코로나-19 역학조사를 위한 블록체인 기반 QR코드 전자출입명부 관리 시스템

한찬희*, 김문선**, 이만희***

*한남대학교(학부생), **한남대학교(대학원생), ***한남대학교(교수)

Hyperledger fabric-based QR code electronic access list management system for Corona-19 epidemiological investigation

Chan-Hee Han*, Moon-Sun Kim**, Man-Hee Lee***

*Hannam University(Undergraduate student),

**Hannam University(Graduate student), ***Hannam University(Professor)

요 약

최근 코로나-19로 인한 팬데믹 상황에 대응하기 위해 출입 명부 관리 시스템이 도입되었다. 해당 시스템은 초기에는 수기로 작성되어 허위 기재 및 개인 정보 유출로 인한 문제가 발생하였다. 향후 도입된 QR코드 기반 전자 출입 명부 시스템은 사용 방법이 상대적으로 복잡하고 중앙에서 모든 정보가 관리되기 때문에 출입 정보에 대한 보안성이 부족하다. 또한 번거로운 본인인증 과정을 거쳐야 하므로 사용성이 불편하다. 본 논문은 전자 출입 명부에 대한 보안성을 강화하고 사용 편의성을 개선한 블록체인 기반 전자 출입 명부 관리 시스템을 제안한다. 이 시스템은 별다른 인증 없이 휴대전화를 암호화한 정보를 바탕으로 개인을 식별하며, RSA 암호화를 바탕으로 개인정보 및 출입 기록을 체인 서버에 저장한다. 제안한 시스템은 기존 전자 출입 명부의 단점을 개선하였으며, 보다 효과적으로 코로나-19 역학조사에 기여할 수 있을 것으로 기대한다.

I. 서론

코로나-19사태가 장기화함에 따라 질병관리청에서는 확산 방지 및 방역을 위하여 카페, 식당, 공공시설 등 모든 다중 이용 시설은 출입 명부 작성 의무 시행하도록 공공시설 출입 명부 작성 시스템을 도입하였다. 하지만 수기로 작성하는 출입 명부는 누구든지 쉽게 열람할 수 있어, 개인 정보 유출의 가능성이 존재한다. 또한 일부 방문자의 허위정보 기재로 인해 확진자 발생 시 코로나-19 역학조사에 혼선을 야기하고 막대한 경제적인 피해가 발생한다[1][2].

이를 방지하기 위해 보건복지부는 QR코드를 통한 전자출입명부 기술을 구축했다. 이는 허위 기재 문제를 효과적으로 해결할 수 있지만, 본인인증 절차가 복잡하다[3]. 또한, 사회보장정보원의 중앙서버에 모든 데이터가 저장되는 문제점이 있다. 이는 데이터센터에 문제가 발생하면 출입 명부 기록이 모두 소실될 수 있는 위험성이 있으며, 코로나-19 역학조사가 불가능해지는 치명적 위험성을 가지고 있다[4].

본 논문은 이러한 문제점을 해결하기 위해 블록체인 기반 분산저장 전자 출입 명부 시스템을 제안한다. 이 시스템은 QR코드 생성 시, 본인인증 과정을 거치지 않으며 오직 전화번호와 출입 시각을 활용하여 QR코드를 생성한다. 생성한 QR코드는 중앙에서 제공하는 RAS 공개키로 암호화되어 체인 서버로 전송된다. 블록체인 서버는 허가형(private) 블록체인인 하이퍼레저 패브릭(hyperledger fabric)으로 구축하여 출입 기록을 더욱 안전하게 저장할 수 있다. 해당 시스템은 하이퍼레저 패브릭과 안드로이드 앱으로 실제 프로토타입이 구현되었다.

본 논문의 구성은 다음과 같다. 먼저 2장에

서는 체인 서버 구축을 하기 위한 블록체인 플랫폼으로 알려진 하이퍼레저 패브릭(Hyperledger fabric)과 관련 연구에 대해 살펴본다. 3장에서는 전체적인 시스템 구조에 관해 설명한 다음, 시스템의 프로토콜에 대하여 설명한다. 마지막 4장에서는 논문의 간단한 결론을 맺는다.

II. 관련 연구

2.1 하이퍼레저 패브릭

하이퍼레저 패브릭(이하 하이퍼레저)은 리눅스 재단에서 관리하는 오픈소스 블록체인 플랫폼이다[5]. 하이퍼레저는 누구나 자유롭게 참여 가능한 기존의 퍼블릭 블록체인이 아닌, 인증 관리 시스템에 의해 허가된 사용자만이 블록체인 네트워크에 참여할 수 있는 허가형 프라이빗 블록체인이다. 따라서 여러 허가된 사업장 간에 데이터가 동기화하여 분산 저장하기 때문에 공격자가 한쪽 노드에 공격을 가하더라도 나머지 노드에서 지속해서 동기화하고 검증하여 더욱 안전한 데이터 관리가 가능하다.

국내에서는 Ye-Jin Choi[6] 등이 하이퍼레저 기반 헬스케어 데이터 공유 플랫폼을 개발하였다. 이 시스템은 블록체인 기반 저장 방식이 수집이 허가된 익명 의료 데이터를 기존의 방식보다 더 안전하게 보관할 수 있음을 보였다. Jin-Suk Bong[7] 등 또한 하이퍼레저를 이용한 의료 데이터를 더욱 안전하게 저장하는 시스템을 제안했다.

2.2 DApp

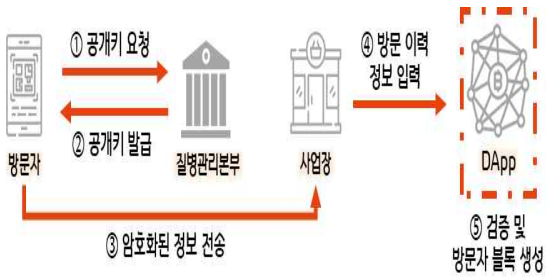
DApp(Decentralized Application)는 탈중앙화 애플리케이션으로 블록체인 기술을 사용하여 중앙서버 없이 네트워크상에서 정보를 분산하고 저장한다. 구동 방식은 스마트 컨트랙트(Smart Contract)를 통해 명령을 수행하고 정보를 불러오고 저장할 수 있다. 스마트 컨트랙트는 블록체인에서 미리 정해진 조건을 달성 시 자동으로 계약의 내용을 수행하는 일련의 소프트웨어 코드이다.

본 논문은 기존 연구와 같이 하이퍼레저가 허가형 프라이빗 블록체인이라는 장점을 활용하여 국가적 재난 속에서 바이러스의 확산을 최소화하기 위한 전자출입명부 관리 시스템을 소개한다.

III. 제안된 시스템 설계 및 구현

본 절에서는 평상시 다중 이용 시설에 출입하는 방문자들을 관리하고 확진자 발생 시 확진자의 동선을 파악하는 일련의 프로토콜을 소개한다.

3.1 평상시



[그림 1] 다중 이용 시설 출입 시

그림 1은 다중 이용 시설을 출입할 때의 상황이다. 방문자는 스마트폰에 본 연구에서 개발한 앱을 사용하여 QR코드를 생성한다. 또한, 사업장도 개발된 앱을 사용하여 방문자의 정보를 검증하고 블록을 생성하여 체인 서버에 저장한다. 프로토콜 순서는 다음과 같다.

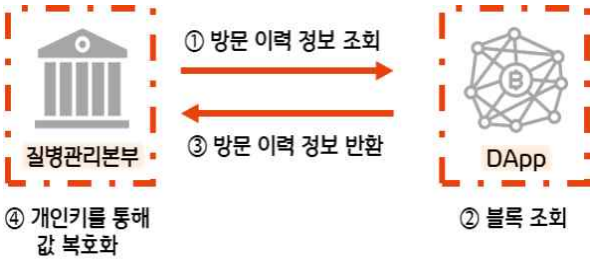
①, ② 생성 날짜의 공개키를 질병관리본부에 요청하여 발급받는다.

③ 발급받은 공개키를 방문자의 휴대전화 번호와 방문 시간에 대한 문자열을 공개키 암호화 알고리즘을 사용하여 암호화를 한다. 암호화한 정보를 바탕으로 QR코드를 생성한다.

④ 사업장에서 QR코드 스캔 시, 방문자 앱에서 생성한 QR코드에 담긴 정보와 사업장 정보(사업자등록번호, 대표자명, 사업장 주소, 휴대전화 번호 등)를 함께 블록체인 서버에 전송한다.

⑤ DApp을 통해 암호화한 방문자의 정보와 사업장 정보를 검증한 후 블록을 생성하여 블록체인 서버에 저장한다.

3.2 확진자 발생 시



[그림 2] 확진자 동선 조사 시

그림 2는 확진자 발생 시 동선을 조사하는 과정을 나타낸다.

① 관리자는 체인 서버에 방문 이력 정보를 조회한다.

② 암호화된 확진자의 정보를 받아 해당하는 블록을 조회한다.

③ 질병관리본부로 방문 이력 정보를 반환한다.

④ 질병관리본부에서 받은 개인 키를 사용하여 암호화되어 있는 정보를 복호화한다.

복호화된 정보를 통해 확진자가 방문했던 사업장들을 조회하고 해당 사업장에 방문한 방문자의 명단을 조회한다.

IV. 결론

본 논문에서는 코로나-19로 인해 의무로 시행하게 된 출입 명부 작성에 대해 허위 정보기재와 개인정보 도난을 방지하기 위한 블록체인 기반 QR코드 전자출입명부 관리 시스템을 제안하였다. 기존의 복잡한 인증 절차를 거쳐 QR코드를 생성하는 방식에서 앱만 켜면 바로 QR코드로 체크인을 할 수 있는 서비스로 개발하였다. 또한, 휴대전화 번호와 방문 시간을 암호화했던 공개키는 14일 이후 자동을 폐기하도록 하여 휴대전화 번호를 제외한 다른 정보(이름, 성별 등)를 제공하지 않기 때문에 개인정보 유출을 최소화한다. 향후 연구로 현재 개발한 앱은 기존의 네이버나 카카오에서 만든 QR코드와 호환이 불가능하여 추후 호환이 가능하도록 연구 및 개발할 예정이다.

블록체인의 특징을 활용하여 분산 저장된 데이터를 동기화하고 검증하여 기존의 중앙통제형 서버 시스템보다 안전하게 관리할 수 있다. 따라서 본 시스템은 방문자의 개인정보를 안전하게 보호하고 확진자 발생 시 정확하고 무결한 데이터를 통한 동선 파악을 제공하는데 효과적일 것으로 기대된다.

[참고문헌]

[1] Nam-E Kim, “내가 적었던 '식당 출입자 명부' 진짜로 불법 거래됐다”, https://news.mt.co.kr/mtview.php?no=2020112208430663386, November, 2020.

[2] So-Yeong Kim, “명부 적으면서도 불안했는데”…. 개인정보 노출 우려 현실화되나“, https://news.joins.com/article/23927707, November, 2002.

[3] Han-Gyeol Joung, Young-Sang Kim, Kang-Jun Lee and Kyong-Hun Jeong, "큐알 머시기가 뭐여? 헬스장 당황한 70대, 그 뒤로 줄줄이…“, https://news.mt.co.kr/mtview.php?no=2020070113080196534, July, 2020.

[4] 중앙방역대책본부, 중앙사고수습본부, June, 2020, ”전자출입명부 활용 안내(안) (이용자 및 시설관리자용)“,

[5] HYPERLEDGER, “Hyperledger Blockchain Performance Metrics”, October, 2018.

[6] Ye-Jin Choi and Kyoung-jin Kim, “Secure Healthcare Data Management and Sharing Platform Based on Hyperledger Fabric”, Journal of Internet Computing and Services(JICS), February, 2020.

[7] Jin-Suk Bong, “A Personal Health Information Sharing Platform based on Hyperledger Fabric Blockchai”, June, 2019.