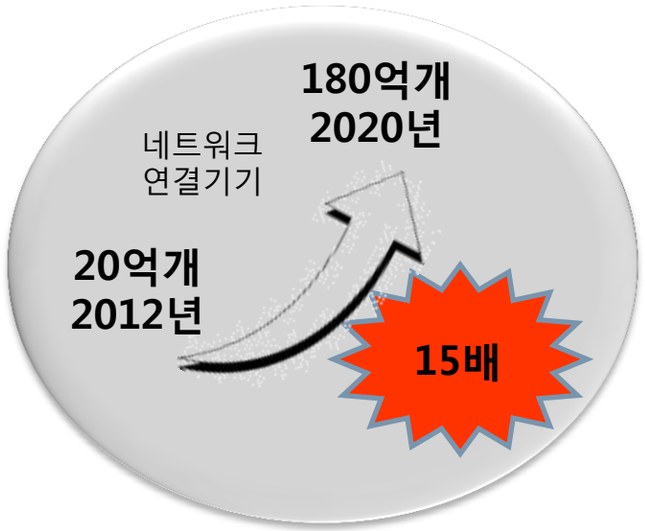
Ubizcore

유무선 구간 암호화 솔루션

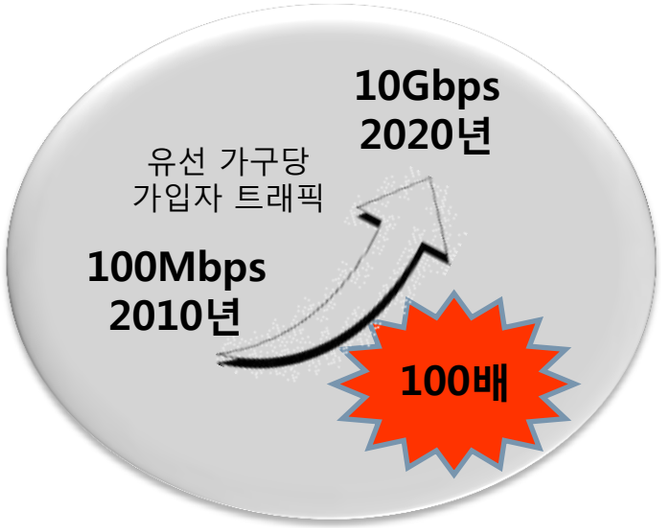
시장개요

전세계의 M2M(IoT) 시장은 이동통신사과 무선을 기반으로 한 시장이 폭발적으로 증가하는 추세로 다양한 디바이스와 서비스가 생기면서 프라이버시와 보안이 가장 중요한 문제점으로 대두되고 있음

디바이스 폭발

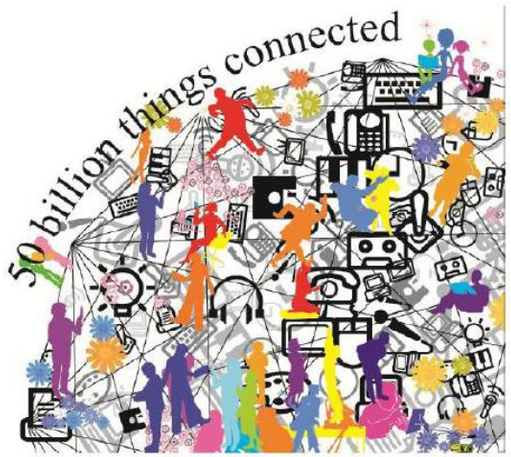


트래픽 폭발



정보 폭발

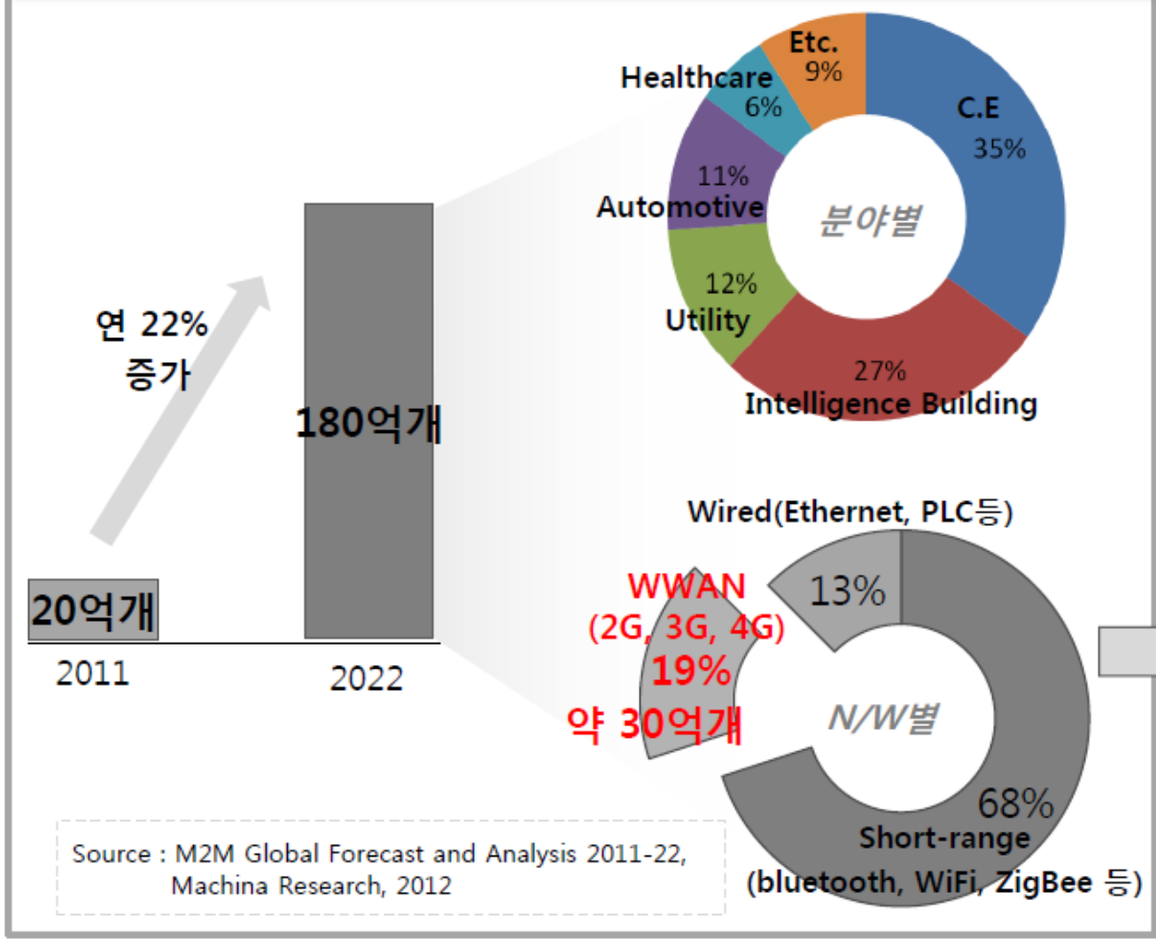
[2012]



[2020] **Source**: IBM

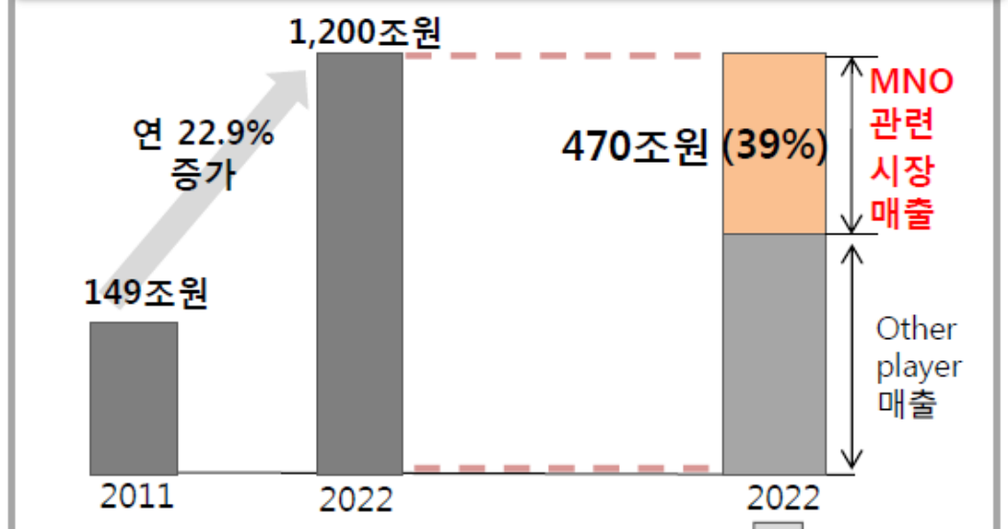
전세계의 M2M(IoT) 스마트폰 출시 후 이동통신사과 무선을 기반으로 한 시장이 폭발적으로 증가하는 추세로 다양한 디바이스가 생기면서 프라이버시와 보안이 가장 중요한 문제점으로 대두되고 있음

Global IoT device 전망, 2022년



Source : M2M Global Forecast and Analysis 2011-22, Machina Research, 2012

Global IoT 매출 전망, 2022년



국내 WWAN 단말수	국내 MNO 관련 매출	
('13년)200만개 → ('22년)2,500만개 (Global 대비 0.8%수준)	('13년)4천억 → ('22년)4조원	
	회선 매출 1.5조원	기타 매출 2.5조원

- MMO: Mobile Network Operator
- WWAN: Wireless WAN

제품소개

사업 초기에는 국가. 공공기관의 보안적합성을 만족하는 암호화 제품으로 공공 시설물 및 원격감시 및 제어시스템에 적용할 수 있는 End-to-End 암호화 제품제품으로 추진하며, 향후 엔터프라이즈로 확대함

제품의 특징

- M2M 공공시설물의 단말기에 ARIAN암호장비를 설치하여 관제센터까지 데이터를 구간암호화 하여 전송할 수 있는 안전한 보안터널을 구성함.

- IT보안인증사무국의 검증 암호(ARIA/SEED)모듈을 탑재함으로써 보안적합성을 만족 할 수 있도록 하였으며, 특히 M2M 소형시설물에 적합한 소형암호화 장비임.

- 유, 무선환경에서 안전한 키 관리를 기반으로 인증 및 키 일치 프로세스로 CCTV, 스마트미터, 원격감시 제어장치 등에 내장 또는 외장으로 장착할 수 있는 암호솔루션

ARIAN 보안 솔루션

암호모듈 & 유선 암호 장비

무선 암호 장비

인증/복호화 장비

기술 및 제품

국내 암호화 구현 적합성(CMVP) 인증을 받은 암호 모듈로 탑재한 H/W제품과 서버 및 브릿지 제품으로 기존의 VPN 또는 서버 및 DB보안이 해결하지 못한 End to End 보안을 해결함

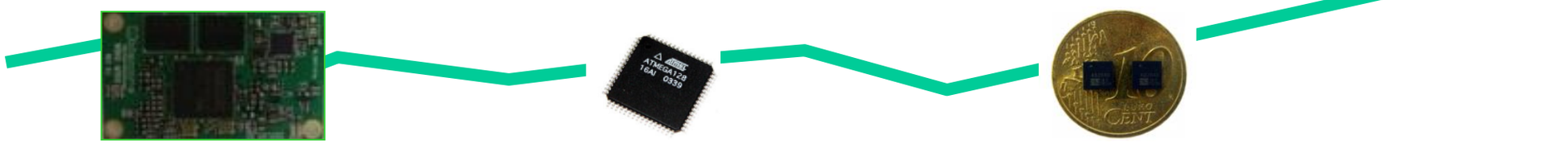
제품		내용
암호화 모듈	1 국산 검증 필 암호 모듈	• 2012년 8월 IT보안인증사무국 암호 검증 완료 • 암호 함수 : ARIA/SEED (ECB, CTR, CBC) 구현 • 대칭 키 암호 모듈 (128Bit, 192Bit, 256Bit)
	2 암호화 모듈(H/W)	• 각종 데이터를 암·복호화 하는 핵심 H/W Module • 암호화 처리 시 지연 및 분실없이 고속으로 데이터 처리가능 • 타 H/W와 연동을 위한 Serial/Ethernet 지원
서버	3 복호화 서버	• 암호화 모듈에서 암호 전송된 데이터를 복호화
	4 인증 및 관리 서버	• 유효단말기 등록 및 기기 인증 • 유·무선 구간 세션 키 분배 • 암호환경 설정 • 데이터 암복호화 키 관리
암호장비	5 TEE-100 (E2E 유선구간) AEW-100(Wi-Fi 무선구간) RML-100(LTE보안라우터)	• 영상 또는 기타 데이터를 암·복호화 • 무선 (Wi-Fi/LTE) 전송 가능 • 유선 to 유선 구간 암·복호화 가능

기술 및 제품 로드맵

소형 스마트 디바이스 및 M2M기기 적용을 위한 암호화 모듈 진화의 최종 목표는 System on Chip이며, Micom과 ARM기반한 TPM형태의 ASIC칩 개발을 목표로 함

AS-IS	TO-BE
Encryption module On Arm 11(9) **Encryption module On MIPS** **Encryption LIB**	**Embedded in MCU(2014)** - 검증암호 탑재 H/W 모듈화 및 암호전용장비 **Encryption module On MCU(2014년 하반기)** - 32bit mcu에 암호화 모듈 porting 및 인증 **Embedded in Encryption module & Authentication (2014)** - 기기인증 및 인증관리 Back-end system **System On Chip(~2017)** - M2M기기 및 소형 디바이스에 적용 가능한 ASIC Chip으로 진화

ARM → **Micro computer** → **System on Chip**



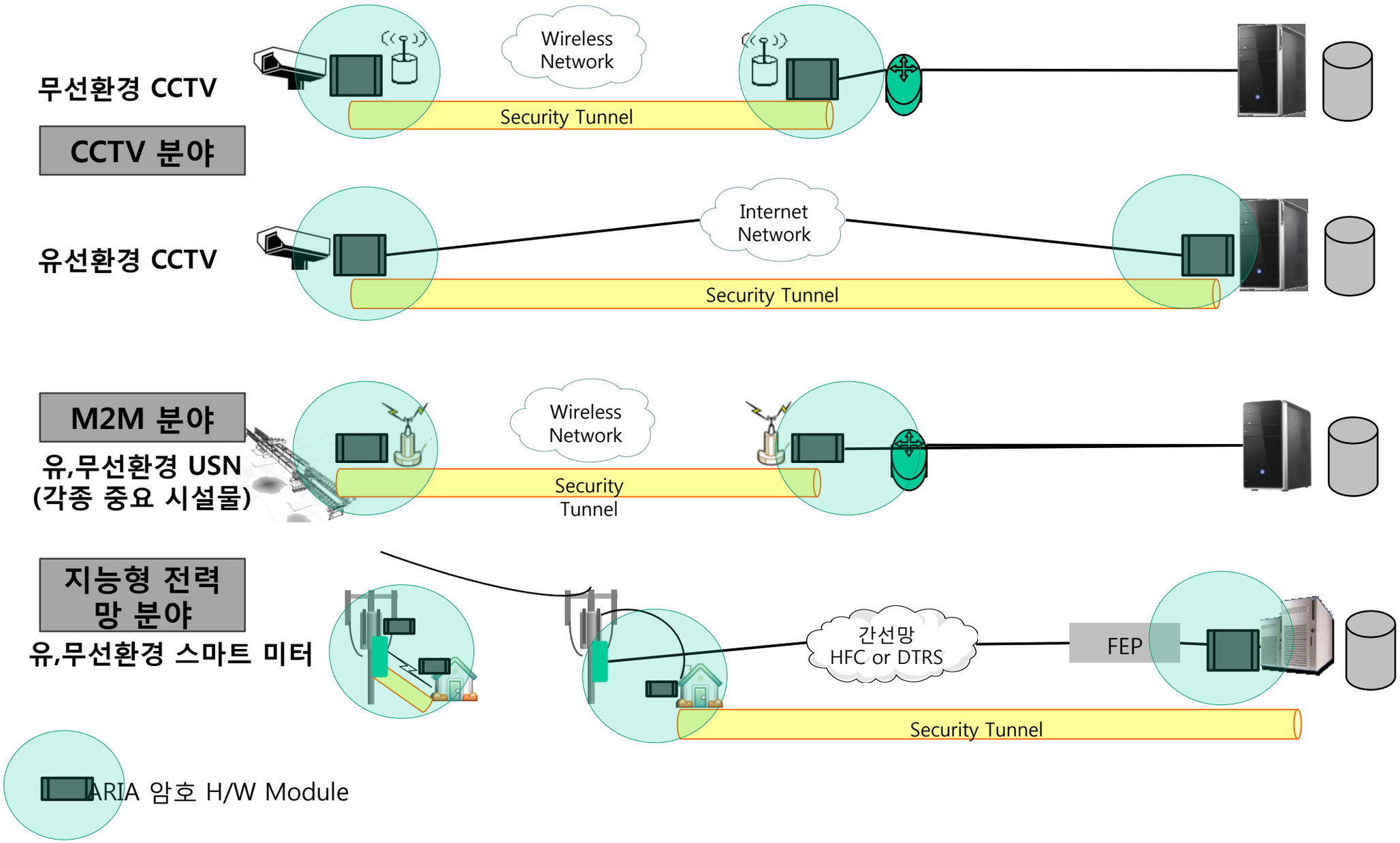
적용분야

공공 부문의 교통, 방범, 방재, 환경, 시설 등 5대 공공 서비스 및 국가의 자원 관리 공기업의 사물인터넷을 포함한 각종 원격감시 및 제어데이터의 암호화 및 보안에 적용 가능

서비스 적용 부분		서비스 적용 대상
공공 부문	CCTV	• 공공기관의 교통, 방범, 방재용 통합관제센터 - 지방자치 단체의 방범, 교통, 환경, 시설, 방재 분야 및 센터 - 공기업의 CCTV 및 센터 - 경찰청, 소방방재청, 산림청 등이 운영하는 CCTV 및 센터
	AMI (지능형 검침 인프라)	• 한국전력의 스마트 그리드 사업 (AMI사업) • 디지털 원격 계량 적용 사업 (가스, 수도, 유량 등) • 스마트워터그리드 및 전력 송배전망의 M2M 관리
	USN M2M	• 농어촌개발공사의 농수로, 갑문제어 관리 등 • 수자원공사의 상하수도 관리 등 • M2M가 필요한 공공부문의 시설물관리, 무선ITS설치 분야
등 정보통신보안 업무규정 대상 공공기관, 지방자치단체 및 공기업		
국방 부문	군 시설물	• 탄약고, 전차, 장갑차 등 내에 설치된 영상정보 암호화 • 군 수송차량 및 외곽 감시 등의 GOP과학화 시설물 • 해외파병부대의 감시장비 및 각종 시설물
민간 부문	CCTV	• 행정안전부의 개인정보 보호법 대상 민간기업 → 향후 지능형카메라로 신규설치 • 민간 보안 서비스 회사 (개인정보 보호법 적용 대상 사업자)
	금융	• 금융기관의 ATM 및 단말기 • 카드사의 POS 및 카드단말기 등

적용 분야 예시

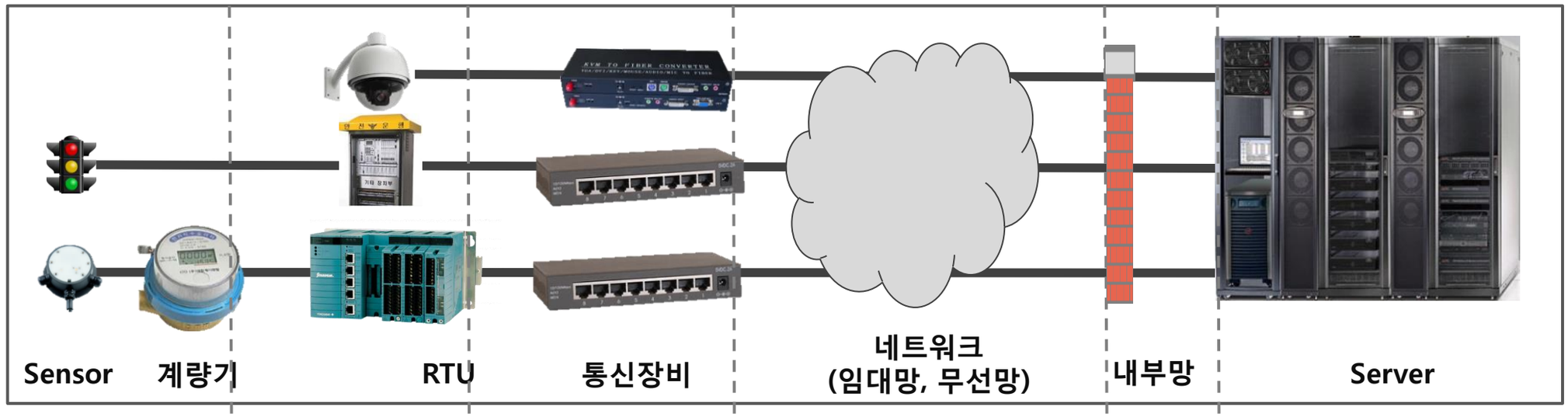
IT보안인증사무국의 암호화 구현 적합성(CMVP) 인증을 받은 암호화 모듈 및 이를 이용한 H/W제품과 서버 및 무선보안 제품은 기존의 VPN의 한계, 서버 및 DB보안이 해결하지 못한 End to End 보안을 해결함



기존 VPN과 차이점

기존 VPN은 가상사설망 장비를 기반으로 한 암호화를 하고 있으나, 당 사의 제품은 순수 데이터 암호화를 위한 구간 암호화 전용 제품으로 실질적인 End-to-End 암호화를 지원하며, 설치가 단순하고 유지보수가 용이하다는 장점을 보유하고 있음

❑ **데이터 암호구간 종류**



기존에 사용 중인 데이터 암호화 구간 (일반 VPN)

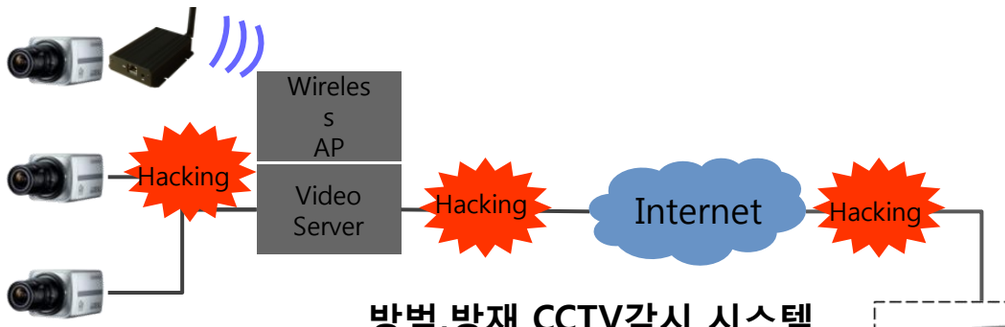
당 사가 제공하는 데이터 암호화 구간

개발 중인 데이터 암호화 구간

End to End 보안의 필요

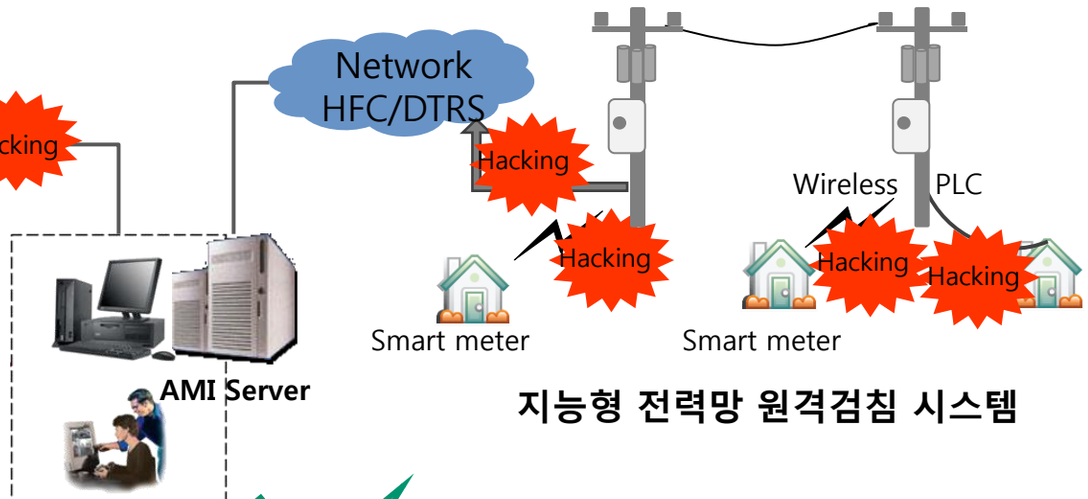
현재의 DB 및 서버 보안으로는 공공의 영상 정보 및 국가 자원 정보의 근원적 보안이 위험에 노출되어 있으며, 이를 해결할 방법은 정보 수집 단계(단말)에서의 검증된 데이터 암호화가 필요함

영상 CCTV 보안 위협

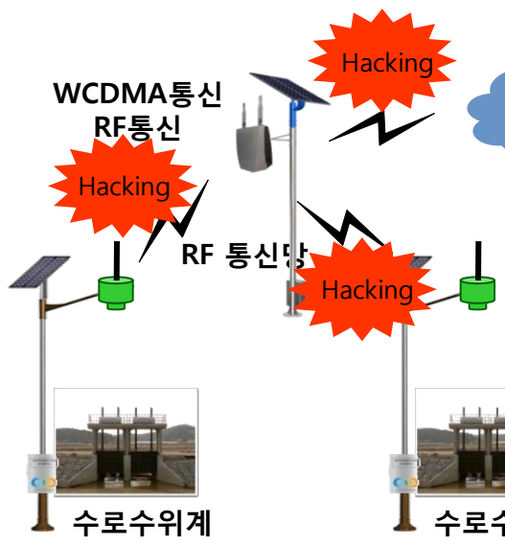


방범,방재 CCTV감시 시스템

스마트 그리드 보안 위협



지능형 전력망 원격검침 시스템



수위 및 유량
산정운용 시스템

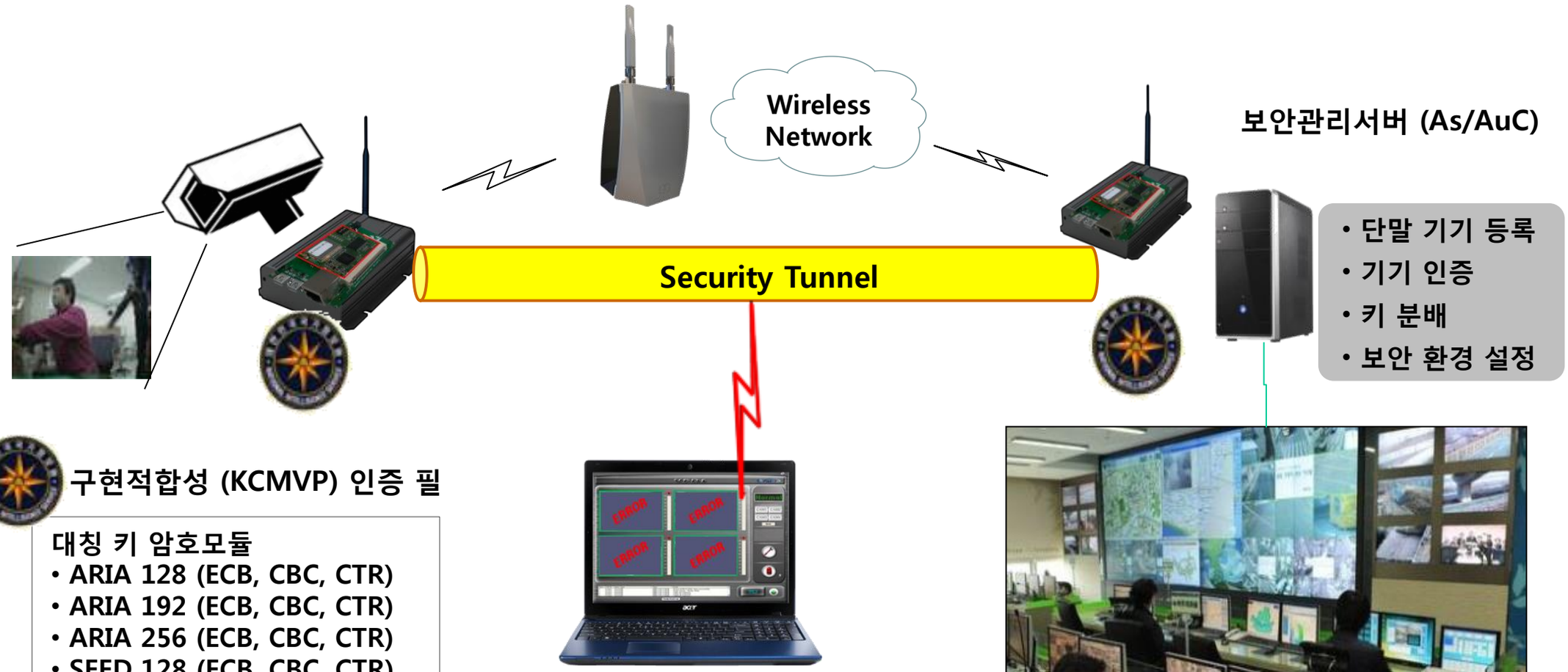
원격감시 및 제어시스템 보안 위협

공공부문 시설물의 데이터 보안 취약

- 공공용 유.무선 네트워크 환경 급속 확장
- 데이터가 네트워크에서 불법탈취, 변조, 허위자료 등의 발생 우려
- 방범, 방재, 환경, 교통 등의 시설물 데이터 수집단계부터 인증, 암호화 필요

End to End 무선보안 시스템 구성

단말에서 수집된 정보가 국산암호로 인증암호화 됨으로 어떤 방식의 무선이나 유선을 사용해도 암호화된 상태로 전송이 되며, 중간에 해킹을 당해도 정보를 볼 수 없음



구현적합성 (KCMVP) 인증 필

대칭 키 암호모듈
- ARIA 128 (ECB, CBC, CTR)
- ARIA 192 (ECB, CBC, CTR)
- ARIA 256 (ECB, CBC, CTR)
- SEED 128 (ECB, CBC, CTR)
- SEED 256 (ECB, CBC, CTR)
- ARIA-128-CCM
- ARIA-192-CCM
- ARIA-256-CCM

※ UBi-Crypto v1.0 ➔ KCMVP 검증필

해킹을 해도 암호화되어 보이지 않음

관제센터에서 모니터링 가능