Blockchain 기반 IoT 서비스의 보안 취약점 분석

저자
(Authors)

이보민, 강한솔, 유승하, 이영숙

출처
(Source)

Proceedings of KIIT Conference , 2018.11, 383-384(2 pages)

발행처
(Publisher)

한국정보기술학회
Korean Institute of Information Technology

URL

http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE07577989

APA Style

이보민, 강한솔, 유승하, 이영숙 (2018). Blockchain 기반 IoT 서비스의 보안 취약점 분석. Proceedings of KIIT Conference, 383-384

Blockchain 기반 IoT 서비스의 보안 취약점 분석

이보민(*), 강한솔(**), 유승하(***), 이영숙(****)
(*) 호원대학교 사이버보안학과, lbom_97@naver.com
(**) 호원대학교 사이버보안학과, rgt2982@naver.com
(***) 호원대학교 사이버보안학과, tmdgk6049@naver.com
(****) 호원대학교 사이버보안학과, ysooklee@gmail.com

요 약

블록체인은 데이터를 분산 저장하여 정보의 투명성과 신뢰성을 제공한다. 네트워크상의 기기들이 서로 통신을 하며 서비스를 제공하는 IoT 기술에서 보안성을 향상시킬 수 있는 기술로 주목 받고 있다. 최근 국내· 기업들은 블록체인 기반 IoT 기술 개발을 위한 컨소시엄을 구성하여 IoT 서비스에 활용할 수 있는 블록체인 기술들을 연구하고 있다. 본 논문에서는 IoT 서비스에 블록체인을 적용했을 때 발생할 수 있는 한계점과 보안 취약점에 대해 분석하고자 한다.

Key words

Blockchain, IoT, Smart Contracts, Certification.

1. 서론

2008년 10월 사토시 나카모토(Satoshi Nakamoto)라는 프로그래머에 의해 암호 화폐 중의 하나인 비트코인이 개발되었다. 비트코인을 개발하는 도중에 이중 지불 등의 취약점이 발견되었고 이를 해결하기 위해 제안된 기술이 블록체인(Blockchain)이다[1]. 블록체인은 Peer-to-Peer 방식의 분산원장 기술이다. 네트워크 내의 참여자가 데이터를 공동으로 소유하고 검증함으로써 거래 내역의 무결성 및 신뢰성을 확보할 수 있다.

최근 국내· 에서 IoT 서비스의 데이터 관리, 거래, 인증을 위한 목적으로 블록체인을 활용하고 있다[2]. 데이터 관리는 IoT 기기가 수집한 데이터를 저장하고 관리하는 것이다. 해시 값을 통한 데이터 감사와 접근권한 정책을 적용한 접근 통제가 이에 해당한다. 거래는 IoT 센서에서 수집된 데이터의 안전한 거래 환경을 제공하는 것을 의미한다. 인증 기술은 블록체인에 IoT 기기들의 인증키를 저장하여 등록과 갱신, 폐기 등의 키관리를 수행하거나 IoT 기기 간의 인증 시 검증하는 것을 말한다. 기존의 블록체인은 가상화폐 거래에 최적화되어 있기 때문에 IoT 서비스에 도입할 경우 문제점이 발생할 수 있다.

본 논문에서는 블록체인을 IoT 서비스에 적용했을 때의 한계점과 보안 취약점을 분석하고 결론을 맺는다.

2.블록체인을 적용한 IoT 서비스의 보안취약점

2.1 한계점

블록체인은 새로운 블록을 생성할 때마다 무결성을 보장하기 위해 이전에 생성된 모든 블록을 검사한다. 이러한 블록체인의 특징 때문에 사용자가 서비스를 이용할수록 블록이 계속해서 쌓이게 된다. 블록 검사시간이 길어지고 서비스 속도는 점점 느려지는 문제가 생긴다.

2.2 데이터 관리

IoT 서비스에 블록체인을 적용시키면 IoT 망의 보안은 눈에 띄게 좋아지지만 기기들의 보안과는 무관하다. 공격자가 보안 수준이 낮은 기기를 해킹하여 잘못된 데이터를 생성할 경우 이 데이터가 그대로 블록에 저장된다. 연결된

블록 내용은 수정을 못하기 때문에 IoT 서비스 사용자에게 잘못된 정보를 제공하게 된다. 블록체인으로 연결된 IoT 기기의 경우 IoT 서비스를 이용할수록 블록이 누적되기 때문에 IoT 기기에 저장하는 데이터 용량이 급증한다[3]. 이 데이터를 모든 노드에 복제하려면 IoT 기기의 용량 문제 뿐 아니라 네트워크 오버헤드가 발생한다. 이를 이용해 정상적인 데이터를 대량으로 누적시키면 IoT 서비스 제공 중 사용자가 원하는 데이터를 나타내려고 할 때 검색 속도가 저하될 수 있다.

2.3 거래

IoT 서비스에 거래 서비스를 적용한 경우 편리한 거래를 위해 스마트 계약을 활용하고 있는 추세이다. 스마트 계약은 스크립트 형태로 이루어져있다. 코드에 결함이 존재할 수 있으며 계약이 복잡할수록 오류가 발생할 가능성이 높다. 이를 악용할 경우 비정상적인 코드 실행을 일으켜 자산을 손실시키거나 개인정보를 침해할 수 있다. 실제 스마트 계약 코드에 존재했던 취약점으로 인해 2016년 750억 원 정도의 손해를 입었던 DAO 사건과 2017년 370억 원 가량 피해를 봤던 Parity 해킹 사건이 발생했다[4]. 또한 스마트 계약을 진행할 때 계약서는 스크립트로 전송된다. 안전성이 결여된 교환 환경일 경우 이 과정에서 스크립트가 훼손되거나 정보가 유출될 가능성이 있다.

2.4 인증

IoT 서비스에서 기기 간 인증은 복잡한 암호 알고리즘을 사용할 수 없다[5]. 이를 이용해 정보를 도청하거나 인증정보를 탈취할 경우 특정 기기를 사칭할 수 있다.

<표 1> 한계점 및 보안 취약점

구분	유형	주요 내용
한계점	누적되는 데이터	- 서비스를 이용할수록 블록이 누적됨 - 용량이 늘어나 속도가 느려짐
데이터 관리	보안수준 불일치	- IoT 기기들의 보안수준이 다 다름 - 보안수준이 낮은 기기를 통해 공격 받을 가능성이 높음
	네트워크 오버헤드	- 공격자가 대량의 데이터를 누적시킬 경우 정상적인 서비스 제공 불가능
거래	자산 손실	- 코드가 변조된 경우 금전적인 손해를 입을 수 있음
	개인정보 침해	- 스크립트 교환 환경이 안전하지 않으면 정보 유출 가능성이 있음
인증	합의 가로채기	- 참여자 중 다반수의 기기를 장악하면 네트워크에 접근 가능

블록체인을 적용할 경우 노드들의 정보를 합의하는 과정을 통해 네트워크에 연결된 기기들을 검증한다. 이 과정을 통해 신뢰성을 보장할 수 있지만 공격자가 참여한 노드 중 과반수의 기기를 장악할 경우 합의를 가로챌 수 있다[6]. 과반수의 동의로 네트워크 상 기기들에게 정상적인 기기로 인식될 경우 해당 네트워크의 접근 권한을 얻게 된다.

3. 결론

본 논문에서는 블록체인 기반 IoT 서비스의 한계점과 데이터 관리, 거래, 인증 세 가지의 항목에서 발생할 수 있는 보안 취약점에 대해 분석하였다. 향후 이와 같은 연구가 활발하게 이뤄진다면 블록체인을 적용한 IoT 서비스의 활용도가 증가될 것으로 기대된다.

참고 문헌

[1] 양재훈, "물류산업의 블록체인 적용효과와 법적 과제에 대한 연구", 융합정보논문지 (구 중소기업융합학회 논문지), Vol.8-1, pp.187-199, Feb 2018.

[2] 보안기술연구팀, "국내외 블록체인 기반 사물인터넷 동향", 금융보안원, June 2017.

[3] 홍은기, 이수진, and 서승현, "사물 인터넷을 위한 블록체인 기술 동향", 정보보호학회지, Vol.28-3, pp.38-46, June 2018.

[4] 김명수, and 임은진. "이더리움 스마트 계약 취약점 검출기", 한국정보과학회 학술발표논문집, pp.1940-1942, June 2018.

[5] 최대선, 옥도민, and 장대훈. "블록체인과 인증", 한국통신학회지 (정보와통신), Vol.35-7, pp.11-17, June 2018.

[6] 보안기술연구팀, "블록체인 기술과 보안 고려사항", 금융보안원, Aug 2017.