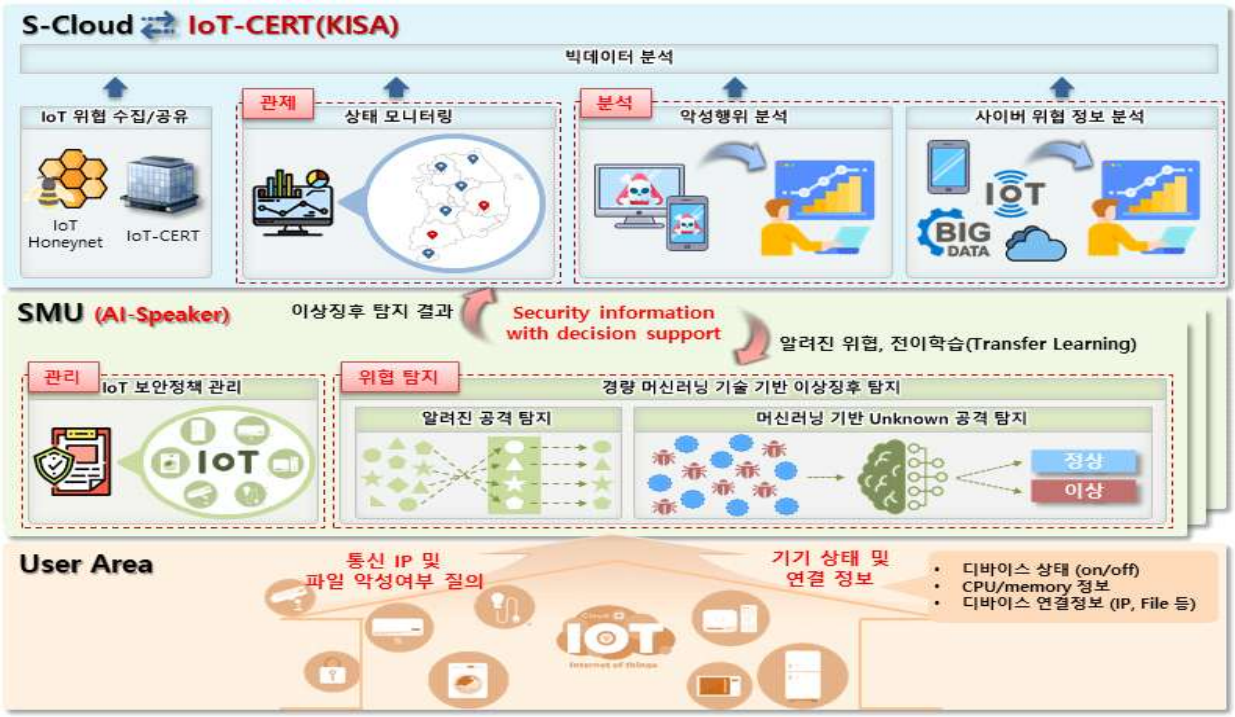
Ⅱ. 21년 기술이전 대상 목록

2 클라우드 기반 IoT 위협 자율 분석 및 대응 기술 ('18.4월 ~ '21.12월(4년))

□ 기술개요

o 실생활에 피해를 유발하는 **IoT 환경의 침해사고**에 즉각적인 대응이 가능한 **실시간 위협탐지 및 자율적 위협 분석 기술 개발**

< 기술 개념도 >



□ 기술의 특징 및 장점

o IoT 기기별 알려진 보안위협 자동 수집·분석·탐지

- IoT 기기 관련 키워드* 기반 CVE, ExploitCode 자동 수집·매핑으로 분석가의 시간 비용 절감

* 키워드 자동 수집, 수동 입력으로 보안위협 수집 범주 조정 가능

o 저사양 환경에서 동작 가능한 경량화된 다중 AI 기반 이상행위 탐지 모델

o 대용량 IoT 관련 정보 연관분석 및 탐지·상태 모니터링/관제 기술

□ 활용 분야

① IoT 기기 보안위협 탐지 솔루션 및 HW 제품 개발(보안위협탐지)
② 클라우드 기반 IoT 보안관제 및 서비스 운용(보안관제)

□ 기술이전 내용 및 범위

구분	시스템	주요 내용
1	IoT 보안 관제 시스템	o 대량의 IoT 기기 운영 환경에서 클라우드 기반 사용자의 기기 사용 및 생활패턴 정보를 수집/분석/관제하는 기술 o 세부 기술 구성 - 기술1 : 사용자 행위별 데이터 패턴분석 및 정규화 - 기술2 : 사용자 행위 연관분석 관계생성
2	IoT 보안 위협 탐지 시스템	o IoT 기기 취약점 등을 대상으로 발생하는 공격 및 학습 기반의 이상행위 탐지 등 소형화·경량화된 IoT 기기 위협 탐지 기술 o 세부 기술 구성 - 기술1 : 키워드 기반 IoT 위협 수집 및 공격유형 분류 - 기술2 : 시그니처/룰 기반 IoT 위협 탐지 - 기술3 : 전이학습 기반 IoT 기기 이상행위 탐지
3	IoT 기기 식별 시스템	o 네트워크 정보를 기반으로 IoT 기기 정보를 상세하게 식별하기 위한 기술 o 세부 기술 구성 - 기술1 : 네트워크 패턴 특성 추출 기반 IoT 기기 유형 식별

※ 기술이전은 시스템 내, 세부 기술 단위로 계약 가능

□ 세부문의

o 기술관련

담당자	고웅 책임연구원(061-820-1262, rndts@kisa.or.kr)