특집 02

블록체인 기반의 IoT 보안 취약점

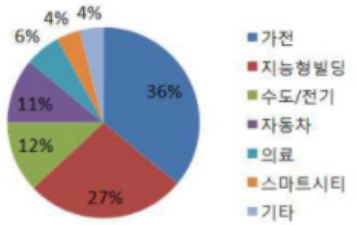
박현정·양혜임·전정훈 (동덕여자대학교)

목차

1. 서 론
2. 블록체인과 IoT의 동향과 취약점
3. 대응 기술
4. 결론 및 향후 전망

1. 서 론

최근 시장조사기관 가트너(gartner)에서는 2017년 세계 IoT(internet of things) 기기가 84억대에 달할 것이라고 예상하였다[1]. 이런 전망에 힘입어 금년 미래창조과학부는 블록체인과 IoT분야에 총 40억 원을 투자하고, 대학IT연구센터 신규 지원을 하는 등 여러 정책을 선보이고 있다[2]. 뿐만 아니라 Machina Research의 2011년도 자료에 따르면 2020년에 분야별 IoT 기기의 수는 (그림 1)과 같이 가전, 지능형 빌딩 등 다양한 분야로 확대 적용 될 것으로 기대된다[3].



(그림 1) 분야별 IoT 연결 수(2020)

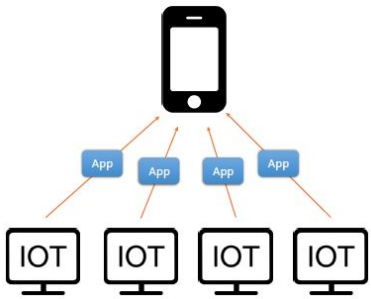
이에 따라 IoT 보안에 대한 관심 또한 높아지고 있으며, 여러 기업들이 블록체인 기술을 기반으로 IoT 기기의 보안성을 끌어올리기 위하여 노력하고 있다. 그러나 블록체인 기반의 IoT 기술을 개발할 때 각 기술의 특성이 결합하면서 새로운 취약점이 발생한다. 특히 IoT기기는 실생활과 밀접한 경우가 많기 때문에 기기의 취약점은 큰 문제로 이어질 수 있다. 따라서 블록체인과 IoT의 결합이 시너지 효과를 일으킬 수 있도록 취약점에 대한 보완방법이 필요한 실정이다. 그러므로 본 논문에서는 현재 각광받고 있는 IoT과 블록체인의 각 특성 및 보안 취약점뿐만 아니라 두 기술의 결합에 따른 문제점과 이러한 문제점을 해결하기 위한 대응 방안들을 알아본다. 먼저 2장에서는 기술의 보안 취약점들을 알아보고, 3장은 보완 기술, 4장에서는 결론으로 글을 마무리하도록 한다.

2. 블록체인과 IoT의 동향과 취약점

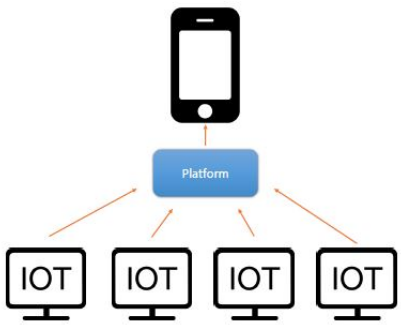
2.1 블록체인 기반 IoT의 기술 동향

2015년 초, 삼성은 IBM과 함께 블록체인(blockchain) 기반 IoT 플랫폼(platform) 어뎁트(ADEPT, Autonomous Decentralized Peer-to-Peer Telemetry)를 개발하였다. 이전의 IoT 환경은 (그림 2)처럼 각 IoT기기를 서로 다른 어플리케이션을 사용하여 제어하였다.

그러나 새롭게 개발된 IoT 플랫폼은 (그림 3)과 같이 여러 IoT기기와 핸드폰을 연결하여 사용자에게 편리한 환경을 제공한다. 여러 IoT 플랫폼들 중 어뎁트는 블록체인 아키텍처와 텔레해시 프로토콜, 비트토렌트 프로토콜 등을 결합하여 개발되었다[4]. IoT 플랫폼 외에도 스타트업 회사인 Ubirch가 2017 MWC에서 블록체인 기반의 IoT 기기를 개발하여 요트의 온·습도 값을 실시간으로 블록체인에 기록하는 등의 기술을 선보인 바 있다[5]. 이처럼 최근 블록체인 기반의 IoT에 대하여 다양한 연구가 진행되고 있는 상황이다.



(그림 2) 기존의 IoT 환경



(그림 3) Platform을 활용한 IoT 환경

2.2 블록체인 기술

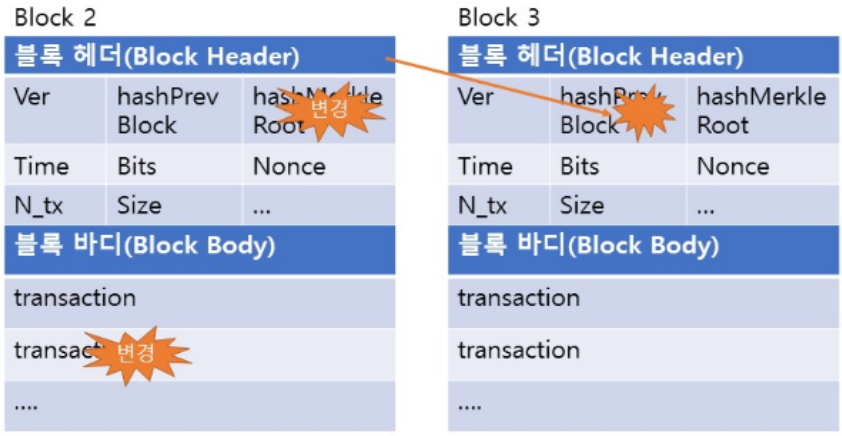
블록체인의 보안 취약점에 대해 언급하기 전에 우선 블록체인의 특징과 원리를 알아본다. 블록체인은 '공공 거래 장부'라고도 부르며 가상화폐로 거래할 때 발생할 수 있는 공격에 대응이 가능한 기술로 알려져 있다[6].

블록체인은 거래가 발생할 때마다 거래 내역을 서비스 참여자 모두에게 전송하고 전체 이용자가 보관하는 분산장부 형식을 띈다. 그리고 거래 내역은 (그림 4)와 같이 블록 형태로 저장되며 블록은 헤더(header)와 바디(body)로 이루어져 있다. 헤더는 버전, 이전 블록의 해시(hash), 페이로드(payload), 시간 등을 기록하고 바디에는 거래 정보 등 주요한 데이터를 저장한다. 블록이 생성될 때마다 기존의 블록에 이어 연결되

Block 1

블록 헤더(Block Header)		
Ver	hashPrev Block	hashMerkle Root
Time	Bits	Nonce
N_tx	Size	...
블록 바디(Block Body)		
transaction		
transaction		
....		

(그림 4) 블록의 구조



(그림 5) 블록 연결 에러 예시

고, 새로 추가되는 블록에는 앞 블록의 내용이 포함되므로 이전에 연결된 블록의 경우 수정이 불가능하다. 예를 들어 (그림 5)에서 Block2의 두 번째 트랜잭션이 누군가에 의해 변경되었다면 헤더에 있는 haskMerkleBlock 값은 블록 바디에 있는 트랜잭션들을 머클 해시(merklehash)한 값이므로 변경한 이는 hashMerkleBlock의 값도 변경해야 한다. 그러나 Block2의 헤더는 Block3의 hashPrevBlock값이 되기 때문에 Block2의 바디 내용을 변경하기 위해서는 Block2 이후 모든 블록을 수정해야 한다. 또한, 블록체인은 분산장부의 형식을 가지기 때문에 트랜잭션을 완벽하게 변경하기 위해 모든 서비스 사용자의 블록을 수정해야 한다. 그러나 이는 사실상 불가능하기 때문에 결과적으로 블록체인은 거래 내역에 대한 무결성을 유지할 수 있다. 이와 같은 특성에 의해 블록체인은 보안성이 높은 기술로 인정받고 있다.

2.3 IoT의 보안 취약점

본 절에서는 IoT의 특성에 의해 발생하는 취약점에 대해 알아본다. IoT는 각종 사물에 센서(sensor)와 통신 기능을 내장하여 인터넷에 연결하는 기술을 의미한다. 최근 IoT 기기의 수요가 늘면서 생활 속 깊은 곳까지 맞닿아 있게 되었다. 이와 같은 상황에서 2016년 2월, 전 세계 약 7만 3000여개의 CCTV가 해킹되어 실시간으로 인터넷상에 생중계 되는 사건이 발생하였다. 이 사건에서 해커는 직장과 학원, 헬스장, 음식점 등에 설치된 웹캠 영상을 관리자나 촬영 대상자의 동의 없이 인터넷상에 공개한바 있다[7]. IoT에는 사용자의 사생활에 깊게 관여하는 기기들이 다수 존재하고 있어, 개인정보가 유출될 경우 큰 피해가 발생한다. 또한 해킹 공격이 발생했을 때 일반 소비자가 피해를 즉시 알아채고 확인하는 것이 쉽지 않아 더욱 취약하며 IoT 기기 사이의 통신이 무선으로 이루어지므로 유선 통신 IT기기에 비해 연결이 안정적이지 않다. 또한, IoT 서비스에서 사용하는 통신 기술의 경우, 표준이 정해지지 않아 네트워크 구조가 복잡하게 형성되어 있어, 현재 이종 네트워크 간의 상호 연동 과정에서 일정 보안 수준을 유지하는 것이 어려운 실정이다[8]. 이 외에도 간단한 기능만 탑재된 IoT 단말의 경우, 자체의 성능이 좋지 않기 때문에

개별적인 보안 SW와 같은 고도의 보안 솔루션을 도입하기가 어렵고[8], 배포 및 설치 후에는 보안 패치 등의 업데이트가 사실상 불가능하거나 큰 비용이 수반된다는 취약점들을 포함하고 있다[9].

2.4 블록체인의 보안 취약점

앞서 언급한 바와 같이 블록체인은 보안 요소 중 하나인 무결성을 높게 보장하지만, 몇 가지 특징으로 인해 보안에 취약한 부분이 존재한다. 본 절에서는 그 중 3가지 취약점에 대해 알아본다.

첫째, 기본 블록체인의 경우 콘텐츠와 레코드 자체는 암호화하지 않거나 쉽게 해독할 수 있는 형태로 이루어져 있고, 분산 장부 형식으로 인해 거래에 참여한 모든 이가 블록의 내용을 볼 수 있게 된다. 따라서 해커가 거래 참여자 중 한명의 컴퓨터를 해킹하여 블록을 획득할 경우, 해커는 콘텐츠와 레코드의 내용을 쉽게 볼 수 있게 된다. 이때 해커가 블록의 주소 소유자를 알게 될 경우, 블록 생성자 정보를 추가로 획득하게 된다. 이는 기밀성을 유지할 수 없게 되는 취약점이 발생함을 의미한다[10]. 이와 같은 상황에서 블록에 개인정보가 저장되어 있을 경우 개인정보가 유출되는 상황이 발생한다. 따라서 현재의 블록체인은 콘텐츠가 유출되더라도 영향이 크지 않도록 사생활과 직접적으로 연관이 없는 데이터만 들어가야 한다는 단점이 존재한다.

둘째, 블록체인의 '수정 불가' 특징에 의해 취약점이 발생하게 된다. 앞서 언급한 바와 같이 블록체인에 연결된 블록은 수정이 불가능하다. 이러한 특징은 높은 보안성을 보장하지만, 오류나 실수에 의해 잘못 작성된 블록 또한 수정할 수 없다는 문제점을 가지고 있다. 잘못 작성된 블록들은 모든 참여자에게 전달되고 결과적으로 네트워크 전역에 잘못된 데이터가 저장되게 된다[11]. 수정 불가 특징에 의해 잘못된 트랜잭션 처리 등의 문제가 발생하게 된다.

마지막으로, 거래 검색의 속도가 저하되는 문제가 발생한다. 블록체인의 경우, 전체를 검증하기 위해서는 모든 블록이 필요하기 때문에 블록체인의 첫 노드부터 마지막 노드까지 모두 저장된다. 따라서 비트코인의 경우 현재 130GB의 블록체인이 누적되어 있고 월 평균 3.9GB의 증가율을 보이고 있으며[12], 거래가 지속되면서 블록체인의 크기는 계속 증가하고 있다. 이때 거래 내역을 확인하기 위해서는 전체 데이터 내에서 차례로 검색해야한다. 현재는 검색 기능에 문제가 발생하지 않았지만 블록의 양이 증가할수록 원하는 트랜잭션을 검색하는 속도가 저하될 것임을 쉽게 유추해 볼 수 있다. 이는 블록체인 사용에 있어서 가용성이 떨어지는 취약점이 발생함을 의미한다.

앞서 언급한바와 같이 블록체인은 위·변조가 불가능하기 때문에 높은 무결성을 가지고 있지만 데이터의 암호화를 제공하지 않아 기밀성이 결여되어 있고, 저장 공간 부족 문제에 의해 가용성이 저하되는 취약점을 가지고 있다. 이밖에도 데이터 수정의 어려움과 같은 부분으로 인해 기술이 다양한 분야에 적용되지 못하고 있다.

2.5 블록체인 기반의 IoT 보안 취약점

최근 글로벌 기업들은 블록체인 기술을 IoT를 비롯한 여러 산업분야에 보안성을 향상시킬 목적으로 활용하는데 노력을 기울이고 있다. 따라서 본 절에서는 기술 적용 시 고려되어야 할 보안 취약점들을 알아본다. 블록체인을 기반으로 하는 IoT 기기의 경우, 기기는 레코드 내용을 블록의 바디 내부에 저장한다. 앞서 2.2절에서 언

급되었던 블록체인의 취약점에 따르면, 블록체인 특성상 IoT 기기에서 받아온 사용자의 사생활 정보들은 암호화를 전혀 하지 않고 블록 내부에 들어간다. 추가적인 보안 솔루션을 도입하려 해도 IoT 기기 자체의 성능이 좋지 않을 뿐만 아니라 비용적인 측면에서도 많은 오버헤드가 발생한다. 이러한 이유로 인해 해커가 블록을 탈취한다면 손쉽게 사용자에 대한 정보를 얻을 수 있게 된다. 또한, IoT 기기는 불안정한 네트워크 환경을 가지고 있어 통신을 하여 받아오는 값이 정확하다는 보장을 하기 어렵다. 2.3절에서 언급했듯이 IoT 기기는 저성능일 뿐만 아니라 통신 기술 표준 부재와 같은 문제가 있기 때문이다. 그러나 블록 체이닝 이후 데이터의 오류를 발견한다면 블록체인의 특성에 따라 실수를 되돌리는 것은 불가능하다. 해커는 이 점을 이용하여 복잡한 네트워크 구조를 통해 기기에 접근한 뒤 악의적으로 기존의 값과 다른 값을 줄 수 있으며, 사용자는 해킹 당한 사실을 알게 되더라도 이미 잘못 생성된 정보를 변경할 수 없게 된다. 이 외에도 IoT 기기의 데이터 검색 성능 부족에 대한 단점이 존재한다. IoT 기기 내부의 컴퓨터는 최소의 비용으로 필요한 연산만 수행하기 때문에 블록체인 내부의 데이터를 검색하려 할 경우 검색 속도가 매우 느리거나 검색이 사실상 불가능할 수도 있다. 그러나 블록체인 기술을 IoT와 결합할 경우, 사용자는 IoT기기의 센서가 측정한 데이터를 확인할 수 있어야 하기 때문에 이에 대한 해결책이 필요하다. 결과적으로 블록체인 기술을 IoT분야에 적용할 경우, 앞서 언급한 보안 취약점으로 인한 문제가 발생할 뿐만 아니라, 보안 취약점들과 연관된 복합적인 취약점들이 발생할 가능성이 있다.

3. 대응 기술

3.1 블록 암호화

개인정보 유출의 경우, 블록체인 내의 데이터에 대한 보안성을 철저하게 유지해야 한다. 기존의 블록체인은 헤더 부분만 해시하여 저장하고 바디 부분은 정보를 그대로 저장한다. 그런데, IoT기기의 경우 기기 특성에 따라 데이터에 개인정보가 입력될 수밖에 없으므로 보안 위험을 방지하기 위하여 내부의 데이터 또한 암호화가 필요하다. 이와 같은 점을 보완하기 위하여 스타트업 기업 Ubirch는 데이터를 블록에 기록할 때 독자적인 공개 키 암호 방식을 사용하여 각 IoT 센서들이 Ubirch로 데이터를 보낼 때 발생할 수 있는 해킹의 위협을 차단하였다. 그러나 위 문단에서 언급한 내용을 제외하면 블록체인 암호화에 대한 연구는 미흡한 실정이다. 블록체인은 높은 무결성을 갖지만 기밀성은 제공하지 않기 때문이다. 보통 IoT 기기의 보안성을 강화하는 경우 MQTT와 SSL/TLS를 사용하는데[13], SSL/TLS는 대칭키 암호화 방식을 채택하여 기밀성을 보장할 뿐만 아니라 해시 알고리즘을 사용하여 무결성 또한 보장한다. 따라서 블록체인 기반 IoT기기를 상용화하기 위해서는 블록 바디의 콘텐츠를 암호화하여 기밀성을 보장하는 방안에 대해 더 많은 연구가 필요하다.

3.2 데이터의 신뢰성 보장

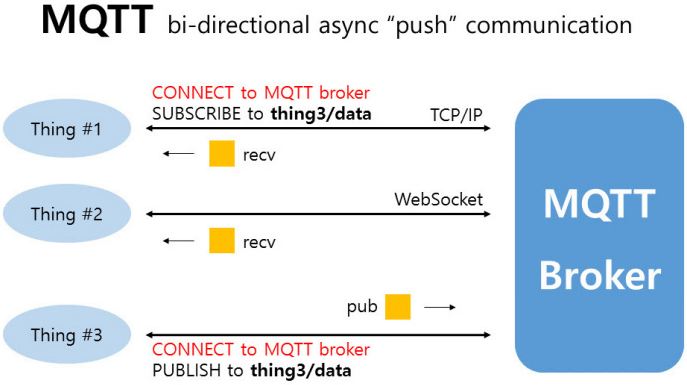
블록체인에 오류 또는 변조된 데이터가 들어가는 경우를 방지하기 위해서 데이터는 반드시 신뢰성이 보장되어야 한다. 원본 데이터가 변경되거나 소실되는 것을 막기 위하여 TCP 환경을 제공하는 IoT 프로토콜을 사용한다. 연결지향성

프로토콜을 이용하여 통신한다면 전송 도중 발생할 수 있는 오류를 확인하고 수정할 수 있다. 그러나 현재 IoT의 '저 전력', '저성능', '저가형' 등의 특성에 의해 모든 프로토콜이 TCP 환경을 제공하지는 않는다. 따라서 현재 존재하는 여러 IoT 프로토콜 중 (그림 6)의 MQTT와 같은 프로토콜의 사용이 필요하다.

MQTT는 (그림 6)에서 볼 수 있듯 토픽을 발행하는 기기(Thing #3)와 토픽을 구독하는 기기(Thing #1)들이 MQTT Broker에 연결되어 통신을 하게 되는데, 이때 통신이 TCP/IP환경에서 실행되어 전송 중 데이터에 발생한 오류를 발견하게 된다. 또한, IoT기기에 여러 개의 센서를 부착해 각 센서가 기기의 상태에 대해 정확한 데이터를 생성하고 있는지 판단하도록 하여 데이터의 신뢰성을 보장할 수 있다. 즉, 같은 행동을 하는 여러 개의 센서를 부착하여 그 센서들의 값이 모두 같은지 확인하도록 하는 것이다. 그 예로 농기계 업체 존 디어(John Deere)의 제품인 이그제트이머지(ExactEmerge) 플랜터(파종하는 트랙터 뒤에서 땅을 다지는 기계)에는 얼마나 많은 씨를 얼마나 빠른 속도로 파종했는지 측정하는 3개의 센서가 존재한다. 이 센서들을 통해 기기는 스스로 제대로 작동하고 있는지 감지하게 된다[14]. 앞에서 언급한 방법을 통해 데이터를 한번 검증한 뒤에 블록체인에 저장한다면 그렇지 않은 경우에 비해 데이터의 신뢰성이 크게 증가한다.

3.3 블록 사이즈의 확장

블록체인은 거래가 승인되거나 원본 데이터가 갱신될 때마다 블록이 추가되기 때문에 블록의 양이 지속적으로 증가하며, 블록 바디의 내용 검색 시 생성된 블록의 전수 검사가 필요하다는 특징을 지닌다. 그러나 IoT 환경의 경우 '저 전력', '저성능'의 특징을 가지고 있기 때문에 블록체인을 활용한 IoT기기에서 성능 및 저장 공간의 부족으로 인하여 메모리에 대한 오버헤드가 발생할 뿐만 아니라 실시간으로 데이터를 확인하지 못하는 가용성 문제점이 발생하게 된다. 따라서 IoT 기기의 보안에 블록체인을 사용하기 위해서는 대표적으로 블록 자체의 사이즈를 확장하는 방법이 있다. 이 방법은 블록이 생성되는 개수가 줄어들어 검색 시간도 짧아지기 때문에 가용성 문제의 해결책이 될 수 있다. 블록 사이즈의 확장은 실제로 논의되고 있는데, 2017년 8월 블록체인을 활용한 비트코인이 부상하면서 세계에서 발생하는 거래량이 크게 증가하여 당시 블록 크



(그림 6) MQTT 프로토콜의 전송 방식

기로 감당할 수 없는 상황이 발생하였다. 이에 비트코인 측은 블록 사이즈 확장에 대해 검토하고 있다[15]. 언급한 해결방법을 채택할 경우 블록의 총 개수가 적어지게 되어 거래 정보 검색 시간 감소에 긍정적인 영향을 주게 된다. 다음으로 최근 새롭게 적용된 방법인 세그윗(segwit)을 이용해 검색 속도를 증가시킬 수 있다. 세그윗은 블록의 트랜잭션에 존재하는 전자서명을 위한 공간을 제거하여 한 블록에 더 많은 트랜잭션을 저장할 수 있도록 하는 기능이다. 이 기능을 사용할 경우, 블록의 크기를 증가시킨 것과 같은 효과를 주게 되므로 검색 속도 저하 및 용량 부족의 해결책이 될 수 있다[16]. 따라서 본 절의 방법을 고려한다면 '저 성능'의 IoT 기기에서도 블록체인 기술을 충분히 사용할 수 있을 것으로 기대된다.

3.4 기술의 표준화

현재 블록체인과 IoT 기술에는 공통 표준이 없는 상태이다. 따라서 각 기업들은 두 기술을 기반으로 하는 아이템을 독자적으로 개발하고 있다. 그러나 이와 같은 현상이 지속된다면 각 산업의 발전에 부정적인 영향을 미칠 수 있다. 이에 따라 블록체인의 표준화를 위하여 2015년 9월 70개 이상의 금융 기관으로 이루어진 세계 최대의 블록체인 컨소시엄 'R3CEV'가 결성되었고[17], 작년부터는 W3C Blockchain CG과 ISO TC 307에서 블록체인의 국제표준화가 시작되었다[18]. 현재는 아마존, 마이크로소프트 등 큰 기업들이 블록체인 기술에 큰 관심을 가지고 독자적인 시스템을 개발하고 있다[19]. 또한, IoT의 경우에도 현재 오픈 커넥티비티 재단과 오픈 인터커넥트 컨소시움이 표준을 정하기 위하여 노력하고 있으며, IEEE의 IEEE p2413 표준 또한 IoT 아키텍처 정의를 위한 통합적인 방법론을 제공할 것으로 기대된다[20]. 이와 같이 IoT와 블록체인 영역에서 표준이 명확하게 정해진다면 현재 금융권에만 한정되게 이용되고 있는 블록체인 기술과 생활 곳곳의 IoT 기기를 안정적으로 접목할 수 있게 될 것이며, 블록체인을 기반으로 한 IoT 기술이 시장에 더 빠르게 자리 잡게 될 것이다.

4. 결론 및 향후 전망

최근 IoT 기기의 수요가 늘어남에 따라 이에 따른 보안 위협이 대두되고 있는 가운데, '합의 수렴 알고리즘'을 기반으로 하는 블록체인 아키텍처가 무결성을 강력하게 보장하는 새로운 기술로 제안되고 있다. 이와 같은 상황을 바탕으로 많은 기업들이 IoT 기기의 보안성 향상을 위해 블록체인 기반의 IoT 기술에 투자하고 있다. 그러나 더 높은 수준의 보안을 위해 IoT와 블록체인 기술이 결합될 때 발생할 수 있는 취약점에 대한 논의가 필요하다. 따라서 본 논문에서는 새로운 기술로 각광받고 있는 블록체인을 IoT에 적용시키며 특히 문제가 될 수 있는 세 가지 취약점과, 이에 대응할 수 있는 세 가지 방법을 제시하였고, 위 내용에서 현재의 블록체인 기술이 IoT 보안을 담당하기에는 기밀성, 가용성의 부족과 같은 취약부분들이 나타나고 있음을 알 수 있었다.

결과적으로 블록체인을 IoT 보안에 활용하기 위해서는 개인정보 유출 위험성, 데이터 오류의 위험성, 스토리지 부족 문제 등과 같은 취약점에 대해 좀 더 많은 연구가 필요하며, 향후 이와 같은 연구가 지속적이고 구체적으로 이뤄진다면, 블록체인을 기반으로 한 IoT 산업은 아주 빠르

고도 안전하게 성장하여 4차 산업혁명의 기폭제가 될 것으로 기대한다.

참 고 문 헌

[1] Rob van der Meulen, “Gartner Says 8.4 Billion Connected ‘Things’ Will Be in Use in 2017, Up 31 Percent From 2016,” Gartner, 2017.

[2] 김현아, “블록체인, 보안 넘어 IoT 인프라로..미래부, 올해 첫 30억 투자”, 이데일리, 2017.

[3] maru, “사물인터넷 가전관련 특허 아이디어, 신제품으로 속속 출시”, 디자인 로그, 2014.

[4] IBM ADEPT Practictioner Perspective - Pre Publication Draft - 7 Jan 2015, https://www.scribd.com/doc/252917347/IBM-ADEPT-Practictioner-Perspective-Pre-Publication-Draft-7-Jan-2015.

[5] Amy Nordrum, “Mobile World Congress 2017: Startup Ubirch Sails the Blockchain Into a New Application—IoT”, IEEE SPECTRUM, 2017.

[6] 이제영, “블록체인(Blockchain) 기술 동향과 시사점”, 동향과 이슈, 2017.

[7] 장우진, “IoT 보안 동향과 기술”, 공개SW포털, 2016.

[8] KISA, “사물인터넷 보안 위협 동향”, 2014

[9] 정용식, 차재상 “IoT 디바이스 보안 점검 기준”, 2017년 한국통신학회지(정보와통신) 34(2), pp 27-33.

[10] 박수민, 홍승필, “P2P 분산 네트워크 환경 내 프라이버시 및 정보보호 방안 - 블록체인 중심으로 -”, 보안공학연구논문지 Vol. 14 No. 2(2017), p170.

[11] 조수환, “사물 인터넷 데이터 무결성 보장을 위한 블록체인 기반의 합의 방법”, 고려대학교 컴퓨터학과 소프트웨어전공 석사학위논문, 2017년 7월, p17.

[12] 유소망, “Stateprune: reduce blockchain size by chainstate based block pruning”, 서강대학교 컴퓨터학과 공학석사 학위논문, 2016년 12월, p2.

[13] 정진희, 조대호, “무선 환경에서 SSL/TLS를 사용하는 IoT의 에너지 효율성 향상을 위한 기법”, 정보보호학회논문지 Vol. 26, No. 3 2016.06, pp 661-666.

[14] Stephen Lawson, “센서의 ‘벌레’, 저질 IoT 데이터로 일어나는 문제들”, CIO, 2016.

[15] 김흥록, “가상화폐, 패러다임 변화인가 신드롬일 뿐인가”, 서울경제, 2017.

[16] 이신철, “롤러코스터 탄 ‘비트코인·이더리움’...이거 대체 투자해야 돼, 말아야 돼?”, 이투데이, 2017.

[17] Stephen Lawson, “여전히 난장판일지라도... 2017년 IoT 표준 생태계 진단”, CIO, 2017.

[18] Jemima Kelly, “Exclusive: Blockchain platform developed by banks to be open-source”, REUTERS, 2016.

[19] 김영재, 김동호, “블록체인 표준화 동향 및 전략적 대응방안 연구”, 2017년 한국통신학회 하계종합학술발표회, pp 730-731.

[20] Bryan Gobin, “IBM Blockchain High security business network service plan”, 2016.

저 자 약 력

박 현 정

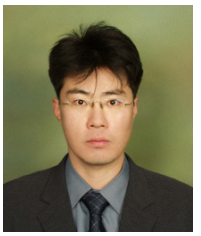
이메일 : lunar1123@naver.com

- 2014년~현재 동덕여자대학교 컴퓨터학과
- 관심분야 : 네트워크 보안, 시스템 보안

양 혜 임

이메일 : cheeezz_@naver.com

- 2015년~현재 동덕여자대학교 컴퓨터학과
- 관심분야 : 시스템 보안, 시스템 소프트웨어



전 정 훈

이메일 : nerdrandy@dongduk.ac.kr

- 2008년 2월 숭실대학교대학원 컴퓨터공학과 공학박사
- 2005년 3월~현재 동덕여자대학교 컴퓨터학과 부교수
- 관심분야: 정보보안, 네트워크 및 시스템 보안, 포렌식