속과 저지연 특성이 필수적임. 특히 스마트 공장은 제품의 기획부터 판매까지 모든 생산과정을 정보통신기술로 통합해 최소 비용과 시간으로 고객 맞춤형 제품을 생산하는 첨단 지능형 공장이며 산업 기밀

정보들이 데이터 내에 그대로 포함될 수 있음. 따라서 이음5G를 활용하되 유연한 확장성과 높은 보안성을 갖춘 모델을 선택해야 함. 앞서 언급했던 4개 시나리오 중 이에 가장 적합한 특성을 가진 이음5G 모델은 독립형 전개 모델이라고 할 수 있음



[그림 10] 제조 생산 서비스에 대한 이음5G 적용 특성
자료: Industrial ethernet book, 5G on test bench for Industry: What's possible in the future?(2021)

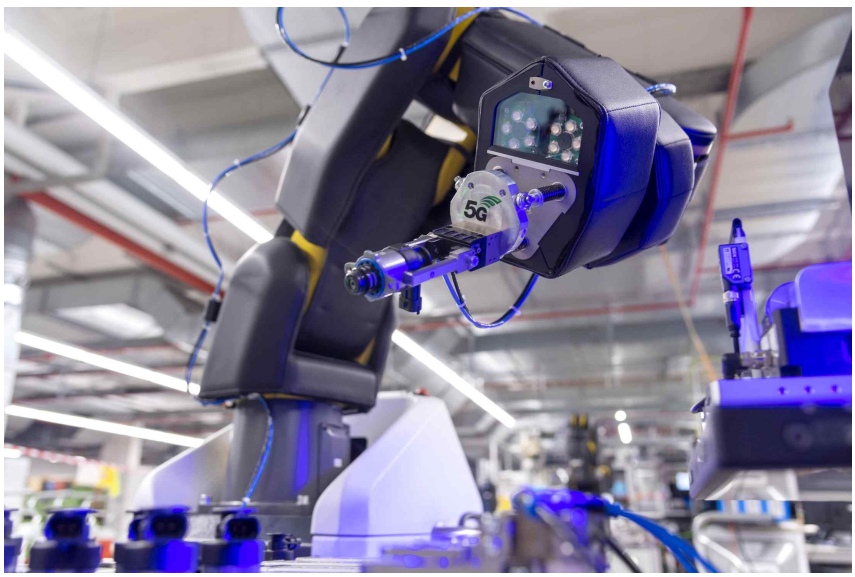
[표 2] 제조, 생산 서비스에 대한 이음5G 적용 모델

서비스	커버리지	SI비용	구축비용	보안성	QoS보장	지연시간	모델
제조생산	Low	High	High	High	High	High	자가구축

▸ (1) 이음5G를 적용한 스마트 공장

- 기존 자동화 설비의 IoT 데이터는 게이트웨이로부터 이음5G를 통해 중앙 서버로 전송이 가능함. 최소 지연 보장 기능을 적용하여 설비별 자동화된 단위 장비의 상태 및 제어 데이터를 주변 설비 및 인프라와 연계하여 최적화 할 수 있음. 작업자 단말로 무선 링크를 통해 알림 메시지를 전달하는 등 스마트 공장 구현에 있어 보다 확장성과 보안성이 뛰어난 무선 환경을 제공함

- 제조과정에서 고화질 이미지 분석 기반 실시간 작업 확인 및 작업자의 AR글래스를 통한 영상기반 원격 작업지시, 3D VR·AR 도면 기반 작업자 기술지원 시스템 등 현장에서의 데이터 라이브러리 열람 및 업로드가 가능함. 무인 운반 시스템(AGV)의 경우 5G네트워크의 정밀 포지셔닝 기술이 더해져 기존 유도선을 따라 이동하는 AGV의 이동한계를 극복한 원격 위치제어가 가능함
- 제조설비의 라인 증축에 있어 밀리미터파 기반의 무선링크로 구성한다면 별도의 유선공사 및 생산라인 중단 없이 설비 증설이 가능하며 외부 수요환경에 맞는 빠른 설차·변경 가능한 생산 환경 구현이 가능함. 타 지역의 공장간 또는 본사 관제시스템과의 이음5G를 연동하는 경우 유선 기간통신사업자의 전용회선 임대를 통해 구현함. 이 경우 이음5G로부터 실시간 수집되는 정보를 공장·제조설비의 3D 모델에 적용한다면 CPS(Cyber Physical System) 또한 구축 가능



[그림 11] 이음5G망 적용된 제조, 생산 서비스

자료: Bosch Press, Bosch puts first 5G campus network into operation(2020)

▸ (2) 이음5G를 적용한 스마트 조선

조선 산업을 친환경적이고 스마트화하기 위해서 이음5G를 적극 활용할 수 있음. 야드 영역 내 작업자의 웨어러블 디바이스와 기존 자동화 설비에서 발생하는 데이터를 이음5G를 통해 수집하고 디지털 트윈 플랫폼 내 3D 모델링 정보와 결합하여, 가상 조선소를 구현할 수 있음

또한, 작업자의 스마트 헬멧 등 웨어러블 기기를 통해 작업장 내 안전사고를 예방하고 AR·VR 등을 활용한 3D 설계정보의 전송 및 원격 작업지시가 가능함. 또한 블록 조립 공장에는 원격 제어 가능한 용접로봇을 도입하는 등 디지털 공법으로의 전환이 가능함. 5G 코어망을 조선소 내 구축하고, 설계도면과 같은 보안성이 요구되는 기업의 주요 디지털 정보를 On-Site MEC 솔루션을 통해 직접보관·관리함으로써 기업 경쟁력을 확보할 수 있고, ESG경영이 주요 화두인 만큼 조선소 내 작업자의 노동환경 개선 및 안전 확보 측면에 있어 핵심 인프라가 될 것

▸ (3) 이음5G를 적용한 스마트 건설

- 건설 현장에서 작업자의 스마트 헬멧으로부터 주요 공정에 대한 고화질 영상 기록을 중앙서버로 전송하고 이동동선 및 현재 위치를 모니터링하여 현장 관리 및 작업자의 안전을 확보할 수 있음. 현장소장 및 감리는 이음5G 전용 단말 또는 AR 글래스를 통해 BIM(Building Information Modeling) 설계와 2D 도면과 같은 대용량 이미지·문서 등 현장에서의 데이터 라이브러리 열람 및 업로드가 가능함. 공사 중장비에 5G 단말을 연동하여 초저지연 기반의 원격제어가 가능한 작업환경을 구성하고, 나아가 중앙서버의 BIM 설계 모델과 현장에서 이음5G를 통해 수집되는 다양한

형태의 정보를 결합시키면 디지털 트윈(Digital Twin)기반의 가상 건설현장 구현도 가능함

- **이음5G 공공·인빌딩 서비스 적용 특성 조사**

▶ 이음5G 적용 특성을 분석하기 위해 5G 적용이 가능한 다양한 분야들 중 공공 및 인빌딩 서비스 분야에 대한 이음5G의 활용 형태를 제시함. 이음5G가 가지는 3가지 특성, 초고속(eMBB), 저지연(URLLC), 초연결(mMTC) 특성을 통해 여러 가지 서비스를 제공할 수 있지만, 자동화된 공공·인빌딩 설비에는 초고속 특성이 필수적임. 또한 스마트 병원 등 의료서비스를 제공하기 위해서는 도심 뿐 아니라 도서산간 지역에도 통신이 가능해야하고 수술 등 생명에 직결되는 통신 서비스를 위해서는 QoS 보장 및 초저지연 특성도 필요함. 따라서 이음5G를 활용하되 QoS 보장과 넓은 커버리지를 갖춘 모델을 선택해야 함. 앞서 언급했던 4개 시나리오 중 이에 가장 적합한 특성을 가진 이음5G 모델은 무선 액세스 공유 모델이라고 할 수 있음

[표 3] 공공 인빌딩 서비스에 적합한 이음5G 정용 모델

서비스	커버리지	SI비용	구축비용	보안성	QoS보장	지연시간	모델
공공인빌딩	High	hIGH	Mid	High	High	High	코어공유

▶ **(1) 이음5G를 적용한 스마트 병원**

• 병원 내 스마트 의료서비스 도입을 위해서 이음5G를 적극 활용할 수 있음. 의료진은 IoT 장비(웨어러블 기기 등)를 활용한 모니터링을 통해 환자의 건강 정보에 대한 연속적인 관리 감독이 가능하며, 질병의 패턴과 순간적인 변화를 실시간으로 전송·공유하여 빠른 대처 및 진단·치료가 가능함. 또한 다양한 의료기기로부터 발생하는 IoMT(Internet of Medical Things)데이터를 이음5G를 통해 중앙서버로 전송함으로써 의료장비의 상태 추적, 원무·

행정·진료 프로세스 개선 등 병원의 운영 효율성 및 의료 서비스 품질향상이 가능함. 환자의 각종 샘플이나 방사선 사진, 의약품 등을 옮기는 천장 레일형 이동 로봇의 경우 이음5G망의 정밀 위치측위 기술 등을 적용해 이동성의 제약없는 자율원격제어 주행이 가능해짐. 무력감에 빠지기 쉬운 환자나 고령자에게는 활동적인 행동을 할 수 있도록 동기 부여가 가능한 가상·증강현실 콘텐츠를 스마트 디바이스를 통해 제공할 수 있으며, 전염병 등으로 인하여 병실 방문이 어려울 경우 가상현실 기술(VR·MR)을 통해 방문객의 면회가 가능함

▸ **(2) 이음5G를 적용한 스마트 캠퍼스**

- 대학 내 융복합 연구 환경 및 첨단 교육 제공을 위해 이음5G를 적극 활용할 수 있음. 독립구축 모델 또는 일부 공유 모델을 활용하여 직접 운영할 경우 관계 교수진들과 학생들의 참여를 통해 네트워크 엔지니어링 및 운영 전반의 실무경험을 쌓을 수 있음. 이음5G를 기반으로 교내 진행되고 있는 자율주행, 드론 등의 ICT 융·복합 연구 과제들에 대한 테스트 베드로서 활용할 수 있음. 또한 코로나와 같은 정상수업 진행이 어려운 환경에서 이음5G망 단말체계를 확보하고 5G 브로드캐스트(Broadcast) 기술을 적용하여 고화질 스트리밍 기반의 캠퍼스 내 시·공간 제약 없는 원격강의 수강환경을 실현시킬 수 있음. 아울러 대용량의 융합현실(XR) 콘텐츠를 전송받거나 360° 매트릭스 뷰 실습실을 구축하여 학생들에게 보다 효과적인 몰입·참여형 교육기회 제공이 가능함.

[그림 12] 5G 특화망 적용된 공공, 인빌딩 서비스

자료: Nokia, Sendai city improves tsunami preparedness with connected drones(2019)

▸ (3) 이음5G를 적용한 스마트 오피스

- 업무 효율 향상 및 스마트 사옥관리 등을 위해 이음5G를 적극 활용할 수 있음. 사옥 보안 및 운영관리 측면에서 영상정보 처리기기(CCTV)를 감시구역 및 주차 관제 설비 등에 적용함으로써 고화질의 영상 데이터를 중앙서버로 실시간 전송시킬 수 있음. 공조설비, 조명, 전력기기 등의 IoT 센서로부터 발생하는 데이터는 게이트웨이와 이음5G를 통해 중앙서버로 연결이 가능하다. 이를 통해 빌딩 자동제어 솔루션, 지능형 에너지 절감 등을 기대할 수 있음. 업무환경에 있어 유선 LAN 환경을 이음5G로 대체하여 외부망과 분리된 내부 업무환경을 구축할 수 있고, 무선화된 모바일 오피스 환경도 구축할 수 있음. 외부 인터넷망 연동 필요시 네트워크슬라이싱 기술 등을 적용하여 논리적으로 분리된 업무망 환경 또한 구현 가능함

- **이음5G 에너지·자원 서비스 적용 특성 조사**

  ▶ 이음5G 적용 특성을 분석하기 위해 5G 적용이 가능한 다양한 분야 중 에너지 및 자원 서비스 분야에 대한 이음5G의 활용 형태를 제시함. 이음5G가 가지는 3가지 특성, 초고속(eMBB), 저지연(URLLC), 초연결(mMTC) 특성을 통해 여러 가지 서비스를 제공할 수 있지만, 자동화된 에너지·자원 설비에는 초연결 특성이 필수적임. 집집마다 들어가는 전기 계량기와 넓은 발전소에는 수많은 이음5G 기기들이 적용될 것임. 또한 수많은 기기들로부터 발생하는 에너지 자원 데이터를 처리하기 위해서는 고성능의 기지국과 코어망을 갖춘 모델을 선택해야 함. 앞서 언급했던 4개 시나리오 중 이에 가장 적합한 특성을 가진 이음5G 모델은 이동통신사 호스팅 방식이라고 할 수 있음

[표 4] 에너지 자원 서비스에 적합한 이음5G 적용 모델

서비스	커버리지	SI비용	구축비용	보안성	QoS보장	지연시간	모델
에너지자원	High	Low	Low	Low	Low	Low	전체공유

▶ **(1) 이음5G를 적용한 스마트 발전소**

- 5G 기반 설비의 원격 모니터링, 제어 등을 위해 이음5G를 적극 활용할 수 있음. 설비 순찰로봇 및 CCTV의 고화질의 영상 데이터와 IoT 센서로부터 발생하는 기존 발전 계통 및 환경설비 정보를 IoT 게이트웨이와 이음5G를 통해 중앙서버로 전송이 가능함. 또한 실시간 수집되는 영상 데이터와 IoT 센싱 데이터를 결합함으로써 주요 발전 및 송전 설비에 대한 실시간 원격 모니터링, 장애 설비의 실시간 절체가 가능함. 나아가 발전소 내 주요 계통 설비를 3D 모델링하고 이음5G를 통해 수집되는 다양한 형태의 정보를 결합시킴으로써 디지털 트윈(Digital Twin)기반의 가상 발전소

를 구축하여 발전소의 가동효율 높이고 장애 예측 및 사전 예방 활동을 수행할 수 있음.

[그림 13] 이음5G 적용된 스마트 발전소
자료: Im-mining, Sandvik and Nokia team up to offer miners LTE and 5G networks(2018)

- **이음5G 교통·수송 서비스 적용 특성 조사**
  - ▶ 이음5G 적용 특성을 분석하기 위해 5G 적용이 가능한 다양한 분야들 중 교통 및 수송 서비스 분야에 대한 이음5G의 활용 형태를 제시함. 이음5G가 가지는 3가지 특성, 초고속(eMBB), 저지연(URLLC), 초연결(mMTC) 특성을 통해 여러 가지 서비스를 제공할 수 있지만, 자동화된 교통·수송 설비에는 초저지연 특성이 필수적임. 자율주행과 같은 교통 자동화에는 운전자 및 보행자의 안전이 필수적이며, 차량이 이동할 수 있는 전국 지역에 서비스를 제공할 수 있어야하기 때문에 서비스 커버리지가 넓어야 함. 또한 공공재의 특성상 구축비용과 SI 비용이 크지 않아야 함. 따라서 구축비용을 최소화하는 이음5G를 활용하되 최소 지연 보장과 넓은 커버리지를 갖춘 모델을 선택해야 함. 앞서 언급했던 4개 시나리오 중 이

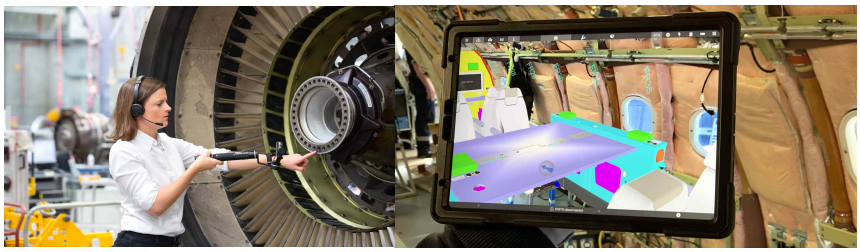
에 가장 적합한 특성을 가진 이음5G 모델은 무선 액세스 및 제어부 공유 모델이라고 할 수 있음

[표 5] 교통수송 서비스에 적합한 이음5G 적용 모델

서비스	커버리지	SI비용	구축비용	보안성	QoS보장	지연시간	모델
교통수송	High	Mid	Low	Low	High	High	전체공유

▶ (1) 이음5G를 적용한 스마트 공항

- 공항을 이용하는 고객 및 공항 인프라 운영, 관리 측면에서 이음5G를 적극 활용할 수 있음. 터미널 내 실감 미디어 콘텐츠, 방역 안내 로봇 서비스 외 실시간, 출국장 및 보안검색 지역 등에 대용량 및 이동성이 보장된 공항 특화 서비스 구현이 가능함. Airside 내 다양한 용도의 자율운행 차량 제어 및 등화 시설 등의 시설물 관리, 유선 공사 없는 고화질 지능형 CCTV 추가 증축, 스마트 헬멧을 활용한 작업자 안전관리 등이 가능함. 독립구축 모델 또는 일부 공유 모델을 활용하여 직접 운영할 경우 항공기 격납고를 이용하는 항공사 및 상업시설 입주사 등을 대상으로 5G 서비스 상품을 제공할 수 있음

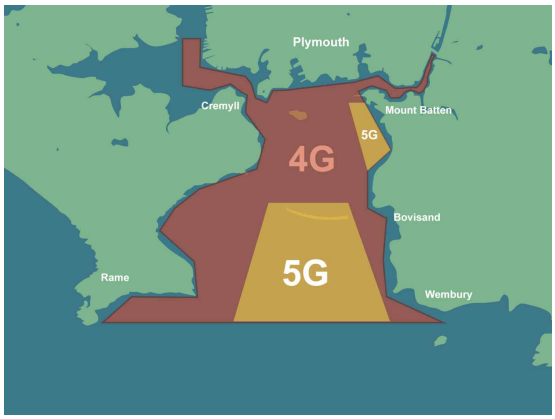


[그림 14] 이음5G 적용된 스마트 공항
자료: Lufthansa Technik, Lufthansa gets spectrum licence, deploys Nokia private 5G for remote engine checks(2020)

▸ (2) 이음5G를 적용한 스마트 항만

- 항만 인프라 운영, 관리 측면에서 이음5G를 적극적으로 활용할 수 있음. 안벽 영역의 크레인 내 고화질 카메라와 센서를 이용하여 원격에서 크레인의 양하 및 적하 제어가 가능하며 별도의 유선 공사 없이 구현할 수 있음. 이송영역에서는 AGV(Automated Guided Vehicle) 등과 같은 자동 운반차량의 이동제어·관리가 가능함. 야드 영역에서는 야드 크레인의 실시간 원격 제어와 스마트 헬멧 등을 활용한 작업자의 안전관리, 지능형 CCTV를 통한 보안 관제 서비스 등을 구현할 수 있음. 독립구축 모델 또는 일부 공유 모델을 활용하여 직접 운영할 경우 항만 내 입주하고 있는 선사, 하역업체 등을 대상으로 5G 서비스 상품 또한 제공 가능함

[그림 15] 이음5G 적용된 스마트 항만1
자료 : Plymouth Marine Laboratory

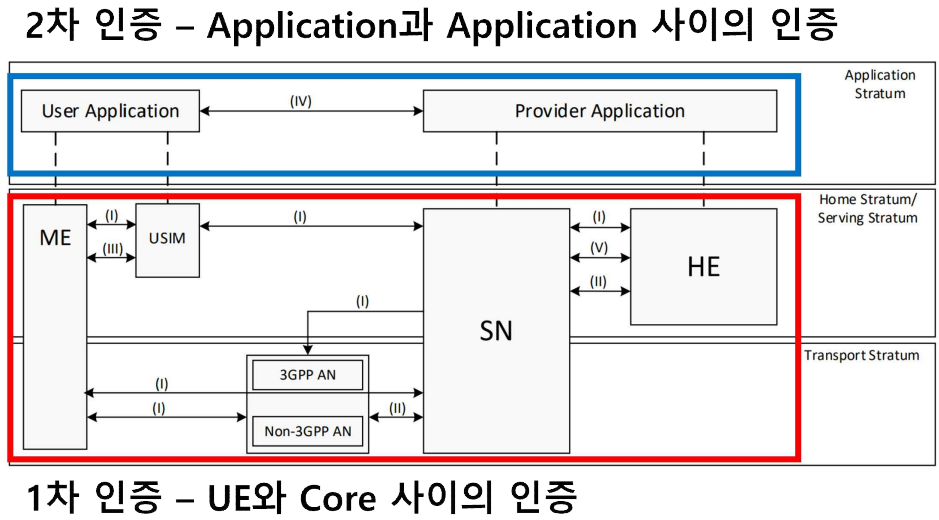


[그림 16] 이음5G 적용된 스마트 항만2
자료 : smartsoundplymouth.co.uk

2. 이음5G 보안구조 및 인증기법 조사

o 5G 표준 보안구조 조사

- 이음5G 보안 고려사항 도출을 위한 표준 기반의 5G 보안구조를 조사함. 5G 보 구조의 표준 3GPP TS 33.501 문서에서 표현한 5G의 보안구조는 [그림 17]과 같음
- [그림 17]에서 사용자 기기인 UE(User Equipment)와 네트워크 코어 사이의 인증을 1차 인증, 인증된 두 주체의 Application 간 인증을 2차 인증이라고 함. APC에서는 데이터의 무결성이 중요하므로, 인증된 센서로부터 데이터를 전달받아야 하며, 인증된 사용자가 원격에서 이런 데이터를 확인하고, 중장비 등의 기기를 제어할 수 있어야 함.



[그림 17] 3GPP 5G 보안구조
자료 : 3GPP TS33.501

- **보안 도메인 여섯 가지**

▶ 1) Network access security : 3GPP 그리고 비3GPP 기반의 접속에 대해서 UE라고 불리는 사용자의 기기가 네트워크를 통해 안전하게 인증받고 서비스에 접속할 수 있도록 하는 보안특성을

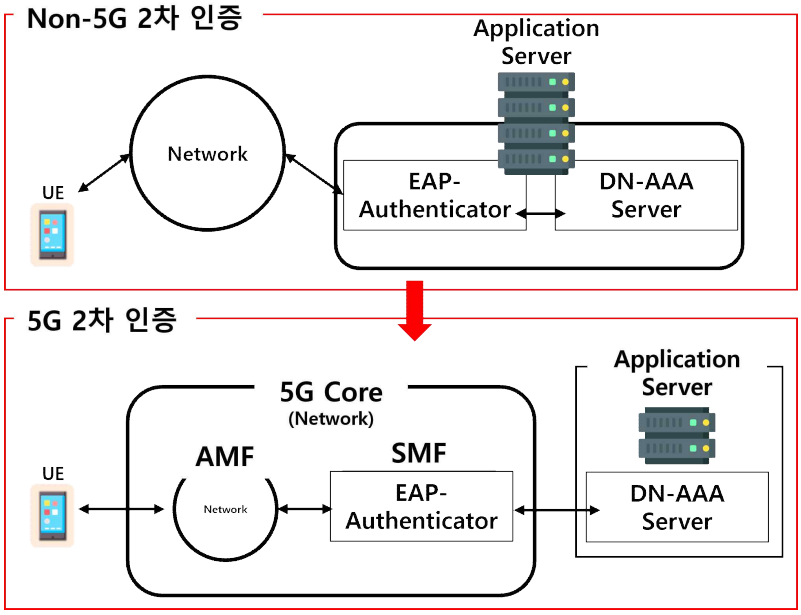
뜻함

- 2) Network domain security : 네트워크 노드들이 안전하게 제어 메시지 또는 사용자 메시지를 안전하게 교환할 수 있도록 하는 보안특성을 뜻함
- 3) User domain security : 사용자 기기에 대한 직접적 보안 도메인
- 4) Application domain security : 사용자 그리고 어플리케이션 제공자 사이에 안전한 데이터 교환을 위한 보안특성을 뜻함
- 5) SBA domain security : 5G는 SBA즉 네트워크 노드가 물리적인 장비가 아닌 클라우드 안에 있는 가상화된 함수로 구성되는 구조를 가짐. 이에 각각의 인스턴스들이 함수를 안전하게 호출하는데 필요한 보안 도메인
- 6) Visibility and configurability of security : 보안 관제 도메인

- **1차 인증 (5G-AKA)**
  - 3GPP는 1차 인증에서 5G-AKA와 EAP-AKA' 두 가지를 표준으로 지정했음. 그러나 EAP-AKA'의 경우 SN(Serving Network)에서 UE를 인증하는 기법이 없으며, HN(Home Network)에서의 연산량이 EAP-AKA'이 더 많음. 이에 1차 인증으로는 5G-AKA가 더 적절할 것으로 판단함

- **2차 인증 (EAP-AKA')**
  - 1차 인증은 네트워크망에서 특정 기기 또는 사용자를 인증하는 것임. 2차 인증은 해당 네트워크를 통해서 연결하는 서비스 서버와 인증을 뜻함. 2차 인증은 5G망에서만이 아닌 모든 네트워크를 통한 서비스에서 사용되고 있음. 그러나 5G를 통한 2차 인증의 경우 기존에 서비스 서버(Application Server)가 제공해야 하는 인증 기능의 일부를 5G 코어가 대체해 서비스 제공자의 인증 서버 구축

및 유지보수의 부담을 줄임. [그림 18]은 해당 구조의 도식임



[그림 18] Non-5G와 5G 네트워크 기반의 2차 인증

▶ 5G코어망 내에 SMF(Session Management Function)가 Non-5G 네트워크에서 2차 인증에서 서비스 제공자, 즉 Application Server를 관리하는 사업자가 구축했어야 했던 EAP-Authenticator를 대체하여 사업자의 부담을 줄임

- AKMA

▶ AKMA(Authentication and Key Management for Applications)는 3GPP의 표준문서 TS33.535에서 정의하는 프로토콜임. 목적은 2차 인증과 마찬가지로 네트워크 인프라 계층을 위한 인증이 아닌 어플리케이션 계층에서 사용자를 인증하고 식별하기 위한 프로토콜. 이는 어필리케이션 서비스가 외부에 구축되는 것이 아닌 5G 코어망에서 지원하는 네트워크 함수의 형태로 만들어지고, 연동되는 것을 시작

으로 함. 1차 인증 이후에 파생되는 키를 코어망에서 안전하게 전달받아 이를 이용해 상호 인증을 다시 한번 수행함. 5G망과 연동되게 Application 서버를 구현해야 하지만 APC에서 사용하는 기기의 특성상 연산 능력에 한계가 있어 2차로 재인증을 하는 것보다는, 기존에 생성한 키에서 파생하여 사용한다는 점에서 더 가벼움. 그리고 스마트 APC 내에 네트워크 관리부터, 어떤 어플리케이션에 대한 관리까지 이음5G에 대한 관리 틀을 통해 한 번에 관리할 수 있게 된다는 점에서 가용성이 증가하고, 이는 관리 비용의 저하로 이어질 수 있음

o 5G 인증기법 조사 및 키 계층 분석

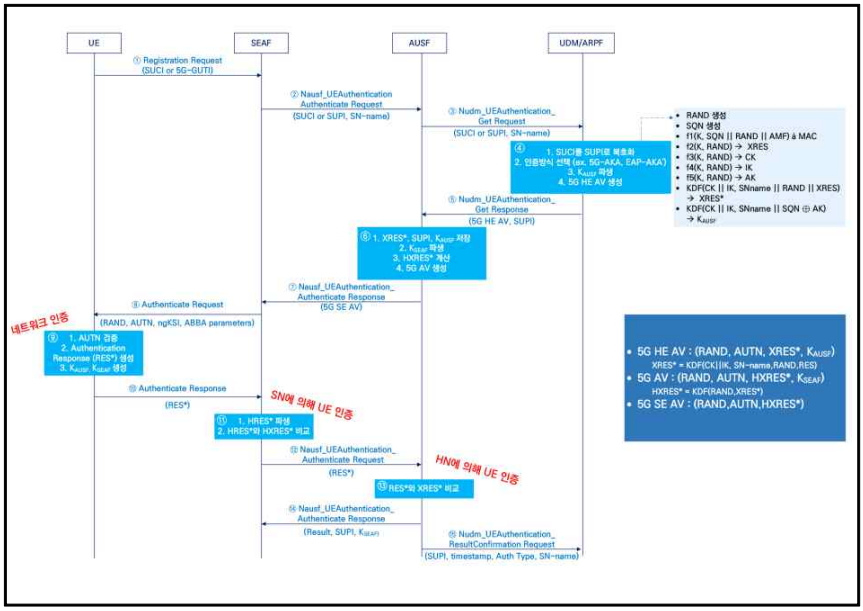
- 5G 인증기법 조사

▸ 3GPP 표준 TS33.501에 의하면 5G에서 1차 인증으로 사용하는 프로토콜은 5G-AKA(5G Authentication and Key Agreement), EAP-AKA'(Extensible Authentication Protocol Authentication and Key Agreement) 두 가지로 기술되어 있음. 두 인증 프로토콜 모두 3GPP 1차 인증 표준이며 UE(User Equipment) 라고 불리는 사용자 기기가 이동통신 사업자의 네트워크에게 정상적인 사용자라는 것을 인증하고, UE 또한 연결하는 네트워크가 정상적인 네트워크라는 것을 확인함. 해당 과정을 진행하면서 추후 데이터의 기밀성과 무결성을 위해 사용할 키를 파생하는 과정임

▸ 5G-AKA

• 5G에서는 UE와 네트워크 간의 상호 인증을 하고 후속 보안 절차에서 UE와 서빙 네트워크 사이에서 사용될 수 있는 키를 파생하기 위해 1차 인증을 수행. 5G-AKA 프로토콜은 이동 단말과 5G 코어망 사이의 상호인증 및 키 교환을 목표로 함. 인증 이후에는 이동 단말과 AUSF(Authentication Server Function) 사이에는 Master Session Key K_SEAF가 공유되게 된다. [그림19]는

5G-AKA 동작 절차.



[그림 19] 5G-AKA 1차 인증 동작 절차
자료 : 3GPP TS33.501

- **절차 설명**

1) 단말은 단말 신원정보인 SUCI(Subscription Concealed Identifier) 또는 임시 신원정보인 5G-GUTI(Globally Unique Temporary UE Identifier를 SEAF/AMF에 전송함. 이때 SUCI는 HN(Home Network)의 공개키로 SUPI를 암호화 한 값을 말하며, 5G-AKA에서 사용하는 알고리즘은 타원 곡선 암호 기반인 ECIES(Elliptic Curve Integrated Encryption Scheme)임. 또한 GUTI의 경우 단말이 초기인증이 아닌 이전 등록과정에서 인증에 성공한 이후 AMF(Access and Mobility management Function)로부터 GUTI를 제공받았을 때 사용하게 되며 GUTI 값은 AMF에서 SUPI로 변환됨

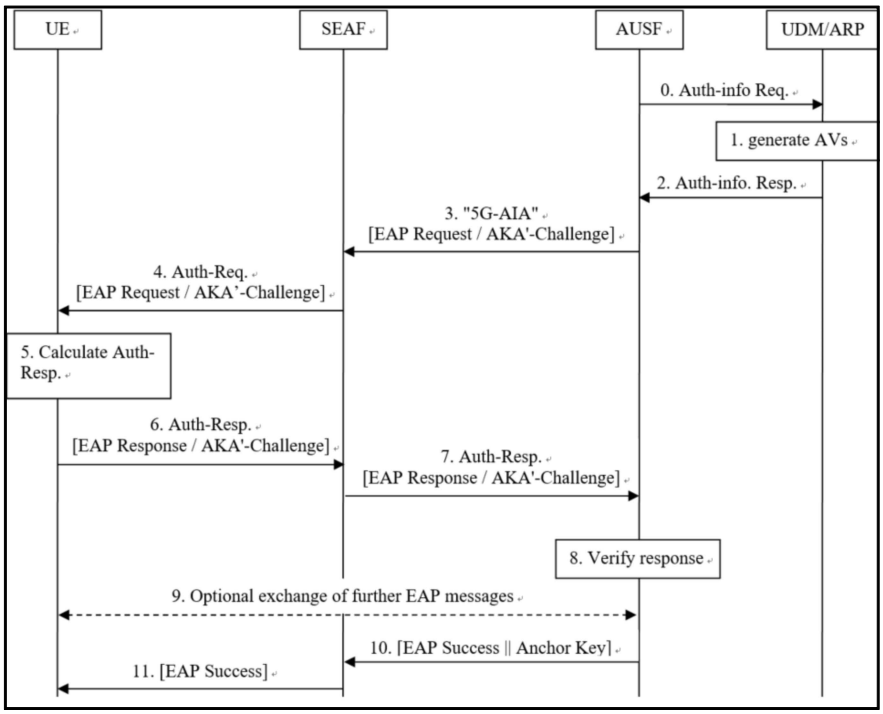
2) Registration Request 메시지를 수신한 SEAF(Security Anchor Function)는 제공받은 SUCI 값을 기반으로 UE가 가입한 이동통신사업자의 정보를 얻음. 그 후, HN의 AUSF로 SN(Serving Network)의 정보와 함께 Authenticate Request를 AUSF에 전송함. 이때 전송되는 SN-name은 서비스 코드인 5G와 SN id를 바인딩한 값
3) AUSF는 인증 요청 메시지를 수신 후, 자신이 알고 있는 SN 리스트와 비교하여 정상 SN 여부를 판단한 후, 다시 UDM에게 전달
4) UDM(Unified Data Management)은 SIDF(Subscriber Identity De-concealing Function)를 통해 SUCI 값을 SUPI로 복호화하여 정상적으로 HN에 등록된 사용자인지 확인을 수행. 그 후, 5G-AKA 또는 EAP-AKA' 중 인증 방법을 선택하여, ARPF(Authentication credential Repository and Processing Function)에 저장된 최상위 키값을 사용해 K_AUSF와 5G HE AV(Home Environment Authentication Vector)를 생성함. 이때 UDM에서는 5G HE AV 값에 포함되는 속성값들을 생성하는데 'RAND'는 임의로 생성된 128비트의 값이다. 또한 AUTN(Authentication Token)은 UE에게 전달되어 활용되는 인증 파라미터로 구성되게 되는데, 이때 포함되는 'SQN'은 순차번호로써 최초 인증 단계에서만 생성되는 값이며 인증절차가 수행될 때마다 증가함. 또한 'CK'는 암호화 키, 'IK'는 무결성 키, 'AK'는 익명성 키임. f1~f5 함수는 모두 128비트 알고리즘이며 f1, f2는 메시지 인증 기능을 수행하고 f3~f5 함수는 키 생성 기능을 수행함. KDF(Key Derivation Function)는 HMAC-SHA-256을 사용함
5) UDM은 AUSF에게 5G HE AV와 SUPI 값을 전달함.
6) AUSF에서는 차후에 수행할 때 필요한 값들은 보관하며, 전달

받은 5G HE AV로부터 5G AV를 생성함

7) 그 후 AUSF는 K_SEAF를 제외한 5G SE AV(Serving Environment Authentication Vector)를 SEAF에게 전달함
8) SEAF는 추후 단계에서 필요한 값들은 보관한 후, UE에게 5G SE AV의 HXRES* 값을 제외한 메시지 Authenticate Request을 단말에게 전달함
9) 단말은 SEAF로부터 수신받은 RAND 값과 단말의 USIM에 저장된 최상위 키를 이용하여 AUTN을 생성. AUTN을 생성한 후, SEAF로부터 전달받은 AUTN 값과 동일한지 검증함. 즉 MAC 값을 검증함으로써 망을 인증하게 된다. 또한 'SQN' 값도 허용 증가치에 있는지 확인을 하며 MAC값과 XMAC값이 다르면 "Cause = Synchronization Failure"를 SQN이 비정상이면 "Cause = Synchronization Failure"를 SEAF에게 전달하여 인증에 오류가 있다는 것을 알려줌. 검증을 완료하면 단말 인증에 사용될 RES* 값과 K_AUSF, K_SEAF 값들을 생성
10) 단말의 인증을 위해 RES*를 SEAF로 전달
11) SEAF는 RES*를 통해 HRES*를 얻음. 그 후, ⑧번과정에서 AUSF로부터 받아 보관한 값인, 5G SE AV의 HXRES* 값과 비교하여 SN의 입장에서 단말을 인증
12) 인증일 됐을 경우, SEAF는 UE로부터 받은 RES* 값을 AUSF에게 전달
13) AUSF는 ⑥번 과정에서 UDM으로부터 받아 보관한 값인, 5G HE AV의 XRES* 값과 비교함으로써 RES*=XRES*이면 HN 입장에서 단말을 인증하고 사용할 키를 확정
14) AUSF는 SEAF에게 단말의 인증 결과 및 SN의 SEAF로 가입자의 신원정보인 SUPI와 K_SEAF 값을 전달
15) UDM에게는 인증 결과를 전달함으로써 Primary Authentication 과정을 마무리

▸ EAP-AKA’

• EAP-AKA‘은 5G-AKA와 동일하게 사용자 기기를 인증하고, 키를 파생하기 위한 프로토콜임. 초기에 사용자가 SUCI를 SEAF를 거쳐 AUSF까지 전달하는 것은 5G-AKA와 동일함. 이후 인증 절차는 다음 [그림 20]과 같음



[그림 20] EAP-AKA’ 1차 인증 동작 절차
자료 : 3GPP TS33.501

• **절차 설명**

1) AUSF는 UDM/ARPF에게 Auth-Info Req를 통해 가능한 인증기법과 이에 필요한 인자를 전송

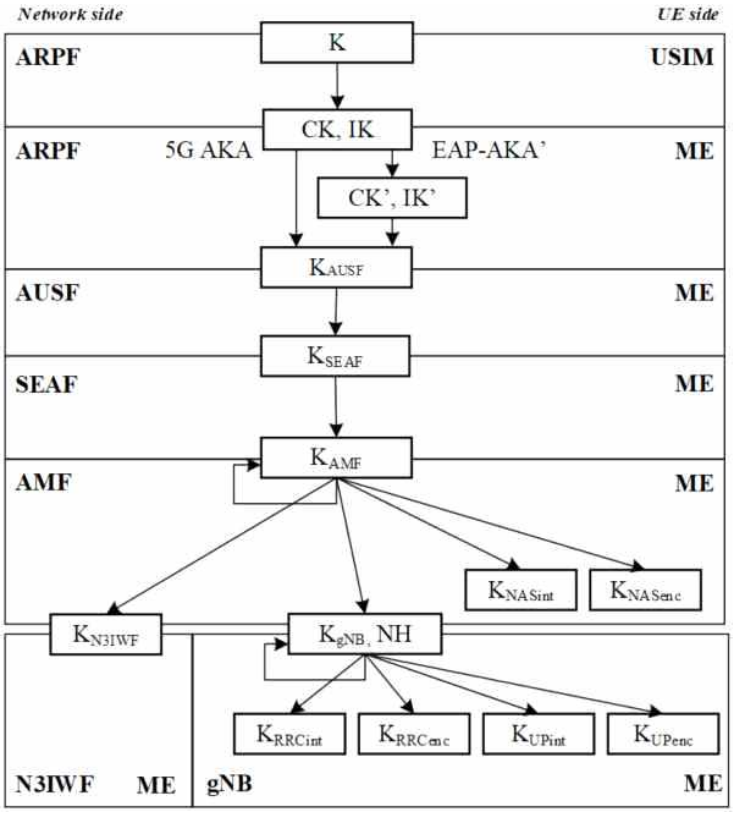
2) UDM/ARPF는 TS 33.102에서 정의된 인증 관리 필드(AMF)를

통해 분리 비트가 1인 인증 벡터를 생성하고, CK'와 IK'를 계산

3) ARPF는 Auth Info Resp 메시지를 통해 AUSF에게 변형된 인증 벡터(RAND, AUTN, XRES, CK', IK')를 전송
4) AUSF는 5G-AIA 메시지를 통해 EAP Request/AKA`-Challenge 메시지를 SEAF에게 전송
5) SEAF는 EAP Request/AKA'-Challenge 메시지를 NAS 메시지인 Auth-Req 메시지로 UE에게 전달
6) UE는 TS 33.402에 따라 AUTN을 검증하고 RES를 계산함. 또한, CK`와 IK`를 유도함.
7) UE는 EAP Response/AKA'-Challenge 메시지를 NAS 메시지 Auth-Resp 메시지를 통해 SEAF로 전달
8) SEAF는 EAP-Response/AKA'-Challenge 메시지를 AUSF에 전달
9) AUSF는 수신한 메시지를 검증함. 메시지가 옳다면 진행하고, 옳지 않다면 오류를 반환
10) AUSF와 UE는 SEAF를 통해 EAP-Request/AKA'-Notification과 EAP-Response/AKA'-Notification을 교환할 수 있음
11) AUSF는 EMSK의 처음 256비트를 KAUSF로 사용하고 KAUSF로부터 KSEAF를 파생하고, AUSF는 EAP Success 메시지를 SEAF에게 전송
12) SEAF는 UE에게 EAP Success 메시지를 전송

- **5G 키 계층 분석**

▶ [그림 21]은 5GC(5G Core)와 NG-RAN(Next Generation-Radio Access Network)가 UE와 5G-AKA또는 EAP-AKA'을 수행할 때 파생되는 키의 도식임. 화살표는 KDF를 뜻하며 해당 과정에서 사용되는 KDF 알고리즘은 HMAC-SHA-256임



[그림 21] 5G 키 계층
자료 : 3GPP TS33.501

▶ **파생 키 종류와 그 역할**

- K_ASUF는 5G초기 인증기법에 따라 파생 방법에 차이가 있음
  - 5G-AKA에서 K_AUSF는 ME와 ARPF가 CK와 IK로부터 파생해 생성하며, AUSF에 의해 수신되어 HE AV의 일부로 전달
  - EAP-AKA'에서 K_AUSF는 ME와 AUSF가 CK'와 IK'로부터 파생해 생성하며, 이때 CK'와 IK'은 AUSF에게 AV의 일부로 ARPF으로부터 수신
- K_SEAF는 K_ASUF로부터 ME와 AUSF에 의해 생성된 앵커

키임. K_SEAF는 AUSF가 서빙 네트워크의 SEAF에게 제공

- K_AMF는 K_SEAF로부터 ME와 SEAF에 의해 파생됨
- K_NASint는 K_AMF로부터 ME와 AMF에 의해 파생됨. 이는 NAS 시그널링의 무결성 알고리즘을 위해서만 사용
- K_NASenc는 K_AMF로부터 ME와 AMF에 의해 파생. 이는 NAS 시그널링의 암호화 알고리즘을 위해서만 사용
- K_gNB는 K_AMF로부터 ME와 AMF에 의해 파생됨. K_gNB는 ME와 ng-eNB 사이의 K_eNB처럼 사용
- K_UPenc는 K_gNB로부터 ME와 gNB에 의해 파생. 이는 UP 트래픽의 암호화 알고리즘을 위해서만 사용
- K_UPint는 K_gNB로부터 ME와 gNB에 의해 파생. 이는 ME와 gNB사이의 UP 트래픽에 대한 무결성 알고리즘을 위해서만 사용
- K_RRCint는 K_gNB로부터 ME와 gNB에 의해 파생. 이는 RRC 시그널링의 무결성 알고리즘만을 위해 사용
- K_RRCenc는 K_gNB로부터 ME와 gNB에 의해 파생. 이는 RRC 시그널링의 암호화 알고리즘만을 위해 사용
- NH는 ME와 AMF에 의해 파생되는 키로, forward security를 보호
- K_(NG-RAN)*는 ME와 NG-RAN에 의해 파생되는 키로, 수직 혹은 수평의 키 파생 과정을 거칠 때 KDF를 이용하여 파생
- K'_AMF는 ME와 AMF에 의해 파생되는 키로, UE가 한 AMF로부터 다른 AMF로 이동할 때 KDF를 이용하여 파생
- K_N31WF는 non 3GPP access를 위해 K_AMF로부터 ME와 AMF에 의해 파생되는 키. K_N31WF는 N31WF 사이에서 전달되지 않음

▶ AKMA

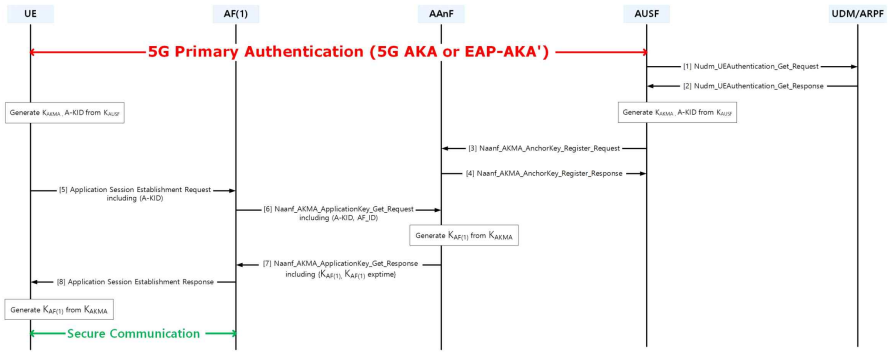


그림 22

- 절차설명
  - AUSF는 5G 1차 인증에서 Nudm_UEAuthentication_Get Request 메시지를 이용하여 UDM/ARPF에게 UE의 가입자 자격 증명과 인증 정보를 요청함
  - UE가 유효한 어플리케이션 사용자인 경우, UDM/ARPF는 K-AKMA의 생성 여부를 판단하고 필요한 정보를 포함하여 Nudm_UEAuthentication_Get Response 메시지로 AUSF에게 응답함
  - AUSF는 UDM/ARPF로 부터 수신한 라우팅 식별자를 사용하여 K_{AUSF}로부터 K_{AKMA}와 A-KID를 파생함
  - UE 또한 AF와의 통신전에 A-KID를 파생함
  - AUSF는 AAnF Selection 절차를 통해 UE에게 서비스를 제공할 AAnF를 선택하고, UE의 SUPI 및 K_{AKMA}를 Naanf_AKMA_Key-Registration Request 메시지에 포함해 전달함
  - AAnF는 UE의 SUPI 및 K_{AKMA}를 저장하며, Naanf_AKMA_Key-RegistrationResponse 메시지를 AUSF로 전송함
  - AUSF는 AAnF와의 통신 후 AKMA 키 정보를 저장할 필요가

없으며, 재인증이 필요할 경우 새 AKMA 키 정보를 생성하여 AAnF에게 전달함

- UE는 AF와의 통신을 시작하기 전에 K_{AUSF}에서 K_{AKMA}와 A-KID를 추출하고, A-KID를 Application Session Establishment Request 메시지에 포함시켜 AF에게 전송함
- AF는 A-KID에 대응되는 Context를 조회하고, 없다면 AAnF Selection을 통해 AAnF를 선택함
- 선택된 AAnF에게 K_{AF}를 요청하기 위해, UE로부터 받은 A-KID와 자신의 ID를 Naanf_AKMA_ApplicationKey_Get_Request 메시지에 포함시켜 AAnF에게 전송함
- AAnF는 AF가 서비스를 제공할 권한이 있는지 확인하고, 받은 A-KID를 통해 K_{AKMA}를 식별함
- K_{AKMA}로부터 K_{AF}를 추출하고, K_{AF}의 유효 기간을 Naanf_AKMA_ApplicationKey_Get Response 메시지에 포함시켜 AF에게 전송함
- AF는 받은 K_{AF}를 저장하고, Application Session Establishment Response 메시지를 통해 세션 설정이 완료되었음을 UE에게 통보함

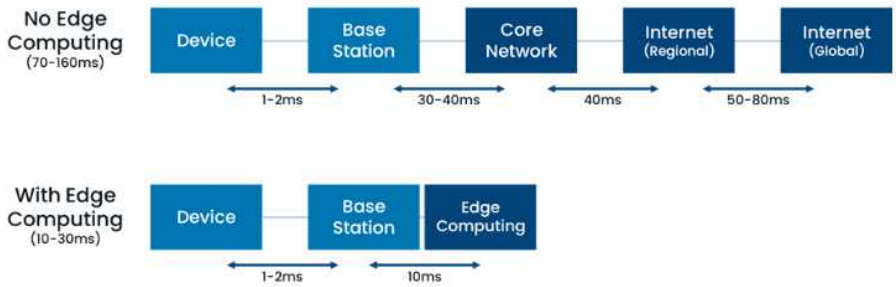
3. 이음5G 적용기술 유형 및 기술별 보안 고려사항 조사

o 이음5G 적용기술 유형

- MEC(Mobile Edge Cloud)

▶ MEC는 데이터가 생성되고, 그것을 처리하고, 최종으로 사용하는 것은 물리적인 거리를 최소화하여 초저지연을 지향하는 기술임. [그림 22]는 MEC를 적용하기 전후의 지연시간에 대한 3GPP 홈페이지의 자료임. 해당 자료를 기준으로 보았을 때 지연시간이 최소 2배 ~ 16배 까지 차이가 날 수 있음. 스마트 APC내에는 무

인 지게차, 카메라를 통해 전달받은 영상을 AI가 분석하는 비전 AI등 영상 데이터와 같은 고용량 데이터들이 순간순간 판단을 요구하는 상황에 이용될 것임. 이에 초저지연성은 현장 인력들의 안전과도 연관이 되므로, MEC를 적용하는 것이 바람직함



[그림 23] 5G MEC 지연시간 비교

- **네트워크 슬라이스**

▶ 네트워크 슬라이스 관리 및 운영에 대한 표준은 3GPP TS28.530 문서임. 해당 문서에서는 5G에서는 과거의 이동통신 네트워크처럼 사용자의 모바일 기기만 연결하는 것이 아니라 자동차 또는 대규모 IoT기기와 같이 다양한 기기들이 연결되기 시작하면서 이런 기기들에게 안정적으로 네트워크 환경을 제공하고, 모니터링까지 제공하기 위해 개발된 기술로 표현하고 있음. 네트워크 장비들의 가상화를 시작으로 물리적인 장비를 통합하고, 그 안에서 논리적으로 자원을 분류하여 다양한 환경에 효율적으로 인프라를 제공할 수 있게 됨. 그러나 물리적으로 분리되어 있지는 않으므로 자원 공유 과정에서 격리가 제대로 이루어지지 않으면 서비스 불능부터 민감한 데이터 유출까지 이루어질 수 있음. 이에 해당 기술을 안전하게 이용하기 위한 보안 가이드라인이 필요하고, 본 연구에서 진행한 보안 고려사항을 정리하여 이를 가이드라인으로 발전시킬 수 있음

- NetApp

▶ NetApp은 “ENVOLED-5G” 단체에서 개발하고 있는 네트워크 연동 어플리케이션에 대한 표준임. AKMA를 이용한 네크워크, 어플리케이션 통합관리가 성공적으로 수행되기 위해서는 어플리케이션 함수와 5G코어망 내에 함수 간의 연동이 원활하게 이루어져야 하고 NetApp은 이러한 과정을 원활하게 만들어주는 기술임

o MEC 보안 고려사항 연구

- 유럽 전기 통신 표준 협회인 ETSI에서 정의한 MEC 표준 구조를 중심으로 선정한 MEC 시스템의 핵심 구성요소는 다음과 같음

▶ 가상화 인프라

• MEC 시스템은 클라우드 및 가상화 기술을 바탕으로 제3자 애플리케이션을 실행

• MEC 호스트는 가상화 인프라에서 MEC 애플리케이션을 실행하고 서비스를 제공하는 필요한 기능들로 구성되며, MEC 애플리케이션의 가상화를 위해 가상머신이나 컨테이너 기술을 사용하여 MEC 애플리케이션 사이에 격리된 공간을 제공

▶ MEC 애플리케이션

• MEC 호스트가 제공하는 가상화 인프라 상에서 실행되며, MEC 서비스를 소비하고 제공하기 위해 MEC 플랫폼과 통신

▶ MEC 오케스트레이터(orchestrator)

• MEC 시스템 레벨 관리의 핵심 기능으로, 배포된 MEC 호스트, 사용 가능한 자원, 사용 가능한 MEC 서비스나 토폴로지 등을 기반으로 MEC 시스템의 전체 뷰를 유지

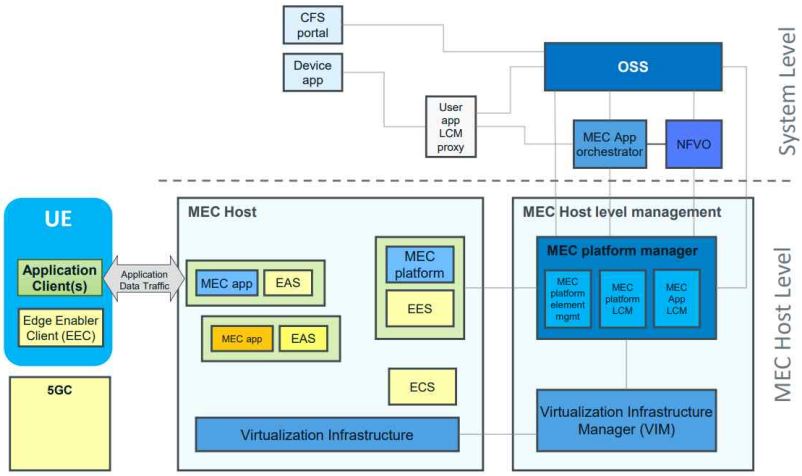


그림 24 ETSI MEC 참조 구조
자료: ETSI

- **MEC 가상화 인프라 관점에서의 보안 위협 및 보안 고려사항 조사**

▶ 가상화 기술 비교

- MEC 애플리케이션이 MEC 호스트에서 구동되기 위해 가상화 기술을 필요하며 주로 컨테이너와 가상머신(Virtual Machine, VM)이 사용됨
- VM은 운영체제가 독립되어 완전히 격리된 환경을 제공하지만 컨테이너의 경우 단일의 운영체제 커널을 공유하며 사용되는 불완전한 격리 환경으로 상대적으로 보안성이 취약

표 6 가상화 기술 특징 비교

	가상머신	컨테이너
가상화	하드웨어 레벨 가상화	OS 레벨 가상화
운영체제	독립적인 이종 다중 운영체제	단일 운영체제 커널 공유
격리	완전한 격리 제공	프로세스 레벨의 격리
효율성	낮음	높음
확장성	제한적	무제한
보안	높은 보안성	낮은 보안성

- 5G에서는 클라우드 네이티브 환경[1]을 지향하기에 MEC 애플리케이션 실행을 위해 가상머신에 비하여 상대적으로 보안이 취약한 컨테이너의 비중이 높아지고 있음
- 컨테이너와 VM 간에는 많은 기술적 차이가 있지만 운영상의 차이도 상당하며 이러한 운영상의 차이는 컨테이너 보안의 여러 측면에 영향을 미치며 두 사이의 운영상의 차이는 다음과 같음
- 컨테이너 및 마이크로서비스를 통해 애플리케이션을 구축하면 해당 애플리케이션을 VM 중심의 단일 모델에서 실행했을 때보다 훨씬 더 많은 개별 구성 요소가 있음
- 또한 컨테이너를 주요 이점 중 하나는 컨테이너가 제공하는 민첩성으로, 신속한 애플리케이션 반복을 통해 비즈니스 요구에 보다 쉽고 빠르게 대응할 수 있음
- 기존의 보안 도구와 프로세스는 훨씬 덜 동적인 환경을 가정하

1) 클라우드 네이티브(Cloud Native) : 클라우드 컴퓨팅 모델의 장점을 최대한 활용할 수 있는 애플리케이션을 개발하고 구축하며 실행하는 방법론으로서, 응용을 가능한 한 작은 단위로 나누고 (Micro-service 구조), 세분화된 응용 단위는 컨테이너로 실행하며, 시장 및 서비스 요구에 따라 즉각적으로 서비스를 실행하고 빈번하게 지속적으로 업그레이드(DevOps)하기 위한 전략

는 경우가 많기 때문에 컨테이너형 환경의 변화 속도에 맞게 구성해야 함

- 퍼블릭 클라우드 테스트 환경, 프라이빗 클라우드 프로덕션 환경 등 다양한 환경에서 컨테이너와 이미지를 이동할 수 있음. 환경이 더 정적이고 예측 가능했던 VM과 달리 운영 과정에서 여러 위치에서 컨테이너를 이동할 수 있음. 따라서 이들을 보호하는 데 사용되는 보안 도구와 프로세스는 특정 클라우드 제공자, 호스트 OS, 네트워크 토폴로지 또는 자주 변경될 수 있는 런타임 환경의 다른 측면에 대해 가정해서는 안됨
- VM 및 베어메탈(Bare-metal) 서버는 일반적으로 관리자가 정적 IP 주소를 할당하며, 이러한 주소는 시간이 지남에 따라 상대적으로 일관성이 유지됨. 반대로 컨테이너는 일반적으로 사용되는 모든 조정 도구를 통해 IP 주소를 할당받음. 지정된 컨테이너에 할당된 IP 주소는 일반적으로 미리 알려져 있지 않으며, 일반적으로 이러한 주소를 할당하는 데 관여하는 관리자가 없음. 컨테이너는 VM보다 생성 및 파괴 빈도가 훨씬 높기 때문에 시간이 지남에 따라 사람의 개입 없이 IP 주소도 자주 변경됨. 이로 인해, IP 주소를 기반으로 트래픽을 필터링하는 방화벽 규칙 집합과 같이 정적 IP 주소에 의존하는 보안 기술을 사용하여 컨테이너를 보호하는 것이 어렵거나 불가능하게 됨

▶ 호스트 운영체제 보안 위협과 고려사항

- 부적절한 사용자 접근 권한
  - 컨테이너별 OS는 일반적으로 컨테이너 배치 및 확장을 제공하는 오케스트레이터(Orchestrator)와 함께 사용함
  - OS는 일반적으로 다중 사용자 시나리오를 지원하도록 최적화되지 않음. 수동적인 구성 및 관리 방식을 사용하는 경우 자신이 호스팅하는 컨테이너형 앱에 필요 이상으로 액세스 가능하

여 위협 당할 수 있음

- 이런 위협에 대응하기 위한 보안 고려사항은 다음과 같음
- 대부분의 컨테이너 배포는 오케스트레이터에 의존하여 호스트 간에 작업을 분산시키지만, 관리자는 OS에 대한 모든 검증을 수행하고 비정상적인 상태를 모니터링해야 함
- 작업을 위해 권한이 상승된 경우와 작업 내용을 모두 기록해야 함. 이러한 과정을 통해 호스트에 직접 접근하고 권한 있는 명령을 실행하는 것과 같은 비정상적인 액세스 패턴을 식별할 수 있음
- 관리자가 작업을 수행하는 데 필요한 특정 리소스에 대해 오케스트레이터가 필요한 특정 액세스만 제공하도록 해야 함. 예를 들어 프로젝트 foo에서 작업하는 개발자는 프로젝트 foo와 관련된 리소스만 관리할 수 있어야 하며 액세스 할 수 없어야 함.. 오케스트레이터가 기본적으로 이 기능을 제공하지 않는 경우 이를 위해 타사 솔루션을 사용해야 함

• 호스트 구성요소의 취약점

- 컨테이너용 OS는 범용 OS보다 공격 표면이 훨씬 작음. 예를 들어 범용 OS가 데이터베이스 및 웹 서버 앱을 직접 실행할 수 있도록 지원하는 라이브러리 및 패키지 관리자는 포함되지 않음
- 하지만 컨테이너용 OS에서도 원격 연결을 인증하는 데 사용되는 암호화 라이브러리와 일반적인 프로세스 호출 및 관리에 사용되는 커널 프리미티브와 같은 호스트 OS가 제공하는 기본 시스템 구성 요소가 있음
- 다른 소프트웨어와 마찬가지로 이러한 구성 요소에는 취약성이 있을 수 있으며, 이러한 취약성은 운영체제의 낮은 레벨에 존재하기 때문에 호스트에서 실행되는 모든 컨테이너 및 애플리케이션에 영향을 줄 수 있음

- 이런 위협에 대응하기 위한 보안 고려사항은 다음과 같음
- 기본 OS 관리 및 기능을 위해 제공되는 구성 요소의 버전을 검증하기 위해 관리 및 도구를 사용해야 함. 컨테이너용 OS는 범용 OS보다 훨씬 더 적은 구성 요소 집합을 가지고 있지만 여전히 취약점이 있고 여전히 문제가 해결되어야 함.
- 호스트는 OS 공급업체 또는 기타 신뢰할 수 있는 조직에서 제공하는 도구를 사용하여 OS 내에서 사용되는 모든 소프트웨어 구성요소를 정기적으로 확인하고 업데이트를 적용해야 함. 이 접근 방식에서 마찬가지로 중요한 것은 앱과 호스트 OS 간에 명확하게 분리하여 앱을 구축, 테스트 및 운영하는 것임
- 컨테이너형 앱은 호스트별 구성이나 데이터 스토리지에 의존해서는 안됨. 의존 시, 종속성으로 인해 호스트 OS를 활용하기가 더 어려워지는 경우가 많음
- 운영 측면에서 여러 노드에 걸쳐 수평적 확장을 통해 복원력을 달성할 수 있도록 앱을 구축하고 운영해야 함. 이는 배포 환경의 모든 호스트에 대한 간단한 업데이트를 가능하게 하여 보안 취약성을 시기적절하게 해결하는 데 가장 일반적인 장벽 중 하나를 제거하기 때문에 호스트 OS 업데이트 적용에 중요함

▶ 컨테이너 런타임 보안 위협과 고려사항

• 안전하지 않은 컨테이너 런타임 설정(Configuration)

- 컨테이너 런타임은 복잡한 소프트웨어이며 일반적으로 구성이 가능한 많은 옵션을 관리자에게 노출시킴. 잘못 구성 시, 시스템의 상대적 보안이 저하될 수 있음
- 컨테이너가 호스트에 중요한 디렉토리를 마운트하도록 허용하는 시 안전하지 않은 상황이 발생 할 수 있음. 컨테이너는 호스트 파일 시스템을 거의 변경하지 않아야 하며 호스트 OS의 기본 기능을 제어하는 /boot 또는 /etc와 같은 위치를 변경하지

않아야 함. 컨테이너가 이러한 경로를 변경할 수 있는 경우 손상된 컨테이너를 사용하여 권한을 높이고 호스트 자체와 다른 호스트를 공격할 수 있음

- 이런 위협에 대응하기 위한 보안 고려사항으로 컨테이너 런타임 구성의 표준 준수를 자동화해야 함. Center for Internet Security Docker Benchmark와 같은 문서화된 기술 구현 지침에서는 옵션 및 권장 설정에 대한 세부 정보를 제공하지만, 이 지침의 운영은 자동화에 따라 달라짐. 따라서 다양한 도구를 사용하여, 한 시점에서 규정 준수를 '검색'하고 평가할 수 있지만, 이러한 접근방식은 확장하기 어려움. 대신 시스템 전반에 걸쳐 구성 설정을 지속적으로 평가하고 적극적으로 시행하는 도구나 프로세스를 사용해야 함
- 또한 SELinux[2] 및 AppArmor[3]와 같은 필수 접근제어 기술은 컨테이너에 대한 향상된 제어 및 격리를 제공할 수 있음. 예를 들어, 이러한 기술은 추가 세분화를 제공하고 컨테이너가 특정 파일 경로, 프로세스 및 네트워크 소켓에만 액세스할 수 있어야 한다는 보장을 제공하여 손상된 컨테이너가 호스트나 다른 컨테이너에 영향을 미치는 기능을 더욱 제한할 수 있음

• 커널 공유

- 컨테이너는 강력한 소프트웨어 수준의 리소스 분리를 제공하지만, 커널 공유를 사용하면 하이퍼바이저에서 환경보다 객체 간 공격 표면이 커짐. 즉, 컨테이너 런타임에 의해 제공되는 격리 수준은 하이퍼바이저가 제공하는 격리 수준만큼 높지 않음
- 따라서 이런 위협에 대응할 수 있는 보안 고려사항은 다음과

2) SELinux(Security Enhanced Linux): 소스코드가 공개되어 있기 때문에 보안이 취약한 리눅스 시스템 액세스 권한을 제어하기 위해 미국 국가안보국(NAS)에서 개발한 보안 아키텍처

3) AppArmor: 시스템 관리자가 프로그램 프로필 별로 프로그램의 역량을 제한할 수 있게 해주는 리눅스 커널 보안 모듈

같음

- 대부분의 컨테이너 런타임 환경은 컨테이너를 서로 분리하거나 호스트 OS로부터 분리하는 효과적인 작업을 수행하지만, 경우에 따라서는 동일한 런타임에 서로 다른 수준의 앱을 함께 실행하는 것은 불필요한 위험이 될 수 있음
- 용도와 민감도에 따라 컨테이너를 세분화하면 심층 방어가 추가로 필요함. 컨테이너를 상대적인 민감도로 그룹화하고 주어진 호스트 커널이 단일 민감도 수준의 컨테이너만 실행하도록 해야 함. 이러한 세분화는 여러 물리적 서버를 사용하여 제공될 수 있지만 최근 하이퍼바이저에서는 이러한 위험을 효과적으로 완화할 수 있을 만큼 강력한 격리 기능을 제공할 수 있음

• 컨테이너 손상

- 기존 호스트 기반 침입 탐지 프로세스 및 도구는 아키텍처 및 운영 방식이 다르기 때문에 컨테이너 내의 공격을 탐지하고 방지할 수 없는 경우가 많음
- 따라서, 컨테이너를 자동으로 인식하고 컨테이너에서 일반적으로 볼 수 있는 규모와 변화율로 작동하도록 설계된 추가 도구를 구현해야 함
- 이러한 도구는 컨테이너형 앱을 자동으로 프로파일링하고 보호 프로파일을 구축하여 관리자와의 상호작용을 최소화할 수 있어야 함
- 또한, 이러한 프로파일은 런타임에 다음과 같은 이벤트를 포함하여 이상 징후를 탐지할 수 있어야 함
  - ✓ 올바르지 않거나 예기치 않은 프로세스 실행
  - ✓ 올바르지 않거나 예기치 않은 시스템 콜 호출
  - ✓ 보호된 구성 파일 및 이진 파일의 변경
  - ✓ 예기치 않은 위치 및 파일 형식에 쓰기

✓ 예기치 않은 네트워크 리스너를 만듭니다
✓ 예기치 않은 네트워크 목적지로 전송된 트래픽
✓ 악성 프로그램 스토리지 또는 실행

▶ 컨테이너 이미지 보안 위협과 고려사항

• 이미지 취약점
  ▫ 이미지는 특정 응용 프로그램을 실행하는 데 사용되는 모든 컴포넌트를 포함하는 정적 아카이브 파일이기 때문에 이 이미지 내의 컴포넌트가 오래되어 중요한 보안 업데이트가 누락되는 경우가 많음
  ▫ 예를 들어 이미지를 완전히 최신 컴포넌트로 생성한 경우 해당 이미지는 생성된 후 며칠 또는 몇 주 동안 계속 취약점이 없을 수 있음. 그러나 추후 어느 시점에서 해당 이미지에 포함된 컴포넌트에는 취약성이 발견될 가능성이 높기 때문에 전체 이미지가 더 이상 최신 상태가 되지 않음
  ▫ 배포된 소프트웨어가 실행되는 시스템에서 '현장'으로 업데이트되는 기존의 운영 패턴과는 달리 컨테이너를 사용하여 이러한 업데이트는 이미지 자체의 업스트림에서 수행되어야 하며, 그런 다음 다시 배포됨
  ▫ 따라서 컨테이너 환경에서 일반적인 위험은 실행 중인 이미지의 버전에 필요한 모든 업데이트가 포함되어 있지 않기 때문에 취약점이 있는 이미지를 배포하는 것
  ▫ 이에 대한 보안 고려사항으로는 컨테이너용 취약점 관리 도구와 프로세스가 필요함
  ▫ 기존의 취약성 관리 도구는 컨테이너형 모델과 근본적으로 일치하지 않는 호스트 내구성, 앱 업데이트 메커니즘 및 업데이트 빈도에 대해 많은 가정이 필요
  ▫ 이러한 도구는 종종 컨테이너 내의 취약성을 탐지하지 못하기

에 파이프라인 기반 빌드 접근방식과 컨테이너 및 이미지의 불변성을 설계에 반영하여 보다 실행 가능하고 안정적인 결과를 제공하는 도구를 사용해야 함.

- 효과적인 도구 및 프로세스의 주요 측면은 다음과 같음
  - ✓ 빌드 프로세스의 시작부터 사용 중인 레지스트리에 이르기까지 이미지 및 컨테이너의 전체 라이프사이클과 통합됨
  - ✓ 이미지의 베이스 레이어뿐만 아니라 사용 중인 애플리케이션 프레임워크 및 사용자 지정 소프트웨어 등 이미지의 모든 레이어에서 취약성을 파악할 수 있음
  - ✓ 정책 기반 시행으로 구축 및 배포 프로세스의 각 단계에서 '품질 게이트'를 만들어 정책을 충족한 이미지만 사용할 수 있도록 해야 함

- 이미지 구성
  - 소프트웨어 결함 외에도 이미지에도 구성 결함이 있을 수 있음. 예를 들어 루트로 실행되도록 이미지를 구성하거나 과도한 권한으로 실행하도록 설정된 실행 파일을 포함할 수 있음. 기존 서버 또는 VM과 마찬가지로, 구성이 잘못되면 공격에 노출될 수 있으며, 구성이 잘못된 이미지에 포함된 모든 구성요소도 위험을 증가시킬 수 있음
  - 해당 위협에 대한 보안 고려사항은 다음과 같음
  - 소프트웨어 취약점 외에도 보안 위험을 높이고 정책을 위반하는 방식으로 이미지를 구성하여 대응할 수 있음. 예를 들어 이미지는 권한이 없는 사용자로 실행되도록 구성되어야 하며 원격 액세스를 허용하지 않아야 함. 이러한 보안 구성 모범 사례를 검증하고 준수하기 위해 도구와 프로세스를 채택해야 함
  - 이러한 도구 및 프로세스에는 다음이 내용이 포함되어야 함
    - ✓ 공급업체 권장 사항 및 맞춤형/제3의 공급자의 모범 사례를 모

두 포함한 이미지 구성 설정 검증

✓ 이미지 컴플라이언스 상태에 대한 중앙 집중식 보고 및 모니터링으로 조직 차원의 취약점과 위험을 파악

✓ 비준수 이미지의 실행을 방지하여 규정 준수 요구사항의 시행

- **MEC 애플리케이션 관점에서의 보안 위협 및 보안 고려사항**

▶ MEC 애플리케이션

▫ MEC 애플리케이션은 MEC 호스트의 가상화 인프라 내에서 구동되는 프로그램

▫ 이동통신사업자의 내부망에 위치하여 일반 사용자의 접근 및 사용이 제한되는 NFV 시스템과는 달리, 제3자 MEC 애플리케이션이 통신사업자 망내에서 실행될 수 있으므로 악성코드 등에 노출될 경우 치명적인 보안 위협을 가져올 수 있음

▫ 따라서, MEC의 컨테이너 가상화 플랫폼 내에서 구동되는 MEC 애플리케이션으로 인한 보안위협에 대한 보안 고려사항이 필요

▶ 런타임 소프트웨어 내의 보안 위협 및 보안 고려사항 분석

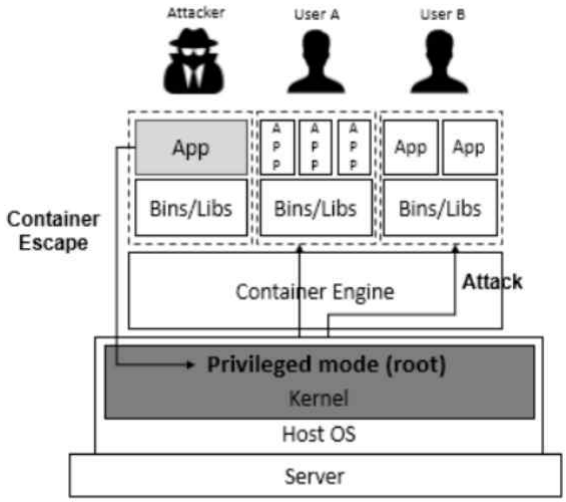
• 소프트웨어 취약점

▫ 악성 소프트웨어가 취약점을 활용하여 다른 컨테이너 및 호스트 OS 자체를 포함한 컨테이너 외부의 리소스를 공격할 수 있는 '컨테이너 탈출' 공격 [그림 **] 시나리오가 이러한 위협에 해당됨

▫ 공격자는 취약점을 이용하여 런타임 소프트웨어 자체를 손상시킨 다음 공격자가 컨테이너에 액세스하고 컨테이너 간 통신을 모니터링할 수 있도록 해당 소프트웨어를 변경할 수 있음

▫ 이 위협에 대응하기 위한 보안고려사항으로 컨테이너 런타임은 취약점에 대해 주의 깊게 모니터링해야 하며 문제가 감지되면 신속하게 대처해야 함

- 취약한 런타임은 호스트 자체뿐만 아니라 모든 컨테이너를 잠재적으로 심각한 위험에 노출시킴.
- 따라서, 도구를 사용하여 배포된 런타임에서 CVE(Common Vulnerabilities and Exposure) 취약점을 찾고, 취약한 인스턴스를 업데이트해야 함



[그림 25] 컨테이너 탈출 공격
자료: 최상훈, 박기웅, 메모리 트랩기법을 활용한 컨테이너 취약점 침입 탐지 프레임워크

- 멀웨어(Malware)
  - 도구를 사용하여 유휴 상태 및 컨테이너에서 실행되는 동안의 이미지의 멀웨어를 모니터링해야 하며, 이러한 프로세스에는 다음이 포함되어야 함
    - ✓ 레지스트리와 호스트 모두에서 이미지 내에서 악성 프로그램 식별
    - ✓ 악성코드 시그니처 탐지
    - ✓ 런타임 시 컨테이너에 침입한 악성 프로그램 탐지(예: 컨테이

너가 전복되고 공격자가 해당 컨테이너에 루트킷을 다운로드 하는 경우)

- 컨테이너 런타임 공격 시나리오
  - 컨테이너 런타임에 문제가 발생할 경우 공격자는 이 액세스 권한을 사용하여 호스트의 모든 컨테이너를 공격하고 호스트 자체를 공격할 수 있음
  - 이 위협 시나리오에 대한 관련 완화 조치에는 다음이 포함된다.
    - ✓ 필수 액세스 제어 기능의 사용은 프로세스 및 파일 시스템 활동이 정의된 영역 내에서 분할되도록 하는 추가적인 경계를 제공할 수 있음
    - ✓ 워크로드를 세분화하면 손상 범위가 호스트를 공유하는 공통 분류 수준의 애플리케이션으로 제한됨
    - ✓ 런타임의 보안 상태를 보고하고 취약한 사용자에게 이미지를 배포하지 못하도록 하는 보안 도구를 사용하면 워크로드 실행을 방지할 수 있음

▶ 어플리케이션 인증 및 통신 암호

- MEC 탑재 어플리케이션의 통신 채널을 보호하기 위해서는 엄격한 인증, 분리 또는 암호화하여야 함
- 에지 도메인이 코어 도메인, 특히 제어 신호·충전 서비스와 통신할 때는 TLS/ IPSec, 5G 프로토콜, 802.11 프로토콜을 활용하여 인증·전송 암호화를 구현해야 함

▶ 어플리케이션 간 접근통제

- MEC는 신뢰할 수 없는 응용 프로그래의 트래픽과 악의적인 행위를 분석하기 위해 어플리케이션 및 API 접근통제 정책 적용해야 함

▶ 감사 및 모니터링

- 보안위협이 MEC의 다른 기능 도메인에 영향을 미치지 않도록 MEC 탑제 3자 어플리케이션 등록, 바이러스 검사, 액세스 제어 등 어플리케이션 모니터링 및 감사로그 기록하여야 함

- **MEC 오케스트레이터 및 네트워크 관점 보안 위협 및 보안 고려사항**

▶ 컨테이너의 언바운드 네트워크 액세스

- 기본적으로 대부분의 컨테이너 런타임에서는 개별 컨테이너가 네트워크를 통해 컨테이너간 및 호스트에 액세스할 수 있음
- 컨테이너가 손상되어 악의적으로 작동하는 경우 이러한 네트워크 트래픽을 허용하면 가상화 환경의 다른 리소스가 위험에 노출될 수 있음
- 이 위협에 대응하기 위한 보안 고려사항으로 컨테이너는 송신 네트워크 트래픽을 제어해야 함
- 최소한 이러한 통제는 네트워크 경계에 배치되어야 하며, 컨테이너가 기존의 아키텍처에 사용되는 패턴과 유사하게 보안 데이터를 호스팅하는 환경에서 인터넷까지와 같이 서로 다른 감도 수준의 네트워크를 통해 트래픽을 전송할 수 없도록 해야 함
- 또한 기존 네트워크 수준 장치와 더 많은 애플리케이션 인식 네트워크 필터링을 함께 사용 시, 효과적인 대응이 가능함

▶ 언바운드 관리자 액세스

- 대게 많은 오케스트레이션 도구는 사용자와 상호 작용하는 모든 사용자가 관리자이며 이러한 관리자는 환경 전반에 걸친 통제권을 가져야 한다고 가정함
- 그러나 많은 경우 오케스트레이터 한 명이 각기 다른 팀에 의해 관리되고 민감도 수준이 다른 여러 가지 앱을 실행할 수 있

음

- 따라서 사용자 및 그룹에 제공된 액세스 범위가 특정 요구 사항에 맞지 않으면 악의적이거나 부주의한 사용자가 오케스트레이터가 관리하는 다른 컨테이너의 작업에 영향을 미치거나 전복될 수 있음
- 이 위협 대응하기 위한 보안 고려사항으로 오케스트레이터는 광범위한 제어 범위 때문에 사용자에게 특정 호스트, 컨테이너 및 이미지에서 특정 작업을 수행할 수 있는 권한만 부여되는 최소 권한 액세스 모델을 사용해야 함

- **MEC 데이터 보호 보안 고려사항**

▶ 데이터 자산 식별

- MEC 구축 및 서비스 운영 중에는 사용자 식별 및 액세스 위치를 포함하되 이에 국한되지 않는 관련 사용자 데이터 자산을 파악 등 데이터 자산 식별이 필요

▶ 데이터 위변조 및 유출 방지

- MEC 플랫폼에 저장되는 기업용 데이터는 IPSec, TLS 등 전송되어 데이터 유출과 변조 방지 기술적 조치가 필요함

▶ 개인정보 및 민감 데이터 비식별 조치

- 개인정보 데이터 프라이버시가 관련되면 개인 데이터를 마스킹 등 비식별 조치를 하여야 함

▶ 저장 데이터 보호

- 서비스 유형과 데이터 등급에 따라 보안 요건이 높은 데이터(개인정보, 민감정보)는 국제표준 암호 알고리즘을 통해 데이터를 보호해야 함

- **MEC 플랫폼 보안 고려사항**

▶ 가상화된 보안 솔루션 구축

• MEC 플랫폼 보안은 클라우드 인프라와 NFV 기술을 기반으로 가상 머신 보안, 컨테이너 보안 등 가상화된 보안 솔루션을 활용하여 구축하여야 함

▶ MEC 소프트웨어 보안

• MEC 소프트웨어 보안을 위해 VNF 소프트웨어 패키지에 대한 서명(발행자)과 검증(수신자) 지원, 벤더가 출시한 소프트웨어 패키지에 대해서는 서명 검증이 필요

▶ MEC 서비스 장애관리

• MEC 리소스 풀을 설정하여 상호 원격 재해 복구를 제공하여 사고가 발생하면 MEC 서비스를 다른 MEC로 신속하게 전환하여 서비스 연속성을 보장이 필요

▶ 보안 인증 획득 플랫폼 활용

• 민간 클라우드 플랫폼 및 서비스를 이용하여 MEC 구축 시 보안 인증 획득한 서비스 도입해야 함

- **MEC 연동 구간 보안 고려사항**

▶ MEC 연결 API 보안

• MEC는 인터넷 인터페이스, 엔터프라이즈 네트워크 인터페이스, 무선 장치 인터페이스, 기능 노출 인터페이스, 타사 애플리케이션 인터페이스를 포함하므로 각각 보안 솔루션 도입하여 운영하여야 함

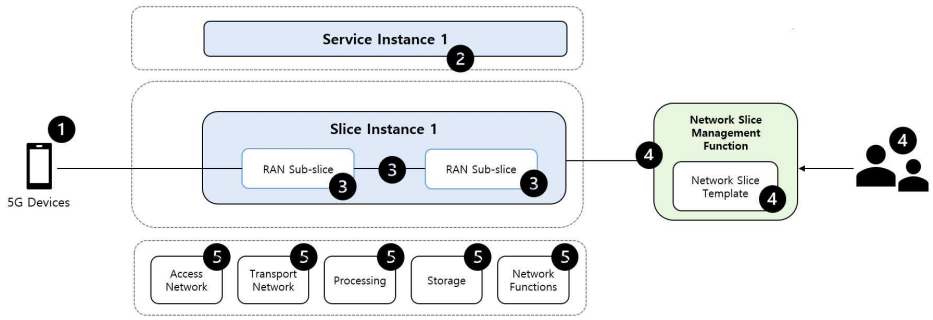
▶ MEC 연동 구간 보안관제

• 네트워크 침입탐지, 비정상적인 트래픽 분석, 악성코드 탐지 등 네트워크 에지에서 MEC 분포를 감안하여, 복수의 감시 지점을 배치하고, 통합 보안 모니터링을 수행해야 함

o **네트워크 슬라이싱 보안 위협 및 고려사항 조사**

- 네트워크 슬라이싱은 슬라이스가 논리적으로 격리되어 서로 다른 특성을 갖는 서비스에 특화된 전용 네트워크를 제공하는 것을 말함
- 그러나, 이러한 슬라이스 간 격리가 제대로 수행되지 않으면 여러 가지 보안 위협을 발생시킬 수 있음
- 따라서 네트워크 슬라이싱을 네트워크 슬라이스 내의 보안 위협과 네트워크 슬라이스 간 보안 위협으로 분류하여 발생 가능한 위협 지점을 식별 후 그에 대한 대응기술 및 보안 고려사항에 대해 조사함

- **네트워크 슬라이스 내 위협 지점 및 대응 기술**



[그림 26] 슬라이스 내 위협 지점

자료: Olimid, Ruxandra F., and Gianfranco Nencioni. (2020). “5G network slicing: A security overview.” J IEEE Access 8, (2020), pp.99999-100009

▶ 5G 고객 단말

• 사용자가 사용하는 고객 장치는 액세스 가능한 공격 지점. 즉각적인 위협에는 슬라이스 또는 서비스에 대한 무단 액세스가 포

함 됨

- 프라이버시 및 기밀성 문제 외에도 무단 액세스는 리소스 소비에 영향을 미치므로 DoS 공격 가능성이 존재
- 또한 슬라이스에 부착한다는 단순한 사실 자체가 고객 개인 정보 보호 문제를 야기할 수 있음. 예를 들어 슬라이스 식별은 동일한 슬라이스를 사용하고 따라서 대부분 동일한 서비스를 사용하는 가입자로 구성된 관심 그룹을 구분함으로써 고객 장치의 영구 식별자와의 상관 관계에서 취약성이 될 수 있음
- 5G 고객 장치와 관련된 위험은 비 3GPP 네트워크를 통해 네트워크 슬라이스에 액세스할 때 증가
- 대응 기술로는 5G 고객 장치에 대한 강력한 인증 및 액세스 제어가 있음
- 장치가 네트워크에 액세스할 수 있도록 하는 기본 인증 외에 슬라이스 수준의 보조 인증 (또는 슬라이스 특정 인증)이 권장됨
- 기본 인증은 로밍 및 다른 기술 상호 연결을 허용하도록 표준화되어야 함. 비용을 줄이고 통합을 용이하게 하기 위해 2차 인증도 표준화되어야 함
- 2차 인증은 슬라이스를 관리하는 엔터티의 책임임. 슬라이스 테넌트의 경우 테넌트는 자신이 관리하는 슬라이스에 대한 액세스 제어에 직접 관여하므로 리소스 할당이 보다 효율적
- 네트워크 슬라이스에 동시에 액세스할 수 있는 고객 장치 수, 동시 활성 세션 수 및 네트워크의 여러 수준에서 수행되는 장치당 데이터 속도의 제한은 DoS와 관련된 위험을 완화할 수 있음

▶ 슬라이스 서비스 인터페이스

- 가능한 공격 지점은 슬라이스와 슬라이스를 사용하는 서비스 간의 인터페이스
- 공격자가 서비스를 공격하여 슬라이스를 손상시킬 수 있음. 이로 인해 동일한 슬라이스에서 실행 중인 다른 서비스가 손상될 수 있음
- 또한 서비스 간 직접 통신의 경우 이 역시 공격 포인트가 될 수 있음
- 대응기술에는 적절한 보안 수준의 구현과 올바른 서비스 구성(예: 권한 및 리소스 제한)이 포함됨
- 서비스 간에 그리고 슬라이스와 소비 서비스 간에 올바른 수준의 격리를 구현해야 함

▶ 하위 슬라이스

- 슬라이스가 여러 하위 슬라이스의 체인으로 정의되면 하위 슬라이스 자체와 하위 슬라이스 간의 상호 연결이 모두 공격 지점을 나타냄. 하위 슬라이스 체인의 전체 보안 수준은 가장 약한 하위 슬라이스에 의해 정해짐
- 대응기술에는 특히 액세스 네트워크가 3GPP가 아닌 경우 상호 연결 시 위험을 줄이기 위한 하위 슬라이스 보안 및 구현 메커니즘이 포함됨
- 서로 다른 기술의 상호 연결에서 보안 문제를 조사하는 것은 여전히 향후 작업의 대상이며 RAN 하위 슬라이스와 관련하여 더 많은 연구가 필요

▶ 슬라이스 관리자

- 슬라이스 관리자는 네트워크 슬라이스 템플릿, API, 액세스 권한, 상호 인증, 신뢰 등과 관련하여 보안 위협을 가져옴. 테넌트

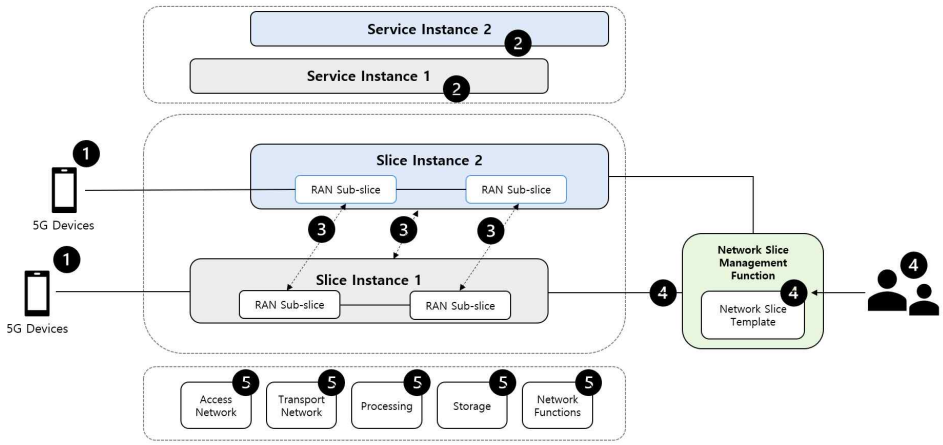
가 슬라이스 관리를 담당할 때 위험이 증가

- 대응기술에는 호스트 플랫폼과 네트워크 관리자 사이에 상호 인증이 설정되어야 함
- 더 많은 슬라이스 관리자가 존재하는 경우 서로를 상호 인증해야 함
- 테넌트가 슬라이스 관리를 담당하는 경우 당사자 간의 약속에 따라 해당 기능이 제한되어야 함
- 보다 정확하게는 테넌트는 합의된 것 이외의 모든 요청, 데이터, 리소스 및 기능에 대한 액세스를 방지해야 함. 3GPP는 또한 다중 테넌트 환경에서 네트워크 슬라이스 성능 및 장애 모니터링을 권장하고 있음

▶ 리소스 및 네트워크 기능

- 자원 및 네트워크 기능은 이를 소비하는 슬라이스를 손상시키기 위해 공격을 받을 수 있음
- 물리적 공격, 소프트웨어 공격 및 보다 일반적인 사이버 공격을 포함하여 매우 다양한 공격이 발생할 수 있음
- 대응기술에는 상호 인증, 보안 부팅, 자격 증명 액세스, 물리적 보안 및 무결성 확인이 포함됨
- 이러한 기술은 신뢰 수준을 높이지만 네트워크 슬라이싱에만 국한되지 않음
- 서로 다른 수준의 보안 또는 민감도를 위해 공동 호스팅을 피해야 함. 특히 민감한 서비스를 제공하는 슬라이스와 실험적 또는 테스트 코드를 사용하는 슬라이스 간의 공동 호스팅은 피해야 함

- 네트워크 슬라이스 간 위협 지점 및 대응 기술



[그림 27] 네트워크 슬라이스 간 위협 지점

자료: Olimid, Ruxandra F., and Gianfranco Nencioni. (2020). “5G network slicing: A security overview.” J IEEE Access 8, (2020), pp.99999-100009.

▶ 5G 고객 디바이스

- 5G 고객 디바이스는 가장 취약한 공격 지점
- 한 슬라이스에 대한 액세스 권한이 부여된 고객 장치가 다른 권한 없는 슬라이스에 대한 액세스 권한을 얻으려고 할 때 보안 위협이 나타남
- 또 다른 위협은 적대적인 장치가 액세스 권한이 있는 슬라이스의 공유 리소스를 과도하게 소비하여 슬라이스의 성능을 손상시키거나 DoS 공격에 성공할 수도 있다는 것
- 성능 공격은 리소스 부족으로 인해 슬라이스가 필요한 수준에서 보안 프로토콜을 수행하는 것을 방지하여 다른 유형의 공격을 용이하게 할 수 있음
- 일반적으로 장치는 단일 슬라이스에 연결할 수 있는 권한이 있어야 함. 하지만 장치에 서비스에 대한 다양한 액세스가 필요한

경우 여러 슬라이스에 동시에 연결하는 것이 허용될 수 있고, 장치가 더 안전한 슬라이스에서 덜 안전한 슬라이스로 민감한 데이터를 유출할 위험이 있는 것처럼 보이기에 위험함

- 대응 기술에는 액세스 제어, 기밀성, 무결성, 신뢰성 및 리소스 소비 측면에서 슬라이스 간의 적절한 격리가 포함됨
- 여기서 특별한 경우는 고객 장치가 두 개(또는 그 이상)의 네트워크 슬라이스에 동시에 액세스하도록 제한되는 경우 네트워크 슬라이스에 대한 상호 배타적 액세스
- 그렇지 않은 경우 각 슬라이스와 고객 장치 간에 별도의 상호 인증을 권장. 리소스는 보안 메커니즘 실행을 위한 가용성을 보장하고 DoS를 방지하도록 구성되어야 함

▶ 서비스-서비스 통신

- 가능한 공격 지점은 서로 다른 슬라이스를 사용하는 서비스 간의 인터페이스임
- 공격자가 일부 서비스를 공격하여 다른 슬라이스 위에서 실행되는 다른 서비스를 손상시킬 수 있음
- 일반적으로 서로 다른 슬라이스에서 실행되는 서비스가 독립적이고 통신이 필요하지 않기 때문에 이를 보안 위험이 낮은 것으로 간주
- 대응기술에는 적절한 격리 구현이 포함됨
- 트래픽 및 행위 분석, 이상 탐지는 슬라이드와 다른 구성요소 사이 또는 내부에서 허용되지 않는 통신을 조사하는 일반적인 기술
- 인공 지능을 사용하는 트래픽 캡처 및 방어 메커니즘에 기반한 특정 기술을 사용하여 기본 필터를 우회하는 지능형 공격으로부터 보호할 수 있음

- 트래픽 격리는 슬라이스 침입을 방지하는 흐름 규칙을 정의하여 네트워크 요소에 의해 시행될 수도 있음

▶ Intra-Slices 및 Intra-Sub-Slices 통신

- 공격자는 덜 안전한 슬라이스(특히 RAN 하위 슬라이스)를 공격하여 더 안전한 슬라이스를 공격하려고 할 수 있음
- 슬라이스 간의 통신이 허용되는 경우 가능한 위협에는 무단 액세스, 공유 매개변수 누출, 슬라이스 간에 전송되는 민감한 데이터가 포함됨
- 대응기술에는 슬라이스 간의 적절한 격리가 포함됨
- 한 슬라이스가 손상되면 다른 슬라이스에 영향을 미치지 않아야 함. 유출을 방지하려면 암호화 매개변수(예: 암호화 키)를 슬라이스 간에 공유해서는 안됨
- 기본 인증의 키가 슬라이스 내에서 사용되는 경우 키 생성 기능을 사용하여 각 슬라이스에 대해 새롭고 독립적인 키를 생성해야 함
- 슬라이스 간 격리 활성화 기술의 예에는 태그(예: MPLS 사용), VPN-(예: SSL/TLS 사용) 또는 VLAN 기반 격리가 포함됨.

▶ 관리 시스템

- 관리 시스템은 공격 지점으로 테넌트는 다른 테넌트의 슬라이스에 액세스하거나 다른 테넌트에 속하는 슬라이스 간에 공유되는 매개변수를 변경하려고 시도할 수 있음
- 대응기술에는 슬라이스 관리자의 개별 슬라이스 간의 적절한 격리와 다른 테넌트에 속하는 슬라이스 간에 공유되는 매개변수에 대한 변경 제한이 포함됨.. 강력한 인증 및 액세스 제어 절차가 수행되어야 함

▶ 자원 인프라

- 리소스 계층은 DoS뿐만 아니라 소프트웨어 공격과 같은 다른 측면에서도 공격 지점
- 예를 들어 공격자는 한 조각의 코드에 액세스하고 변조하여 동일한 코드를 사용하는 모든 코드 조각의 실행을 변경시킬 수 있음
- 대응기술에는 코드 보호 기술 및 코드 격리가 포함되며, 이는 네트워크 슬라이싱에만 국한되지 않음

- 네트워크 슬라이스 보안 고려사항

▶ 네트워크 슬라이스 내 보안 고려사항

- 슬라이스는 종단 간 논리 네트워크이므로 종단 간 보안을 고려해야 함
- 모든 통신(예: 슬라이스와 리소스 계층, 슬라이스와 슬라이스 관리자, 슬라이스의 하위 슬라이스, 네트워크의 고객 장치 및 액세스 포인트)은 대상 보안 수준을 보장하기 위해 적절한 메커니즘을 사용해야 함. 최소한의 요구 사항에는 데이터의 기밀성, 무결성, 신뢰성 및 피어 간의 상호 인증이 포함되어야 함
- 5G 고객 장치는 1차 인증과 선호하는 2차 인증을 통해 강력하게 인증되어야 함
- 슬라이스에서 사용하는 모든 리소스와 네트워크 기능은 보호되어야 함
- 민감한 식별자는 보호되어야 하며 식별자 간의 상관관계가 유출되어서는 안 됨
- 합법적인 차단은 슬라이스 및 서비스 계층 모두에서 액세스할 수 있어야 함

- 테넌트 액세스, 권한 및 구성 기능은 당사자 간의 계약을 준수해야 함
- 모든 3GPP 일반 보안 요구 사항도 슬라이스 수준에서 충족되어야 함

▶ 네트워크 슬라이스 간 보안 고려사항

- 모든 슬라이스에 대해 최소한의 권한을 부여해야 함
- 슬라이스 간의 격리는 덜 안전한 슬라이스를 통한 공격을 방지할 수 있을 만큼 충분히 되어야 함
- 슬라이스 간의 통신은 최소한으로 줄여야 하고 엄격한 규칙에 따라 정의되며 보안 채널을 통해 구현되어야 함
- 암호화 키(및 기타 민감한 매개변수)는 슬라이스 간에 공유되어서는 안됨
- 리소스 할당은 각 슬라이스에 대해 최소 수준의 가용성을 보장해야 합니다. 특히 보안 메커니즘은 리소스 소비에 관계없이 실행할 수 있어야 함
- 보안 수준에 상당한 차이가 있는 슬라이스는 리소스 또는 네트워크 기능을 공유해서는 안됨. 특히 런타임 단계의 슬라이스와 함께 테스트 모드의 슬라이스를 실행하면 안됨
- 고유한 인증, 권한 부여 및 액세스 제어 메커니즘은 각 슬라이스에 대해 독립적이어야 함
- 5G 고객 장치가 여러 슬라이스에 동시에 연결되도록 허용되는 경우 고객 장치에서도 (데이터의) 격리가 가능해야 함
- 테넌트는 다른 테넌트의 슬라이스 및 서비스에 영향을 미치는 구성 변경을 수행하지 못하도록 해야 함

o **NetApp 보안 고려사항 조사**

- NetApp(Network Application)

- NetApp(Network Application)은 표준화되고 신뢰할 수 있는 환경에서 API를 사용하여 모바일 네트워크의 제어 평면과 상호 작용하는 소프트웨어
- NetApp을 통해 개발, 테스트 및 인증 사이의 주기 단축을 지원할 수 있으며, 5G 환경에서 NetAPP 배포를 위한 핵심 기술로 NFV, SDN(Software-Defined Network), 클라우드 컴퓨팅 및 MEC (Multi-Access Edge Computing)가 있음
- NetApp은 버티컬 산업을 위한 서비스를 구성해야 하며, 버티컬 애플리케이션의 통합 부분으로 API를 제공하여 버티컬 애플리케이션 서비스를 제공해야 함
- 서비스가 버티컬에 제공되는 방식을 고려할 때, NetApp은 다음과 같이 분류할 수 있음
  - 독립형 NetApp: 독립형 NetApp은 직접 또는 수직 애플리케이션에 대한 통합으로 하나 이상의 버티컬 산업에 서비스를 제공함
  - 비독립형 NetApp: 비즈니스 API 기반 서비스를 제공하기 위해 Northbound API의 래퍼로 작동하는 NetApp이며, 비즈니스 API가 앱에서 활용될 때 기능하는 비독립형 소프트웨어
- NetApp은 스마트팩토리와 같은 제조업에 활용될 수 있으며, NetApp 개발의 주요 그룹인 “ENVOLED-5G”은 스마트 제조 부분에 NetApp을 적용하는 것을 목표로 개발 진행 중임
- “ENVOLED-5G”가 제안한 목표는 산업 서비스 제공업체에서 근무하는 작업자의 지식이 부족한 경우 발생할 수 있는 문제를 해결할 수 있음
- 또한 산업 부문에 NetApp을 제공할 수 있는 가능성에 대응하기 위해 EVOLVED-5G에서는 다음과 같은 산업 서비스의 4개 그룹을 대상으로 함

- Interaction of Employees and Machines (IEM)
- Efficiency in FoF Operations (FoF)
- Security Guarantees and Risk Analysis (SEC)
- Production Line Infrastructure (PLI)

- **NetApp 보안 고려사항**

▶ 새로운 최첨단 네트워크 애플리케이션에 대응하기 위해, 5G 버티컬의 서비스 요구사항과의 상호 운용성을 보장하는 테스트베드인 Advanced 5G Testbed를 통해 구현 및 검증을 해야 함

▶ 통신 사업자는 시설에 DevOps 원칙을 적용하고 기존 테스트베드 및 인프라를 구축하고 미래를 위한 네트워크 지원을 제공하기 위해 인공 지능 알고리즘의 지원, 종단 간 네트워크 자동화 기능을 도입해야 함

▶ 5G 네트워크에 대한 테스트. 통신 사업자의 활동은 5G가 컴퓨팅 및 스토리지 리소스의 동적 할당, 5G NFV 기반 참조 아키텍처를 기반으로 하는 새롭고 혁신적인 NetApp, 앱의 개발 및 테스트를 지원할 수 있어야 함

▶ 5G 서비스는 NetApp의 종단 간 요구사항을 충족하기 위해 물리적 및 가상화된 네트워크 요소 전반에 걸쳐 엔터티 간의 종단 간 제어 및 데이터 평면 연결에 필요한 전송 수준을 고려하여 필요한 곳이면 어디든지 제공되어야 함

- KCMVP, VPN 기술 적용 등으로 발생하는 지연 극복 기술

▶ VPN은 농협중앙회와 APC 현장의 데이터를 공유하기 위해 농협주관의 APC에서는 VPN을 사용하고 있음. 스마트 APC의 적용으로 이음5G망이 구축된 후에도 서로 다른 LAN이므로, VPN을 통해 인증하고, 암호화하여 데이터를 전송해야함

- 또한, 이음5G 구출 모델 중 Core CP공유형을 사용하는 경우에는 APC와 이음5G 사업자의 클라우드 또는 서버와 통신할 때 공용망을 사용하거나, 전용선을 매설해야 하는데, 전용선 매설 비용을 고려할 때 VPN을 사용하는 것이 합리적임
- VPN은 인증, 키 교환, 그리고 암호화 통신이 이루어짐. 이 과정에서 사용되는 알고리즘은 KCMVP 인증을 받은 암호 알고리즘을 사용해야 함. KCMVP 알고리즘은 국가에서 검증된 암호 알고리즘 프로그램으로, 해당 알고리즘을 적용한다고 해서 속도가 특별히 느려지거나 하지는 않음. 다만 암복호화 과정을 수행함에 발행하는 필연적인 지연시간이 존재하고, 이는 다음 세 가지를 통해 극복할 수 있음
  - 장비 이중화
    - 암복호화로 인한 지연시간이 문제 되는 이유는 해당 기기가 당장 처리해야 하는 일은 암복호화 때문에 처리하지 못해 발생함. 이러한 문제를 해결하기 위한 가장 쉬운 방법은 장비 이중화임
    - 장비를 이중화는 APC 내부 데이터 처리를 위한 장비, VPN을 수행하여 외부와 연결하는 장비로 이중화를 할 수 있음
    - APC 내부 서버 장비 간 데이터 유전 공유 시스템의 경우 데이터 암복호화 또는 네트워크 보안 요소가 필요하지 않으므로 실시간 공유가 가능하고, 외부 연결 장비가 VPN을 수행하여 외부 서버와 데이터 공유 작업을 수행함
    - 이중화의 이점으로 한 기가가 특정 이유에서 불능이 되는 경우 백업을 통해 멈추지 않고 작업 수행을 할 수 있다는 이점이 추가로 존재함
  - 암호 가속 지원 하드웨어
    - 인텔 프로세서의 경우 스카이레이크 아키텍처 이상부터 x86 어셈블리에서 AES-NI 명령어를 통해 AES 암복호화의 가속을 지원함. 스카이레이크 이하의 아키텍처에서는 특정 CPU만이 가속화를 지원하므로 장비 선정 시 확인이 필요함

- ARM 프로세서의 경우 Armv8-A부터 FEAT-AES 명령어를 통한 가속을 지원함.

• 데이터에 따른 정책 차등

- 현장 방문 회의 결과 데이터 중 기밀성 보장이 요구되지 않는 데이터의 종류도 있음을 확인함. 이에 보안 정책상 특정 데이터에 대한 암복호화만을 진행하여 컴퓨팅 자원을 효율적으로 사용 가능함

- E-SIM

▶ APC 내에 이음5G망을 사용하기 위해 고려되어야 할 기술 중 하나는 E-SIM임

▶ 일반 사용자 기기의 경우 사람이 소지하기 때문에 기기에 대한 관리가 철저하고, 물리적인 공격에 대한 여지가 적지만 IoT 기기는 그러하지 않고, 특히 산지에 있는 APC 특정상 현장의 물리적인 보안 강도가 높지 않음

▶ 기존 5G망은 사용자 편의성을 위해 탈부착이 가능한 USIM을 사용함. 기기를 변경할 때 단순히 USIM칩을 교환하여 사용자 정보를 옮기는 것이 가능해 편리하지만, 단순 USIM칩을 탈취하는 것으로 사용자 기기를 사칭하는 것이 가능하다는 의미임

▶ APC에서는 IoT 기기에서 생산되는 데이터의 무결성이 매우 중요함. 단순 수집 데이터에 대한 혼선으로 기업의 의사 결정을 어렵게 하는 것뿐 아니라, CCTV와 같은 방범 기기, 자동화 시스템이 의사 결정을 내리는 데이터인 메라 데이터 등을 허위로 보내 현장에서 사고를 일어나게 하거나 APC에 손해를 일으킬 수 있음

▶ E-SIM은 ETSI에서 만든 eUICC칩 표준에 따라 만들어진 칩에 GSMA에서 제정한 SIM 프로비저닝 과정을 통해 SIM 정보를 다운로드하는 기술을 뜻함

- 이 과정에서 프로비저닝을 수행하는 인프라에 대한 설비가 필요하지만, 물리적인 보안이 취약한 APC 내에서 기기의 메인보드에 SIM 정보가 부착되어 기기 사칭을 위한 정보 탈취가 어려운 E-SIM 기술의 도입을 고려할만함
- 또한, SIM 정보에는 5G망에서 영구적으로 사용되는 K값이 존재하는데, 기존의 USIM에선 해당 정보를 USIM을 교체하는 방법 외에는 갱신할 수가 없음. 그러나 E-SIM은 SIM정보를 주기적으로 원격에서 간편하게 갱신할 수 있으므로, K값이 유출되는 경우에 대한 보안성이 한층 더 강화됨

제 2 절 농산물 산지유통센터(APC) 내 이음5G망 구축을 위한 보안 모델 조사

1. 농산물 산지유통센터(APC) 사례 분석

o 천안배원예농협

- 스마트 APC 사업에 참여 중인 천안배원예농협 청과물종합유통 센터를 1차 방문지로 선정하여 현장 답사 및 현업 관계자 미팅 진행

- 현장 사례 분석 내용

▶ **스마트 APC 과실 입고, 선별, 저장, 출고 과정**

- 과실은 입고 시 컨테이너라고 불리는 플라스틱 박스에 담겨 입고됨. 이는 다시 팔레트 위에 적재하여 저장고에 저장함. 출고 요청이 들어오는 경우 저장된 배를 꺼내 선별, 포장 후 출고
- 출하 요청이 들어올 때까지 배는 저장고에 저장되어 있음. 이 과정에서 상폐 발생 가능성 있고, 이렇게 발생한 과실 로스에 대한 책임 소재가 민감
- 선별 과정에서 엣지 디바이스로부터 과실에 대한 데이터가 생성되고, 선별기까지 해당 데이터 전송됨. 그러나 선별기가 각자 다른 업체의 시스템으로 데이터통합이 결국 별도의 인력에 의해 진행되어야 함. 그리고 최종 출고되는 데이터와 일부 차이가 발생할 수 있어서 본 APC의 경우 출고 시 데이터를 수기로 작성하여 이를 데이터화 하고, 농협과 VPN을 통해서 공유

▶ **선과장 현장 답사 [선과장]**

- 출고 요청이 있는 경우 저장소에 팔레트 단위로 과실을 선과장으로 이동
- 디파레타이저에서 팔레트와 컨테이너를 분리 후 과실을 컨베이

어 위에 올림

- 컨베이어 위에 올려진 배는 우선 탈봉이 진행됨. 이후 육안상에 상폐, 미숙등의 과실을 선별
- 이후 세척을 거쳐 약품 또는 외관상 벌레를 제거. 이후 선별 및 포장 진행
- 선별기에서는 과실의 크기, 내부적인 상폐, 당도 등을 측정하여 과실을 분리
- 분리되어 전달된 과실은 포장
- 위 과정에서 현재 수집되는 데이터는 선별기를 통해서 수집되는 데이터가 전부. 다양한 IoT장비를 통해 더 많은 데이터가 생산되는 경우 과실 및 생산장비(컨테이너 및 팔레트)추적 및 과실 관리 등에 도움이 될 것
- 선별기에서 발생하는 데이터는 두 가지 문제점이 있음. 첫째는 선별기의 제조사가 모두 달라 데이터통합이 사람에 의해 진행되어야 함. 두 번째는 농협과 이런 데이터 공유가 자동화 되어 있지 않고 분리되어 있음. VPN으로 농협 내부망으로 접속하여 데이터 전달해야 함

▶ **선과장 현장 답사 [저장소]**

- 현재는 관리 감독을 사람이 실제 현장에 와서 진행. 아침 7시, 주말에도 담당자를 배정하여 주기적으로 관리
- 과실의 로스를 줄이기 위해 선입 선출을 원칙으로 하고 있는데, 현재는 과실 추적을 특정 저장소에 저장되어 있다는 것까지만 추적 가능. 저장소 하나도 규모가 크므로 특정 저장소의 어느 위치에 있다는 것까지 추적 가능할 경우 과실 관리에 도움이 될 것

▶ **스마트 APC연관 주요 질의 사항**

- Q. 현재 설치되어 있는 센서 종류 및 대수, 설치 위치 및 분포 상태

  A. 스마트APC사업의 이용이 RFID를 비롯한 장비를 활용하여 데이터를 빅데이터화 하는데 목적이 있는것으로 알고있는데, 현재 저희 농협의 경우 2017년에 신축한 1개의 선과장을 제외한 나머지 선과장들은 대부분 10년 이상의 오래된 전통적인 선과시설을 보유하고 있음. 2017년 신축한 선과장의 경우에도 RFID를 이용하여 입고를 등록하고, 선별데이터를 엑셀화하여, 정산데이터까지 나오는 장비로 계획, 운용할 예정이었으나, 작업여건상 어려움으로 현재는 단순작업화 하여 선별된 데이터를 다시 이용하는데에도 한계가 있는것이 현실. 스마트APC 개념도를 봤을 때 생산정보를 농가에서 입력하여 데이터화 한다는 것은 사실 현실적으로 불가능하고, 수출 업무시 활용하는 "농집"조차도 실제로는 농가에서 입력이 안되고 있는것이 현실. 생산 이후에 APC에 과일 원물이 왔을 때 입고를 RFID로 관리 할 수 있는 장비, 또 입고 데이터가 선과 장비를 통하여 정산데이터로 결과가 나오고, 이 모든 데이터가 빅데이터화 하여 농협 자체 전산망과 연동되는 장비가 필요할 것으로 생각.

- Q. 센서 데이터의 저장 및 활용 위치

  A. RFID로 입고된 과일 데이터와 선별데이터는 농협전산망을 통하여 연동된다면, 수확량이나 개별 농협의 저장된 과일 원물의 수를 파악하는데 도움이 될 것이고, 이는 농산물 가격 안정화 측면에서 도움이 될 것으로 보임

- Q. 내부 네트워크 구성도

  A. 내부 네트워크가 어떤 내용인지는 모르겠으나, RFID 를 생성할수 있는 키오스크가 입구에 있고 선별된 데이터를 농협망까지 공유할수있는 내부 네트웍이 구성되어야 하고, 개별 저장

고마다 입고 출고를 확인해야 하니 리더기가 저장고 입구마다 있어야 할 것 같음. 단 농산물 보관상자(컨테이너)를 RFID로 구성한다면 30개 또는 36개로 적재되어있는 컨테이너가 정확히 리딩되기 어려움으로 이 부분은 생각해볼 필요가 있다고 생각

- Q. 농협과 공유하는 정보에는 어떤 것이 있고, 그런 정보들이 지금은 어떻게 공유되고 있는가?

  A. 농원에서 들어온 과실의 데이터, 그리고 조합원의 정산 내역이 전달됨. 이런 정보는 APC 내에서 자체적으로 엑셀화 하고 VPN을 통해 농협 망에 접속해서 정보를 입력함. 해당 과정이 전부 수기로 이루어지는 부분은 선별기가 각자 다른 업체에서 만들어진 기기로, 데이터 호환 안됨. 이런 농협과의 데이터 전송 과정이 자동화되어 있는 시범 APC가 상주에 있음
- Q. 스마트 APC 사업을 통해 자동화되었을 때 현업에서 가장 큰 효용을 느끼는 구간은 어느 구간인가?

  A. 스마트 APC의 일환으로 자동화되었을 때 현장에서 가장 필요로 하는 부분 중 하나는 입고 자동화. 이를 위해 키오스크 도입을 고려해 봤으나 농촌 상황에 따라, 현실성이 아직은 의문. 추가로 입고 과정에서 물리적인 컨테이너 적재 작업을 자동화하기 위한 기기 도입의 필요성 또한 느끼고 있지만 이를 위해서는 컨테이너 및 팔레트의 규격에 대한 엄밀한 표준화 필요
- Q. 원격 제어 또는 실시간으로 제어되는 장비 있나?

  A. 당도 측정 기계의 경우 사용 최소 한 시간 전에 작동시켜 놓아야 정상 작동함으로 원격에서 작동 및 관리 감독

▶ 주요 애로사항 및 해결 방안

- **데이터통합의 어려움**
  - 스마트 APC 내에 선별장은 확장될 때마다 엣지 기기의 정보를 유선으로 수집하여 정리하는 선별기를 수주함[그림 28]. 이에

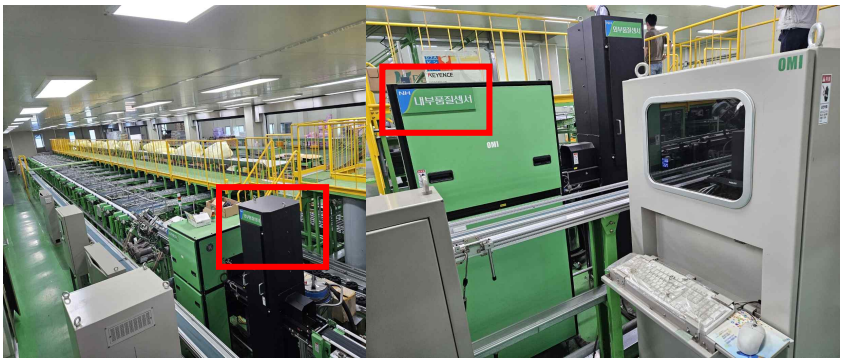
선별장마다 선별기의 제조사가 다르고 이기종 시스템에 따른 데이터통합의 어려움이 있음. 이는 유선 방식의 데이터 전송이 가지는 확장성의 한계에 기인함. 이에 이음5G 망을 적용하는 경우 엣지 기기로부터 MEC로 무선 기반에 원격 데이터수집이 가능해짐. 이렇게 수집된 데이터는 서로 다른 선별기를 통해서 데이터가 수질 될 때부터 확장성과 보안성에 있어 우위에 있음

- **농협과 데이터 공유 어려움**
  - 현재 농협 망에 VPN을 사용해 접속하고, 데이터를 입력하여 공유함. 이음5G 망의 구조 중 코어 공유형을 사용하는 경우 농협 소속의 APC는 농협 망에 있는 인증 시스템을 이용해 인증을 받음. 이렇게 인증된 기기로부터 자동으로 데이터를 공유받으면 망이 분리되어 있어 인력을 요구하던 데이터 공유 업무가 안전하게 자동화됨

- **민감한 장비들에 대한 제어**
  - 과실 폐기율에 직접적인 영향을 미치는 저장소 관리, 엄밀한 품질 측정을 위해 한 시간 전에 작동이 되어 있어야 하는 당도 측정기 등 APC 내에 과실의 품질에 직접적으로 영향을 미치는 기기의 경우 현재는 원격으로 정확하게 제어하고 관리할 방법이 없어 인력이 투입됨. 이를 이음5G 적용을 통해 정확하고 안전한 APC 관리가 필요

- **현장 사진**

▶ [그림 28]은 선별실에서 과실의 외부, 그리고 내부의 당도, 상폐 여부 등을 확인하는 데이터 생성 기기

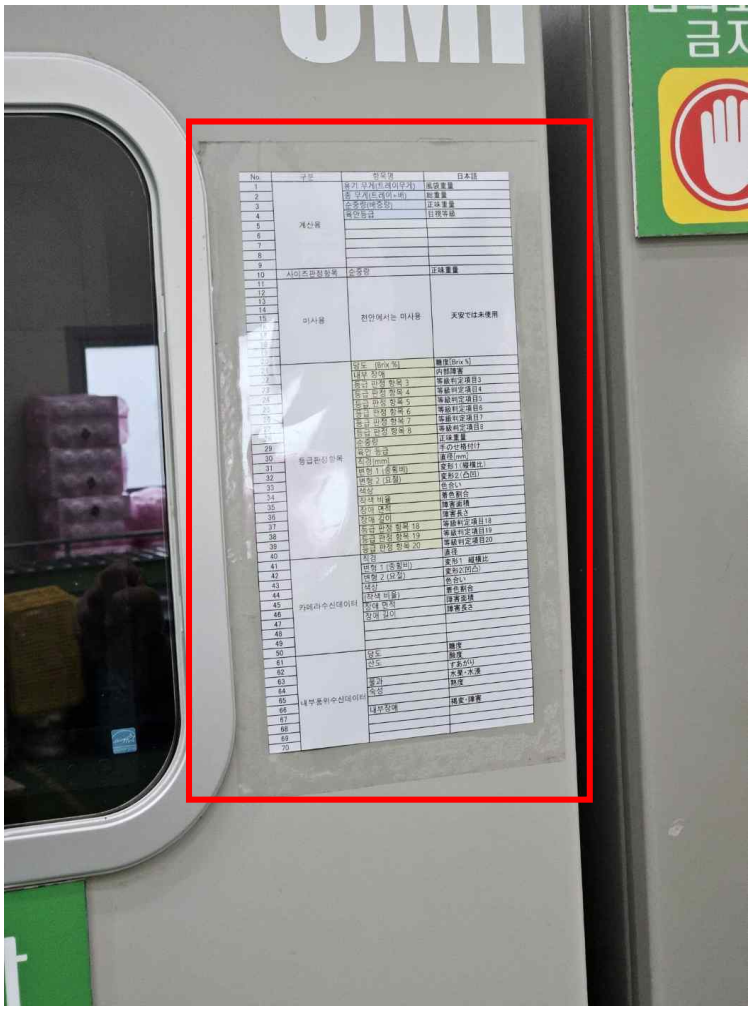


[그림 28] 1차 방문 선별실 엣지 기기

▶ [그림 29]는 과실을 선별하는 엣지 기기에서 측정된 과실의 당도 등과 같은 데이터가 집계되는 기기

[그림 29] 1차 방문 APC 선별기

▶ 해당 기기에서는 [그림 25]에서 볼 수 있는 데이터들이 집계됨

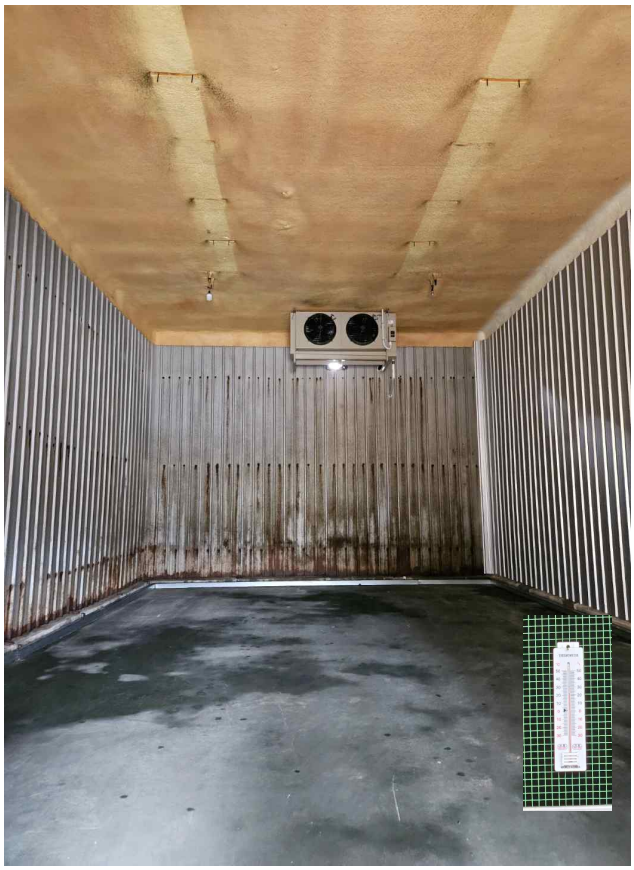


[그림 30] 1차 방문 데이터 표

▶ [그림 31]은 입고된 과실이 출고 요청이 들어오기 전까지 보관되는 저장고. 0~1도를 유지해야 과실이 상하지 않으며 현재는 원격에서 조작 또는 모니터링이 불가능하여 매일 담당자가 방문하여 온도 및 과실의 상태를 확인함

▶ 저장고에서 과실이 상하는 것은 정산 과정에서 책임 소재의 문제가 있어 예민한 단계임. 이에 스마트 APC를 통한 과실 관리가

용이해지고, 나아가 가장 오래전에 입고된 과실을 창고 내에 특정 위치까지 추적할 수 있으면 과실이 상하는 것을 방지 가능



[그림 31] 1차 방문 저온 저장고 사진

o **고창황토배기고구마**

- 스마트 APC 사업에 참여 중인 고창 황토배기 청정 고구마 연합의 유통센터를 2차 방문지로 선정하여 현장 답사 및 현업 관계자 미팅 진행

- 현장 사례 분석 내용

▶ **스마트 APC 과실 입고, 선별, 저장, 출고 과정**

- 작물 수확 -> 센터 입고 -> 저장 -> 세척 -> 선별 -> 박스 포장 -> 적재 및 출고
- 센터에서 입고될 때는 컨테이너에 있는 QR코드를 이용해 재고 정보 저장. 이 정보는 입고 시간 등을 이용해 재고 관리에 이용되기도 하며, 입고량을 이용해 각 농원의 수확량으로 잡고, 한해 농업 피드백. 해당 데이터를 기밀로 하기 위해 보안을 추가하는 것은 가용성 저하를 가져올 수 있음. 그러나 해당 데이터를 통해 APC운영 정책을 결정하므로, 데이터 생산 및 저장 과정에서의 무결성이 중요함
- 저장돼있는 작물을 세척 하고, 선별, 포장, 출고하는 모든 과정에서 인력이 투입됨. 최종 상품으로 포장된 수량 정보 또한 수기로 작성하여, 이후에 엑셀로 정리함
- 해당 과정에서 세척, 건조 컨베이어 기기 등이 현장에서 담당자가 직접 제어하는 방식으로 진행하고 있음

- 스마트 APC 적용방안 논의 내용

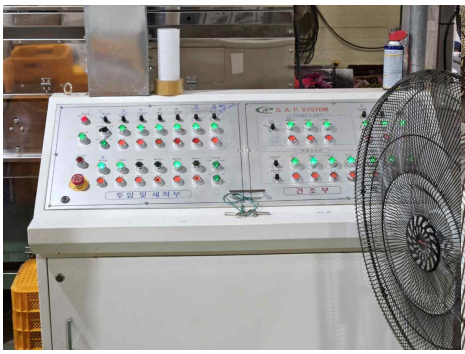
▶ 본 연구는 스마트 APC를 위한 이음5G 구축에 있어 보안 고려사항 연구로, 구축된 이음5G에 어떤 기기들과 서비스가 연동될 것인지에 따라 보안 고려사항이 바뀌므로 아래와 같은 내용 들은 우선 논의함

- (선별장) 육안 선별 이후 세척, 크기측정, 당도측정 등을 거쳐 포장 진행. 해당 과정이 현재는 현장에 인력투입으로 이루어지고 있고, 가장 많은 인력이 투입되는 과정 중 하나로 스마트 APC 적용에 따른 효용을 크게 볼 수 있는 과정임. 해당 과정에서 가장 중요한 것은 자동화 기기가 상품을 훼손하지 않고 선별을 진행하는 것이지만, 해당 내용은 보안을 통해서 해결할 수 있는 내용이 아님. 보안을 통해서 해결할 수 있는 가장 주요한 내용은 데이터에 대한 무결성임. 측정 데이터가 상품 분류에 사용될 것이고, 이는 상품 가격 결정에 근거가 되기 때문에 데이터 측정부터, 저장, 사용까지 무결성이 보장되어야 함
- (저장고) 저장소는 유통센터에 재고 관리 및 품질 관리가 이루어지는 곳으로 매우 중요함. 그래서 해당 시설에 대한 무인화 장비 도입을 과거 시도했었으나 섬세함이 인력이 현장에 투입되는 것에 미치지 못해 원복. 그러나 현장에서 인력이 투입되는 것만큼 스마트 APC에서 관리 기능이 제공될 수 있다면 가장 무인화를 진행하고 싶은 곳임. 실시간 모니터링 및 시설에 대한 원격 제어가 관건임
- (폐수 처리) 고구마 세척 과정에서 나오는 폐수를 처리하는 시설이 존재함. 폐수 처리 과정에 제대로 수행되고 있는지 센서들을 통해 원격에서 관제할 수 있는 시스템이 구축되면 효용이 높음. 해당 과정에서도 데이터의 무결성이 매우 중요하며, 문제 발생 시 즉각 대응할 수 있도록 초저지연이 중요함

- 현장 사진
  - [그림 31, 32, 33, 34]는 고창 황토배기의 선별장 내 사진임. 고구마 선별 이전에 세척 및 건조 과정을 거침. 해당 기기들 모두 현장에서 버튼을 조작하는 방식으로 제어됨

[그림 32] 2차 방문 APC 선별장

[그림 33] 2차 방문 APC 선별장 세척 및 건조 컨베이어



[그림 34] 2차 방문 APC 선별장 컨베이어 제어기기

[그림 35] 2차 방문 APC 선별장 분류 작업 진행

▶ [그림 36]은 자동화를 시도했으나 다시 원복을 진행한 현장의 저장소 사진임

[그림 36] 2차 방문 APC 선별장 APC 내 저장고

▶ [그림 37]은 폐수를 처리하는 시설의 사진임

[그림 37] 2차 방문 APC 선별장 폐수처리 시설

2. 현장 방문 기반 APC 내 보안 요구 사항 및 구축모델 제안

o 스마트 APC 도입을 준비하고 있고, 과거 자동화를 위한 시설구축을 시도한 경험이 있는 업장 방문을 통해 현장에서 가지고 있는 시각을 공유받음. 이를 기반으로 스마트 APC 내 이음5G를 적용하기 위한 보안 요구 사항과 제안하는 스마트 APC 내 이음5G 구축모델 다음과 같음

o 현장 보안 요구 사항

▶ (기밀성) 과실의 당도 정보, 생산량 등은 기밀성을 필수로 요구하지 않음. 그러나 안전한 프로토콜을 이용해 적시성을 가지는 암호화 키를 통해 무결성을 보조하는 방식으로 이용할 수 있음

▶ (무결성) 선별장에서 측정하는 데이터를 통해 상품을 분류하고,

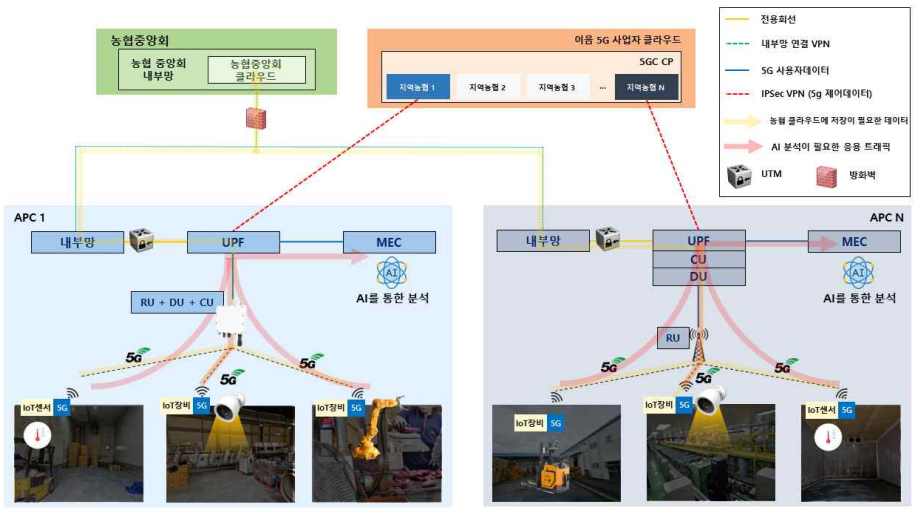
이는 상품 가격 결정에 영향을 미침. 이러한 데이터는 인증된 기기로부터 무결성 검증이 가능한 방식의 통신을 이용해 전송되어야 함

▶ (가용성) 보안의 적용이 농민들의 생산성을 저하하는 것은 기피되어야 함. 이에 두 가지 접근을 할 수 있음. 하드웨어적 또는 보안 정책적 접근이 가능함

암복호화의 성능을 높이기 위해 암호화 알고리즘에 대한 하드웨어 가속을 지원하는 장비를 사용할 수 있음

보안 정책적 접근은 기기에 대한 인증 빈도 조절, 그리고 데이터 형식에 따른 암호 라이브러리 차등적용 등을 통해 네트워크에서 암호 연산에 대한 부담을 줄이는 것임

o 스마트 APC 내 이음5G 구축모델 제안



[그림 38] APC 적용 이음5G 구조도

- 현장 답사 및 사례 조사를 기반으로 도출한 APC 적용 이음5G 구축모델은 [그림 38]과 같음
- 5G Core CP 공유형을 기반으로 이음5G 기반의 스마트 APC를

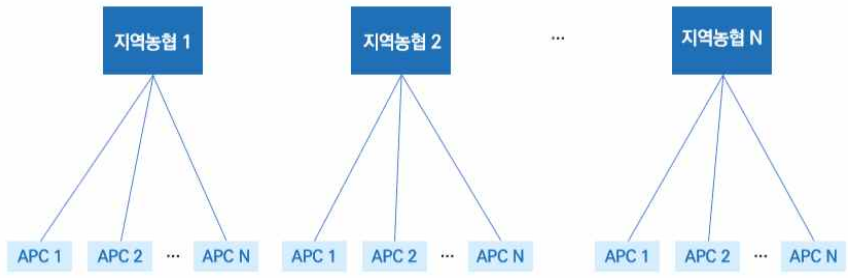
설계하였으며, 사유는 다음과 같음

- 농협은 [그림 39]와 같이 지역 주민들이 조합원으로 출자해 설립한 협동조합인 지역농협과 지역별로 설립된 지역농협(또는 단위농협)이 모여 만든 조직인 농협중앙회로 구성되어 있음

▶ **현장 답사 결과**

[그림 39] 농협 조직도

[출처] 농협 중앙회



[그림 40] APC와 지역 농협 관계

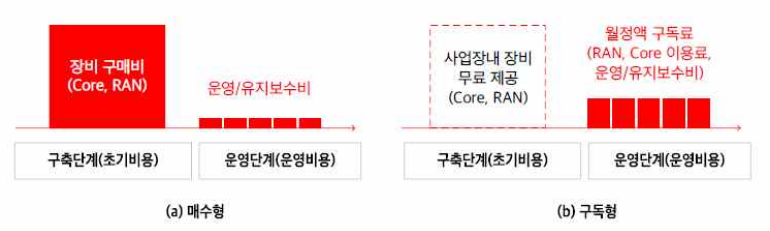
- 각 지역 농협은 [그림 40]과 같이 여러 개의 APC를 운영하고 있

으며, APC를 통해 나온 데이터는 지역 농협이 농협중앙회에서 구축한 전산망을 이용하여 데이터를 관리함

- 지역농협의 경우 전산망 또는 네트워크와 같은 전문적인 장비를 유지·보수하는 인력이 부족하며, 비용적 측면에서도 부담이 있기에 농협중앙회의 전산망을 사용함
- 또한, APC 현장 답사 결과, 지역 농협의 경우 전문 기술 인력의 부족 현상으로 인해 현재 사용 중인 간단한 IoT 장비에 대한 유지·보수조차 어려움을 겪는 상황임
- 따라서 추후 APC를 스마트 APC로 확장할 시, 장비에 대한 유지·보수 인력 확보는 중요한 사항으로 판단됨
  - 현재 스마트 APC 사업의 경우 농협경제지주가 시범사업을 진행하고 있으며 추후 지역 농협의 APC로 확대할 계획임
  - 따라서 지역 농협에서의 스마트 APC 내에 운용되는 장비에 대한 유지·보수가 필요할 것으로 보임
- 하지만 추후 지역 농협에서 운영하는 스마트 APC의 경우 이음 5G 도입 시 전문 인력의 부재로 인해 운영 측면에서 어려움이 있을 것으로 판단됨
- 또한, 지역 농협의 경우 지역 주민들이 조합원으로 출자된 하나의 조합으로써 지역별로 매출이 상이하며, 수익이 한정적이기에 금전적 요소도 중요한 항목임
- 스마트 APC 내 이음5G 구축 시, 높은 금액이 요구되면 사업의 어려움을 초래할 수 있음
- 따라서 지역농협이 관리하는 APC 개별로 이음5G망의 코어를 전부 설치하여 운용하는 것은 고비용을 초래하기에 조건에 맞지 않은 모델로 판단됨
  - 5G 장비의 경우 이동통신사용으로 출시되어 시장가격이 고가로 형성되어 있으며, 메이저 벤더사 기준 이음5G망 코어를 전부 구축하는데 투자되는 초기비용은 10억원 가량에 이름

▫ 이에 기업 자가구축형 또는 이음5G 사업자 자가구축형 모델을 사용 시, 고가의 초기 투자비용이 발생할 것으로 예상

▫ 또한, 지역 농협의 경우 유지·보수 인력을 보유하고 있지 않기에 기업 자가구축형 모델은 어려울 것으로 판단되며, 유지·보수에 장점이 있는 이음5G 사업자 자가구축형 모델로 운영하는 것이 현실성 있음



[그림 41] 이음5G 사업자 자가구축형 모델 서비스 요금 방법

[출처] 넷마니아즈

▫ 하지만 이음5G 사업자 자가구축형 모델도 고가의 투자비용이 수반됨

▫ 또한, 초기 투자비용을 감소시키기 위해 [그림 41]과 같이 구독형 모델 사용 시, 고가의 구독료 발생으로 지역 농협의 금전적 부담을 증대시킬 것으로 예상함

• 따라서 스마트 APC 내 이음5G 활성화를 위해선 On-Premise형 모델은 옳지 않으며, 5G Core를 공유하는 모델을 이용해야 함

▶ 사례분석 결과

• 5G Core를 공유하는 모델은 크게 5G Core CP 공유형과 5G Core 전체 공유형으로 나뉘며 각 모델 별 특징은 [표 *]와 같음

	5G Core CP 공유형	5G Core 전체 공유형
보안	사업장내에서 발생한 데이터가 사	사업장내에서 발생한 데이터가 전

	업장 내부에서만 유통되고 관리되며 사업장 외부로 유출되지 않아 기업이 데이터를 완전하게 통제할 수 있음	부 사업장 외부로 유출됨. 따라서 기업의 정보가 유출될 수 있기에 5G Core 전체 공유형 모델은 데이터 유출을 허용할 수 있는 기업만 적합함
성능	사업장 내에 UPF와 MEC가 존재하므로 저지연 서비스와 대용량 서비스가 가능함. 또한 기지국과 UPF를 독점하여 사용하므로 사업장 내에 충분한 수의 네트워크 슬라이스를 생성·운영할 수 있음	UPF와 MEC가 이음5G 사업자 센터에 존재하기에 사업장과 센터간 백홀회선의 통신거리가 멀어져 백홀 전송 지연이 늘어남. 따라서 저지연 서비스 성능이 저하되며, 저지연 서비스를 지원하기 위해 고가의 품질 보장형 백홀 회선이 필요함
안정성	센터나 백홀망에 장애/정전/화재 등 재해 발생시 이음5G망 통신 장애/ 단절이 발생하며 백홀 회선 이중화, 센터의 지리적 이중화등이 확보될 수 있는 망설계가 필요	센터나 백홀망에 장애/정전/화재 등 재해 발생시 이음5G망 통신 장애/ 단절이 발생하며 백홀 회선 이중화, 센터의 지리적 이중화등이 확보될 수 있는 망설계가 필요
백홀망	5G Core 제어부가 사업자 센터에 있으므로 센터와 기업사업장간에 제어 메시지 전달용 백홀이 필요	UPF가 이음5G사업자측에 존재하므로 사업장내 발생한 UP 트래픽을 UPF로 나르기 위한 고품질의 대용량 백홀회선이 필요
Full Control	이음 5G 사업자의 서비스 정책에 따라 제공해주는 범위 내에서 제한적으로 이음 5G망에 대한 기업의 제어가 가능	이음 5G 사업자의 서비스 정책에 따라 제공해주는 범위 내에서 제한적으로 이음 5G망에 대한 기업의 제어가 가능
비용	사업장마다 5G Core CP를 설치하지 않고 이음5G 사업자의 클라우드와 같은 서버에 구축된 CP를 공유하므로, On-Premise형 서비스에 비해 초기 투자비용을 줄일 수 있음. 또한 이음5G 사업자도 CP를 사업장마다 구축하지 않기에 서비스 이용료를 저렴하게 제	사업장마다 5G Core를 설치하지 않고 이음5G 사업자의 클라우드와 같은 서버에 구축된 Core를 공유하기에 On-Premise형이나 5G Core 제어부 공유형에 비해 초기 투자비용이 저렴함. 또한 이음 5G 사업자 입장에서 기업 사업장당 투자비용을 가장 크게 줄일 수 있

	공할 수 있음	어 서비스 이용요금이 가장 저렴
운영	이음 5G사업자가 사업장내 5G망을 설계, 인테그레이션, 운영을 대행해주므로 내부에 5G 전문 인력이 없어도 되어 기업은 운영 비용을 절감할 수 있음	이음 5G사업자가 사업장내 5G망을 설계, 인테그레이션, 운영을 대행해주므로 내부에 5G 전문 인력이 없어도 되어 기업은 운영 비용을 절감할 수 있음

- 스마트 APC 내 이음5G 설치 시 서비스 측면에서 중요한 항목은 데이터에 대한 보안과 초저지연 서비스임
  - 사업장 내에서 발생한 데이터는 농협중앙회에서 관리하는 전산망을 통해 공유되는 데이터도 존재하기에 데이터에 대한 보안성은 중요한 항목임
  - 추후 스마트 APC 내 이음5G가 활성화될 시 무인 지게차, AR 기기와 같은 초저지연 서비스가 필요한 장비가 사용될 것으로 보이며, 이런 장비를 안전하게 사용하기 위해서는 초저지연 서비스가 보장되어야 함
- 하지만 5G Core 전체 공유형의 경우 UPF가 이음5G 사업자의 클라우드 혹은 서버 내에 존재하기에 UP 트래픽이 외부로 노출되며, 사업장에서 발생한 데이터에 대한 유출 위험이 존재함
- 또한 UPF와 MEC가 이음5G 사업자 센터 내에 존재하기에 사업장과 센터 간 백홀 회선의 통신거리가 길어져 초저지연 성능이 저하될 수 있음
  - 일본의 이음5G 실증사례에 따르면, 사업장과 이음5G 사업자의 코어가 설치된 클라우드가 680Km인 경우 평균 지연시간은 상향 42.1ms ~ 43.8ms, 하향 21.2ms ~ 25.5ms로 측정되며 평균 Throughput은 상향 65Mbps ~ 384Mbps로 측정됨
  - 하지만 UPF를 사업장과 직선거리 19Km인 경우의 지연시간을 측정한 결과, 평균 지연시간은 상향 38.6ms, 하향 10.3ms로 측정되었으며, 평균 Throughput은 상향 73Mbps, 하향

545Mbps가 측정됨

- ▫ 따라서 UPF를 사업장과 가까이 설치할수록 초저지연 서비스가 제공되는 것을 확인할 수 있으며, 사업장 내에 UPF를 설치 시 더 높은 성능의 초저지연 서비스가 제공될 것으로 보임

- 따라서 데이터에 대한 보안성과 초저지연 서비스를 제공하기 위해선 5G Core CP 공유형 모델이 적합함
- 5G Core CP 공유형 모델의 경우 일본에서는 구독형, 매수+구독형 2가지 서비스 요금 방법을 채택하여 운영 중임

[표 8] 5G Core CP 공유형 서비스 요금 방법

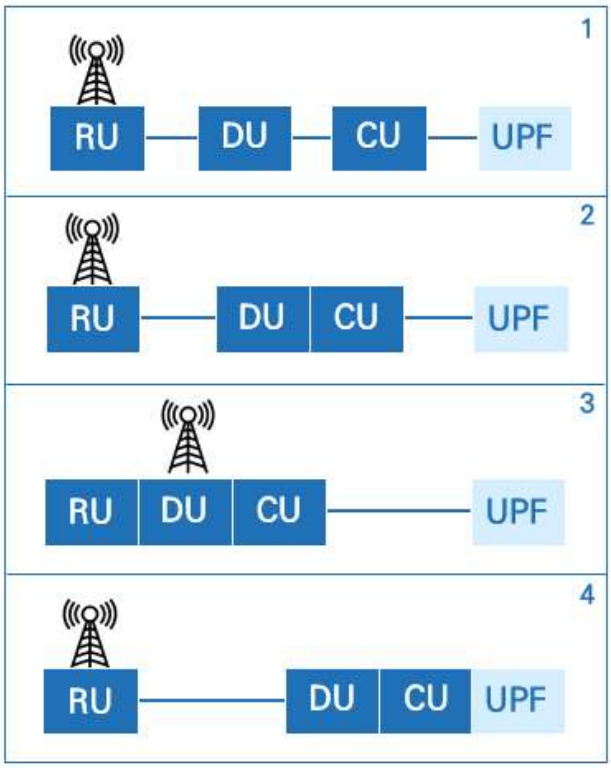
구독형	사업장 내에 장비 (UPF, RAN)을 제공해주고 5GC CP을 구독형으로 이용함	NTT 동일본: 30만엔/월 NTT Com: 150만엔/월 NEC: 100만엔/월 ~ 160만엔/월
매수+구독형	사업장내 UPF, RAN 장비를 구매하고 5GC CP을 구독형으로 이용함. 장비를 구매하기에 구독형 대비 초기 투자비용은 더 요구되지만 구독료가 낮음	NEC: 장비 구매비 498만엔, 구독료 300만엔/연

- ▫ 구독형, 매수+구독형 중 지역 농협의 상황에 따라 선택하여 서비스를 받을 수 있음

- 현장 답사와 사례 분석을 기반으로 5G Core CP 공유형 모델이 스마트 APC에 적합한 모델임을 도출함

▸ 5G Core CP 공유형 기반의 스마트 APC

- 5G Core CP 공유형 기반의 스마트 APC의 경우 [그림 42]와 같이 5G RAN의 구조에 따라 다양한 모델을 선택할 수 있음



[그림 42] 5G Core CP 공유형 RAN 모델

- 일본의 경우 SI사인 NESIC은 1번 모델을 통해 서비스를 제공하고 있으며, 유선통신사 NTT Com, SI사 NEC는 2번 모델을 통해 서비스를 제공하고 있음
- 또한, 일본의 NEC는 중소규모 네트워크 대상의 이음5G 서비스를 제공하기 위해 RU, DU, CU를 일체형으로 개발하여 3번 모델의 서비스를 제공하고 있음. 일체형 기지국을 통해 분리형 기지국에 비해 가격을 절반으로 줄임
- 미국의 Google과 AWS는 4번 모델을 통해 서비스를 제공하고 있으며 Google의 경우 UPF, RAN은 기업사업장내 Google의

GDCE(Google Distributed Cloud Edge) 서버에 구축되며, AWS의 경우 AWS가 개발한 사설 5G H/W (AWS Outpost 서버, RU)를 기업에 배송해주고 기업이 설치함

- 이러한 4가지 모델 중 현재 스마트 APC에 적합만 모델은 2번 모델이며, 추후 4번과 같은 모델로 발전되어야함
  - 스몰셀과 같은 일체형 기지국은 고가의 5G 장비의 가격을 감소시킴으로써, 구축비용에 대한 부담을 해결할 수 있기에 적합한 도입을 고려하기 적합한 장비로 판단됨
  - DU, CU를 기업의 자사 클라우드에 구축함으로써 유지·보수가 편리하다는 장점을 갖으며, 사업장 내에 소형의 랙장비 내에 구축이 가능하기에 장비의 경량화가 가능함

- 따라서 5G Core CP 공유형 모델 중 일체형 기지국과 DU, CU, UPF 일체형이 스마트 APC에 적합한 모델임을 도출하였으며 [그림 38]과 같이 모델을 설계함
- 5G Core CP 공유형으로 구축된 스마트 APC를 안전하게 구축하기 위해서는 다음과 같은 보안 기술을 활용해야 함

▶ VPN·전용회선

- 5G Core의 CP가 이음5G 사업자 클라우드에 구축되어 있기에 사업장의 제어 데이터가 외부로 유출될 수 있음
- 따라서 제어 데이터를 안전하게 보호하기 위해서는 백홀 구간을 IPSec VPN을 사용하여 데이터를 전송해야 함
- VPN을 통해 제어 트래픽은 암호화되고 안전한 터널을 통해 전송되므로 더 높은 보안 수준을 제공할 수 있음
- 또한, 내부망에 연결하기 위해 강력한 보안이 요구되기에 전용회선 또는 VPN을 통해 연결하여 강력한 보안성을 지원해야 함

▶ 보안 장비(방화벽, UTM)

- 클라우드 앞 단에는 방화벽을 설치하여 비정상적으로 전송되는 트래픽에 대한 탐지·차단을 수행하도록 함
- 이를 통해 클라우드에 대한 보안성을 지원할 수 있으며, 불필요한 트래픽을 차단하여 네트워크 성능을 최적화할 수 있음
- 또한, 제어 평면으로 전송되는 데이터의 경우, 방화벽을 통해 악의적인 인증 정보 또는 제어 명령을 감지하고 차단하여 무단 액세스를 방지할 수 있음

▶ 5G 인증 모듈

- 많은 IoT 센서들은 5G 통신을 지원하지 못하기에 IoT 기기에 5G 모듈을 부착하여 5G 통신을 지원해야 함
- 하지만 IoT 기기로부터 수신한 데이터를 완전히 신뢰하기 위해서는 부착한 통신 모듈을 기반으로 단말(IoT 기기)에 대한 인증 절차가 우선시 되어야 함
- 이때 인증은 5G 표준 인증 프로토콜을 통해 수행되어야 하며, 이를 통해 단말에 대한 신뢰와 안전성을 확보할 수 있음
- 그러나 기존의 단말은 탈부착이 가능한 USIM 기반으로 제작되고 있음. 이는 물리적인 보안에 취약한 APC에서는 공격자가 단순 USIM을 탈취해 다른 기기에 USIM을 장착하는 것으로 공격을 성공시킬 수 있음
- 이에 앞서 언급한 물리적으로 단말의 메인보드에 부착된 E-SIM 기술의 도입으로 이러한 문제를 해결할 수 있음

제 3 장 최종연구결과 참고자료

- NTT (2022). “Private 5G: rising adoption collides with CIOs’ security concerns.” White paper.
- 5G-ACIA (2019). “5G Non-Public Networks for Industrial Scenarios.” White Paper.
- Fortinet (2021), “Securing 5G Private Mobile Network.” White paper.
- Fortinet (2022), “Security Considerations in Industrial 5G Environments.” White paper.
- Cisco public (2022), “Cisco's Private 5G solution Security Overview.”
- GSMA (2020), “5G IoT Private & Dedicated Networks for Industry 4.0.”
- Lufthansa Technik (2020), “Lufthansa gets spectrum licence, deploys Nokia private 5G for remote engine checks.”
- Samsung (2021), “Virtualized RAN-vol.2.” White paper.
- Industrial ethernet book (2021), “5G on test bench for Industry: What’s possible in the future?”
- Bosch Press (2020), “Bosch puts first 5G campus network into operation.”
- Nokia (2019), “Sendai city improves tsunami preparedness with connected drones.”
- Smart sound plymouth (2022), “Vodafone, Plymouth city council and Plymouth marine laboratory announce use cases for world’s first 5G marine focused testbed.”
- Im-mining (2018), “Sandvik and Nokia team up to offer miners

LTE and 5G networks."
- RFC3748: https://www.rfc-editor.org/rfc/rfc3748
- 3GPP TS 33.102, "3rd Generation Patnership Project; Technical Specification Group Services and System Aspects; 3G Security, Security architecture", June 2003
- Draft-arkko-pppext-eap-aka-12.txt "Extensible Authentication Protocol for UMTS Authentication and Key Agreement(EAP-AKA)," Apr. 2004
- Olimid, Ruxandra F., and Gianfranco Nencioni. (2020). "5G network slicing: A security overview." J IEEE Access 8, (2020), pp.99999-100009.
- Sattar, Danish, and Ashraf Matrawy. (2019). "Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices." 2019 IEEE Conference on Communications and Network Security (CNS). pp.82-90.
- Madi, Taous, et al. (2021). "NFV security survey in 5G networks: A three-dimensional threat taxonomy." Computer Networks 197.
- Bonfim, Michel, et al. (2020). "A real-time attack defense framework for 5G network slicing." Software: Practice and Experience 50.7. pp.1228-1257.
- Barakabitze, Alcardo Alex, et al. (2020). "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges." Computer Networks 167 (2020)
- ETSI. (2022). "MEC Security; Status of standards support and future evolutions."ETSI White Paper No. 46
- C. Benzaid and T. Taleb (2020), "AI-Driven zero touch network

and service management in 5G and beyond: Challenges and research directions," IEEE Network, vol. 34, no. 2, pp. 186-194, 2020.

- P. P. Ray and N. Kumar (2021), "SDN/NFV architectures for edge-cloud oriented IoT: A systematic review," Computer Communications, vol. 169, pp. 129-153, 2021.
- R. Rosa and C. Rothenberg (2020), "Experiences in IETF-bMWG: Towards a methodology for VNF benchmarking automation," in Anais do VII Workshop Pré-IETF (WPIETF 2020), Porto Alegre, RS, Brazil, pp. 43-56.
- I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck (2018), "Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions," IEEE Communications Surveys & Tutorials, vol. 20, no. 3, p. 2429-2453, 2018.
- A. Esmaeily, K. Kralevska, and D. Gligoroski (2020), "A Cloud-based SDN/NFV Testbed for End-to-End Network Slicing in 4G/5G," in 6th IEEE Conference on Network Softwarization, 2020.
- .A. Cunha, E. Silva, M.B. Carvalho, D. Corujo, J.P. Barraca, D. Gomes, L.Z. Granville, and R.L. Aguiar (2019), "Network slicing security: Challenges and directions," Internet Technology Letters, 2(5):e125, Sep. 2019.
- Xiaoting Huang, Vlasios Tsiatsis, Anand Palanigounder, Li Su, and Bo Yang (2021), "5G Authentication and Key Management for Applications," IEEE Communications Standards Magazine, vol. 5, no. 2, June 2021.
- Christine Jost (2020), "Security for 5G Service-Based

Architecture: What you need to know," Ericsson Blog, Aug. 2020. Available: https://www.ericsson.com/en/blog/2020/8/security-for-5g-service-based-architecture [Online; accessed on Oct. 25, 2021]

- [Case Study] KT MOS의 5G 특화망 서비스 (삼성서울병원) 2023/05/23 손장우 대표이사 https://www.netmanias.com/ko/?m=view&id=oneshot&no=15789
- [Case Study] 한국수력원자력의 5G 특화망 구축 사례(발전소) 2023/04/29 손장우 대표이사 https://www.netmanias.com/ko/?m=view&id=oneshot&no=15731
- [교통] 일본 로컬 5G 실증사례 (9): 로컬 5G를 활용한 원격형 자율운행버스의 공도 실증 2022/08/16 손장우 대표이사 https://www.netmanias.com/ko/?m=view&id=blog&no=15542
- 이통사의 Private 5G 서비스: AWS 클라우드와 이통사 5G망의 통합 2023/03/06 손장우 대표이사 https://www.netmanias.com/ko/?m=view&id=blog&no=15663
- Bosch Press, Bosch puts first 5G campus network into operation(2020)
- Lufthansa Technik, Lufthansa gets spectrum licence, deploys Nokia private 5G for remote engine checks(2020)
- Nokia, Sendai city improves tsunami preparedness with connected drones(2019)
- Im-mining, Sandvik and Nokia team up to offer miners LTE and 5G networks(2018)
- Vodafone, Plymouth City Council and Plymouth Marine Laboratory announce use cases for world's first 5G marine-focused testbed(2022)

제 4 장 연구수행 상 애로점 및 건의사항

없음