

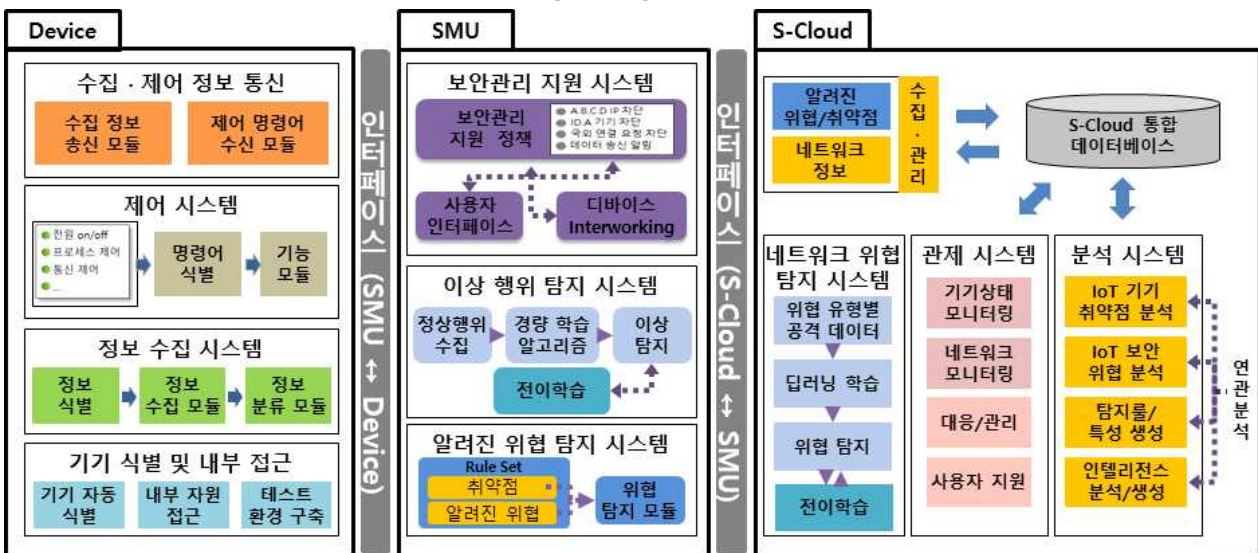
II. 20년 기술이전 대상 목록

③ 클라우드 기반 IoT 위협 자율 분석 및 대응 기술 ('18.4월 ~ '21.12월(4년))

□ 기술개요

- 실생활에 피해를 유발하는 IoT 환경의 침해사고에 즉각적인 대응이 가능한 실시간 위협탐지 및 자율적 위협 분석 기술 개발

< 기술 개념도 >



□ 기술의 특징 및 장점

- 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
- 저사양 환경에서 동작 가능한 경량화된 다중 AI 기반 이상행위 탐지 모델
- 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	<ul style="list-style-type: none"> ○ 대량의 IoT 기기 운영 환경을 대상으로 클라우드 기반의 오토스케일링, 실시간/배치 분석 등 플랫폼 구축과 탐지·상태정보 등을 모니터링하는 기술 ○ 세부 기술 구성 <ul style="list-style-type: none"> - 기술1 : 컨테이너 기반의 오토 스케일링 - 기술2 : 실시간 스트리밍/배치 분석
2	IoT 보안 위협 탐지 시스템	<ul style="list-style-type: none"> ○ IoT 기기 대상 보안위협을 대응하기 위한 소형화·경량화된 탐지 기술 ○ 세부 기술 구성 <ul style="list-style-type: none"> - 기술1 : 공개된 IoT 보안 위협 정보 자동 수집 - 기술2 : 시그니처/룰 기반 알려진 위협 탐지 - 기술3 : IoT 기기 네트워크 행위 기반 경량 이상징후 탐지
3	IoT 기기 식별 시스템	<ul style="list-style-type: none"> ○ 네트워크 정보를 기반으로 IoT 기기 정보를 상세하게 식별하기 위한 기술 ○ 세부 기술 구성 <ul style="list-style-type: none"> - 기술1 : IoT 기기 네트워크 정보 기반 식별

□ 기술이전 문의

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