

QR코드 및 스마트 글라스 활용 개인 정보 보호 블록체인 택배 시스템

최승주¹ · 심민주² · 서화정^{3*}

The Blockchain Delivery System for Secure Privacy with QR Code and Smart Glasses

Seung-Joo Choi¹ · Min-Joo Sim² · Hwa-Jeong Seo^{3*}

¹Graduate Student, Department of IT Engineering, Hansung University, Seoul, 02876 Korea

²Undergraduate Student, Department of IT Engineering, Hansung University, Seoul, 02876 Korea

^{3*}Associate Professor, Department of IT Engineering, Hansung University, Seoul, 02876 Korea

요 약

개인정보 보호의 중요성이 어느 때보다 주목을 받고 있다. 그러나 택배 시스템은 이러한 개인정보 보호에 대한 움직임을 아직 따라가지 못하고 있다. 택배 상자에는 수취인에 대한 개인정보가 적혀있는 운송장이 붙어있어 누구나 손쉽게 개인 정보를 탈취해 갈 수 있다. 이러한 문제점을 개선하기 위해 본 논문에서는 운송장의 내용을 사람이 눈으로 읽고 접근할 수 있는 글자가 아닌 QR 코드로 대체할 것을 제안한다. 또한 해당 QR 코드의 내용에 대한 무분별한 접근을 방지하기 위해 해당 내용에 대한 접근은 택배 블록체인 네트워크에 등록된 스마트 글라스만을 사용하여 접근할 수 있게 한다. 마지막으로 접근 가능한 스마트 글라스를 보유한 사람으로부터 해당 내용이 유출되는 것을 방지하기 위해 해당 접근 기록을 블록체인에 기록할 것을 제안한다.

ABSTRACT

The importance of protecting personal information is getting attention more than ever. However, the package delivery system has yet to keep up with the privacy movement. The waybill attached to the package contains personal information about the recipient in text form, which is exposed to anyone with visible eyesight. In order to remedy the problem, this paper proposes that the contents of the waybill should be replaced by QR code instead of plain text which can be read and accessed through the human eye. In addition, in order to prevent indiscriminate access to the contents of the QR code, the access is only permitted using smart glasses registered in the delivery blockchain network system. Lastly, to prevent leaking the contents of the QR code from the person who has access to the registered smart glasses, an inside job, the access record is recorded on the blockchain.

키워드 : 블록체인, 개인 정보 보호, QR 코드, 스마트 글라스

Keywords : Blockchain, Privacy, QR Code, Smart Glasses

Received 17 February 2020, Revised 20 February 2020, Accepted 27 February 2020

* Corresponding Author Hwa-jeong Seo(hwajeong@hansung.ac.kr, Tel:+82-2-760-8033)

Associate Professor, Department of IT Engineering, Hansung University, Seoul, 02876 Korea

Open Access <http://doi.org/10.6109/jkiice.2020.24.5.630>

print ISSN: 2234-4772 online ISSN: 2288-4165

© This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright © The Korea Institute of Information and Communication Engineering.

I. 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 정보 유출이 발생하는 주된 경로 중 하나로 뽑히는 것이 택배이다.

모든 택배에는 운송장이 부착되어 있으며 이 운송장의 내용은 품목 정보, 고객 정보, 배달표 등으로 구성된다. 이와 같은 운송장에는 물품 수신인이 주문한 물품 정보와 수신인의 성명, 주소 그리고 전화번호가 그대로 적혀있다. 이런 개인 정보는 보이스피싱, 스미싱 등에 이용이 될 수 있다. 실제로 2016년 중국에서 택배 운송장 실명제를 도입하였다가 개인정보 유출사고가 심각해져 운송장에 개인정보 없이 바코드만 붙이는 택배사가 등장하기도 했다[2]. 한국에서는 택배를 통한 정보 유출에 대한 대응 방침으로 운송장의 성명과 전화번호의 일부를 표기하지 않거나[3] 택배를 받은 뒤 개인정보가 적혀있는 운송장을 쉽게 떼어 파기할 수 있게 운송장을 제작하는 등의 대응방안을 실행하고 있다. 그러나 수령인이 택배를 수령하기 전에 운송장에 적혀있는 정보들은 누구든지 접근이 가능하며 유출될 수 있다. 또한 앞서 언급한 운송장에 적힌 개인정보들을 일부 가리는 대안 방안은 가려진 정보들만을 조합하여도 온라인상에서 쉽게 해당 배송물 수취인에 대한 신상과 사생활을 캐낼 수 있기 때문에 사실상 정보 보호 효과가 미비하다. 이처럼 택배를 통한 개인정보 유출은 심각한 문제이며 해결책이 필요하다.

본 논문의 구성은 다음과 같다. 2장에서는 블록체인 기반 개인 정보 보호 택배 시스템 개발을 위한 블록체인, 스마트 컨트랙트, QR 코드 및 바코드, 스마트 글라스(Smart glasses) 등 관련 연구에 대해 살펴보고, 3장에서는 QR 코드 및 스마트 글라스를 활용하여 개인 정보를 보호해주는 택배 시스템 개발을 위한 제안 기법 및 시스템 동작 절차 등을 설명한다. 4장에서는 본 논문에서 제안한 시스템에서 사용되는 스마트 컨트랙트의 알고리즘에 대한 분석을 진행하며, 마지막으로 5장에서는 기존 시스템과 제안하는 시스템간의 차이를 비교 분석하며 결론을 맺도록 한다.

II. 관련 연구

2.1. 블록체인

블록체인이란 P2P(Peer-to-Peer) 네트워크에서 동일한 전자 장부에 대한 데이터를 네트워크에 참여하고 있는 노드들이 공유하고 관리하는 네트워크이다. 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. 이러한 블록체인의 특징을 이용하여 블록체인 상에서는 코인이라는 가상 화폐 개념을 이용하여 제 3의 공인기관이나 중개자의 개입 없이 익명의 대상간의 거래가 이루어지기도 한다.

구체적인 블록체인의 공유 전자 장부에 대한 관리 및 위조 방지는 그림 1과 같은 구조에 의해 가능해진다. 블록체인 네트워크에서 발생된 모든 트랜잭션은 블록이라는 구조에 시간, 논스 값 그리고 이전 블록의 해시 값 등이 저장된다. 이때 이전 블록의 해시 값이 저장되기 때문에 해시 값을 바탕으로 각 블록이 연결된 형태가 형성이 된다. 이러한 블록은 채굴자(miner)에 의해 형성이 되며 가장 많은 블록이 형성된 장부의 기록을 검증 과정을 통해 공식 장부로 인정을 하게 된다. 이와 같은 구조로 인해 악의적인 네트워크 참여자가 특정 블록의 데이터를 위조 및 변조를 하려고 시도할 경우 해당 블록 이후의 모든 블록들에 대한 해시 값들이 전부 변경이 되게 된다. 이처럼 변경된 블록체인의 모든 블록의 해시 값을 변경하면서 동시에 다른 채굴자들의 블록 형성 시간을 앞지르는 것은 사실상 불가능하기 때문에 위조 및 변조에 대한 내성을 지니고 있다.

최초의 블록체인은 비트 코인[4]으로 퍼블릭 블록체인 형태를 띠고 있다. 이는 블록체인 네트워크에 누구나

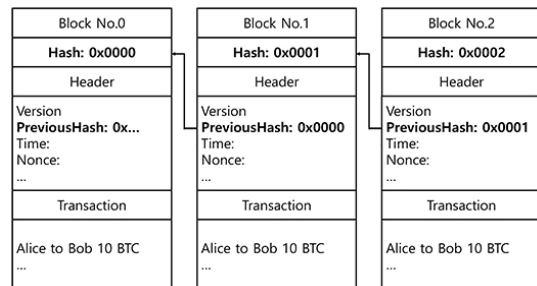


Fig. 1 Blocks connected by previous block's hash value

참여할 수 있으며 누구나 블록체인에 블록을 형성하는 채굴자가 될 수 있음을 뜻한다. 그러나 최근에는 퍼블릭 블록체인의 현실적인 한계점[5]을 고려하여 프라이빗 블록체인 형태도 출시되고 있다. 이러한 프라이빗 블록체인의 특징은 블록체인 네트워크에 참여할 수 있는 대상이 해당 네트워크를 운영하고 있는 기업 혹은 개인의 허락을 받아야 참여할 수 있다는 점이다. 프라이빗 블록체인의 특징을 이용하여 퍼블릭 블록체인에서 블록 생성을 위해 진행해야 했던 컴퓨터 연산 과정을 투표 형식으로 대체하거나 블록 생성 시간을 단축하는 등 기업과 같이 블록체인 네트워크를 공개한 상태로 운영할 필요가 없는 기관에서 활용된다.

본 논문에서는 해당 프라이빗 블록체인을 활용하여 운송장 정보에 대한 무결성을 보장하기 위해 QR 코드에 대한 해시 값을 블록체인 네트워크에 기록하고 QR 코드를 어떤 직원 또는 택배 기사가 조회를 하였는지 기록할 것을 제안한다. 이는 추후에 정보 유출이 발생했을 시 유출 경로 및 대상을 추적할 때 활용될 수 있다.

2.2. 스마트 컨트랙트

스마트 컨트랙트는 1994년 최초로 제안된 개념으로 디지털로 만들어진 계약서를 의미한다. 이렇게 디지털화된 스마트 컨트랙트는 조건에 따른 계약 결과가 명확하고 계약 내용을 조건이 충족되면 즉각 이행할 수 있다는 특징을 갖고 있다. 이러한 특징을 활용하여 2세대 블록체인이라고 불리는 이더리움에서 처음으로 블록체인에 스마트 컨트랙트를 적용하였다[6].

이러한 스마트 컨트랙트는 탈중앙화 어플리케이션(DApp, Decentralized Application)을 제작하는데 많이 사용이 되며 대표적인 퍼블릭 블록체인인 이더리움 뿐만 아니라 기업형 블록체인인 하이퍼레저[7] 등 다른 블록체인에서도 많이 활용이 되고 있다.

해당 스마트 컨트랙트를 활용하여 택배 블록체인 상에서 운송장 QR 코드에 대한 정보를 볼 수 있는 주체를 결정하여 택배와 연관된 주체가 아닌 사람은 확인할 수 없게 설정한다.

2.3. QR 코드

바코드 형식으로 정보를 저장하고 읽어내는 방식은 전 세계적으로 많이 쓰이고 있다. 이러한 방식이 갖고 있는 특징인 정보를 매우 빨리 읽어 낼 수 있다는 특징

과, 정보의 무결성 그리고 편리성 때문에 많은 분야에서 사용이 되고 있다. 이와 같은 바코드 방식은 지금까지 더 많은 정보를 담을 수 있고 더 빠르게 정보를 읽을 수 있기 위한 많은 연구가 진행되어져 왔었다.



Fig. 2 Difference between Barcode and QR Code

QR 코드의 QR은 'Quick Response'의 약자로 빠른 응답을 얻을 수 있다는 의미를 뜻한다. 이러한 QR 코드의 특징으로는 여러 가지가 있는데 먼저 종래에 많이 사용하던 1차원 형태의 바코드의 용량을 확장하고 보다 많은 양의 정보를 담을 수 있는 것이 가장 큰 특징이다. 그림 2에서 볼 수 있는 것처럼 기존 바코드는 1차원적 구조로 데이터를 담을 수 있는 반면에 QR 코드는 2차원적으로 데이터를 담을 수 있다. 이와 같은 구조를 가진 바코드는 특정 상품명이나 제조사 등의 정보 정도만 기록할 수 있지만 QR 코드는 URL, 사진, 위치 정보 등 다양한 정보를 담을 수 있으며 숫자는 최대 7089자, 영문자와 숫자 최대 4296자 등 많은 정보를 담을 수 있다. QR 코드의 또 다른 특징으로는 오류복원 기능이 있어 코드의 일부분이 오염되거나 손상돼도 데이터 정보를 복원할 수 있으며 기존의 바코드보다 인식률이 우수하다는 점이다. 마지막으로 QR 코드의 형태는 정사각형을 취하고 있어 360도 어느 방향에서든 코드를 스캔하여도 정확하게 인식이 된다는 점이 있다[8].

이러한 QR 코드의 특징은 택배 배송 정보를 저장하기에 매우 적합하다. QR 코드는 앞서 말한 것과 같이 URL 또는 이미지 또한 담을 수 있기 때문에 택배 서비스의 서버로부터 QR 코드에 담겨있는 운송장 정보를 빠르게 조회할 수 있다.

2.4. 스마트 글라스

최근 많은 웨어러블 디바이스들이 출시되고 있다. 그 중에서 가장 잘 알려진 디바이스로는 스마트 워치와 스마트 글라스이다. 스마트 글라스는 헤드 마운티드 디스플레이(HMD; Head Mounted Display)가 장착된 착용 컴퓨터이다[9]. 특정 정보를 확인하기 위해서는 테이블릿, 스마트 폰 등의 디바이스를 손에 들고 이용하여 확인해

야하는 반면 스마트 글라스는 사용자가 보고자 하는 정보를 바로 시야에 보여줄 수 있다는 장점을 갖고 있다. 이러한 특징을 갖고 있는 스마트 글라스는 두 손을 모두 사용해야하는 제조 업종 등에서 많이 활용이 될 수 있는 잠재력을 가지고 있다. 뿐만 아니라 증강현실과 같은 기술의 발전으로 인해 해당 기술을 스마트 글라스에 적용하는 연구 또한 많이 이뤄지고 있다. 이러한 스마트 글라스는 삼성, 화웨이 그리고 구글 등 다양한 기업들에서 개발 중에 있으며 최근 구글에서는 과거 공개 했었던 구글 글라스를 발전시킨 기업용 구글 글라스 2를 발표한 상황에 있다[10]. 이러한 스마트 글라스를 이용하여 싱가포르의 공항에서는 실시간 지시 사항 전달, 공지 사항 전달, 수하물 분류 등에 활용하여 사용하고 있으며 양손이 자유로운 스마트 글라스를 도입한 이후 수하물 하차 시간이 약 25% 감소하였다는 결과 발표가 있다[11].

이와 같은 스마트 글라스를 사용하면 택배 운반 기사들의 두 손은 편리하게 택배를 옮기는데 사용하면서 동시에 해당 물품에 대한 운송 정보를 확인할 수 있게 된다.

III. 시스템 설계

앞에서 언급한 개인정보 유출을 막기 위해서는 먼저 운송장에 적혀 있는 개인정보를 최소한으로 축소시켜야 한다. 이를 위해 운송장의 정보를 텍스트 형식이 아닌 QR 코드 형식으로 택배에 부착한다. 이를 통해 육안을 통한 정보 유출을 방지할 수 있다. 해당 QR 코드는 택배를 운반하는 직원들이 착용하고 있는 스마트 글라스를 통해 배송 정보를 인식하여 배달 장소를 파악 후 배달을 진행한다. 해당 방식을 사용할 때 고려해야할 점은 다음과 같다.

먼저 QR 코드는 스마트폰을 갖고 있는 사람이라면 누구든지 스캔하여 해당 정보를 볼 수 있다는 특징을 갖고 있다. 하여 택배에 부착되어 있는 QR 코드 정보에 대한 접근을 택배 운반 기사로 제한한다. QR 코드의 정보는 택배 서비스의 서버에서 관리를 하고 등록되어 있는 스마트 글라스로의 요청이 아닌 경우 접근을 거부한다.

다음으로 운송장의 내용을 전부 QR 코드에 담게 된다면 택배를 받은 수령인이 해당 수하물이 본인의 물건인지 확인할 수 없게 된다. 하여 개인정보는 감추면서 본인의 물건임을 확인할 수 있는 방법이 필요하다. 이를

위해서 택배를 주문한 사람의 실명을 사용하지 않고 임시 가명 혹은 ID를 QR 코드와 같이 첨부하도록 하고 해당 정보는 문자 및 메일로 택배 수령인에게 전송하여 받은 물품이 수취인의 것이 맞는지 판단할 수 있게 유도한다.

또 고려되어야 하는 점은 택배 운송 중 택배가 잘못된 주소로 배송이 되는 등 문제가 발생하는 경우이다. 해당 문제를 해결하기 위해 보존되어야 할 정보는 운송장번호로 만약 배송이 된 물품이 도착을 하지 않았거나 물품 파손이 발생해 물품 운반에 관련이 되어 있는 대상들에 대한 조회가 필요하기에 운송장번호에 대한 정보는 택배에 남겨둔다.

마지막으로 QR 코드에 대한 정보 및 접근 관련 연산을 블록체인 스마트 컨트랙트를 통해 처리한다. 이를 통해 운송장에 대한 정보의 무결성과 해당 정보에 대한 접근 과정을 기록하여 남겨둘 수 있다. 이는 추후에 내부자 소행으로 인한 해당 택배에 대한 개인 정보 유출이 발생한 경우 해당 물품을 담당할 택배 기사에 대한 무결성이 보장된 기록을 얻을 수 있다.

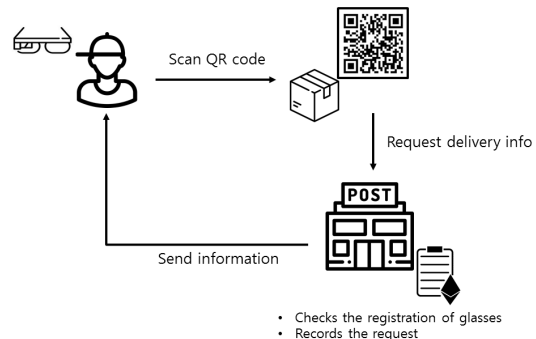


Fig. 3 Diagram of Delivery System with Secure Privacy

제안 시스템의 전체적인 흐름은 그림 3과 같으며, 그 과정은 다음과 같다. 먼저 스마트 글라스를 이용하여 택배를 운반하는 사람이 택배물에 부착되어 있는 QR 코드를 스캔한다. 그러면 해당 배달 블록체인 네트워크에 요청을 하게 된다. 이때 네트워크에서는 해당 요청이 스마트 컨트랙트에 등록이 되어있는 스마트 글라스로부터 온 요청인지 확인을 한다. QR 코드를 스캔하는 것은 누구나 갖고 있는 스마트 폰으로 얼마든지 가능하기에 이러한 과정을 거쳐 아무나 QR 코드의 정보에 접근할 수 없도록 한다. 정보 요청을 한 스마트 글라스가 스마트 컨트랙트에 등록되어 있는 기기라면 해당 QR 코드에 기록되어 있는 정보들을 글라스의 마운티드 디스플레이

레이를 통해 택배 운반자에게 전송하고 만약 등록되지 않은 기기나 스마트 글라스로부터의 요청이라면 거절한다. 그리고 이때 요청을 보낸 스마트 글라스의 정보를 블록체인에 저장해 추후 정보에 대한 내부 유출이 발생했을 시 사용할 수 있게 한다. 배달 관련 정보를 성공적으로 전송받게 된다면 운반자는 해당 택배를 배달해야 하는 장소에 안전하게 전달을 한다. 전체적인 구조를 알고리즘 형태로 표 1에 정리하였다.

Table. 1 The algorithm of suggested system

Suggested system algorithm	
1.	Courier scans the QR code on the package and request the waybill information
2.	The request gets sent to the Blockchain network
3.	The Smart Contract checks the validation of the request
3.1	If the request sender is registered, save request record and send waybill information
3.2	If the request sender is not registered, deny request
4.	If the request was successful, delivery package according to the information sent

IV. 시스템 구현

4.1. 제안 기법 구현

본 논문에서 제안하는 기법을 구현하여 동작을 확인하였으며 구현 환경은 표 2와 같다.

Table. 2 Development environment

OS	Windows 10 Pro
IDE	Remix IDE v0.9.4
Language	Solidity 0.5.2
Hardware	Raspberry Pi 3 B+
API	Web3
Module	The Raspberry Pi Camera V2

리믹스는 이더리움 IDE와 도구들을 지원해주는 웹상 개발 환경을 뜻한다. 해당 환경에서는 실제 이더(Ether)가 거래되는 이더리움 메인넷에 접속해 리믹스에서 제작한 스마트 컨트랙트를 이더리움 블록체인 네트워크에 올릴 수도 있으며 롭슨(Ropsten) 또는 리믹스 자체적 가상 환경 같이 테스트넷 환경에서도 스마트 컨트랙트의 기능을 테스트 해볼 수 있는 환경 등을 지원해준다. 또한 메타 마스크(Metamask) 등과 같은 가상 화폐

지갑 서비스와의 연동, 파이썬 및 자바 스크립트 API와의 연동 등 이더리움 블록체인 네트워크에서 스마트 컨트랙트를 제작하는데 있어서 다양한 기능을 제공해준다. 본 논문에서는 구현 결과물에 대한 편리한 테스트를 위해 스마트 컨트랙트를 리믹스 IDE에서 작성하였으며 리믹스에서 제공하는 파이썬 Web3 API 연동 기능을 이용하였다.

Web3는 이더리움과 상호 작용을 위해 이더리움에서 제공하는 라이브러리이다. Web3는 자바스크립트와 파이썬 언어 등을 지원하며, 해당 라이브러리에서 제공하는 API를 사용하여 리믹스와 같은 이더리움 IDE에서 배포한 스마트 컨트랙트와 상호 작용 할 수 있다. 본 논문에서는 파이썬의 Web3 라이브러리를 이용하여 스캔된 QR 코드의 데이터를 블록체인 상에 배포된 스마트 컨트랙트에 전송하여 해당 데이터에 할당하는 주소 정보를 요청할 수 있게 구현하였다. 이때 스마트 컨트랙트에 전송이 되는 데이터로는 QR 코드의 데이터 값과 요청을 보낸 스마트 글라스의 주소 정보가 전송이 된다. 블록체인 네트워크에서 데이터를 전송받으면 해당 데이터를 바탕으로 요청을 보낸 글라스에 대한 검증이 스마트 컨트랙트 상에서 이뤄진다. QR 코드 정보에 대한 추출은 라즈베리파이에 카메라 모듈을 연결하고 이미지 프로세싱 라이브러리 OpenCV와 바코드 및 QR 코드 판독 라이브러리 ZBar을 이용하여 처리하였다.

스마트 컨트랙트 구현은 크게 네 가지 부분을 구현하였다. 먼저 QR 코드에 접근 가능한 택배 기사들의 주소 값을 관리하는 배열 선언, 둘째는 QR 코드와 해당하는 URL 값을 할당해주는 매핑 구조 선언, 세 번째로는 QR 코드에 할당되어 있는 해당 URL 값을 요청하는 함수 부분이며, 마지막으로 해당 QR 코드에 요청을 했던 택배 기사의 주소 값을 저장하는 배열 부분이다. 각 데이터에 대한 구체적인 선언은 표 3과 같다.

Table. 3 Variable definition

Data class	Data Type
Courier	address array
QR code to URL	uint to String mapping
QR code Accessed Address	uint to Address mapping

표 4는 스마트 컨트랙트의 구현부분 중 택배 기사 스마트 글라스를 이용해 QR 코드를 스캔하면 해당 QR 코드에 할당하는 정보를 전송하는 해주는 알고리즘이다.

Table. 4 Algorithm of requesting QR code information

Algorithm1

```

for(uint i = 0; i<courier.length; i++){
    if(msg.sender == courier[i]){
        QRcodeAccessedAddress[QRCode] = msg.sender;
        return QRcodeToURL[QRCode];
    }
    else{ return "Access Denied";
    }
}

```

QR 코드에 담긴 요청이 택배 시스템 블록체인 네트워크 상에 존재하는 스마트 컨트랙트에 전송이 되면 해당 하는 함수가 호출이 되고 함수 내부에서 먼저 요청을 보낸 택배 기사가 네트워크 상에 등록이 되어 있는 사람인지 확인을 한다. 만약 등록되어 있지 않은 대상으로부터의 요청이라면 접근 거부라는 메시지를 반송한다. 등록이 되어있는 대상이라는 것이 확인이 되면 먼저 요청을 한 택배 기사의 정보를 해당 QR 코드와 함께 저장해 추후에 해당 QR 코드와 관련된 택배로부터 개인 정보에 대한 유출이 발생했을 때 어떤 스마트 글라스로부터 요청이 왔는지 확인할 수 있게 기록을 저장한다. 해당 정보 저장 후에 QR 코드 정보에 대한 요청이 코드에 해당하는 운송 및 택배 물품 수취인 관련 정보를 택배 기사에게 반환해준다.

제안한 시스템에 대한 구현물을 테스트하기 위해 시스템에 QR 코드 번호와 해당 번호에 해당하는 URL을 입력한다. 또한 QR 코드에 접근이 가능한 배달기사 1명을 등록하고 시스템에 등록되지 않은 사람 1명을 생성한다. 그림 4는 IDE 상에서 해당 데이터를 입력한 값에 대한 결과이다. 0x147로 시작하는 주소를 갖고 있는 배달기사가 등록이 된 것을 확인할 수 있으며 QR 코드 '0' 번에 임의로 입력한 URL 정보가 성공적으로 들어가 있는 것을 확인할 수 있다.

DeliverySystem at 0x5e7...26e9f (memory)

- addCourier: 0x14723a09acff6d2a60dcdf7aa4aff308fddc160c
- addQRCodeToURL: "0","www.QRtoURLInformation.com"
- QRCodeAccessedAddress: uint256 QRCode
- courier: 0

0: address: 0x14723a09acff6d2a60dcdf7aa4aff308fddc160c

QRcodeAccessedAddress: uint256

QRcodeToURL: 0

0: string: www.QRtoURLInformation.com

Fig. 4 System Implementation data result

해당 데이터 값을 갖고 택배 기사가 택배물에 부착되어있는 QR 코드를 스캔하여 QR 코드에 해당하는 URL을 조회하는 요청을 하게 되었을 시 표 4에 해당하는 알고리즘을 통해 해당 요청이 시스템에 등록이 된 배달기사의 주소로부터의 요청인지 확인을 하고 맞으면 해당하는 URL을 성공적으로 반환한 것을 그림 5를 통해 볼 수 있다.

status	0x1 Transaction mined and execution succeed
transaction hash	0x90de16243af8debe410e6545e6a39fd59506c7f3b78c5d274d5414e595937b7f
from	0x14723a09acff6d2a60dcdf7aa4aff308fddc160c
to	DeliverySystem: QRCodeAccessAndReturnURL(uint256) 0x5e72914535f202659083db3a02c9841881a26e9f
gas	3000000 gas
transaction cost	44211 gas
execution cost	22811 gas
hash	0x90de16243af8debe410e6545e6a39fd59506c7f3b78c5d274d5414e595937b7f
input	0x8f4...,00000
decoded input	{ "uint256 QRCode": "0" }
decoded output	{ "0": "string: www.QRtoURLInformation.com" }
logs	[]
value	0 wei

Fig. 5 Request result using QR code number '0'

또한 해당 요청을 보낸 택배 기사의 정보를 저장해 추후에 해당 택배에 대한 개인 정보 유출이 발생한 경우 사용될 무결성이 보장된 기록이 성공적으로 저장된 것을 그림 6에서 확인할 수 있다.

status	0x1 Transaction mined and execution succeed
transaction hash	0x023f a261d4670e684eac758d120c580a74426e734ede093e20c5f a6cd729f45b
from	0x14723a09acff6d2a60dcdf7aa4aff308fddc160c
to	DeliverySystem: QRCodeAccessedAddress(uint256) 0x5e72914535f202659083db3a02c9841881a26e9f
transaction cost	22071 gas (Cost only applies when called by a contract)
execution cost	671 gas (Cost only applies when called by a contract)
hash	0x023f a261d4670e684eac758d120c580a74426e734ede093e20c5f a6cd729f45b
input	0xecb...,00000
decoded input	{ "uint256 ": "0" }
decoded output	{ "0": "address: 0x14723a09acff6d2a60dcdf7aa4aff308fddc160c" }
logs	[]

Fig. 6 Address of delivery person requesting QR code information

4.2. 성능 평가

기존 택배 시스템에서는 운송장의 정보에 대한 접근이 모두에게 허용이 되어있지만 제안하는 시스템에서

는 허가된 택배 기사들만 가능하다. 또한 제안하는 방식에서는 운송장에 최소한의 식별 데이터만 제외하고 모든 정보를 가리기 때문에 기존의 택배 정보 중 일부분만 가리는 방식보다 안전하다. 또 QR 코드를 사용하기 때문에 해당 배송지에 파손이 발생해도 QR 코드의 정보 복구 기능을 이용하여 정보 손실을 방지할 수 있다. 마지막으로 스마트 글라스를 이용하기 때문에 기존 운반 방식에서는 한 손으로 판독기(Reader)를 사용해야 했던 것과는 다르게 스마트 글라스를 이용하기 때문에 양 손이 자유로워 택배 운반에 있어 편리성을 보장한다. 표 5에서 본 제안 기법과 기존 기법의 비교를 정리한다.

Table. 5 Comparison between conventional and proposed method

	Conventional	Proposed
Access to Information	Everyone	Authorized person only
Information Protection Scope	Cover part of the information (Vulnerable)	Cover all of the information (Well Protected)
Information Recoverability	Impossible	Possible through QR code
Convenience of Delivery	One hand required to hold Reader	Hands free (HMD)

V. 결 론

초 연결 시대가 되어감에 따라 개인정보 보호가 어느 때보다 중요해진 상황이다. 개인정보 유출이 가장 많이 일어나는 곳 중 하나가 택배물의 운송장임에도 불구하고 개인정보 유출을 사전에 방지하는 실용적인 방법이 시행되고 있지 않다. 이에 본 논문에서는 QR 코드를 이용한 개인정보 유출 방지 기법을 제안하였다. 이를 통해 단순히 눈으로는 개인정보를 유출할 수 없게 유도하였고 해당 QR 코드에 대한 무분별한 탈취를 방지하기 위해 해당 정보에 대한 접근 권한을 택배 블록체인 상에 미리 등록되어 있는 스마트 글라스만으로 접근할 것을 제안하였고 해당 정보에 대한 접근 기록을 남겨 추후 내부 유출이 발생할 경우 역추적이 가능할 수 있도록 하였다. 마지막으로 제한하는 방안이 운반업에 관련되어 있는 만큼 운반에 사용하는 두 손이 자유로워야 한다는 점에 중점을 두어 헤드 마운트 디스플레이가 장착되어 있

는 스마트 글라스를 통해 두 손은 택배를 운반하는데 사용할 수 있으면서 동시에 운송장의 정보를 읽을 수 있는 기법을 제안하였다.

본 논문에서 사용된 기술들은 컴퓨터 공학의 기술이지만 이를 바탕으로 사회 공학적인 문제점에 대한 해결책을 제안하였다. 이와 같이 개인정보 유출 방지를 위한 대안을 한 분야만으로 접근하는 것이 아닌 다양한 분야와 기술의 융합[12, 13]을 통해 더 안전하고 나은 방안을 모색할 수 있도록 지향되어야 할 것이다.

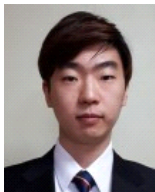
ACKNOWLEDGEMENT

This work was partially supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2017R1C1B5075742) and this work was partially supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services). This research was financially supported by Hansung University for Hwajeong Seo.

References

- [1] The Radio News. (2018, October). 6 billion unauthorized leaks of personal information over 10 years [Internet]. Available: <http://www.jeonpa.co.kr/news/articleView.html?idxno=59734>.
- [2] JTBC. (2018, April). The personal information by the delivery package is still exposed [Internet]. Available: http://news.jtbc.joins.com/article/article.aspx?news_id=NB11622256.
- [3] Security News. (2016, May). Personal information accidentally leaked by delivery service [Internet]. Available: <https://www.boannews.com/media/view.asp?idx=50589&page=1&kind=1>.
- [4] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic cash System" *metzdowd.com*, Oct. 2009.
- [5] J. Y. Lee, C. W. Woo, Prospects, "Limitations and Implications of Blockchain Technology," *FUTURE HORIZON*, vol. 38, no. 4, Dec. 2018.
- [6] Ethereum. A Next-Generation Smart Contract and

- Decentralized Application Platform [Internet]. Available: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf.
- [7] Hyperledger. An Introduction to Hyperledger [Internet]. Available: <https://www.hyperledger.org/>.
- [8] M. Shniberg, Y. Nemet, and E. Sali, "Method for automatic identification and data capture," US Patent US6801245B2, Jan. 2002.
- [9] CNET. (2020, January). The smart glasses that could be ready for my eyes[Internet]. Available: <https://www.cnet.com/news/the-smartglasses-that-could-be-ready-for-my-eyes/>.
- [10] Google AR & VR. (2019, May).Google Enterprise Edition 2: A hands-free device for smarter and faster hands-on work [Internet]. Available: <https://www.youtube.com/watch?v=5IK-zU51MU4>.
- [11] CNA. (2017, September).Ground Handlers at Changi Airport to get smart glasses to help speed up operations [Internet]. Available: <https://www.channelnewsasia.com/news/singapore/ground-handlers-at-changi-airport-to-get-smart-glasses-to-help-9187596>.
- [12] Y.-B. Kwon, K.-H. An, H.-D. Kwon, and H.-J. Seo, "CCTV Cooperation Authentication Model Using Block Chain," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 23(4), 462 - 469. Apr. 2019.
- [13] K. An and H. Seo, "Donate system development using Blockchain technology," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 22(5), 812-817, May. 2018.



최승주(Seung-Joo Choi)

2019년 2월: 한성대학교 영어영문학과 학사
2019년 3월~현재: 한성대학교 IT융합공학과 석사과정
※관심분야: 블록체인, IoT



심민주(Min-Joo Sim)

2020년 2월 : 한성대학교 IT융합공학부 학사 졸업예정
※관심분야: 네트워크 보안, 시스템 보안



서화정(Hwa-Jeong Seo)

2010년 2월 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월 부산대학교 컴퓨터공학과 석사 졸업
2012년 3월~2016년 1월: 부산대학교 컴퓨터공학과 박사 졸업
2016년 1월~2017년 3월: 싱가포르 과학기술청
2017년 4월~현재: 한성대학교 IT 융합공학부 조교수
※관심분야: 암호 구현