블록체인을 활용한 공공기관 정보시스템에서의 개인 정보 유출 방지 시스템 제안

최승주*, 박재훈*, 서화정**
*한성대학교 IT 융합공학과
bookingstore3@gmail.com, p9595jh@gmail.com, hawjeong84@gmail.com

A proposal of preventing the leakage of personal information from public institution information system using blockchain

Seung-Joo Choi*, Jae-hoon Park*, HwaJeong Seo**
*Dept. of IT Convergence Engineering, Hansung University

요 약

보건 복지부, 병원, 동사무소 등의 공공기관에서는 업무 처리를 위해 사람들의 주민등록번호, 연락처, 주소 등 수많은 개인정보를 업무 처리를 위해 각 기관마다 사용하는 정보 시스템을 통해 다룬다. 그런데 이러한 정보 시스템을 통한 내부 정보 유출 사건이 지속적으로 발생하고 있다. 이와 같이 유출된 정보는 단순 유출자의 호기심으로 끝나기도 하지만 다른 영리 기관들에 팔려 악용되기도 한다. 이에 본 논문은 정보 시스템을 통한 개인 정보 유출을 방지하기 위해 블록체인을 활용한 시스템을 제안한다.

1. 서 론

최근 잇따른 개인정보 유출 사건이 지속적으로 발생함에 따라 개인정보에 대한 사회적 관심이 증가하고 있다. 지난 10년간 국내에서 발생한 개인정보 유출 사례는 60억 건이 넘으며[1] 이러한 개인정보 유출이 발생되는 주된 경로 중 하나는 공공 기관에서 사용되는 정보 시스템이다[2].

정보 시스템은 각 부서에서 업무를 처리할 때 사용되는 시스템으로서 보건복지부와 같은 경우 사회보장 정보시스템을 사용하며 이를 통해 각종 복지 혜택을 제공할 때 정부부처나 지자체에서 심사목적 등으로 연람하는 통합 망을 사용하고 있으며 병원과 같은 경우 병원 정보 시스템을 통해 환자의 정보 및 신체에 대한 정보들을 공유하는 시스템을 사용하고 있다. 정보 시스템은 이름만 입력을 하면 해당 사람의 연락처, 주소 정보, 학력 정보, 건강 정보, 계좌 정보 및 상담 내역 등의 민감한 개인 정보를, 각 기관마다 사용되는 정보시스템에 따라 표시되는 정보의 차이는 있지만, 손쉽게 열람할 수 있다. 이처럼 공공기관에서 업무 처리를 진행할 수 있게 도와 국민들의 삶에 도움을 줘야하는 시스템이 오히려 공공기관 내부자에 의해 개인정보가 유출이 되는 주된 경로가 되고 있다.

이와 같은 개인정보 유출의 원인으로는 단순한 다른 사람의 상담 내역에 대한 호기심, 팬의 유명 연예인에 대한 호기심과 같이 단순 호기심과 같은 이유도 있지만 건강 관련 정보를 빼내어 해당 사람들에게 요양원 시설 등을 홍보하는 등 악용하기 위한 원인도 존재한다.

이와 같은 정보 시스템에 등록되어 있는 사람의 수는 천백만 명이 넘으며 이를 열람할 수 있는 공무원의 숫자는 약 3만 7천명임을 감안하였을 때 정보 통신을 통한 개인정보 유출은 심각한 문제이며 해결책이 반드시 필요하다. 이에 본 논문에서는 블록체인을 활용하여 개인정보 사용 시 해당하는 개인에게 허락 및 알람이 가며 조회 기록을 변조되지 않고 유지할 수 있기 위한 블록체인을 활용한 정보 시스템을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 블록체인 기반 개인 정보 보호 정보 시스템을 위한 블록체인, 스마트 컨트랙트 등 관련 연구에 대해 살펴보며, 3장에서는 본 논문에서 제안한 시스템에서 사용되는 스마트 컨트랙트의 알고리즘을 간략히 구현하여 실제 시스템을 재현한 결과를 살펴본다. 마지막으로 5장에서는 제안 시스템에 대한 분석과 향후 필요한 연구 과제에 대하여 논의하며 결론을 맺도록 한다.

2. 관련 연구

2.1 블록체인

블록체인이란 동일한 전자 장부에 대한 데이터를 네트워크에 참여하고 있는 노드들이 함께 공유하고 검증하는 네트워크 시스템이다. 블록체인에서 사용되는 전자 장부의 내용은 다수의 노드가 함께 공유하고 해당 장부 기록이 동일한지 검증하기 때문에 공유 장부에 적힌 내용을 하나의 노드가 단독으로 위조 및 변조하기 어렵다는 특징이 있다. 이와 같은 블록체인의 특징을 이용하여 가상 화폐 개념을 도입하여 제 3의 공인기관이나 중개자의 개입 없이 익명간의 거래

를 진행할 때 사용되기도 한다.

블록체인에서 사용되는 공유 전자 장부가 위조 되지 않을 수 있었던 이유는 그림 1과 같은 구조를 통해 장부 내용의 위변조를 방지하기 때문이다. 블록체인 상에 기록을 남기는 행위를 트랜잭션이라 하며 이러한 트랜잭션은 블록이라는 구조에 담겨 블록체인 네트워크에 기록이 된다. 이때 블록에는 트랜잭션의 내용과 함께 시간, 논스 값 그리고 이전에 생성되었던 블록의 해시 값 정보 등이 같이 저장이 된다. 해시 함수란 임의의 길이의 데이터를 고정된 길이의 데이터로 만들어주는 함수로서 하나의 데이터만 달라져도 완전 다른 결과의 데이터가 도출이 되기 때문에 무결성을 증명하기 위한 용도로 많이 사용이 된다. 블록체인에서는 이런 해시의 특징을 이용해 공유 장부의 무결성을 보장하기 위해 블록 간에 이전 블록 해시 값을 저장해 각 블록이 해시 값으로 연결된 형태를 구성한다.

이와 같은 블록은 네트워크 참여자 중 블록을 형성하고 형성한 대가로 소량의 가상 화폐와 수수료를 받는 체굴자(miner)에 의해 형성이 된다. 이때 네트워크 참여자 중 가장 많은 블록이 형성된 장부의 기록을 검증 과정을 통해 네트워크 공식 장부로 인정을 하게 되고 해당 기록을 바탕으로 다른 기록들을 무효화해 모두가 같은 기록을 갖는 공유 장부를 소유할 수 있게 만든다.

만약 악의적인 네트워크 참여자가 특정 블록의 데이터를 위조 및 변조를 하려고 시도했을 때 변조된 블록 이후의 모든 블록들에 대한 해시 값을 다시 연산을 하고 다른 네트워크 참여자보다 더 많은 블록을 형성해야한다. 그러나 이러한 전체 네트워크의 연산 능력의 절반을 넘는 연산 능력을 악의적인 참여자 한명 또는 소수의 그룹이 보유하는 것은 사실상 불가능하기 때문에 블록체인 공유 장부는 위조 및 변조에 대한 내성을 지닐 수 있게 된다.

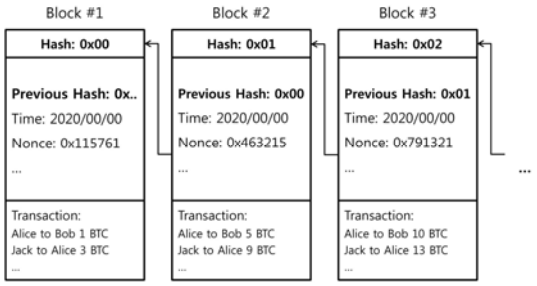

Fig. 1 Blockchain network's block structure

최초의 블록체인은 가명의 인물 사토시 나카모토가 2008년에 발표한 비트 코인[3]으로 공개형 블록체인 형태를 띠고 있다. 이는 해당 네트워크에 누구나 참여하고 싶은 주체는 누구나 참여할 수 있으며 누구나 블록을 형성하는 체굴자가 될 수 있는 구조이다. 그러나 최근에는 공개형 블록체인의 한계점[4]을 고려하여 기업형 또는 허가형 블록체인 형태도 출시되고 있다. 허가형 블록체인의 특징은 블록체인 네트워크에 참여할 수 있는 대상이 정해져있으며 해당 네트워크에 참여하기 위해서는 네트워크를 운영하고 있는 주체의 허락을 받아야 참여할 수 있다는 점이다. 허가형 블록체인의 특징을 블록 형성을 위한 컴퓨터 연산 과정을 투표 형식으로 대처하거나 블록 생성 시간을 단축하는 등 기업과 같이 블록체인 네트워크를 공개한 상태로 운영할 필요가 없는 기관에서 사용된다.

2.2 스마트 컨트랙트

스마트 컨트랙트는 디지털로 만들어진 계약서를 의미하며 1994년 최초로 제안되었다. 이와 같이 디지털 상으로 존재하는 스마트 컨트랙트는 작성된 계약 조건이 만족되면 3자의 개입 없이도 즉각 이행될 수 있으며 해당 이행에 대한 결과가 명확하게 도출된다는 특징을 갖고 있다. 이와 같은 무결성과 정확성의 특징을 갖고 있는 스마트 컨트랙트의 개념을 2세대 블록체인이라고 불리는 이더리움에서 최초로 블록체인 네트워크에 가져와 적용하였다[5].

이와 같은 스마트 컨트랙트를 통해 많은 탈중앙화 어플리케이션(DApp, Decentralized Application)이 제작이 되고 있으며 대표적인 공개형 블록체인인 이더리움 뿐만 아니라 기업형 블록체인인 하이퍼레저[6] 등 다른 여러 종류의 블록체인 네트워크에서도 많이 제작 및 배포가 되어 여러 서비스에서 사용이 되고 있다.

이와 같은 스마트 컨트랙트를 이용하여 본 논문에서는 정보 시스템을 통한 개인 정보 열람 시 처리되어야할 절차들 및 스마트 컨트랙트의 구조를 3장에서 제안한다.

3. 시스템 제안

개인 정보 유출이 발생해도 알기 어려운 것은 공공 기관에서 정보 시스템을 통해 해당 정보를 조회해도 일반적인 업무에 참조하는 자료로서 사용되기 때문에 별다른 조치가 이뤄지지 않기 때문이다. 조회를 위해서는 신청이 이뤄져야 하지만 해당 정보를 갖고 실제로 어디에 쓰였는지 등에 대한 처리는 이뤄지지 않고 있다.

이를 해결하기 위해서는 우선 개인 정보의 소유는 엄연히 개인에게 존재하기 때문에 이를 바탕으로 개인의 정보를 조회 시 해당 사람에게 그 사실을 알려주는 시스템을 정보시스템에 적용하는 것이 우선이다. 가장 좋은 방법은 공공 기관에서 개인 정보를 이용한 업무를 처리해야할 때 개인 정보 조회 민원뿐만 아니라 해당하는 개인에게 사용하는 때마다 동의를 구하는 것이다. 그러나 현실적으로 업무 처리에 있어 해당하는 사람이 연락이 되지 않을 수도 있으며 답변이 없다면 무한정 업무가 처리되지 않을 수 있기 때문이며 이는 시간적으로 너무 소요가 되는 방법이다. 하여 조회를 할 때마다 동의를 받지 않고 조회 사실과 조회 목록에 대한 알림을 해당 사용자에게 실시간으로 전송하는 할 것을 제안한다. 이와 유사한 시스템으로는 구글의 알림 서비스를 볼 수 있다. 구글에서는 다른 컴퓨터에서 계정에 대한 새로운 접근이 발생하면 접근을 시도한 아이피 주소와 시간대 그리고 해당 접근의 주체에 대한 질문을 이메일과 알림을

통해 계정 소유자에게 전달한다. 이와 마찬가지로 개인 정보에 대한 조회가 정보 시스템을 통해 일어날 때마다 어떠한 기관에서 어떤 개인 정보에 대한 조회가 일어났는지를 개인 정보 주체에게 알림을 보낼 것을 제안한다. 해당 시스템은 미리 작성된 스마트 컨트랙트를 통해 일어나며 순서는 다음과 같다.

먼저 개인 정보를 정보 시스템을 통해 조회하고자 하는 기관에서 조회하고자 하는 정보의 종류와 사유 그리고 기관명을 스마트 컨트랙트에 트랜잭션을 보내 요청한다. 그럼 해당하는 정보를 요청할 수 있는지 트랜잭션 요청자에 대한 권한을 검증하고 만약 권한이 있는 자라면 각 기관에서 해당 정보를 볼 수 있게 허락하는 권한을 가진 사람의 동의를 기다린다. 해당 동의가 일어나면 요청한 정보가 전송이 되며 이때 정보에 해당하는 개인에게 개인 정보 조회 사실이 앞서 말한 사유와 기관 등의 정보와 함께 알람이 전송된다.

제안하는 시스템에서 사용되는 스마트 컨트랙트 구조는 그림 2 와 같다.

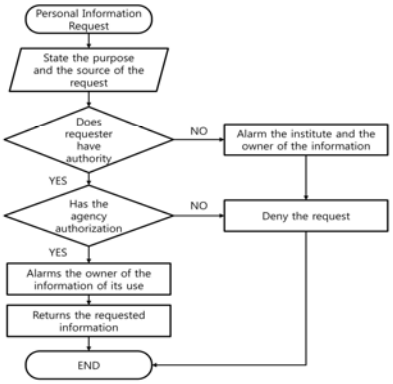

Fig. 2 Structure of Information system smart contract

기관에서 업무를 처리하기 위해 개인 정보 조회 요청을 블록체인에 등록되어 있는 스마트 컨트랙트에 요청을 보낸다. 이때 조회하고자 하는 정보에 대한 자세한 명세와 요청을 보낸 기관 등에 대한 구체적인 정보를 함께 전송한다. 해당 요청을 받은 스마트 컨트랙트에서는 요청을 보낸 사람이 개인 정보를 취급할 수 있는 인물로 스마트 컨트랙트에 등록이 되어있는 사람인지 확인을 한다. 만약 허가되지 않은 사람이라면 해당 기관과 개인 정보의 주인에게 해당 사실에 대한 알림을 전송하고 요청을 거부한다. 요청 권한이 있는 사람이라면 해당 요청에 대한 기관의 상부의 허가를 기다린다. 만약 상부에서 허가를 해 주지 않는다면 요청을 기각하며 이때는 알림을 보내지는 않는다. 허가가 난 경우 요청 정보의 주체에게 해당 개인 정보가 어느 기관에서 어떠한 목적으로 언제 조회가 되었는지 알림을 보내고 요청을 보냈던 사람에게 해당 개인 정보의 정보를 전송한다.

이와 같은 블록체인 네트워크는 각 기관의 정보 시스템을 통합하여 공개형 블록체인으로 구성하여 기록에 대한 조작을 각 기관에서 견제하여 정보의 무결성을 보장할 수 있다. 또한 개인 정보 조회에 대한 사실을 실시간으로 전달함으로서 개인 정보의 사용 사실을 명확히 할 수 있으며 만일 개인 정보가 불분명한 이유로 조회가 되면 바로 알 수가 있어 조치가 가능하다.

4. 시스템 구현

4.1 제안 기법 구현

본 논문에서 제안하는 기법을 구현하여 동작을 확인하였다. 구현은 이더리움에서 제작한 스마트 컨트랙트 언어 솔리디티(Solidity)를 사용했으며 개발 IDE는 리믹스(Remix) 환경을 사용하였다.

스마트 컨트랙트는 컨트랙트 배포자의 주소, 조회 권한이 있는 직원의 주소의 값을 저장하며 추가로 이름, 주민등록번호, 전화번호 그리고 집 주소에 대한 값을 배열로 저장하게 구현하였다. 이때 스마트 컨트랙트 배포자의 주소는 리믹스에서 임의로 생성한 주소 0xca3로 시작하는 주소를 사용했으며 직원의 주소는 0x147로 시작하는 주소 값을 지정하였다. 해당 값들을 이용해 구현한 결과는 그림 3과 4와 같다.

Fig. 3 Personal information request permitted

그림 3의 from, 즉 정보 요청을 보낸 주소를 보면 0x147, 즉 정보 시스템에 등록된 직원의 주소임을 알 수 있다. 해당 직원의 요청에 대한 허가가 나면 decoded output 부분을 보면 임의로 임력해 놓은 홍길동에 대한 이름, 주민등록번호, 전화번호 그리고 집 주소가 반환된 것을 알 수 있다. 또한 logs을 보면 개인 정보가 현재 허가 받은 직원으로부터 조회되고 있다는 로그가 성공적으로 뜬 것을 볼 수 있다.

Fig. 4 Personal information request denied

그림 4와 같은 경우 from, 즉 정보 요청을 보낸 주소를 보면 0x4b0으로 시작하는, 즉 정보 시스템에 등록되지 않은

주소로부터 개인 정보에 대한 조회 요청이 온 것을 볼 수 있다. 허가되지 않았기에 decoded output 부분을 보면 반환된 값이 없음을 알 수 있으며 logs에서 해당 개인 정보가 노출 되었으니 즉시 해당 기관에 연락을 취하라는 알람이 보내진 것을 볼 수 있다.

4.2 성능 평가

기존 정보 시스템과 같은 경우 접근 기록은 남지만 정보 주체에게 조회 사실이 알려지지는 않았고 이 때문에 개인 정보 유출에 대한 대응이 늦어질 수밖에 없었다. 그러나 본 논문에서 제안한 방식을 통하면 실시간으로 이러한 유출 사태를 알 수 있다 또한 각 개인 정보에 대한 관리는 각각의 기관에서 진행하였지만 본 논문에서 제안한 블록체인을 활용하면 정보에 대해 같이 공유하여 관리하기 때문에 저장된 정보들에 대한 무결성 또한 보장이 된다. 표 1에서 본 논문의 제안 기법과 기존 조회 기법의 비교를 정리한다.

Table 1. Comparison between conventional and proposed personal information referencing method

	Conventional	Proposed
Send notification to information owner	None	Real time
Manipulation possibility	Possible through internal operation	Impossible
Data integrity	Unverified	Verified by network

5. 결 론

본 논문에서는 블록체인의 스마트 컨트랙트를 활용하여 정보 시스템의 개인 정보 유출을 방지하는 시스템을 제안하였다. 개인 정보 주체에게 조회 사실이 전송되게 하는 구조를 통해 어떤 기관에서 무슨 사유로 인해 개인정보를 열람하는지 알 수 있는 구조를 제안하였다. 이를 통해 개인의 엄연한 자산인 개인 정보가 어디에서 사용되는지 실시간으로 알 수 있을 것으로 판단된다.

개인 정보 유출은 정보화시대가 가속화 되면서 앞으로 더욱 심각한 사건으로 받아들여져야 하는 요소이다. 그러나 개인 정보의 유출에 관한 불감증은 여전히 낮은 상태이다 [7]. 앞으로 개인 정보에 대한 보호는 기술적인 측면에서도 접근이 필요하지만 무엇보다 정보들의 주체가 개인 정보의 중요성을 인지하고 적극적으로 보호할 필요가 있을 것으로 보인다.

References

[1] The Radio News. “6 billion unathorized leaks of personal information over 10 years” [Internet]. Available: http://www.jeonpa.co.kr/news/articleView.html?idxno=59734

[2] United News, “Welfare officials continue to illegally access personal information”. [Internet], https://www.yna.co.kr/view/AKR20181010043300017

[3] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic ash System” metzdowd.com, Oct. 2009.

[4] Jae Young Lee, Cheong Won Woo, Prospects, “Limitations and Implications of Blockchain Technology”, FUTURE HORIZON, vol. 38, no. 4, Dec. 2018.

[5] Ethereum. A Next-Generation Smart Contract and Decentralized Application Platform [Internet]. Available: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf

[6] Hyperledger. An Introduction to Hyperledger [Internet]. Available: https://www.hyperledger.org/.

[7] United News. “Hana Tour penalty 30 million won, Personal information protection insensitivity” [Internet]. Available: https://www.yna.co.kr/view/AKR20180206100300004?input=1195m