공동 현관 비밀번호 유출 방지를 통한 블록체인 기반의 안전한 배송 시스템

김현지*, 권용빈*, 최승주*, 서화정*†
*한성대학교 IT융합공학부
khj1594012@gmail.com, vexyoung@gmail.com, bookingstore3@gmail.com,
Hwajeong84@gmail.com

Secure delivery system based on blockchain through preventing leakage of common entrance password.

Hyun-Ji Kim*, Yong-Been Kwon*, Seung-ju Choi*, Hwa-Jeong Seo*†
*Dept. of IT convergence engineering, Hansung University

요 약

최근 변화하는 소비패턴으로 인해 당일 및 새벽 배송 등의 서비스가 보편화되고 있다. 해당 서비스는 배송 정보를 입력 시 건물에 자유롭게 출입할 수 있는 공동 현관 비밀번호를 기입해야 한다. 이는 이미 빈번하게 발생하고 있는 무단 주거 침입 등의 범죄에 더 쉽게 노출되도록 할 수 있는 위험요소이다. 본 논문에서는 신뢰할 수 있는 사용자만이 참여 가능한 프라이빗 블록체인 네트워크에서의 차량 번호판 인식 및 스마트 컨트랙트를 통해 랜덤한 마스터 비밀번호를 제공하여, 보안적으로 취약한 비밀번호 기입 절차를 없애고 검증 받은 사용자에게만 출입을 허가하는 방식을 제안한다.

1. 서론

최근 발생한 코로나 바이러스 감염증-19 (COVID-19)로 인해 생활 및 소비패턴이 변화하고 있다. 특히, 일상생활에서 거를 수 없는 요소인 배달 음식과 신선식품 전자상거래의 수요가 가파르게 증가하였으며, 당일 및 새벽 배송 업체는 최근 평균 300만개의 주문량을 기록했다.

관련 어플리케이션을 사용해보면 빠른 배송 서비스를 제공하기 위해 새벽 배송을 하고 있으며 이를 위해 공동현관 비밀번호를 직접 명시하도록 되어있다. 해당 비밀번호는 각 세대별 비밀번호와 마스터 비밀번호로 구성되어 있으며, 초기 설정 후 거의 바꾸지 않기 때문에 노출되면 외부인의 자유로운 출입이 가능해진다. 이러한 배송 시스템은 관련 범죄들에 더 쉽게 노출될 수 있다.

최근 5년간의 경찰청 범죄 통계에 따르면, 택배기사를 사칭하여 무단으로 주거침입을 하는 등의 관련 범죄들이 1600건 이상 발생하였고, 배송 업체 직원들 간에 공동 현관 비밀번호를 공유하고 심지어 이를 악용하는 사례도 있다.

따라서 앞으로 보편화 될 전망인 배송 서비스는 더욱 안전하게 운영되어야 할 필요가 있다.

2. 관련 연구

2.1 스마트 컨트랙트

스마트 컨트랙트는 실행 조건과 계약 내용을 구현한 코드이며 해당 조건을 만족하면 자동으로 계약 내용을 수행한다. 디지털 데이터의 경우 위변조의 문제가 존재하지만 이를 블록체인 플랫폼에서 적용할 경우 정보의 무결성이 보장되어 제 3자의 개입 없이 신뢰할 수 있는 거래가 가능하다[1].

트랜잭션 발생 시 블록체인 상의 모든 노드는 해당 트랜잭션을 공유하여 블록을 생성한 후 브로드캐스팅한다. 블록을 전달 받은 노드들은 해당 블록을 각자의 블록체인에 추가한 후 동기화한다. 이러한 과정을 통해 모든 데이터가 공유 및 기록되기 때문에 계약 내용을 조작할 수 없다. 또한 추적이 가능하며 실행 조건 만족 시 자동 이행되므로 거래 비용을 줄일 수 있다.

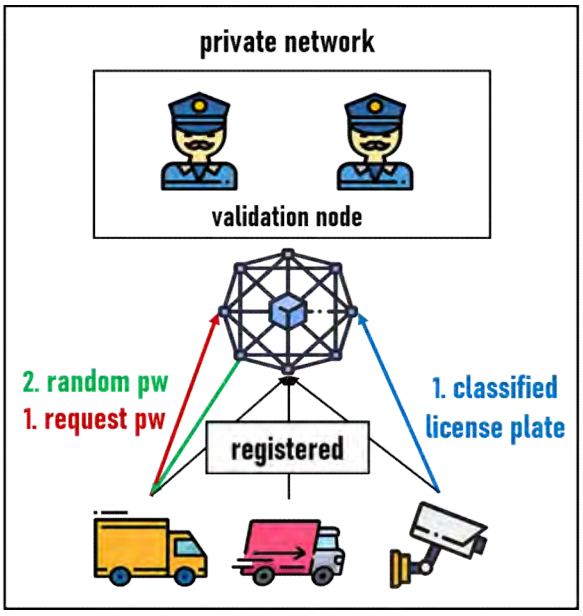
2.2 차량 번호판 인식

노이즈 필터링과 외곽선 검출 등의 영상 처리 과정을 거쳐 차량 번호판을 검출해낼 수 있다. 또한, Convolutional Neural Network 등의 딥 러닝 모델을 통해 번호판 이미지를 학습하여 검출해낼 수도 있으며 현재 상용화 되어 사용되고 있는 기술이다.

3. 시스템 제안

본 논문에서 제안하는 시스템은 프라이빗 블록체인 네트워크를 활용하여 허가 받은 노드만이 참여 가능하며 배송 차량 노드, 차량 인식 카메라 노드, 경비실 노드로 구성된다. 합의 알고리즘으로는 권한증명(Proof of Authentication, PoA)을 사용하여 신원이 검증된 경비실 노드를 검증 권한이 있는 노드로 사전 승인한다.

그림 1은 제안 시스템의 동작과정을 나타낸 구성도이다. 해당 시스템을 이용하기 위해 배송 차량 노드와 차량 인식 카메라 노드를 해당 블록체인 네트워크에 사전 등록한다. 배송 차량이 아파트 입구에 들어서면 차량 인식 카메라 노드는 해당 차량의 번호판을 인식하고 배송 차량은 랜덤 마스터 비밀번호를 요청한다. 사전 등록된 정보와 일치하는지 확인한 후 랜덤 마스터 비밀번호를 제공하며, 해당 비밀번호는 일정 시간 후 폐기된다.



(그림 1) 시스템 구성도.

3.1 노드

제안 시스템은 신원이 확인된 차량 및 차량 인식 카메라만이 프라이빗 블록체인 네트워크에 노드로서 참여할 수 있고, 사전에 등록된 정보와의 비교를 통해 인증을 받아야 마스터 패스워드를 얻을 수 있다.

3.1.1 배송 차량 노드

대부분의 배송 시스템은 각 배송 차량에 할당된 지역이 있으므로 프라이빗 블록체인 네트워크에 신원이 확인된 배송 차량의 정보가 사전 등록되어 있으며 항목은 표1과 같다. 배송 차량의 번호판, 계정 주소, 트랜잭션 생성 시 입력할 비밀번호가 등록되어 있으며 해당 비밀번호를 입력하여 랜덤 마스터 패스워드를 요청한다.

<표 1> 배송 차량 노드의 사전 등록 정보

registered infomation
license plate
account address
key

3.1.2 차량 인식 카메라 노드

차량 인식 카메라 노드 또한 신원이 확인된 기기를 사용하며 표2와 같은 해당 기기의 정보를 프라이빗 블록체인 네트워크에 사전 등록한다.

<표 2> 차량 인식 카메라 노드의 사전 등록 정보

registered infomation
device id
account address

배송 차량이 입구에 들어오면 블록체인에 사전 등록된 차량 인식 카메라는 광학 문자 인식(Optical Character Recognition)을 통해 차량의 번호판을 검출한다. 검출 결과는 해당 기기의 아이디, 계정 주소, 타임 스탬프와 함께 블록체인 네트워크로 전송된다.

3.1.3 경비실 노드

신뢰할 수 있는 데이터를 통해 신원이 검증되어 사전에 권한을 얻은 노드로서, 권한증명(PoA) 합의 알고리즘을 통해 배송 차량 노드와 카메라 노드로부터 발생한 트랜잭션의 유효성을 검증하고 블록체인 네트워크에 반영하는 역할을 한다.

3.2 스마트 컨트랙트

배송 차량 노드에서 서버에 저장된 값과 동일한 비밀번호를 입력하여 랜덤 마스터 비밀번호를 요청하는 트랜잭션이 생성되고, 동시에 차량 인식 카메라노드에서는 카메라를 통해 검출한 차량 번호판 정보를 전송하는 트랜잭션이 생성된다. 생성된 두 트랜잭션은 각각 다른 컨트랙트 어카운트로 전송되며 해당 컨트랙트들은 내부 코드를 실행한다.

배송 차량 노드로부터 발생한 트랜잭션은 랜덤 마

스터 패스워드를 생성하는 컨트랙트(컨트랙트 A)로 전송된다.

차량 인식 카메라 노드로부터 발생한 트랜잭션은 디바이스 정보와 번호판 검출 결과를 저장하는 컨트랙트(컨트랙트 B)로 전송된다.

컨트랙트A가 컨트랙트 B를 호출하여 차량 인식 카메라의 디바이스 아이디, 계정 주소, 번호판 검출 결과를 얻는다. 사전에 해당 배송 차량 계정에 등록된 정보들을 비교하여 등록된 차량임이 인증될 경우 마스터 랜덤 비밀번호를 전송한다.

<표 3> 스마트 컨트랙트에 저장될 데이터

contract A	contract B
key	account address (camera)
account address	device ID
account address (camera)	license plate
device ID	
license plate	

따라서 자주 갱신하지 않고 공동으로 사용하는 현관 비밀번호를 허가 받지 않은 사용자에게 노출하지 않을 수 있게 되고 발급 받은 랜덤 마스터 비밀번호는 일정 시간 후, 트랜잭션 발생 시 랜덤으로 다시 생성된다. 또한, 출입에 관련된 정보가 블록체인 상에 기록되며 프라이빗 블록체인의 특성 상 책임소재를 파악할 수 있다. 이는 서론에서 언급한 어플리케이션 등을 통해 노출된 현관 비밀번호를 사용하여 택배기사를 사칭하는 등의 악의적인 무단 침입 범죄를 방지할 수 있다.

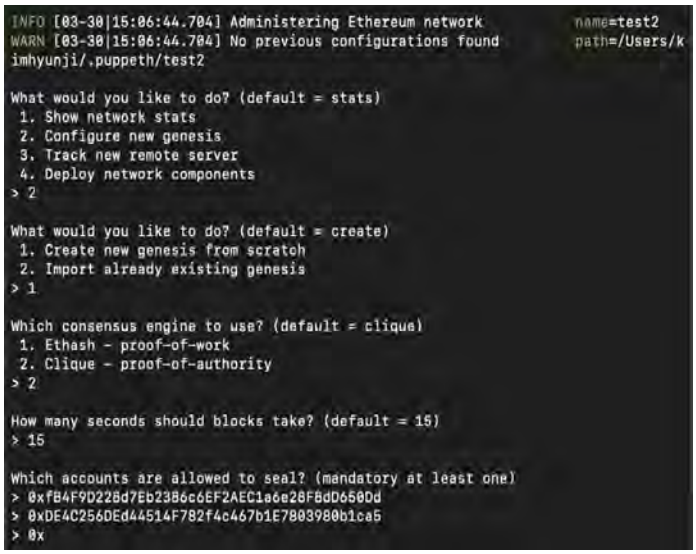
4. 구현

본 시스템의 구현은 go language를 기반으로 한 go-ethereum(geth)를 사용하여 프라이빗 블록체인 네트워크를 구성한 후 remix와 연동하여 배포하며 솔리디티 언어로 스마트 컨트랙트를 작성한다. 또한 python과 openCV 라이브러리를 활용하여 차량 번호판 인식을 진행하였다.

4.1 네트워크 구성

go language와 geth를 설치한 후 총 5개의 노드 디렉터리와 계정을 생성하여 프라이빗 네트워크를 구성하였다. 해당 네트워크의 노드는 3개의 일반 노드(배송 차량 노드 2개, 차량 인식 카메라 노드 1개)와 2개의 검증자 노드(경비실 노드)로 구성된다.

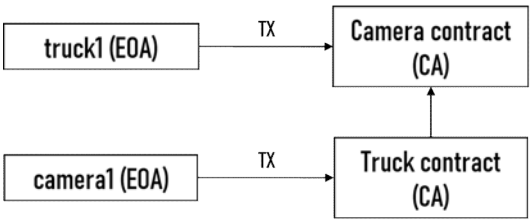
genesis 파일을 생성 및 네트워크 설정은 그림2와 같이 puppeth을 통해 진행하였다. 합의 알고리즘은 프라이빗 네트워크에서 더 효율적인 권한증명(PoA)인 clique를 사용하며, 검증자 역할을 할 노드의 계정에 블록 생성을 권한을 승인하였다.



(그림 2) puppeth를 이용한 블록체인 네트워크 설정

4.2 스마트 컨트랙트 구성

본 시스템을 위해 두 개의 스마트 컨트랙트를 작성하였다. 배송 차량이 아파트 입구에 진입할 경우 각 노드는 트랜잭션을 발생시키고 그림 3과 같이 진행된다. 또한, 각 컨트랙트는 표 4, 표 5와 같이 구성된다.



(그림 3) 노드 계정과 스마트 컨트랙트

<표 4> Camera contract

Camera contract	

constructor (생성자)	constructor(string _plate, string _deviceID) public {
	camowner = msg.sender;
	licenseplate = _plate;
	deviceID = _deviceID;
	}

function (함수)	setfromcam

<표 5> Truck contract

Truck contract	

constructor
(생성자)
	constructor(uint32 _privatekey) public {
	truckowner = msg.sender;
	privatekey = _privatekey;
	}

function (함수)	setAddress
	setInfo
	genPW

Camera 컨트랙트의 경우, 차량 인식 카메라로부터 검출한 번호판 데이터와 해당 카메라의 디바이스 식별자를 매개변수로 받아온다. 스마트 컨트랙트 실행 시 가장 먼저 실행되는 생성자를 통해 표 4의 변수에 저장하며 트랜잭션을 발생시킨 계정의 주소는 camowner로 설정한다. 해당 정보들은 setfromcam 함수를 통해 camowner를 키값으로 하는 구조체 배열(Infofromcams)의 각 멤버변수에 저장된다.

Truck 컨트랙트는 배송 차량이 사전에 등록한 비밀번호를 입력하여 트랜잭션을 발생시키면 생성자를 통해 트랜잭션을 생성한 계정과 입력한 비밀번호를 저장한다.

해당 계정에 등록된 정보가 현재 인식한 정보와 동일한지 비교해야하므로 그림 4와 같이 setAddress 함수를 통해 Camera 컨트랙트를 호출한다. 호출한 컨트랙트로부터 번호판 검출 결과와 디바이스 식별자 및 계정 정보를 참조하여 키값이 truckowner인 구조체 배열(trucks)의 각 멤버변수에 저장한다. 이 과정은 그림 5를 통해 확인할 수 있다.

```
Camera c;
function setAddress(address _address){
    c = Camera(_address);
  }
```

(그림 4) Camera 컨트랙트 호출

(그림 5) 카메라로부터 수신한 정보 저장(왼쪽) 및 Camera 컨트랙트 호출하여 두 트랜잭션에 대한 정보 저장(오른쪽)

이 과정에서 그림 6과 같이 이벤트로그로 기록되므로 차량의 출입에 관한 정보가 남게 되며 이상 트랜잭션 발생 시 추적이 가능하다.

이 후 배송 차량의 계정 주소에 해당하는 정보들을 사전에 등록된 정보와 비교하여, 동일한 경우 genPW 함수를 통해 그림 7과 같은 랜덤 마스터 비밀번호를 발급한다.

```
"tprivatekey": 9876,
"taddr": "0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c",
"caddr": "0x14723A09ACff6D2A60DcdF7aA4AFf308FDDC160C",
"licensePlate": "12A3456",
"dID": "1234:5678",
"length": 5
```

(그림 6) 이벤트로그

```
"uint256: 7860"
```

(그림 7) 발급된 랜덤 마스터 비밀번호

5. 결론

본 논문에서는 프라이빗 블록체인과 차량 번호판 인식 기술을 활용하여 건물 출입에 필요한 마스터 비밀번호를 랜덤하게 발급하는 방법을 제안하였다. 허가 받지 않은 사용자의 경우 비밀번호를 발급 받을 수 없으며, 이를 통해 건물에 자유롭게 출입할 수 있는 비밀번호의 노출 가능성을 줄여 무단 주거 침입 등의 범죄를 예방할 수 있을 것으로 기대된다.

그러나 현재 특별한 신원 확인 절차 없이 관련 업체에 배송 기사로 등록이 가능한 경우가 있어 본 시스템의 적용을 위해서는 신원 확인 절차가 필요하다. 또한 손으로 눌러야 하는 비밀번호는 뒤에서 훔쳐보는 경우 노출될 위험이 있다. 따라서 QR 코드 등을 통해 허가된 사용자만 이용할 수 있도록 하여 보안성을 강화하는 방법 등을 고려할 필요가 있다.

참고문헌

[1] Jun-hyeok Yun, Mihui Kim. Private Blockchain and Smart Contract Based High Trustiness Crowdsensing Incentive Mechanism. Journal of The Korea Institute of Information Security and Cryptology (JKIISC), 28(4), 999-1007. (2018).

[2] Chul-Jin Kim. A Static and Dynamic Design Technique of Smart Contract based on Block Chain. Journal of the Korea Academia-Industrial cooperation Society(JKAIS). 110-119. (2018.6)