‘2018년 정보보호 해커톤’ 개발기획서

팀명(팀대표 성명)	BLUE(이대화)
최종 결과물 등 개발 목표 개요	비인가 IoT Device의 접근과 중앙화된 서버 보안 문제를 블록체인으로 해결하는 솔루션
주요 활용 기술	ARTIK, ARTIK Cloud, Raspberry Pi, Hyperledger Fabric, Kafka Consensus, Go, C, JavaScript, PHP, HTML

1. 과제 분석

1-1. 기존 IoT환경에서의 보안 문제점 도출 및 분석

비인가 Device의 네트워크에 무단 침입

비인가 Device가 스마트 홈 네트워크에 침입할 경우, 스니핑을 통해 Privacy Data가 모두 유출되거나 스푸핑을 통해 데이터를 조작한 뒤 출력할 수 있으며, 네트워크 전반에 치명적 결함을 야기할 수 있다. 조작된 데이터가 다른 Device의 작동에도 영향을 미치기 때문에 스마트 홈 네트워크에서는 인가된 Device만을 사용하는 것이 강조된다.

중앙화된 서버 보안 문제

기존 IoT네트워크는 대부분 중앙화된 클라우드나 서비스를 통해 통신하여 SYN Flooding 등의 공격으로 서버가 마비될 경우 IoT 네트워크의 정상적인 작동이 불가능해진다. 실제로 대부분의 해킹 사례는 모바일 어플리케이션 취약점을 이용한 중앙 클라우드 루트 권한 탈취였으며 IoT의 보안성을 높이기 위해서는 Blockchain과 P2P 네트워크를 통한 탈중앙화가 필요하다.

1-2. 1-1에서 도출한 문제점을 극복할 수 있는 블록체인 기술을 활용한 탈중앙화 · 분산화된 신규·개선된 IoT 서비스 아이디어를 제시

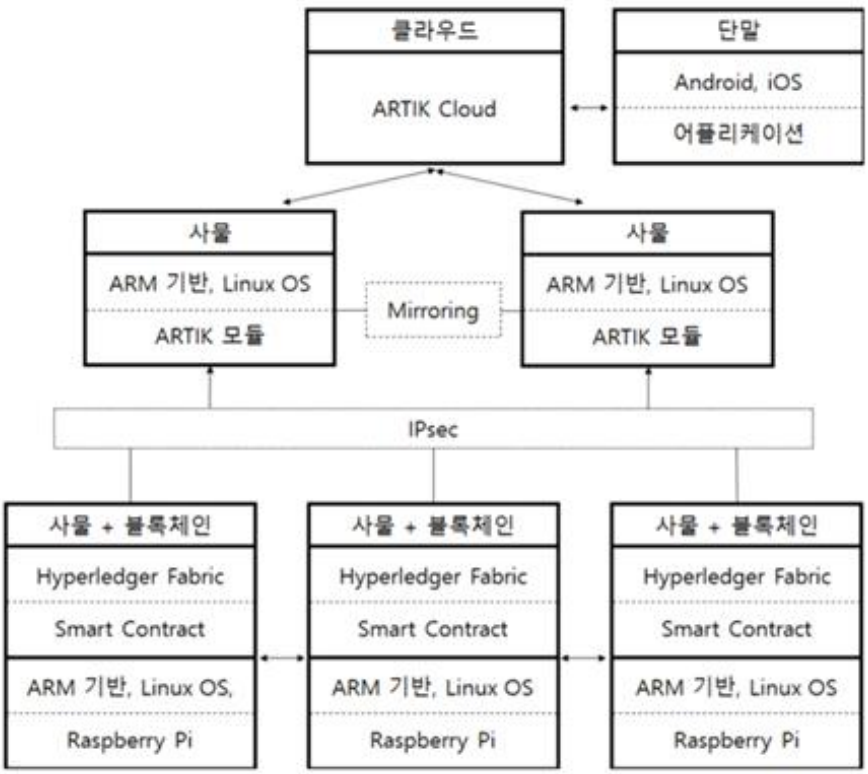
본 기획은 블록체인을 활용한 스마트홈 네트워크를 구성하여 위 문제를 해결하기 위해 IBM Hyperledger Fabric 플랫폼과 IoT의 빠른 처리를 위해 PoW와 PoS 보다 트래픽이 적은 Fabric의 KAFKA 합의 알고리즘을 선택하였다. 또한 Composer에서 생성된 ID를 통해 네트워크 접근 권한을 얻는 Hyperledger 특성을 사용하여 비인가 Device 문제를 해결하고 각 IoT Device들은 각각 Hyperledger의 Node로서 P2P로 참여하며, 각 Device State값을 공유하는 형태의 블록체인을 구성한다. 각각의 Device들은 서로의 State값을 스마트 컨트랙트의 체인코드를 통해 저장해두는 방식으로, 만약 State가 외부의 침입에 의해 조작된다면 KAFKA 컨센서스 알고리즘을 통해 노드 각각에 저장된 데이터를 대조하며 조작을 방지할 수 있다. 또한 각 홈 네트워크를 구성하는 IoT Device들은 ARTIK과 IPsec을 통해 안전하게 연결되어있다. ARTIK은 강력한 보안기능을 가지고 있기 때문에, 홈 네트워크의 미들웨어 역할을 하며, 외부 Device(Android 등)와의 상호작용을 위해 클라우드와의 소통이 필요할 시 ARTIK Cloud을 사용하여 안전한 상호작용이 가능하도록 하였다. 또한 미들웨어로 사용되는 ARTIK도 2대를 사용하여 미러링을 통해 분산, 이중화하였다.

2. 개발 목표 및 내용

2-1. 서비스 아이디어의 구현을 위한 개발 내용, 범위, 성능, 품질 등의 개발 목표

다수의 Raspberry Pi를 Node로 구성하여 Hyperledger Fabric를 사용한 Private Network를 구성하고 Go 언어를 이용하여 State 정보를 실시간으로 공유할 수 있도록 Smart Contract를 작성 외부에 의한 조작을 방지한다. 또한 ARTIK과 Raspberry Pi 노드 사이를 IPSec을 사용한 패킷 통신을 통해 안전하게 연결하여 ARTIK이 미들웨어로서 작동하도록 한다. ARTIK은 외부 Device(Android 등)과 상호작용해야 할 경우, 직접 통신이 아닌 보안성이 강조된 Cloud인 ARTIK Cloud를 통해 간접적으로 연결되도록 하여, 보다 안전하게 상호작용이 가능하다. 또한 ARTIK 모듈의 중앙화를 막기 위해, ARTIK 모듈 2대가 서로 Mirroring 하도록 네트워크를 구성하여 분산화 / 이중화하였다. Fabric의 Lightweight 합의 방식과 빠른 TPS를 이용하여 State 정보의 실시간 공유가 가능하도록 하고, 최종적으론 외부 해킹과 조작이 불가능한 스마트홈 네트워크 구성을 목표로 한다.

2-2. 서비스 아이디어의 시스템 구성 및 구조(도)의 환경 설명



본 서비스 아이디어는 다수의 Raspberry Pi와 2대의 ARTIK 모듈로 구성되었다. Raspberry Pi 다수는 Hyperledger Fabric을 통한 Private Blockchain의 노드로서 이용되며 ARTIK 모듈 2대는 Mirroring하며 미들웨어로서의 기능을 한다. 미들웨어와 Blockchain의 노드들은 IPsec 통신을 통해 명령 또는 정보를 주고 받는다. 또한, 미들웨어의 ARTIK은 ARTIK Cloud와 연결되어 Cloud에 등록된 단말기에 의해서만 ARTIK Cloud를 통해 명령을 전달한다.

3. 주요 특징 및 핵심 기술

3-1. 서비스 아이디어 구현 시 IoT 디바이스의 활용 방법 설명

Raspberry Pi는 Hyperledger Fabric의 노드로서 이용되며 각 노드는 Private Blockchain Network에 포함되어 있는 모든 노드들의 State 정보를 갖고 있으며 소유하고 있는 State 정보와 실제 Device의 State를 비교하고 달라지게 되면 합의에 의해 단말기에 상태 이상 알람을 전달한다.

ARTIK은 자체적으로 강력한 보안 기능을 가지며 ARTIK Cloud와의 연계를 통해 보안이 강화된 통신이 가능하기 때문에 가장 중요한 미들웨어로서 동작한다.

ARTIK과 Raspberry Pi 사이의 통신은 보안성을 위해 IPSEC을 사용하여 진행되며미들웨어로 동작하는 ARTIK 모듈은 또 다른 ARTIK 모듈에 Mirroring 시켜 미들웨어에 문제가 발생했을 경우 데이터의 손실을 막고 문제가 해결된 후에 데이터를 손쉽게 복구할 수 있다.

3-2. 서비스 아이디어 구현 시 블록체인 기술의 활용 방법 설명

본 팀에서 제시하는 서비스 아이디어에서는 Permissioned blockchain이라고도 불리는 Private Blockchain인 Hyperledger Fabric을 활용한다. Private Blockchain은 해당 Blockchain Netwrok에 들어가기 위해서는 네트워크 상에서 만든 인증방식을 통해서 검증된 노드만이 Private Blockchain에 참여할 수 있다. 본 팀은 Private Blockchain의 이러한 특성을 활용하여 비인가 Device의 접근을 막는다. 또한, 모든 노드가 각 노드의 State 정보를 갖고 있기 때문에 비정상적인 접근에 의한 Device State 변경을 감지하고 KAFKA 합의 알고리즘에 의해 이를 검증하여 ARTIK Cloud에 등록되어 있는 단말기에 알린다.

3-3. 서비스 아이디어의 정보보호 핵심 기능 및 사용할 기술 설명

본 기획에서는 블록체인의 특성을 적용하여 Device의 State 조작을 방지할 수 있으며, 탈중앙화를 통해 보안을 강화할 수 있다.

하지만 이더리움과 같은 Public Blockchain은 합의 과정에서 엄청난 컴퓨팅 파워를 소모하기 때문에 IoT 환경과는 부합하지 않는다. 또, TPS가 Private Blockchain에 비해 상대적으로 낮기 때문에 정상적인 서비스가 어려울 수 있으며, 실시간 감시가 필요할 경우 연산량에 따라서 네트워크 수수료인 Gas를 내야하기 때문에 적합하지 않다. 본 기획안에서 채택한 플랫폼인 Hyperledger Fabric은 Private Blockchain으로, Ethereum 등의 Public Blockchain과 달리 Composer를 통해 인가받은 Device만 네트워크에 참여할 수 있어, 비인가 Device를 참여를 방지할 수 있다. 또한 PoS/PoW 등의 합의알고리즘보다 연산량이 적고 빠른 Kafka 합의 알고리즘을 사용하여 IoT Device에 부하를 줄이고 빠른 작업 처리가 뿐만 아니라, 개별 트랜잭션을 모두 인증서를 통해서 검증하기 때문에 보안성에 강점을 갖고 있다.

또한 통신의 경우 IoT Device와 ARTIK 간 통신에 IPsec을 이용하여 패킷 통신에서 일어날 수 있는 보안 문제를 해결하였다. 외부 Device(Android 등)과의 상호작용의 경우 보안성이 뛰어난 HIPAA - Compliant Cloud인 ARTIK Cloud를 사용하고 ARTIK Cloud의 Authentication API를 이용 보안성을 높인다.

4. 비즈니스 활용

4-1. 서비스 아이디어 적용이 가능한 산업 분야, 비즈니스 모델, 운영 시나리오

스마트 홈 시큐리티 분야

기존 제품 사용자들을 대상으로 블록체인을 통한 보안 솔루션을 ARTIK 과 ARTIK Cloud를 통해 기존 제품에 보안성을 추가하는 방식의 비즈니스 모델을 제시한다. 특히 삼성의 SmartThings는 이미 ARTIK과 ARTIK Cloud를 통합하여 제공하고, SKT의 SmartHome아파트도 SmartHome App과 Server를 제공하기 때문에 보다 쉽게 우리의 솔루션을 도입하여 보안성을 향상시킬 수 있을 것이라 생각한다.

시큐어 스마트 홈 분야

블록체인을 통한 보안 솔루션을 ARTIK과 ARTIK Cloud를 통해 보안성이 추가되어 생산하는 시큐어 스마트 홈 방식의 비즈니스 모델을 제시한다. 고객은 제품의 편의성과 활용성만큼 보안성 역시 매우 중요하게 생각하기 때문에 다수의 고객의 선택을 받을 수 있을 것이라 생각한다.

IoT 제품 모든 분야

IoT 표준화 단체인 Open Connectivity Foundation가 다양한 Device와의 연동 서비스를 강화하며 개방형 생태계 구축을 위해 만든 OCF 규격에 보안부문 가이드 라인을 제시하여 앞으로 출시되는 IoT 제품 모든 분야에 적용 가능할 것이라 생각한다. 이 경우 단기적인 경제적 이익보다는 IoT 생태계에 공헌함으로써 기업에 신뢰도를 높여 장기적인 경제적 이익을 추구할 수 있을 것이라 생각한다.

4-2. 4-1에서 제시한 산업 분야에서의 경쟁자 및 경쟁자 대비 차별점

LG 스마트 홈

LG 전자는 삼성 전자와 더불어 스마트 홈 업계에서 활발한 활동을 보이고 있다. 그러나 얼마 전 SmartThinQ Device에서 발견된 홈핵을 이용하여 LG 계정에 대한 제어권이 확보되면 공격자가 모든 LG Device 및 Appliance 의 제어권을 가지는 보안 취약점이 발견됐다. 이 공격은 로봇 진공 청소기의 카메라로 자택의 활동을 엿보는 프라이버시 침해라거나 스마트 가스의 밸브를 열어 생명을 위협할 수 있는 등의 심각한 문제를 초래할 수 있다. 그러나 우리가 제안하는 블록체인 위에서 통신하는 스마트 홈은 이러한 보안 문제를 개선하였기 때문에 개인의 프라이버시를 중요시 여기고 각종 위협으로부터 안전하고 싶은 고객들의 선택을 받을 수 있을 것이다.

펜타 시큐리티

펜타 시큐리티는 지난 십 수 년 동안 수행한 데이터를 바탕으로 기업별 맞춤형 보안환경을 구축함으로써 데이터 조작 및 무결성 훼손을 방지한다고 광고하지만 조작 및 무결성 훼손 방지 분야는 블록체인을 통해 해결하는 것이 보다 확실한 방법이라고 생각한다. 지향하고자 하는 최종 목표는 같지만 수행 방식에 있어서 과거의 경험이 아닌 보다 진보된 블록체인 기술을 활용하는 것이 차별점이다.

5. 팀관리 및 일정

5-1. 팀원 별 역할, 수행내용

이대화 : 기획자, 프로젝트 매니저, 블록체인 및 IoT 보안 연구, 블록체인 개발

하현수 : 개발자, 블록체인 및 스마트 컨트랙트 개발, IoT 개발

정구익 : 개발자, 디자이너, 블록체인 및 스마트 컨트랙트 개발, IoT 개발

5-2. 최종 결과물 완성까지의 개발방법 및 개발 일정

개발 방법은 애자일 방식과 워터폴 방식을 결합하여 사용한다.

기획 - 설계 - 검증 - 적용 - 완료 순서의 큰 방향성은 워터폴 방식을 적용하여 방향성을 확실히 하고, 이 중 가장 중요한 설계 - 검증 - 적용 단계는 기능별로 애자일 방식을 적용하여 빠른 피드백 및 기능별 완벽성을 목표로 한다.

특히 핵심 작업인 ARTIK - ARTIK Cloud - Raspberry Pi 와 Hyperledger Fabric 연계는 크리티컬 패스로 관리하여 지속적으로 전 기간에 걸쳐 연구 및 개발할 예정이다.

	~ 05.14	~ 05.19	~ 05.24	~ 05.29	~ 06.03
문제점 및 솔루션 도출	◎				
Raspberry Pi를 통한 Hyperledger Fabric Blockchain Network 개발		◎	◎		
ARTIK과 ARTIK Cloud 간 통신 환경 구축			◎	◎	
Raspberry Pi와 ARTIK 간 IPSEC 통신 환경 개발			◎	◎	
스마트 컨트랙트 작성				◎	◎
보고서 작성 및 결과 보고	◎	◎	◎	◎	◎

향후 작업으로 타 솔루션과 성능을 비교하여 블록체인과 ARTIK이 IoT 환경에서 보안적으로 얼마나 더 효과적인지 검증해보고 싶고 실제 이 아이디어가 시장에 관심을 받을 수 있는 단계까지 프로토타입이 만들어지면 여러곳으로부터 피드백을 반영하여 더 발전시키고 싶다. 또한 오픈소스로 프로젝트를 전환하여 더 많은 사람들이 기술을 활용하여 IoT 와 Blockchain 생태계에 공헌하길 바란다.