블록체인 네트워크를 이용한 코로나19 역학조사

서지원, 정재훈
성균관대학교 소프트웨어학과
{sjw6136, pauljeong}@skku.edu

Epidemiological Investigation of COVID-19 using Blockchain Network

Jiwon Suh and Jaehoon (Paul) Jeong
Department of Computer Science and Engineering, Sungkyunkwan University

요 약

2019년 발발한 코로나 바이러스가 세계적으로 유행하며 코로나19의 확산을 사전에 방지하는 것이 국가의 최우선 과제가 되었다. 우리나라의 같은 경우, 확진자에 대한 역학조사를 통해 2차 감염을 통한 코로나의 추가 확산을 억제하고 있다. 그러나 현재 실행하고 있는 역학조사에는 두 가지 큰 문제점이 존재한다. 첫 번째로는 역학조사가 완료되는 기간이 코로나19의 확산세를 억제하기에는 다소 길다는 점이고, 두 번째로는 무분별하게 수집되는 확진자와 밀접 접촉자의 개인정보를 효과적으로 관리하지 못하는 경우가 발생한다는 점이다. 본 논문에서는 인접추적(Proximity Tracing) 기법을 사용하여 모든 접촉자들의 데이터들을 블록체인의 형태로 저장하여 확진자의 개인정보를 보호하는 동시에 빠르고 정확하게 밀접 접촉자들을 가려낼 수 있는 방법을 제안한다.

1. 서 론

2019년 발발한 코로나 바이러스가 세계적으로 유행하며 코로나의 확산을 사전에 방지하는 것이 국가의 최우선 과제가 되었다. 우리나라는 확진자에 대한 역학조사를 통해 2차 감염을 통한 코로나의 추가 확산을 억제하고 있다.

이러한 역학조사엔 두 가지 큰 문제점이 존재한다. 첫 번째로는 역학조사의 기간이 코로나19의 확산세를 억제하기에 다소 길다는 점이다. 밀접 접촉자를 가려내기 위해서는 기존의 방역 시스템을 통한 정보 수집과 더불어 확진자에게서 추가적인 정보를 제공받아 확진자의 동선뿐만 아니라, 같은 장소와 시간대에 있던 사람들을 가려내야 한다. 하지만 대화만을 통해 이를 정확히 파악하는 것은 한계가 있으며, 현장의 CCTV를 활용하거나 신용카드 정보를 대조하고, 휴대폰 기지국의 협조를 받아 정보를 확인하는 시간은 밀접 접촉자에게 접촉 사실을 고지하는데 걸리는 기간을 늦추는 결정적인 역할을 한다.

두 번째 문제점은 수집되는 확진자와 밀접 접촉자의 개인정보를 효과적으로 관리하지 못하는 경우가 발생할 수 있다는 점이다. 역학조사 과정에서 확진자의 신용카드 사용내역과 같은 거래 기록, 위치정보와 이동 경로를 토대로 개인의 취향과 사회적 관계 등 민감한 개인 정보들이 수집된다. 확진자의 개인 정보들은 조사관이 확진자와 인터뷰를 하면서 추가적인 정보가 필요하다고 판단되면 수집이 가능하다. 감염 경로 및 접촉자 파악이라는 목적에 부합한다면 문제가 되지 않지만, 이러한 개인정보의 수집은 조사관의 자의적인 판단에 맡겨져 있을 뿐, 이를 통제할 수 있는 아무런 법적 장치가 마련되어 있지 않다[1].

본 논문에서는 기존의 역학조사는 밀접 접촉자를 가려내는 시간이 재생산수(Reproductive Number)를 억제하기에 시간이 길다는 점과, 확진자의 개인정보가 무분별하게 수집되어 유출되거나 악용될 수 있다는 점을 해결하기 위해 인접추적(Proximity Tracing) 기법을 사용하여 모은 접촉자들의 데이터들을 블록체인의 형식으로 저장하여 확진자의 개인정보를 보호하는 동시에 빠르고 정확하게 밀접 접촉자들을 가려낼 수 있는 방법을 제안한다.

본 연구는 스마트폰의 앱을 이용하여 인접추적을 활용한 밀접 접촉자들의 데이터를 수집했다. 밀접 접촉자들의 데이터를 BLE(Bluetooth Low Energy) 비콘(Beacon)을 통해 수집하고, 스마트폰의 외부 저장소에 엑셀 파일의 형식으로 저장된다. 엑셀파일에 저장된 데이터는 블록체인 네트워크(Blockchain Network)에 저장된다. 저장되는 데이터는 기기의 Device ID로 제한하는데, 이는 Device ID가 앱의 이용자들을 식별하는 가장 쉬운 방법이기 때문이다[2].

관련된 연구로는 스마트폰을 사용하여 인접추적 기법으로만 확진자를 추적하는 방법[3]과 블록체인 기반 가상화폐인 BitCoin 연구가 있다[4].

2. 시스템 제안

2.1 시스템 요구사항

본 논문에서 제안하려는 시스템은 기존 역학조사의 문제점을 보완하고, 보다 투명하고 정확한 역학조사를 수행할 수 있도록 돕는다는 목표를 가지고 있다. 보다 더 나은 역학조사와 관련한 시스템의 요구사항은 다음과 같다.

(1) 완전성 - 각 데이터베이스에 저장된 정보들은 사실과 정확하고 완전하게 이루어져야 한다.

(2) 무결성 - 각 디바이스가 가진 데이터베이스의 값은 모두 일치하며 그렇지 않은 데이터가 입력될 경우 값이

저장되지 않아야 한다.

(3) 검증성 – 관리자는 참여자들이 접촉한 디바이스들을 확인할 수 있으며 어느 누구도 데이터를 조작할 수 없어야 한다.

(4) 편리성 – 데이터베이스에 대한 쿼리를 통하여 확진자와 밀접 접촉자를 빠르고 정확하게 분류할 수 있어야 한다.

2.2 시스템 구성

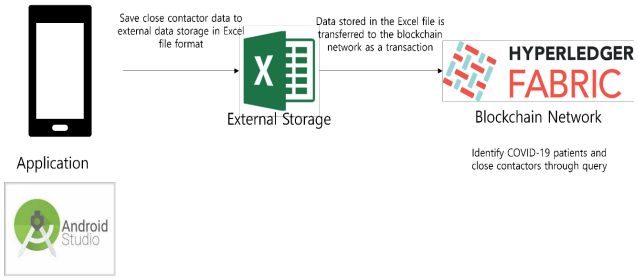

그림 1. 시스템 구조

그림 1과 같이 본 시스템은 사용자와 접촉한 디바이스에 대한 정보들을 수집하기 위하여 블루투스 리시버, 레코더를 안드로이드 스튜디오로 구성된다. 디바이스는 블루투스 비콘을 만들어 전파하고, 동시에 주변 기기의 블루투스 비콘을 받아 기기 내 외부 저장소에 엑셀파일의 형식으로 저장하도록 하였다.

블록체인 네트워크는 허가형 블록체인을 사용하는 하이퍼레져 패브릭을 이용하여 구성하였다[5]. 관리자에게 허가(인증)을 받은 사용자들로만 블록체인 네트워크가 구성될 수 있도록 하였으며 트랜잭션은 외부 저장소에 기록된 밀접 접촉자들의 데이터를 저장하는 것으로 설정하였다.

2.3 시스템 흐름도

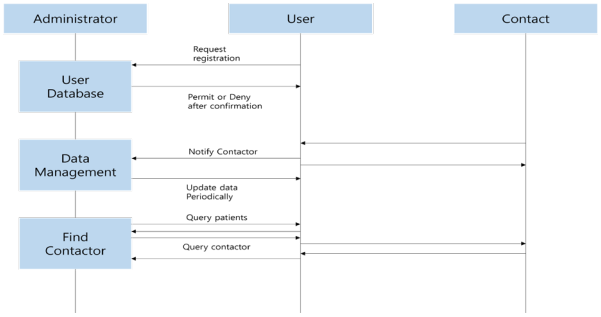

그림 2. 시스템 이벤트 추적도

허가형 블록체인에서는 거래를 인증하기 위한 참여자와 거래에 참여할 참여자를 등록하고, 관리하는 관리자가 필요하다. 그림 2는 참여자, 관리자와 시스템 간의 관계도다.

(1) 관리자

- 시스템을 사용할 참여자를 등록한다.
- 일정 주기로 데이터를 업데이트하여 데이터의 무결성을 보장한다.
- 확진자로 분류된 참여자의 밀접 접촉자를 찾아낸다.

(2) 참여자

- 시스템을 사용할 수 있도록 일련의 과정을 거쳐 참여자가 된다.
- 자신을 인증하고 밀접 접촉한 사람의 데이터를 블록체인 네트워크에 저장한다.

3. 시스템 구현

3.1 BLE 비콘

사용자가 앱을 실행하면 디바이스는 BLE 비콘을 만들어 주위로 송신하는 동시에 주위의 비콘들을 수신해 엑셀파일의 형식으로 디바이스 내에 있는 외부 저장소에 동일한 형식으로 저장된다.

3.2 사용자 등록 허가

관리자는 블록체인 네트워크를 사용할 사용자를 등록한다. 사용자의 데이터는 Device ID, Device Address, 그리고 감염여부인 infected로 구성된다. 다음으로 자산인 Contactor를 등록한다. Contactor의 데이터는 앞서 등록한 사용자와 동일한 Device ID, Device Address를 가지며 자신과 접촉한 Device의 ID를 담는 ContactedUser란 문자열의 배열로 이루어져 있다.

그림 3. User와 Contactor

3.3 트랜잭션

트랜잭션은 디바이스 내 엑셀파일에 저장된 접촉자의 Device ID를 자신의 Device ID와 동일한 Device ID를 가지고 있는 자산, Contactor의 배열에 저장하도록 하였다.

```
/**
 * Adding a User to a Contacted list
 * @param {org.example.contactor.AddContactor} addC
 * @transaction
 */

async function Addcontactor (addC) {

  if (typeof addC.contactor.Contacteduser == 'undefined') {
    addC.contactor.Contacteduser = new Array();
    addC.contactor.Contacteduser[0] = addC.user;
  }
  else {
    addC.contactor.Contacteduser.push(addC.user);
  }

  const assetRegistry = await getAssetRegistry('org.example.contactor.Contactor');
  await assetRegistry.update(addC.contactor);
}
```

그림 4. Chaincode of Transaction

3.4 쿼리를 통한 밀접 접촉자 추적

관리자인 역학조사관은 블록체인에 등록된 접촉자의 데이터를 보고 코로나19에 감염될 수 있는 밀접 접촉자에 해당하는지 판단한다. 이를 위해 관리자는 확진자의 Device ID와 접촉자의 Device ID와 관련된 Transaction을 쿼리를 통해 조회한다. 조회한 Transaction 중 Timestamp가 확진자의 증상 발현 2일 이내라면 밀접 접촉자로 분류하고 Device ID를

서버에 있는 Device ID와 비교하여 실제 기기에 알린다.

```
/**
 * New query file
 */

query getContactor {
  description: "find Contacted people based on UUID"
  statement:
    SELECT org.example.contactor.Contactor
        WHERE (ContactedUser CONTAINS _$ContactedUser)
}

query getInfectedUser {
  description: "find infected user"
  statement:
    SELECT org.example.contactor.User
        WHERE (Infected == true)
}
```

그림 5. Chaincode of Query

Response Body


```
[
  {
    "$class": "org.example.contactor.Contactor",
    "UUID": "2f234454cf6d4a0fadf2f4911ba9ffab",
    "DeviceAddress": "78:46:D4:34:C2:EA",
    "Contacteduser": [
      "resource:org.example.contactor.User#412cbcb3fc4445534b544f502d4f344b"
    ]
  },
  {
    "$class": "org.example.contactor.Contactor",
    "UUID": "c7f914c5759aac6cc4fc0cf6ce8ba503",
    "DeviceAddress": "1D:99:C1:3A:65:B0",
    "Contacteduser": [
      "resource:org.example.contactor.User#412cbcb3fc4445534b544f502d4f344b"
    ]
  }
]
```


그림 6. Query Close Contactor

Response Body


```
[
  {
    "$class": "org.example.contactor.AddContactor",
    "contactor": "resource:org.example.contactor.Contactor#412cbcb3fc4445534b544f502d4f344b",
    "user": "resource:org.example.contactor.User#2f234454cf6d4a0fadf2f4911ba9ffab",
    "transactionId": "3d922798f95174152312f00ec2ce2f23e900b89782faf82b3833ce97e891f851",
    "timestamp": "2021-09-04T15:36:37.212Z"
  },
  {
    "$class": "org.example.contactor.AddContactor",
    "contactor": "resource:org.example.contactor.Contactor#412cbcb3fc4445534b544f502d4f344b",
    "user": "resource:org.example.contactor.User#c7f914c5759aac6cc4fc0cf6ce8ba503",
    "transactionId": "688228cfaf6caf7a28e8ea9c75e3ccd69d1192c55bd4d402f4ca023688032a1",
    "timestamp": "2021-09-04T15:36:54.202Z"
  }
]
```


그림 7. Timestamp of Transaction

3.5 평가 및 분석

본 논문에서는 블록체인 기반 밀접 접촉자 추적 시스템을 구현하였고, 이에 대한 가상 데이터들을 만들어 본 연구를 시스템을 운용하였다. 실제 많은 양의 데이터를 활용하여 보다 실용적인 블록체인 기반 밀접 접촉자 추적 시스템을 만들기 위해 본 논문에서는 다음과 같은 과제를 도출하였다.

첫째로 보다 실용적인 시스템 운용을 위해서는 많은 사용자의 등록이 필요하다. 그러나 등록된 사용자가 많아질수록 블록체인에서의 저장 공간이 늘어나 비용이 증가하게 된다. 이런 경우, 사용자의 정보를 블록체인에 등록하지 않고 기존의 다른 앱이나 사이트에서 등록된 로그인을 병행하여 사용할 수 있다. 하지만 등록을 블록체인에서 분리하여 실행한다면 시스템 공격에 의해 시스템에 대한 안정성이 훼손될 수 있다. 사용자 등록은 검증성과도 관련이 있다. 검증이 가능하도록 사용자 개인별 자산인 Contactor에 기록된 디바이스의 ID를 블록체인에 저장하게 되면 비용이 발생하게 된다. 따라서 시스템의 실용성을 위해 대규모의 사용자를 등록하여야 한다면 상당한 저장공간이 필요하게 된다.

둘째로 본 논문에서는 디바이스 주위에 있는 모든 비콘, 즉, 스마트폰이 아닌 TV와 같은 다른 블루투스 기기들의 정보마저 데이터베이스에 저장하여 실험을 진행하였다. 또한, 블루투스 비콘의 신호는 거리가 얼마인지 상관하지 않고 모든 데이터를 데이터베이스에 저장하여 블록체인 네트워크에 등록하였다. 실제로 이런 형식의 데이터들이 모두 사용자의 디바이스에 저장되어 블록체인에 등록된다면 상당한 저장공간이 필요하게 된다. 또한 밀접 접촉자들이라 분류하기 어려운 데이터이기 때문에 공간과 비용에 대한 낭비로 이어지게 된다. 따라서 블루투스 신호 세기인 RSSI와 노출 시간도를 종합하여 코로나 노출 위험도를 측정하는 알고리즘을 통해 일정 역치를 상회하면 데이터베이스에 추가하는 알고리즘, 인식되는 비콘이 사용자가 들고 다니는 스마트폰일 경우에만 데이터베이스에 저장되는 알고리즘을 활용하여 블록체인에 저장되는 데이터를 줄일 수 있다.

4. 결론

본 논문에서 제안한 시스템은 허가형 블록체인을 사용하여 모든 데이터들은 관리자만 열람할 수 있도록 하였고, 데이터들이 각 사용자들의 디바이스에 분산 저장되어 있는 블록체인의 분산 원장을 활용하여 시스템을 구성하였기 때문에 기존 역학조사에서 보였던 개인 정보 유출의 위험성과 실용성을 보완할 수 있다. 본 연구에서 활용된 데이터는 가상의 적은 데이터를 토대로 진행한 연구이다. 향후연구로는 대규모 사용자들의 등록을 지원하고, 스마트폰 뿐만 아니라 블루투스를 이용하는 다른 디바이스들의 데이터를 블록체인에 저장한 뒤 확진자 밀접 접촉자들을 블록체인에서 고속으로 탐색하는 알고리즘을 개발할 계획이다.

Acknowledgments

본 논문은 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구 센터지원사업의 연구결과로 수행되었음(IITP-2021-2017-0-01633). 본 논문은 또한 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. 2019-0-01343, 융합보안핵심인재양성). 교신저자는 정재훈 교수임.

참고 문헌

[1] 오병일, “코로나19와 정보인권”, 국가인권위원회, https://www.humanrights.go.kr/site/inc/file/fileDownload?fileid=10701&filename=b77ebe30cfc919257c7c0324a2f74734.pdf

[2] Adjust, “기기 ID란 무엇인가요?”, https://www.adjust.com/ko/glossary/device-id/

[3] Carmela Troncoso et al., “Decentralized Privacy-Preserving Proximity Tracing”, May 2020. https://arxiv.org/abs/2005.12273

[4] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf

[5] HyperLedger Fabric, https://www.hyperledger.org/use/fabric