

석사학위논문

스마트 글라스 활용 택배 운송
효율성 향상 및 개인 정보 보호
블록체인 시스템

2021년

한 성 대 학 교 대 학 원

I T 융 합 공 학 과

I T 융 합 공 학 전 공

최 승 주

석 사 학 위 논 문
지도교수 서화정

스마트 글라스 활용 택배 운송
효율성 향상 및 개인 정보 보호
블록체인 시스템

Blockchain system for improving delivery efficiency and
protecting personal information using smart glasses

2020년 12월 일

한 성 대 학 교 대 학 원

I T 융 합 공 학 과

I T 융 합 공 학 전 공

최 승 주

석사학위논문
지도교수 서화정

스마트 글라스 활용 택배 운송
효율성 향상 및 개인 정보 보호
블록체인 시스템

Blockchain system for improving delivery efficiency and
protecting personal information using smart glasses

위 논문을 공학 석사학위 논문으로 제출함

2020년 12월 일

한성대학교 대학원

IT융합공학과

IT융합공학전공

최 승 주

최승주의 공학 석사학위 논문을 인준함

2020년 12월 일

심사위원장 _____(인)

심 사 위 원 _____(인)

심 사 위 원 _____(인)

국 문 초 록

스마트 글라스 활용 택배 운송 효율성 향상 및 개인 정보 보호 블록체인 시스템

한 성 대 학 교 대 학 원

I T 융 합 공 학 과

I T 융 합 공 학 전 공

최 승 주

개인정보 보호의 중요성이 어느 때보다 주목을 받고 있다. 그러나 택배 시스템은 이러한 개인정보 보호에 대한 움직임을 아직 따라가지 못하고 있다. 택배 상자에는 수취인에 대한 민감한 개인정보인 이름, 전화번호, 주소 등이 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 운송장의 정보가 들어있는 QR 코드에 대한 무분별한 접근을 방지하기 위해 정보에 대한 접근은 택배 시스템의 블록체인 네트워크에 미리 등록되어 있는 스마트 글라스만을 사용하여 접근할 수 있게 한다. 또한 블록체인에 등록되어 있는 스마트 글라스를 보유한 사람인 택배 기사로부터 운송장 QR 코드에 담겨있는 개인정보가 택배 회사 내부적으로 유출되는 것을 방지하기 위해 운송장 정보에 대한 접근 기록을 블록체인에 기록할 것을 제시한다. 마지막으로 택배 운송의 효율성을 높이기 위해 AR 기술을 스마트 글라스를 통해

택배 운송에 적용할 것을 제안하며 표를 통해 기존 택배 시스템과 본 논문에서 제안하는 방식의 차이를 비교한다.

【주요어】 개인 정보 보호, 블록체인, 스마트 글라스, QR 코드, AR

목 차

제 1 장 서 론	1
제 1 절 택배 시스템	1
제 2 절 문제 제기 및 해결 방안 제안	3
제 3 절 논문 구성	5
제 2 장 관련 연구	6
제 1 절 훔쳐보기 공격	6
제 2 절 운송장 정보 보호 방안	7
제 3 절 블록체인	8
1) 블록체인의 무결성 및 종류	8
2) 스마트 컨트랙트	10
제 4 절 스마트 글라스	11
제 5 절 QR 코드	12
제 6 절 AR	13
제 3 장 공격 시나리오	15
제 1 절 외부 공격 시나리오	15
제 2 절 내부 공격 시나리오	17
제 4 장 제안 기법	18
제 1 절 개인 정보 보호	18
1) 시스템 설계	18
2) 시스템 구현	23
제 2 절 운송 효율성 향상	33

제 5 장 성능 평가	38
제 1 절 실험 환경	38
제 2 절 기존 시스템 평가	38
제 3 절 제안 시스템 평가	39
제 6 장 결론 및 향후 연구 방안	41
참 고 문 헌	42
ABSTRACT	44

표 목 차

[표 4-1] 택배 보안 단계별 특성	22
[표 4-2] 제안 시스템 구현 환경	23
[표 4-3] 스마트 컨트랙트 변수 및 구조체 정의	25
[표 4-4] QR 코드 운송장 정보 조회 요청 알고리즘	27
[표 5-1] 기존 시스템과 제안 시스템 비교	39

그 립 목 차

[그림 1-1] 택배 운송 절차	1
[그림 1-2] 택배 운송장 예시	2
[그림 1-3] 국민 1인당 택배이용 횟수 추이(개)	3
[그림 1-4] 공공 및 민간 분야 개인정보보호 현황	4
[그림 2-1] 훔쳐보기 공격 및 과정	6
[그림 2-2] 현존하는 운송장 개인 정보 유출 방지 방안	7
[그림 2-3] 해시 값으로 연결된 블록체인 구조	9
[그림 2-4] 스마트 컨트랙트를 활용한 중계자 없는 거래	11
[그림 2-5] 바코드와 QR 코드	12
[그림 3-1] 운송장 개인 정보에 대한 외부 공격 시나리오	16
[그림 3-2] 택배 운송장 취합을 통한 원본 정보 취득	17
[그림 4-1] 개인 정보 유출 방지 택배 시스템 프로세스	19
[그림 4-2] 택배 시스템 각 단계별 절차	21
[그림 4-3] QR 코드의 운송장 정보 요청 흐름도	26
[그림 4-4] 스마트 글라스 운송장 조회 권한 등록	29
[그림 4-5] 운송장 정보 및 정보 조회 비밀번호 등록	30
[그림 4-6] 등록된 스마트 글라스로부터의 운송장 정보 조회 요청	31
[그림 4-7] 물품 수취인으로부터의 운송장 정보 조회 요청	32
[그림 4-8] 악의적 공격자로부터의 운송장 정보 조회 요청	32
[그림 4-9] 스마트 글라스의 시야 방해 현상	34
[그림 4-10] 증강 현실 활용 직관적 운송장 조회 및 운송 효율성 향상	35
[그림 4-11] 색깔 밝기와 명도를 활용한 직관적 거리 계산	36

제 1 장 서론

제 1 절 택배 시스템

택배, 즉 물류는 화물이 수송, 보관, 하역을 거쳐 이동하는 과정을 뜻한다. 이러한 물류 산업은 대한민국 GDP의 약 10%를 차지하는 거대한 산업 중 하나이다. 이러한 택배는 [그림 1-1]과 같은 절차를 통해 소비자들이 물건을 구매하기 위해 직접 물건을 판매하는 상점을 갈 필요 없이 물품을 소비자들에게 전송해주며 이러한 시스템을 활용해 접근하기 특히 힘든 해외에서 물건을 구매하는 것 또한 가능하다.



[그림 1-1] 택배 운송 절차

택배로 전송되는 물품에는 [그림 1-2]과 같은 해당 물품의 정보가 들어있는 운송장(Waybill)이 부착되어있다. 운송장은 화물의 운송에 필요한 정보를 기록해둔 서류로서, 줄여서 ‘송장’이라고 부르기도 한다. 운송에 필요한 기본적인 정보로는 물품을 보내는 사람과 물품을 받는 사람의 이름, 주소, 전화번호, 물품 정보가 들어간다. 또한 전산 처리를 위해 운송장마다 고유번호를 붙여 관리를 용이하게 만든다. 온라인 쇼핑몰에서 물건을 주문하는 경우, 해당 물품에 부여된 운송장의 송장 번호를 통해서 해당 물건에 대한 배송 추적이 가능하다. 뿐만 아니라 전달 받은 물품이 파손되거나 분실되는 경우 사건이 일어난 위치를 추적하여 책임소재를 분명히 할 수 있게 해준다. 이처럼 운송장은 택배 운송에 있어 필수적인 요소이다.

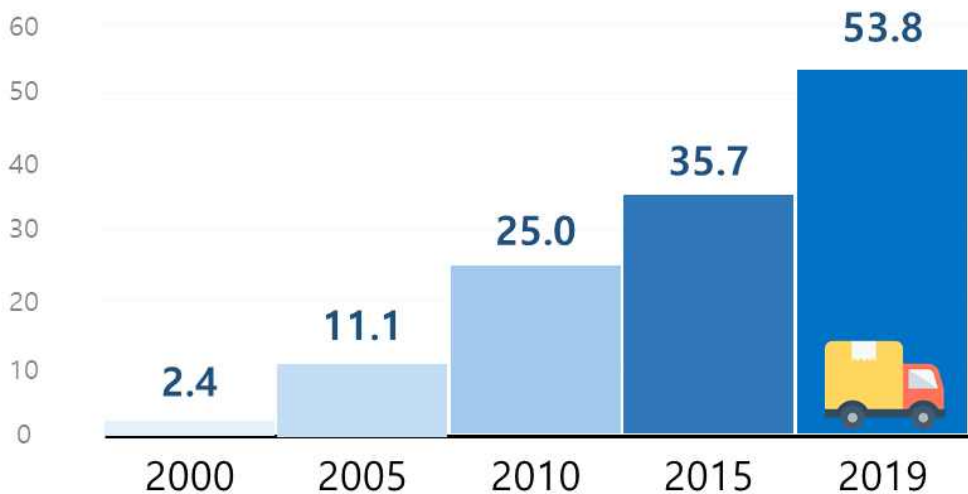
 D21-0d	SENDER: 000 Info :
SAMPLE WAYBILL	RECEIVER: 000 Info :
	WAYBILL NUMBER: 6381-0011-3333 

[그림 1-2] 택배 운송장 예시

최근 코로나 19 확산 사태로 인해 비대면 경제 상황이 예상보다 장기화되면서 비대면 서비스들이 전성시대를 맞고 있다. 특히 앞서 설명한 사람과 접촉하지 않아도 필요한 생활품이나 소비자들이 원하는 물건을 운반해주는 택배 및 배송 서비스의 사용은 작년에 비하여 대폭 상승하였다. 한국통합물류협회에 의하면 지난해 대한민국 국민의 평균 택배 이용회수는 [그림 1-3]에서 보는 것과 같이 꾸준히 증가하고 있으며 2019년 기준으로 53.8회를 달성하였다. 또한 경제활동 인구 한명 당 평균 택배 이용 회수는 99.3회에 이르렀다. 코로나 19 사태로 인해 택배물동량은 약 30%가량 증가하였으며 이로 인해 국내 1, 2위 택배 회사의 2020년 2분기 영업 이익은 동년 대비 각각 16.8%, 24.7% 늘게 되었다.

해외 또한 국내의 상황과 마찬가지로 택배 이용률이 매년 증가하고 있다. 특히, 코로나 19 사태로 인해 2020년 택배 서비스 산업의 성장률은 5.11%를 달성하였으며 연평균 성장률은 6%가 될 것으로 예상되고 있다.

이처럼 택배 시스템은 물류를 전달해주는 산업뿐만 아니라 코로나 19 사태에 대응하는 중요한 방안 중 하나로 성장해나가고 있다.



[그림 1-3] 국민 1인당 택배이용 횟수 추이(개)

제 2 절 문제 제기 및 해결 방안 제안

1절에서 언급한 것과 같이 코로나 19 사태 등으로 인해 택배 서비스의 사용이 크게 증가함에 따라 매년 증가해 왔던 택배 관련 범죄 역시 크게 증가하였다. 특히 민감한 개인정보를 포함하고 있는 택배의 운송장으로부터 개인정보를 탈취해가 악용하는 범죄 사례가 점점 증가하고 있다.

현재 개인정보의 보호에 대한 사회적 관심은 과거에 비해 많이 증가한 상태이다. 특히 2019년에 시행된 데이터 3법 개정 추진, 국외사업자에 대한 대리인 지정제도 신설, EU 적정성 결정 대응 등의 일들을 통해 우리 사회의 개인정보 보호에 대한 관심은 그 어느 때보다 주목을 받았다. 이러한 움직임에 맞춰 [그림 1-4]에 나온 것과 같이 공공 민간분야의 개인정보보호 교육률은 각각 47.03%, 13.65% 증가하였으며 개인정보 비식별 조치 기술 지원 비율은 2018년에 비하여 2019년에는 113.7% 증가하였다. 이러한 사회적 관심 덕분에 개인정보침해 신고센터의 상담 접수 건수는 약 3.2%로 감소해 나가고 있는 추세이다.



[그림 1-4] 공공 및 민간 분야 개인정보보호 현황

그러나 2010년부터 2020년 사이 국내에서 발생한 개인정보 유출 사례 60억 건 중에서 정보 유출이 발생하는 주된 경로 중 하나로 뽑히는 것이 택배임에도 불구하고 택배 상자의 운송장에 포함되어있는 이름, 전화번호, 거주자 정보 등 민감한 개인정보에 대한 보호는 여전히 무관심한 상태이다.

모든 택배에는 택배의 정보를 담고 있는 운송장이 부착되어 있으며 운송장의 내용은 운반 품목 정보, 고객 정보, 배달표 등으로 구성이 된다. 운송장에는 물품 송신인이 보낸 또는 수신인이 주문한 물품에 대한 정보와 수신인의 성명, 거주지 정보 그리고 전화번호가 그대로 적혀있다. 이런 개인 정보들은 탈취가 되면 장난전화, 성희롱 전화, 택배기사로 위장 접근 등의 사건을 발생하는데 악용이 되며 특히, 보이스피싱 등 다양한 개인정보 악용 범죄의 표적이 될 수 있다. 이와 같은 개인정보 유출로 인한 피해 현황은 2017년 2,431억 원보다 82.7%, 약 2009억 원 증가한 4,440억 원으로 역대 최고치에 도달한 상태이다. 피해자의 수는 3만919명에서 4만8,743명으로 57.6% 증가하였다.

해외 사례로는 2016년 중국의 한 택배사에서 택배 운송장 실명제를 도입하였다가 개인정보 유출사고가 매우 심각해져 운송장에 개인정보를 표기하지 않고 대신 바코드만 붙이게 된 사례가 있다. 국내에서는 택배의 운송장에 적힌 개인정보를 통한 정보 유출 및 악용에 대한 대응 방침으로 운송장에 적혀 있는 이름과 물품 수신자의 전화번호의 일부를 표기하지 않거나 택배를

받은 뒤 택배에 부착되어 있는 운송장을 쉽게 떼어 파기할 수 있게 운송장을 제작하는 등의 방안을 실행하고 있다. 일반적으로 택배 상자와 운송장은 수령인이 택배를 수령하기 전에 운송장에 적혀있는 정보를 누구든지 쉽게 접근할 수 있으며 유출될 수 있는 상태이다. 또한 앞서 언급한 운송장에 적힌 개인정보를 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 논문에서는 택배의 운송장이 지난 개인정보 유출 취약점을 개선할 수 있는 새로운 택배 시스템을 제안한다. 제안하는 기법을 통해서는 일반적인 시각적인 방법으로는 운송장에 담겨져 있는 개인정보를 읽을 수 없게 된다. 해당 방식을 위해 QR 코드와 이를 읽을 수 있는 기기 그리고 블록체인을 사용할 것을 제안한다. 또한 운송장의 정보에 보안을 적용하는 만큼 발생할 수 있는 실용성 및 편의성 저하를 방지하기 위해 스마트 글라스와 증강 현실 기법을 사용할 것을 제안한다.

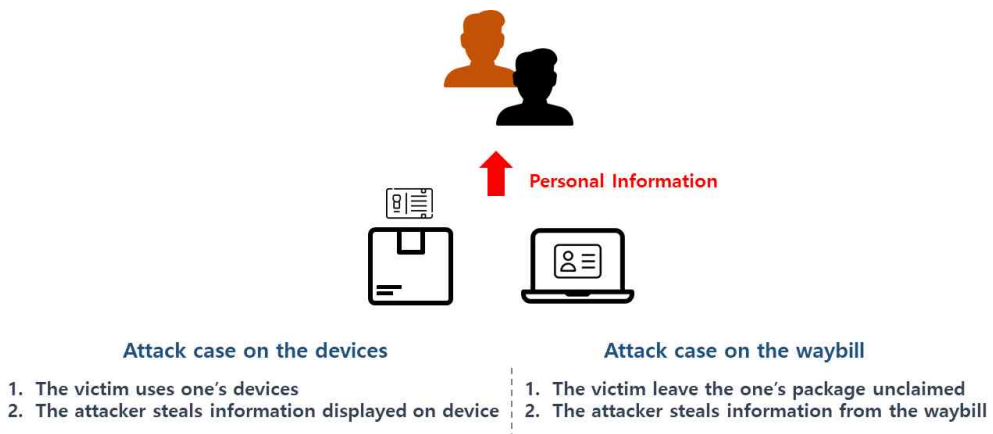
제 3 절 논문 구성

본 논문의 구성은 다음과 같다. 2장에서는 훔쳐보기 공격에 대한 기법과 현존하는 운송장 정보 방법들에 대한 소개를 한다. 또한 블록체인과 스마트 컨트랙트, QR 코드 및 바코드, 스마트 글라스(Smart glasses), 증강 현실(AR) 등 관련 연구에 대해 살펴보며, 3장에서는 공격 시나리오에 대해서 확인한다. 이어서 4장에서는 제안하는 기법에 대한 소개와 제안 기법의 보안적인 측면과 택배 운송의 효율성에 대하여 설명한다. 5장에서는 제안한 기법을 구현한 프로토타입에 대한 실험 환경 소개와 기존 택배 시스템과 제안하는 택배 시스템에 대한 분석과 비교를 진행한다. 마지막으로 6장에서는 본 논문의 결론을 내리고 향후 과제를 제시한다.

제 2 장 관련 연구

제 1 절 훔쳐보기 공격

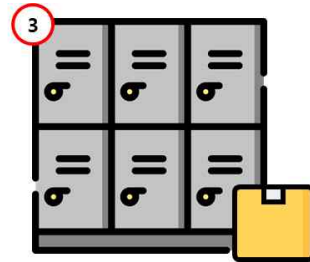
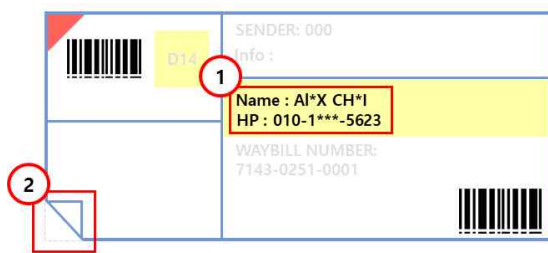
훔쳐보기 공격(Shoulder Surfing Attack)은 기본적으로 보안적인 측면에서 사용되는 용어이다. 특정 장치의 키(Key) 입력이나 또는 말하고 있는 내용을 피해자의 어깨 너머로 개인 식별 번호(PIN), 암호 및 기타 기밀 데이터와 같은 정보를 얻는데 사용되는 일종의 사회 공학 기술이다. 쉽게 말하면 어깨 너머로 다른 사람이 사용하고 있는 기기의 화면을 몰래 훔쳐봐 암호나 정보 등을 탈취하는 행위나 도청행위라고 볼 수 있다. 본 논문에서는 이러한 훔쳐보기 공격의 정의를 조금 더 확장해 꼭 피해자가 사용하고 있는 기기 등으로부터의 탈취뿐만 아니라 사용자의 정보가 적혀있는 텍스트에 대한 허가되지 않은 모든 접근 및 탈취 방식을 훔쳐보기 공격이라고 정의한다. 구체적인 공격 형태는 [그림 2-1]과 같다. 이러한 훔쳐보기 공격의 특징으로는 서비스 거부 공격(Distributed Denial of Service)이나 네트워크를 통한 해킹 등과 같은 공격과는 다르게 공격 방식이 사람의 오감 중에서 특히 시각과 청각을 통해서 이루어진다는 점이다.



[그림 2-1] 훔쳐보기 공격 및 과정

제 2 절 운송장 정보 보호 방안

운송장을 통해 개인 정보가 유출이 되는 것을 방지하기 위해 [그림 2-2]과 같은 여러 가지 방식이 도입되고 있다. 먼저 운송장에 적혀있는 이름과 전화번호의 일부를 별 표시와 같은 다른 텍스트로 변경하여 내용의 일부를 가리는 방식을 택하고 있다. 또한 운송장의 정보가 유출이 되는 많은 경우가 택배 상자에 붙어있는 운송장을 제거하지 않은 상태에서 상자를 버렸다가 일어나는 경우에 대해 대응하기 위해 운송장을 쉽게 떼어 파기할 수 있게 운송장을 제작하는 등의 대응 방안을 택하고 있다.



1. Masking some of the information

- Can be combined to reveal original information
- Related information can be searched through online

2. Easily removable waybill

- Effective only when receiving the package immediately

3. Unmanned parcel dropbox

- Installation is required
- Non-installed area cannot be protected

[그림 2-2] 현존하는 운송장 개인 정보 유출 방지 방안

그러나 각 방식의 한계점으로는 먼저 운송장의 일부를 가리는 방식이 각 택배사마다 다르기 때문에 결국 여러 택배의 운송장의 정보를 조합하면 원본 정보를 알아낼 수 있다. 설령 모든 택배사가 동일한 부분의 정보를 가린다고 하여도 남은 정보들의 조합만을 갖고도 온라인상에서 쉽게 수취인을 찾아낼 수 있으며 이를 통해 수취인에 대한 신상과 사생활을 캐낼 수 있다. 택배 운송장을 쉽게 떼어 버리는 방식은 수취인이 택배가 도착했을 때 바로 택배를

받을 경우에만 정보 보호의 효과가 있다. 그러나 일반적인 직장인들의 생활 특성상, 특히 코로나 19 사태로 인해서 많은 경우, 택배가 문 앞 또는 지정된 보관 장소에 오랜 시간 방치가 되어 있는 경우가 대부분이다. 물론 무인택배 보관소 등과 같은 대응 방안도 존재하지만 이와 같은 보관소가 설치되어 있는 곳은 매우 한정적이다.

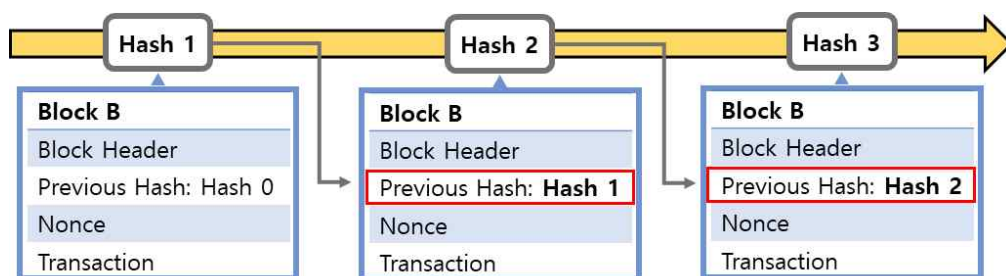
제 3 절 블록체인

블록체인이란 P2P(Peer-to-Peer) 네트워크 환경 상에서 기록하고 있는 동일한 전자 장부에 대한 데이터를 네트워크에 참여하고 있는 노드들이 공유하고 관리하는 네트워크이다. 블록체인에서 사용되는 전자 장부에 기록된 내용은 네트워크에 참여한 다수의 노드가 함께 장부의 내용을 공유하고 각 노드가 갖고 있는 장부의 내용이 동일한지 검증한다. 이 때문에 공유 장부에 적힌 내용을 하나의 노드가 악의를 품고 단독으로 위조 및 변조하기 매우 어렵다는 특징이 있다. 이러한 블록체인의 특징을 바탕으로 블록체인 상에서는 코인 또는 토큰이라는 가상 화폐 개념을 도입하여 제 3의 인증기관이나 중개자의 개입 없이 익명의 대상간의 거래에 사용하기도 한다.

1) 블록체인의 무결성 및 종류

블록체인의 공유 전자 장부의 기록은 [그림 2-3] 같은 구조에 의해 처리가 되기 때문에 기록에 대한 위조 방지가 가능해진다. 블록체인 네트워크상에서 발생된 모든 거래 내역, 즉 트랜잭션에 대한 정보는 블록이라는 구조체에 저장되어 네트워크에 기록이 된다. 이러한 블록은 채굴자(miner)라는 네트워크 참여자에 의해 형성이 되며 가장 많은 블록이 형성된 장부의 기록을 검증 과정을 통해 공식 장부로 인정을 하게 된다. 블록에 들어가는 내용으로는 거래 발생 시간, 논스 값 그리고 이전 블록의 해시 값 등이 저장 된다. 이때 이전 블록의 해시 값을 저장하는 구조 때문에 해시 값을 바탕으로 마치 각 블록이 체인으로 연결된 듯한 형태가 형성되

된다. 만일 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 블록을 형성하는 다른 채굴자(miner)들의 연산 속도를 앞지르면서 본인만의 블록체인을 형성하는 것은 사실상 불가능하기 때문에 위조 및 변조에 대한 내성을 지니고 있다.



[그림 2-3] 해시 값으로 연결된 블록체인 구조

최초로 세상에 공개된 블록체인은 비트 코인으로 개방형(Public) 블록체인 형태를 띠고 있다. 개방형, 또는 퍼블릭 블록체인이란 블록체인 네트워크에 누구나 참여할 수 있으며 해당 블록체인 네트워크에 블록을 형성하는 채굴자가 될 수 있음을 의미한다. 그러나 최근에는 이와 같은 퍼블릭 블록체인의 불필요한 연산 문제, 익명성 문제, 탈중앙화의 실패 등 여러 가지 한계점을 고려하여 개인형, 즉 프라이빗 형태의 블록체인도 공개되고 있다. 이러한 프라이빗 블록체인의 특징으로는 해당 블록체인 네트워크에 참여하고자 하는 대상은 해당 프라이빗 블록체인 네트워크를 운영하고 있는 기업 또는 개인의 허락을 받아야 참여할 수 있다는 점이다. 이와 같은 프라이빗 블록체인의 특징을 이용하여 퍼블릭 블록체인이 갖고 있었던 불필요한 연산 처리 과정 등을 생략할 수 있으며 아예 블록 형성의 방식을 투표 형식으로 대처하거나 블록 생성 시간을 단축하는 등 블록체인 네트워크를 공개한 상태로 운영할 필요가 없는 기관에서 주로 활용한다.

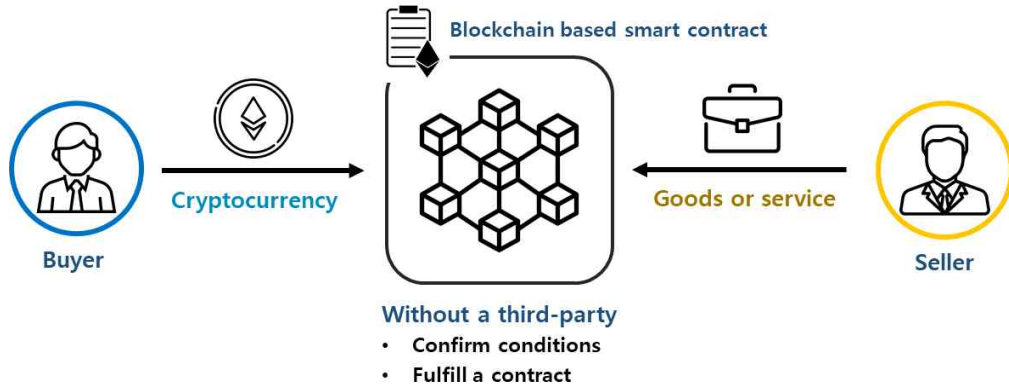
본 논문에서 제안하는 블록체인 활용 개인 정보 보호 시스템에서는 앞서 설명한 프라이빗 블록체인 환경에서 시스템을 구축할 것을 제안한다.

제안하는 시스템에서 블록체인 네트워크는 운송장 관련 정보를 저장하며 또한 해당 운송장 정보에 대한 접근 기록을 남겨 외부뿐만 아니라 내부적으로도 발생할 수 있는 개인 정보 유출 사태에 활용할 수 있게 할 것을 제안한다. 이를 통해 개인 정보 유출 경로 및 접근 대상을 쉽게 추적할 수 있게 된다.

2) 스마트 컨트랙트

1994년 최초로 제안된 스마트 컨트랙트란 디지털로 만들어진 계약서를 뜻한다. 이와 같이 디지털화 된 스마트 컨트랙트는 계약 시행 결과가 명확하고 계약 내용에 의거, 조건이 충족되면 즉각 이행할 수 있다는 특징을 갖고 있다. 블록체인은 기본적으로 무결성이라는 특징을 바탕으로 하기 때문에 이러한 특징은 스마트 컨트랙트의 개념을 도입하기 매우 적합하였다. 하여 제 2세대 블록체인이라는 이더리움에서 블록체인에 스마트 컨트랙트를 도입하였다. 이러한 스마트 컨트랙트는 이더리움에서 제작한 솔리디티(Solidity)라는 컴퓨터 언어를 통해 계약과 관련된 로직을 형성할 수 있으며 블록체인 네트워크 상에 등록할 수 있다. 현재는 이더리움 이후에 나온 거의 대부분의 블록체인은 이러한 스마트 컨트랙트 개념을 각자의 블록체인 네트워크에 포함시켜 배포를 하고 있는 상태이다.

이와 같은 블록체인의 스마트 컨트랙트는 탈중앙화 어플리케이션(DApp, Decentralized Application)을 제작하는데 많이 사용이 되며 이를 통해 토큰 개념이 등장하는 등 다양한 재산과 서비스, 또한 비즈니스를 함에 있어서 [그림 2-4]에서 볼 수 있는 것과 같이 중개자를 없애 절차와 비용을 간소화 시키는 등 다양한 방식으로 활용되고 있다.



[그림 2-4] 스마트 컨트랙트를 활용한 중계자 없는 거래

제 4 절 스마트 글라스

스마트 글라스는 헤드 마운티드 디스플레이(HMD; Head Mounted Display)가 장착된 착용 컴퓨터이다. 테블릿, 스마트 폰 등과 같은 디바이스의 경우 본인이 확인하고 싶은 정보를 보기 위해서는 해당 디바이스를 손에 들고 확인하고자 하는 정보를 검색해 확인해야하는 반면 스마트 글라스는 사용자가 보고자 하는 정보를 바로 시야에 보여줄 수 있다는 편리함의 장점을 갖고 있다. 이와 같이 정보를 확인하기 위해 따로 손을 사용하지 않아도 된다는 핸즈프리(Hands Free) 특징을 갖고 있는 스마트 글라스는 두 손을 모두 사용해야하는 제조 업종 등에서 매우 유용하게 활용이 될 수 있는 잠재력을 가지고 있다. 뿐만 아니라 증강현실(AR; Augmented Reality)과 같은 기술의 발전으로 인해 증강현실 기술을 스마트 글라스에 적용하는 연구 또한 활발히 이뤄지고 있다.

스마트 글라스는 삼성, 화웨이 그리고 구글 등 다양한 기업들에서 개발 중에 있으며 2019년 구글에서는 2012년 공개 했었던 구글 글라스를 발전 시킨 기업용 구글 글라스 2를 발표하였다. 싱가포르 공항에서는 스마트 글라스를 공항 물류 관련 직원들에게 배포하여 실시간 지시 사항 전달, 공지 사항 전달, 수하물 분류 등에 적극적으로 활용 하였으며 스마트 글라스를 도입한 이후 더 이상 추가적인 디바이스를 수하물 처리 과정에 있어서 손

에 들고 있을 필요가 없는 덕분에 수하물 하차 시간이 스마트 글라스를 사용하지 않았을 때보다 약 25% 감소하였다는 보고가 있다.

이와 같은 스마트 글라스를 사용하면 택배 운반 기사들의 물품 운반 편리성을 극대화 할 수 있으며 동시에 운반 물품에 대한 운송 정보 또한 손쉽게 확인할 수 있다.

제 5 절 QR 코드

바코드(Barcode)는 컴퓨터가 읽을 수 있도록 고안된 굵기가 다양한 흑백 막대들을 조합시켜 만든 코드로, 주로 제품의 포장지에 인쇄가 되어 제품의 가격, 정보 등을 담고 있다. 이런 막대의 형태의 바코드를 선형 바코드 또는 1차원 바코드라고 한다.

제품에 대한 가격, 정보 등을 바코드 형식으로 저장하고 읽어내는 방식은 전 세계적으로 가장 흔하게 쓰이고 있다. 이와 같은 방식이 갖고 있는 특징으로는 정보의 판독 속도가 매우 빠르다는 점과, 담겨진 정보가 잘 손상되지 않는 정보의 무결성 그리고 편리성 때문에 다양한 분야에서 사용이 되고 있다. 바코드의 첫 출현 이후 지금까지 바코드에 더 많은 정보를 담고 더 빠르게 정보를 읽을 수 있게 하기 위한 연구가 오랫동안 진행되어져 왔다.



[그림 2-5] 바코드와 QR 코드

바코드에 대한 연구의 결과물로 바코드를 개선해서 나온 것이 QR 코드이다. QR 코드는 ‘Quick Response’ 코드라는 의미로 말 그대로 빠른 응답을 얻을 수 있다는 뜻을 지니고 있다. QR 코드의 장점으로는 여러 가지가 있다.

먼저 물류 업계에서 가장 많이 사용되어 왔던 1차원 형태의 바코드의 용량을 확장하여 바코드 보다 더 많은 양의 정보를 담을 수 있다. [그림 2-5]에서 볼 수 있는 것처럼 바코드는 1차원적 구조로 데이터를 담는 반면에 QR 코드는 2차원의 형태로 데이터를 담는다. 바코드와 같은 경우 특정 상품명이나 제조사 등의 정보 정도의 데이터만 저장할 수 있지만 QR 코드와 같은 경우 URL, 위치 정보, 심지어 사진 등 훨씬 더 많고 다양한 정보를 저장할 수 있으며 숫자는 최대 7089자, 영문자와 숫자 최대 4296자를 담을 수 있다. QR 코드의 또 다른 장점으로서는 데이터의 무결성을 바코드보다 훨씬 더 강력하게 보장해준다는 점이다. 이는 QR 코드에는 바코드와는 다르게 오류복원 기능이 있기 때문이다. 이 때문에 QR 코드의 일부분이 손상되거나 오염이 되어도 담고 있던 데이터를 복원할 수 있다. QR 코드의 마지막 장점으로서는 기존의 바코드보다 인식이 쉽고 편리하다는 점이다. QR 코드의 형태는 정사각형을 띄고 있어 360도 어느 방향에서든 코드를 스캔하여도 정확하게 인식이 된다.

이러한 QR 코드가 갖고 있는 장점은 특히 택배 배송에 사용되기 매우 적합하다. 360도 어느 방향에서 스캔을 하더라도 정보가 읽히기 때문에 택배 운반자가 택배를 스캔할 때 편리함을 줄 수 있다. 또한 택배 운반 과정에서는 택배 운송장에 물품간의 충격으로 인해 손상이 갈 수 있는데 QR 코드는 오류복원 기능이 있기 때문에 물품에 대한 정보를 훨씬 더 안전하게 보호할 수 있다. 또한 QR 코드는 앞서 말한 것과 같이 URL 또는 이미지 또한 담을 수 있기 때문에 운송장에 담겨져 있는 정보를 텍스트뿐만 아니라 이미지의 형태로도 조회가 가능하며 이를 통해 택배 운반자가 운송장의 정보를 빠르게 조회할 수 있게 된다.

제 6 절 증강 현실

증강 현실이란 실제로 존재하는 환경에 가상의 사물이나 정보를 합성하여 마치 원래의 환경에 존재하는 사물처럼 보이도록 하는 컴퓨터 그래픽 기법을 뜻한다. 스마트폰, 태블릿 PC 또는 앞서 말한 스마트 글라스

형태 등의 디바이스를 통해 보이는 이미지에 추가적인 정보를 실시간으로 덧붙여 향상된 현실을 보여주는 기술이다. 이러한 증강 현실 기술의 목적은 기술 사용자가 증강된 가상정보와 상호작용함으로써 작업 효율성을 향상시키는 것을 목적으로 한다. 최근 VR 기술의 대중화와 더불어 같이 주목을 받고 연구되어진 증강 현실의 개념은 이미 오래전부터 존재해왔던 기술이다. 1997년 로널드 아즈마에 의해 구체화 되었으며 증강 현실을 현실의 이미지와 가상의 이미지를 결합한 것, 실시간으로 상호작용이 가능한 것, 3차원의 공간 안에 놓인 것으로 정의를 하였다.

증강 현실의 장점으로서는 현실감이 뛰어나고 편리하다는 점에 있다. 또한 감성적 측면의 만족도가 높기 때문에 방송은 물론 게임, 교육, 오락, 쇼핑 같은 다양한 분야에서 응용이 가능하다. 특히, 증강 현실이 가장 대중적으로 알려지게 된 계기가 된 2016년 출시한 포켓몬스터 고(Pokemon GO)를 통해 증강 현실의 뛰어난 현실감과 편리성 그리고 오락성이 증명되었다. 이와 같은 증강 현실은 앞서 말한 스마트 글라스와 같이 활용하면 오락뿐만 아니라 물류 기업, 장비 제조사 등 다양한 분야에서 업무 효율성과 편의성 모두 증가시킬 수 있다. 실제로 농업용 장비 제조사 AGCO, 물류기업 외, 종합 제조기업 GE 등을 비롯한 다양한 기업에서 증강 현실을 적용하였다. 그 결과 제조업에서의 조립시간은 25% 단축시킬 수 있었으며 완성품 검사시간을 30% 줄이는 효과 등을 볼 수 있었다.

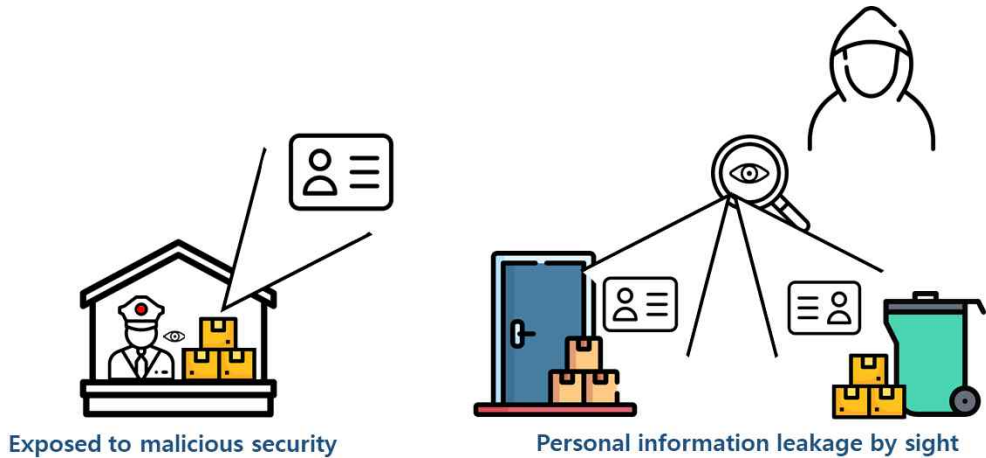
이와 같은 증강 현실 기술과 앞서 언급한 스마트 글라스를 택배 운송업에 적용을 하면 택배 운송장 정보를 양 손이 모두 자유로운 상태에서 확인할 수 있을 뿐만 아니라 택배 상자 위에 증강 현실 기술을 이용해 운송장이나 배달 정보를 표시하여 현실성과 직관성 그리고 편리성을 보장할 수 있다.

제 3 장 공격 시나리오

제 1 절 외부 공격 시나리오

가장 흔하고 일반적인 택배 운송장 정보에 대한 공격 및 탈취는 택배에 대한 수취가 바로 일어나지 않는 경우에 발생한다. 택배 수취인이 부재시인 경우에는 경비실에 맡겨 안전하게 보관하는 경우도 있다. 이러한 경우에는 개인 정보 유출에 대한 안전성이 높아지지만 여전히 경비원에게 노출이 되는 것 또한 사실이다. 그러나 많은 경우 경비실의 위치상 택배를 수취하러 가기 번거롭다는 이유로 인해 또는 거주하는 건물이 단독 주택이나 경비실이 없는 건물이기에 수취인의 문 앞에 택배를 보관하는 경우가 존재한다. 유출이 되는 또 다른 경로로는 택배 물품 수취 후에 택배 상자에 붙어 있는 운송장에 대한 정보를 지우지 않거나 운송장 자체를 파괴하지 않아 일어나게 된다.

최근에는 택배를 받은 후 운송장의 정보를 파괴하지 않았다가 유출이 일어난다는 사실을 뉴스나 미디어를 통해 많은 사람이 접한 덕분에 과거에 비하면 운송장을 파괴해야 한다는 사실은 많은 사람들이 인지하고 있는 상태이다. 그러나 여전히 운송장을 쉽게 파괴하는 방법 등이 제안이 되었음에도 불구하고 운송장의 내용을 팬으로 지우거나 운송장을 뜯어내는 일 또한 번거롭다 여겨져 운송장의 내용을 파괴하지 않고 상자를 버리는 사태가 발생하고 이를 통해 운송장의 정보가 유출이 되는 주된 경로 중 하나로 사용이 된다. 이와 같이 외부에서의 운송장 정보 탈취 공격을 시도하는 경우 [그림 3-1]과 같은 절차에 의해 발생한다.

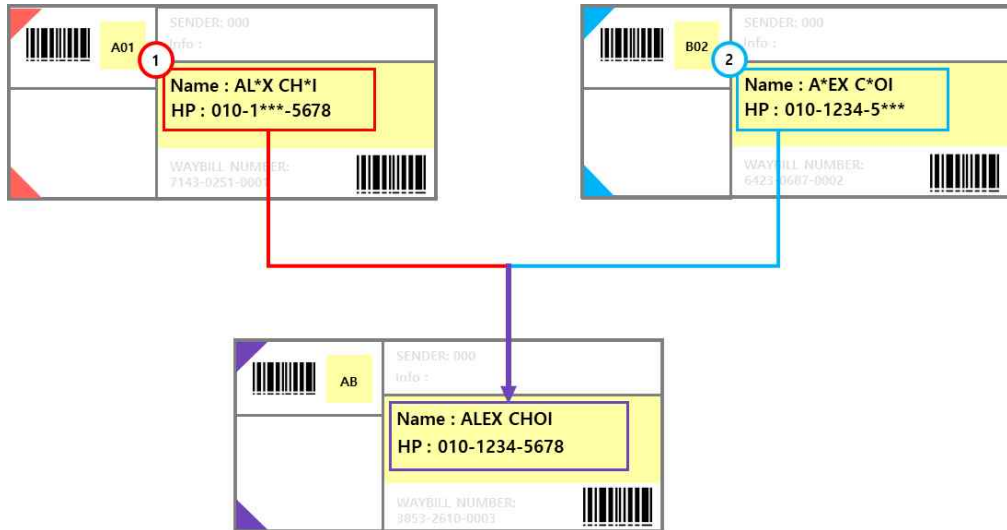


[그림 3-1] 운송장 개인 정보에 대한 외부 공격 시나리오

우선 택배의 운송장이 바로 수취되지 못하고 특정 공간에 일정 시간동안 보관이 된다. 이때 전제 조건으로는 무인택배함과 같이 완전히 보호받는 특별한 경우가 아닌 무인택배함이 설치되지 않은 대부분의 지역에서 보관이 된다고 가정한다. 택배가 택배 수취인의 문 앞이나 경비실 근처 등에 보관이 되는 동안에는 많은 사람들에게 노출이 될 수 있으며 이때 해당 택배 운송장의 정보를 탈취하고자 하는 사람을 공격자라 칭한다. 해당 공격자는 운송장의 정보를 읽을 수 있는 충분한 시력과 정보를 읽어 내용을 습득할 수 있는 능력을 가진 사람이라는 조건을 갖는다.

보관이 되던 택배가 공격자에 의해 발견이 된다. 공격자는 특정 수취자의 택배 운송장에 대한 정보를 찾으려는 의도를 갖고 있을 수 있으며 보이스피싱 등에 악용하기 위해서 특정 수취인의 운송장을 목표로 하지 않고 랜덤하게 택배 운송장 정보를 수집할 수 있다.

이때 운송장 정보가 앞 2장 2절에서 언급한 것과 같이 특정 정보의 일부가 가려져 있는 경우도 생각할 수 있다. 랜덤하게 정보를 수집하려는 경우 이와 같이 가려져 있는 경우 원본 개인 정보를 찾는 것이 어려울 수 있다. 그러나 공격자가 특정 수취인의 정보를 수집하려는 경우 [그림 3-2]와 같이 여러 개의 택배 운송장을 종합해 원본 운송장 개인 정보를 알아낼 수 있다.



[그림 3-2] 택배 운송장 취합을 통한 원본 정보 취득

제 2 절 내부 공격 시나리오

택배 운송장에 대한 정보는 운반하려는 물품과 관련된 기관의 서버에 저장되기 때문에 얼마든지 택배 상자위에 적혀있는 운송장의 정보를 통해서 뿐만 아니라 서버 등에 접근을 해 정보를 알아낼 수 있다. 실제로 택배 정보 조회 프로그램을 통해서 운반 회사 직원과 택배기사 등이 382 명의 택배 이용 회원들의 개인정보를 수집한 뒤 팔아 7천138만원을 챙겼다가 적발이 된 사례 또한 존재한다.

이와 같은 개인 정보에 대한 내부적인 접근 또는 내부인의 접근은 현재 택배 정보 조회 프로그램 설치 장소 제한 등 여러 가지 대안 방안을 두어 접근을 막고 있는 상황이다. 그러나 정보에 접근 하는 것을 완벽히 막는다는 것은 택배 업무 상 사실 상 불가능한 상태이다.

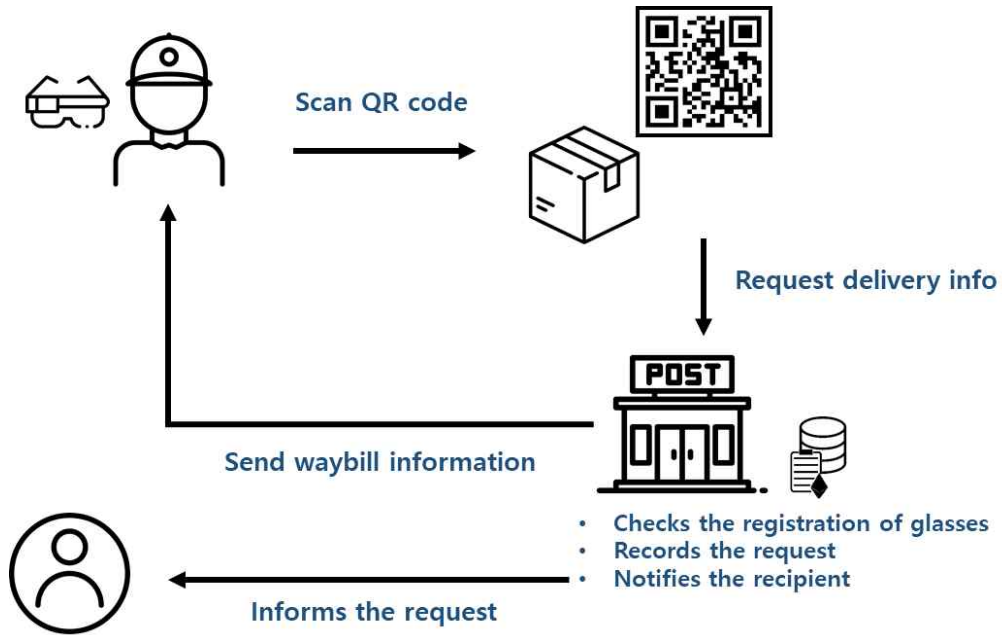
제 4 장 제안 기법

제 1 절 개인 정보 보호

운송장을 통한 개인 정보 유출 경로는 3장 1절의 외부 공격 시나리오가 주된 경로이며 대부분 시각을 통한 유출이 가장 많은 경우의 수를 차지한다. 본 장에서는 외부 및 내부 공격을 방지하기 위한 제안 시스템에 대한 설계와 해당 시스템에 대한 구현을 설명한다. 이후 운송장에 대한 개인 정보 보호에 대한 보안성을 갖추면서 동시에 효율성을 보장할 수 있는 대안 방안을 제시한다.

1) 시스템 설계

운송장의 개인정보 유출을 방지하기 위해서는 먼저 운송장에서 노출되는 개인 정보를 최소한으로 감소시켜야 한다. 이를 위해 운송장의 정보를 텍스트 형식이 아닌 QR 코드 형식으로 택배에 부착 할 것을 제안한다. 이를 통해 일반적인 사람의 육안을 통한 정보 유출을 방지할 수 있다. 해당 QR 코드를 읽기 위해서는 택배 관련 기관에서 검증을 받은 스마트 글라스로 또는 해당 택배의 수취자만 접근이 가능하다. 스마트 글라스는 택배를 운반하는 직원들이 착용을 하게 되며 이를 통해 택배 운송장에 적혀 있는 배송 정보를 인식하여 운반 장소를 파악 후 배달을 진행한다. 전체적인 제안하는 택배 프로세스의 절차는 [그림 4-1]과 같으며 이와 같은 제안 방식을 사용할 때 고려해야할 점은 다음과 같다.



[그림 4-1] 개인 정보 유출 방지 택배 시스템 프로세스

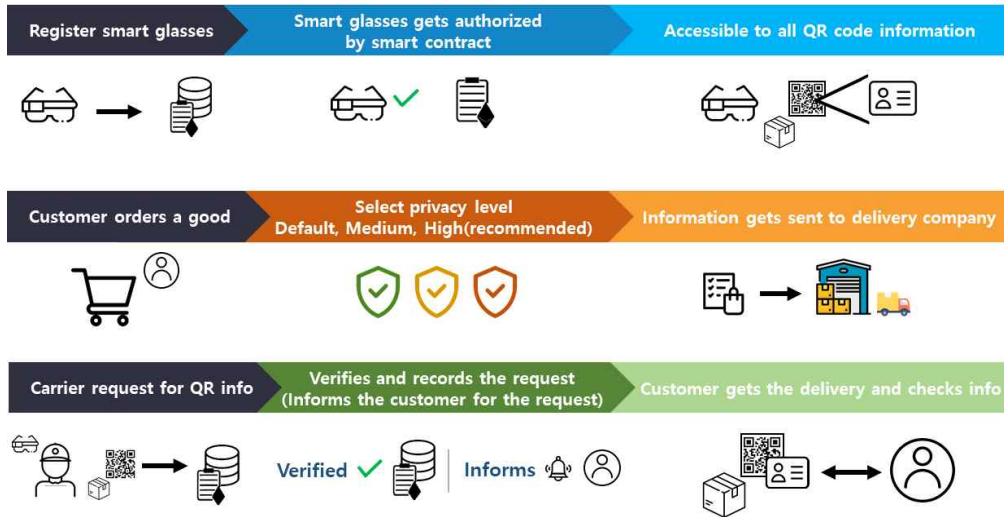
먼저 운송장의 정보를 담고 있을 QR 코드에 대한 무분별한 접근을 막아야한다. QR 코드는 코드를 읽을 수 있는 기기나 대부분의 사람들이 보유하고 있는 스마트폰을 통해 누구든지 스캔하여 해당 정보에 접근할 수 있다는 특징을 갖고 있다. 하여 QR 코드 정보에 대한 접근을 택배 운반자와 해당 택배 물품 수취자로 제한한다. QR 코드에 담겨져 있는 운송장에 대한 정보는 택배 서비스의 서버에서 관리를 하고 택배 회사에서 운영하고 있는 블록체인에 등록되어 있는 스마트 글라스로부터의 요청 또는 물건 수취자의 요청이 아닌 경우 접근을 제한한다.

다음으로 운송장에 적혀있는 개인 정보 전부를 QR 코드에 담게 되는 경우 수취인이 해당 택배의 QR 코드를 스캔해야만 해당 물품이 본인의 물품인지를 확인할 수 있게 된다. 그러나 항상 QR 코드를 읽을 수 있는 기기나 스마트 폰이 준비되지 않을 수 있기 때문에 수취한 물건이 본인의 물품임을 확인할 수 있는 추가적인 방안을 제시한다. 이를 위해서 택배를 주문한 사람의 실명이나 전화번호를 표기하지 않고 사전에 수취자가 원하는 임시 가명 혹은 ID 등을 QR 코드와 같이 첨부하도록 하고 해당 정보

는 문자 및 메일로 택배 수령인에게 전송하여 받은 물품이 수취인의 것이 맞는지 판단할 수 있게 할 것을 제안한다.

택배 운송 도중에 발생할 수 있는 문제로는 택배가 잘못된 주소로 배송이 되는 등의 상황이 발생할 수 있다. 이와 같은 문제에 대응하기 위해서 보존되어야 할 운송장의 정보는 운송장번호로 주문을 한 물품이 배송 과정에서 분실이 되어 도착을 하지 않았거나 배송된 물품에 파손이 발생해 물품 운반에 참여한 대상들에 대한 조치가 필요할 때 사용이 된다. 그렇기 때문에 운송장 번호에 대한 정보는 택배에 남겨둔다. 이는 택배를 받은 사용자가 택배를 주문한 사람이 아닌 경우 QR 코드에 접근을 해 운송장 정보를 조회할 수 없기 때문이다.

마지막으로 고려되어야 할 사항으로는 QR 코드와 연결된 운송장에 대한 정보와 접근 및 개인 정보가 담긴 운송장에 대한 조회 사실을 정보의 주인에게 알리는 연산 과정 등을 블록체인의 스마트 컨트랙트를 통해 처리해야 한다는 점이다. 이를 통해 운송장에 담겨져 있는 정보의 무결성을 보장할 수 있으며 운송장 정보에 대한 접근 과정 대상들을 기록하여 남겨둘 수 있으며 접근 사실에 대해 즉각 개인 정보의 주인에게 스마트 컨트랙트 연산 과정을 통해 즉각 알릴 수 있게 된다. 또한 택배 정보 서버에 접근을 할 수 있는 내부자의 소행으로 인한 개인 정보 유출이 발생한 경우 해당 물품을 담당하는 택배 기사 또는 직원에 대한 무결성이 보장된 기록을 얻을 수 있어 후에 유출 경로와 대상을 추적할 때 사용될 수 있다.



[그림 4-2] 택배 시스템 각 단계별 절차

구체적인 제안 시스템의 전체적인 흐름은 [그림 4-2]와 같으며, 그 과정은 다음과 같다.

먼저 스마트 글라스를 택배 관련 기관 서버에 등록을 한다. 등록을 통해 해당 스마트 글라스가 택배 운송장의 정보에 접근을 할 수 있는 권한을 부여받게 된다. 권한의 여부는 서버에서 운영하고 있는 블록체인의 스마트 컨트랙트의 연산 과정을 통해 등록 및 접근 허가 권한을 부여한다. 하여 추후에 스마트 글라스로 QR 코드의 정보를 읽고자 하면 스마트 컨트랙트에 등록이 되어있는 스마트 글라스인지 또 허가가 되어 있는 기기인지 확인을 통해 운송장 관련 정보에 대한 전송을 결정한다. 이와 같은 절차를 통해 권한을 부여받게 된 스마트 글라스는 택배를 운반하는 직원 및 기사가 착용을 하며 이를 통해 필요한 경우 운송장 정보를 조회할 때 사용하게 된다.

다음으로 고객의 주문 절차는 다음과 같다. 물건을 주문하고자 하는 고객이 물품을 주문을 하게 된다. 이때 주문절차에서 해당 물품 배송에 대한 보안 레벨을 3가지 중에 하나를 선택하게 된다. 먼저 기본(Default) 보안 수준은 택배를 운반하게 될 기관에서 사용하고 있는 운송장 양식을 따르거나 정보가 다 개방이 되어 있는 것을 의미한다. 이는 택배 운송장에 대

한 보안 절차를 생략하여 편의성을 추구하는 고객들이 선택할 수 있는 선택지이다. 그러나 정보가 대부분 공개되어 있는 형식이기 때문에 개인 정보 유출에 취약하다. 다음 수준으로는 운송장의 정보 중 일부를 무조건 가리는 보안 수준이다. 해당 보안 방식은 현존하는 몇몇 운송장의 개인 정보 보호 방식과 같이 이름, 전화번호 등의 일부를 가리는 방식이다. 기본 보안 방식과 같이 모든 정보가 개방이 되어 있지는 않기 때문에 보안성은 어느 정도 보장이 되어있으나 운송장 여러 장을 조합하는 등의 방식으로 원본 운송장 정보를 복원할 수 있다는 취약점이 있다. 마지막으로 본 논문이 제안하는 가장 높은 수준의 보안 방식이다. 해당 방식을 선택하면 운송장번호 및 주문자가 선택한 가명 등만 운송장에 표기가 되며 이외의 정보는 다 QR 코드로 표기가 된다. 또한 해당 방식을 선택하면 주문자가 후에 운송장에 대한 정보를 조회하고 싶을 때 사용할 비밀번호를 입력받게 된다. 각 보안 레벨에 따른 특성은 [표 4-1]과 같다.

[표 4-1] 택배 보안 단계별 특성

	Low(Default)	Medium	High(Proposed)
Security	None	Moderate	High
Intuitive	Instant	Tolerable	Tolerable
Requirement	None	None	Password

주문한 물품에 대한 운반 절차는 다음과 같다. 사전 등록된 스마트 글라스를 이용하여 택배 기사 또는 운반 직원이 택배 상자에 부착되어 있는 QR 코드를 스캔해 운송장 정보에 대한 요청을 보낸다. 해당 요청은 택배 기관 서버의 블록체인에 올려져있는 스마트 컨트랙트로 가게 된다. 스마트 컨트랙트의 연산 과정을 통해 먼저 요청을 보낸 스마트 글라스인지 확인을 한다. 만약 허가가 된 스마트 글라스라면 다음 연산으로 진행을 하고 허가 받지 않은 기기로부터의 요청이라면 해당 요청을 반려한다. 정상적으로 등록이 된 기기라면 블록체인 서버에 등록이 되어 있는 운송장 정보 중에 해당 요청에 맞는 운송장 정보를 스마트 글라스의 마운티드 디스플레이

레이 등을 통해 택배 운반자에게 전송한다. 그리고 동시에 요청을 보낸 스마트 글라스의 요청자 정보를 블록체인에 기록해 추후 정보에 대한 내부 유출이 발생할 경우 추적을 할 수 있게 남겨둔다. 또한 운송장의 개인 정보에 대한 조회 사실을 해당 택배 주문자에게 알림을 보낸다. 운송장에 대한 정보를 성공적으로 전송받게 되면 물품 운반자는 해당 택배를 배달 장소에 안전하게 전달을 한다.

2) 시스템 구현

본 논문에서 제안하는 개인 정보 보호 택배 시스템의 일부를 구현하여 동작을 확인하였다. 구현은 블록체인의 스마트 컨트랙트 부분을 구현하였으며 QR 코드에 담겨 있는 운송장 정보에 접근할 때 처리되는 프로세스를 구현하였다. 해당 프로세스에는 접근 하려는 주체의 권한 확인, 운송장 정보 반환 그리고 개인 정보 조회 사실 알림 등이 포함이 된다. 구현 환경은 [표 4-2]와 같다.

[표 4-2] 제안 시스템 구현 환경

OS	Windows 10 Pro
IDE	Remix IDE
API	Web3
Language	Solidity 0.7.1+
Hardware	Raspberry Pi 3 B+
Environment	JavaScript VM Web3 Provider
Modules	Solidity Compiler Delply & Run Transactions

제안하는 시스템을 구현하기 위해 사용한 개발 통합 환경 리믹스(Remix)는 블록체인 상에서 처음으로 스마트 컨트랙트를 도입한 2세대 대표 블록체인인 이더리움의 IDE(Integrated Development Environment, 통합 개발 환경)와 개발 도구를 제공해주는 개발 환경을 뜻한다. 리믹스의 장점으로는 먼저 웹상에서 개발 환경을 제공해주기 때문에 인터넷만 연결된 컴퓨터가 있다면 어디에서든지 이더리움의 스마트 컨트랙트 개발을 할 수 있다는 점이 있다. 또한 메타 마스크(Metamask) 등과 같은 블록체인 상에서 사용되는 가상 화폐를 관리해주는 가상 화폐 지갑 서비스와 연동을 해주어 실제 이더리움 블록체인 상에서 사용되는 화폐 단위인 이더(Ether)를 통해 이더리움 메인넷에 접속해 리믹스에서 제작한 스마트 컨트랙트를 실제로 운영중인 이더리움 블록체인 네트워크에 올릴 수도 있다. 또한 메타 마스크에서 지원해주는 테스트 용 가상 화폐들과의 연동 또한 지원을 해주기 때문에 실제로 이더리움 블록체인에 스마트 컨트랙트를 배포하기 전에 자신이 작성한 스마트 컨트랙트가 네트워크상에서 잘 작동하는지를 롱슨(Ropsten) 등과 같은 테스트 네트워크 환경에서 작성한 스마트 컨트랙트의 작동 검사를 해볼 수 있다. 물론 실제 스마트 컨트랙트를 이더리움에 배포하려는 목적뿐만 아니라 단순히 구상하고자 하는 스마트 컨트랙트를 이용한 블록체인 서비스를 구현해보고자 할 때에도 사용될 수 있다. 이와 같은 경우에는 테스트 블록체인 네트워크에 배포를 하지 않더라도 리믹스 IDE 웹상 환경에서 테스트해볼 수 있게 자바스크립트(JavaScript VM)를 이용한 가상 테스트 환경 또한 제공한다. 본 논문에서는 제안하는 시스템의 스마트 컨트랙트 구현 결과물에 대한 정상 동작 여부 확인을 위해 스마트 컨트랙트를 리믹스 IDE에서 개발하였으며 리믹스에서 제공하는 Web3 API, JavaScript VM 등의 기능을 이용하였다.

제안하는 시스템에서 사용되는 스마트 컨트랙트의 구현은 변수들에 대한 선언과 기능을 담고 있는 함수로 구성이 된다.

제안하는 시스템에서 사용이 되는 변수들로는 먼저 스마트 컨트랙트를 배포한 주체, 즉 해당 블록체인을 운영하고 있는 기관의 권한 있는 사람의 주소를 담고 있는 주체에 대한 변수를 선언했다. 다음으로는 운송장 정보를 요청을 한 스마트 글라스가 조회 권한을 갖고 있는지 여부를 담고 있는 매핑 구

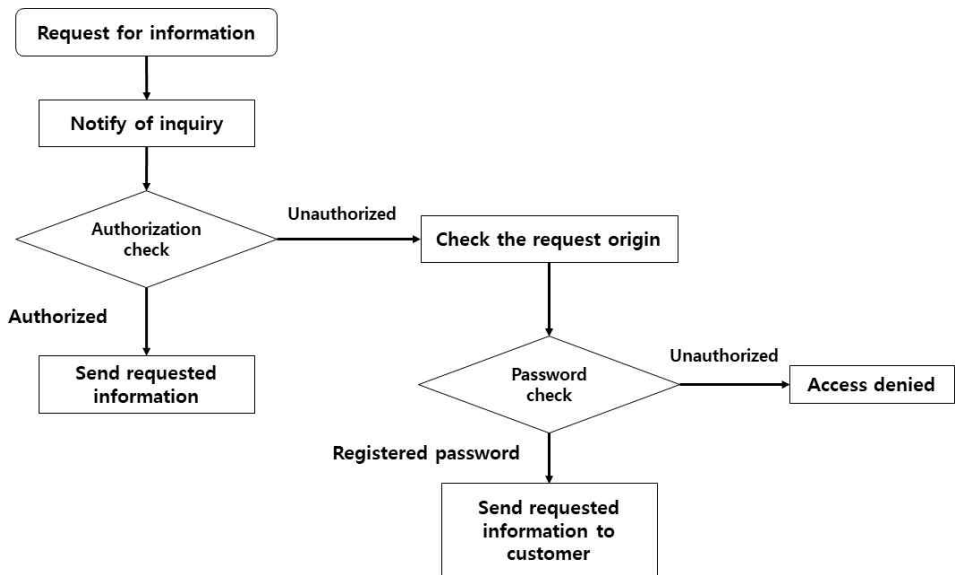
조체를 선언하였고 운송장에 대한 정보를 담고 있는 구조체와 매핑 구조체를 선언하였다. 각 데이터에 대한 구체적인 선언은 [표 4-3]과 같다.

[표 4-3] 스마트 컨트랙트 변수 및 구조체 정의

Data class	Data Type
Owner	address
QR code to Delivery Info	uint256 to Struct mapping
Smartglasses authorization	address to Bool mapping
Delivery Info	structure(uint, string, string)

다음으로는 함수들에 대한 구현이다. 함수는 크게 스마트 글라스를 스마트 컨트랙트에 등록을 하여 운송장에 대한 정보를 조회할 수 있게 등록하는 함수와 QR 코드를 스캔하여 QR 코드에 해당하는 운송장 정보를 반환해주는 함수를 구현하였다. 스마트 글라스에 대한 등록은 스마트 컨트랙트를 배포한 주체, 즉 택배 기관의 권한 있는 인물들만이 등록을 가능하도록 구현하였다. 제안하는 시스템의 핵심인 QR 코드 스캔을 통한 정보 요청에 대한 함수의 처리에 대한 흐름도는 [그림 4-3]와 같다. 먼저 QR 코드의 운송장에 대한 정보 요청이 오면 운송장에 연관된 고객에게 개인 정보 조회 사실을 알린다. 그 후 해당 요청이 누구에게서 온지 확인을 한다.

이때 QR 코드에 대한 요청을 보내는 주체는 2가지로 나뉘 수 있다. 먼저 조회를 허가 받을 수 있는 스마트 글라스를 보유한 택배 기사가 조회를 요청할 수 있다. 그 다음 요청을 하는 주체는 운송장에 대한 정보를 조회하고자 하는 고객이나 혹은 운송장 정보를 탈취하고자 하는 악의적 공격자가 될 수 있다. 택배 기사인 경우 스마트 글라스의 권한을 검증한 후에 운송장 정보를 반환하고 그렇지 않은 경우에는 요청을 보낸 주체가 사전에 운송장 조회 비밀번호를 설정한 사람인지를 송신한 비밀번호를 확인하여 운송장 정보 반환 여부를 결정한다.



[그림 4-3] QR 코드의 운송장 정보 요청 흐름도

함수의 구현은 크게 3가지로 구현하였다. 먼저 스마트 글라스를 등록하는 함수이다. 해당 함수는 스마트 컨트랙트를 배포한 주체, 즉 택배 기관에서 권한을 부여한 사람만이 호출하여 스마트 글라스의 등록 작업을 할 수 있다. 그 외에 다른 주체의 접근은 모두 권한이 없다는 사유를 반환하며 함수가 종료된다. 권한이 있는 주체가 해당 함수를 호출할 때 등록할 스마트 글라스의 주소 값을 입력 값으로 입력하여 해당 주소 값을 키의 값으로 사용하여 스마트 글라스의 운송장 조회 여부 사실을 담고 있는 매핑 구조에 등록을 한다. 이를 통해 QR 코드의 운송장 정보를 등록된 스마트 글라스에서 요청을 보낼 시 배열이 아닌 매핑 구조를 통해 효율적으로 정보를 반환해줄지 여부를 판단할 수 있다. 두 번째로는 상품에 대한 등록 함수이다. 이 또한 앞서 말한 스마트 글라스 등록 함수와 같이 택배 기관의 권한 있는 주체가 등록할 수 있게 구현 하였다. 함수를 호출한 주체가 권한이 있는 주체임이 확인이 된 후에 함수를 호출할 때 입력 값으로 받은 운송장에 대한 정보와 운송장 정보를 후에 고객이 조회할 때 사용할 비밀번호를 사전 정의한 구조체에 입력한다. 마지막으로 구현한 함수는 본 논문에서 제안하는 시스템에서 가장 핵심이 되는 QR

코드의 운송장 정보를 요청하고 해당 정보를 반환하는 함수이며 해당 함수의 알고리즘은 [표 4-4]과 같다.

[표 4-4] QR 코드 운송장 정보 조회 요청 알고리즘

Algorithm1

Input: uint256 waybillNumber, uint256 customerPassword

```

1.  if(registeredSmartGlasses[msg.sender]==true){
2.      nameOut = DeliInfo[waybillNumber].customerName;
3.      addressOut = DeliInfo[waybillNumber].customerAddress;
4.
5.  }
6.  else{
7.      if(customerPassword== DeliInfo[waybillNumber].password){
8.          nameOut = DeliInfo[waybillNumber].customerName;
9.          addressOut = DeliInfo[waybillNumber].customerAddress;
10.
11.     }
12.     else{
13.         nameOut = "Not Authorized";
14.         addressOut = "Not Authorized";
15.     }
16. }

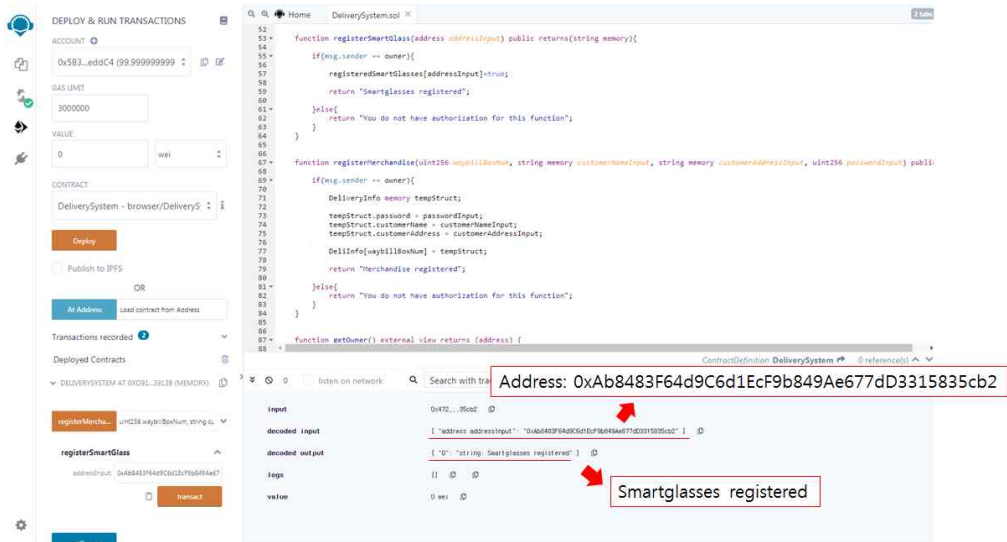
```

함수의 입력 값으로 운송장의 번호와 고객이 사전에 운송장 조회를 위해 설정한 비밀번호를 입력 값으로 받는다. 만약 해당 요청이 고객이 운송장의 정보를 요청하는 경우가 아닌 경우 즉, 택배 기사의 스마트 글라스를 통한 요청이라면 비밀번호는 초기화된 값으로 입력이 된다. 먼저 함수를 호출한 메시지 송신자가 택배 기사인지를 확인을 한다. 이는 앞서 말한 스마트 글라스 등록 함수에서 스마트 글라스를 등록할 때 사용했던 매핑 함수를 통해 이뤄진다. 이를 통해 요청을 보낸 스마트 글라스의 주소에 해당하는 권한 여부 값이 참(TRUE)으로 되어 있는지 확인을 한다. 만약 값이 참이라면 권한이 있는 택배 기사가 보낸 요청이기에 운송장 번호에 해당하는 운송장 정보들을 반환하고 함수를 종료한다.

만약 요청을 보낸 주체가 물건을 운송하는 택배 기사가 아닌 경우 요청을

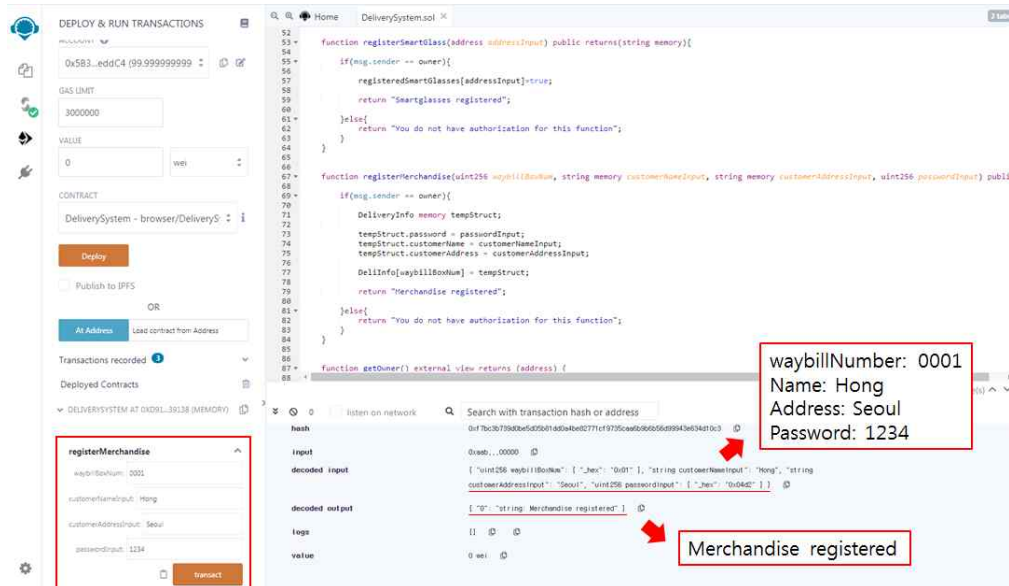
보낸 주체를 2가지로 나눌 수 있다. 먼저 물품을 전달 받은 고객의 요청일 경우가 있다. 만약 요청을 보낸 주체가 물품 수취인이라면 해당 함수를 호출할 때 운송장의 번호 뿐만 아니라 사전에 할당한 올바른 비밀번호를 함께 함수의 입력 값으로 입력했을 것이다. 하여 해당 비밀번호가 해당 운송장에 맞는 비밀번호로 매핑 구조에 사전에 등록이 되어있는지를 확인한 후에 만약 비밀번호가 동일하다면 물품 수취인이라는 사실이 증명이 된다. 그 후 운송장 번호에 해당하는 운송장 정보를 반환해준다. 만약 QR 코드를 이용한 운송장 정보 요청을 보낸 주체가 정당한 물품 수취인이 아니라면 택배에 적혀있는 운송장 번호를 통해 요청을 보낼 수는 있지만 결국 등록되어 있는 스마트 글라스를 보유하고 있지 않고 또한 사전 등록된 비밀번호를 알지 못하기 때문에 해당 정보의 요청은 거절이 되며 권한이 없는 사용자의 접근이라는 메시지만 반환이 된다.

제안한 시스템에 대한 구현 결과물을 테스트하기 위해 먼저 리믹스 IDE를 이용해 JavaScript Vm 환경에 스마트 컨트랙트를 배포한다. 이때 배포한 주체, 즉 제안한 시스템에서는 택배 기관 중 권한이 있는 사람이 되며 테스트 환경에서는 블록체인 주소 값 0x5B3이 된다. 성공적으로 스마트 컨트랙트가 배포가 되었으면 다음 단계인 택배 기사의 등록, 즉 스마트 글라스를 등록을 한다. 이때 스마트 글라스의 주소 값은 임의의 값인 0xA8 값으로 설정한다. 해당 값의 등록은 앞서 말한 것과 같이 권한이 있는 주체가 등록을 해야하며 0x5B3의 주소로 0xA8의 값을 성공적으로 등록하면 [그림 4-4]와 같은 결과를 볼 수 있다.



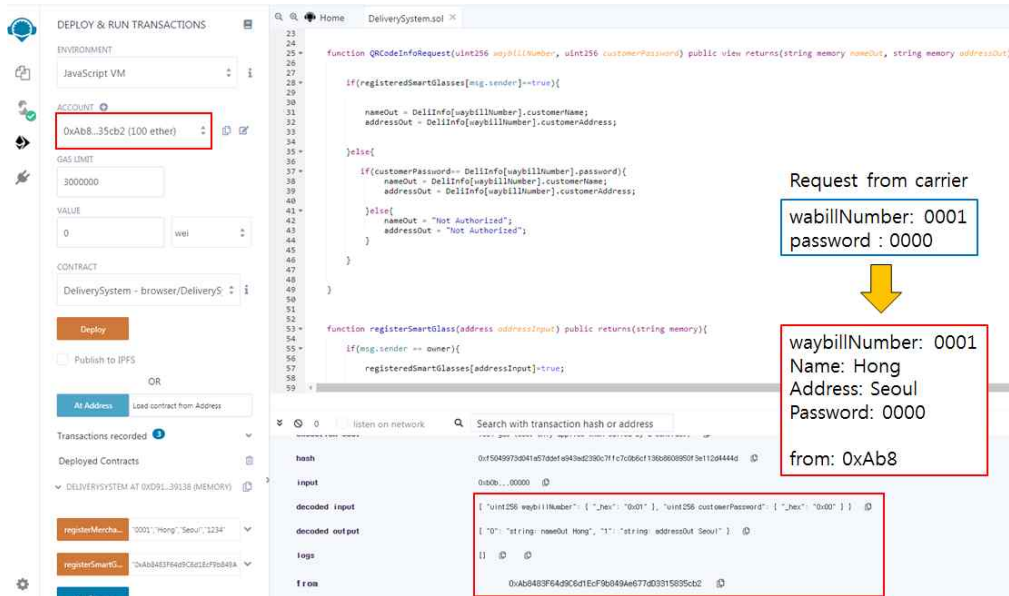
[그림 4-4] 스마트 글라스 운송장 조회 권한 등록

다음으로는 물품에 대한 등록이다. 물품 및 운송장에 대한 등록을 위해 임시 운송장 번호 0001과 물품을 주문한 수취인의 이름, 주소를 각각 임의로 ‘Hong’과 ‘Seoul’로 설정하였다. 마지막으로 수취인이 운송장 정보를 요청할 때 사용할 비밀번호로 임의의 값 ‘1234’를 설정하여 물품의 운송장 정보를 등록한다. 이때 또한 역시 스마트 컨트랙트를 배포한 0x5B3의 주소를 통해 배포를 하며 배포가 성공적으로 완료된 것을 [그림 4-5]를 통해 볼 수 있다.



[그림 4-5] 운송장 정보 및 정보 조회 비밀번호 등록

마지막 단계로 QR 코드에 담겨진 정보 조회 요청에 대한 처리이다. QR 코드를 통해 운송장에 대한 정보 요청을 하는 경우는 총 3가지다. 먼저 택배 기사가 등록된 스마트 글라스를 이용하여 정보를 요청하는 경우이다. 이와 같은 경우 운송장의 번호만 사용이 되며 해당 스마트 글라스가 등록이 된 글라스인지만 확인을 하고 검증이 완료되면 [그림 4-6]과 같이 정보를 반환한다. 해당 테스트에서는 스마트 글라스의 주소를 0xAb8로 등록을 했었는데 성공적으로 관련 정보가 반환이 되었으며 또한 정보를 요청한 스마트 글라스의 주소가 등록이 된 것을 볼 수 있다.



[그림 4-6] 등록된 스마트 글라스로부터의 운송장 정보 조회 요청

다음은 물건을 주문한 물품 수취인으로부터의 요청이다. 이때 운송장의 번호와 사전에 설정해 놓은 비밀번호를 보내 요청을 하게 된다. 고객의 번호는 0xdD8이라고 임의로 설정해 놓고 임의 운송장 번호 '0001'과 비밀번호 '1234'를 입력 값으로 정보 요청을 보낸다. [그림 4-7]을 통해 해당 요청이 성공적으로 이뤄졌다는 사실을 알 수 있다.

마지막으로 악의적인 목적을 갖고 운송장 정보를 요청하는 경우이다. 이와 같은 경우 운송장의 번호만 알고 비밀번호는 모른 상태에서 정보를 요청하게 된다. 이와 같은 경우 스마트 컨트랙트에 등록 되어 있는 비밀번호를 맞추지 않는 이상 운송장 정보를 받을 수 없으며 악의적 임시 공격자 0x787이 QR 코드에 해당하는 운송장 정보를 요청하였으나 정보 반환이 되지 않는 것을 [그림 4-8]을 통해 볼 수 있다.

DEPLOY & RUN TRANSACTIONS

ENVIRONMENT

JavaScript VM

ACCOUNT

0xD8...92148 (100 ether)

GAS LIMIT

3000000

VALUE

0 wei

CONTRACT

DeliverySystem - browser/DeliveryS

Deploy

Publish to IPFS

At Address Load contract from Address

Transactions recorded

Deployed Contracts

DELIVERYSYSTEM AT 0xD8...39138 (MEMORY)

registerMercha... '0001', 'Hong', 'Seoul', '1234'

registerSmartC... '0xD8...39138' (MEMORY)

QRCodeInfoRequest

waybillNumber: 0001

customerPassword: 1234

call

function QRCodeInfoRequest(uint256 waybillNumber, uint256 customerPassword) public view returns(string memory nameOut, string memory addressOut){

if(registeredSmartClasses[msg.sender]==true){

nameOut = DelInfo[waybillNumber].customerName;

addressOut = DelInfo[waybillNumber].customerAddress;

}else{

if(customerPassword== DelInfo[waybillNumber].password){

nameOut = DelInfo[waybillNumber].customerName;

addressOut = DelInfo[waybillNumber].customerAddress;

}else{

nameOut = "Not Authorized";

addressOut = "Not Authorized";

}

}

function registerSmartClass(address addressInput) public returns(string memory){

if(msg.sender == owner){

registeredSmartClasses[addressInput]=true;

return "SmartClasses registered";

}else{

return "You do not have authorization due this function";

}

}

transaction cost

30235 gas (Cost only applies when called by a contract)

execution cost

8515 gas (Cost only applies when called by a contract)

hash

0x02749f3e6b1f0c443e30c0b08f51561f72c9420355d8427a775d70c30c

input

0x0b...0042

decoded input

["uint256 waybillNumber": { "hex": "0001" }, "uint256 customerPassword": { "hex": "00042" }]

decoded output

["0": "string: nameOut Hong", "1": "string: addressOut Seoul"]

from

0xD870F4167C4700P200714423602125F7396148

Request from customer

waybillNumber: 0001

password: 1234

from: 0xD8

[그림 4-7] 물품 수취인으로부터의 운송장 정보 조회 요청

DEPLOY & RUN TRANSACTIONS

ENVIRONMENT

JavaScript VM

ACCOUNT

0x787...cabaB (100 ether)

GAS LIMIT

3000000

VALUE

0 wei

CONTRACT

DeliverySystem - browser/DeliveryS

Deploy

Publish to IPFS

At Address Load contract from Address

Transactions recorded

Deployed Contracts

DELIVERYSYSTEM AT 0xD8...39138 (MEMORY)

registerMercha... '0001', 'Hong', 'Seoul', '1234'

registerSmartC... '0xD8...39138' (MEMORY)

QRCodeInfoRequest

waybillNumber: 0001

customerPassword: 9999

call

function QRCodeInfoRequest(uint256 waybillNumber, uint256 customerPassword) public view returns(string memory nameOut, string memory addressOut){

if(registeredSmartClasses[msg.sender]==true){

nameOut = DelInfo[waybillNumber].customerName;

addressOut = DelInfo[waybillNumber].customerAddress;

}else{

if(customerPassword== DelInfo[waybillNumber].password){

nameOut = DelInfo[waybillNumber].customerName;

addressOut = DelInfo[waybillNumber].customerAddress;

}else{

nameOut = "Not Authorized";

addressOut = "Not Authorized";

}

}

function registerSmartClass(address addressInput) public returns(string memory){

if(msg.sender == owner){

registeredSmartClasses[addressInput]=true;

return "SmartClasses registered";

}else{

return "You do not have authorization due this function";

}

}

transaction cost

34815 gas (Cost only applies when called by a contract)

execution cost

8595 gas (Cost only applies when called by a contract)

hash

0x090eb0a04db8a535096c228840173a23925a87a750a3a7b8d7f0101

input

0x0b...020f

decoded input

["uint256 waybillNumber": { "hex": "0001" }, "uint256 customerPassword": { "hex": "0020f" }]

decoded output

["0": "string: nameOut Not Authorized", "1": "string: addressOut Not Authorized"]

from

0x7873100c0b07E54c0P804442a70c1B4A950e0a5

Request from malicious attacker

waybillNumber: 0001

password: 9999(?)

waybillNumber: 0001

Name: Not Authorized

Address: Not Authorized

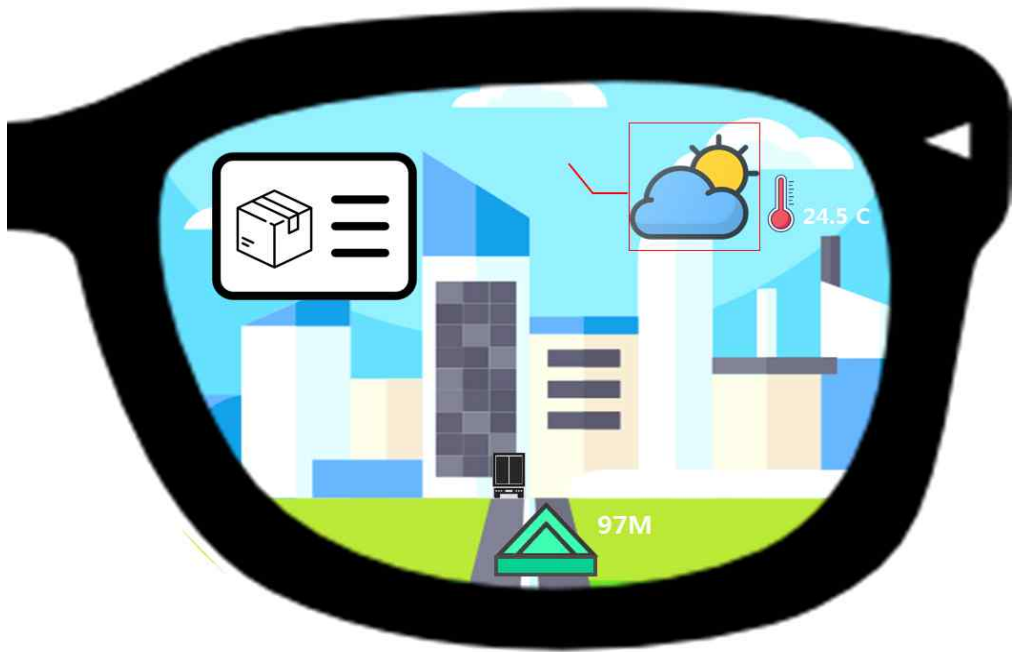
from: 0x787

[그림 4-8] 악의적 공격자로부터의 운송장 정보 조회 요청

제 2 절 운송 효율성 향상

일반적으로 보안성을 강화하게 되면 그만큼 편의성이 저하가 된다. 예를 들어 집을 보호하기 위해 문에 잠금 장치를 설치하게 되면 열쇠를 항상 지니고 있어야 문을 통해 집에 들어갈 수 있는 만큼 편의성이 저하되게 된다. 그렇기 때문에 항상 보안적인 측면을 강화하면 그만큼 사람이 사용함에 있어서 편의성 또한 반드시 고려가 되어야 한다. 제안하는 방식을 통해 개인 정보를 QR 코드를 활용하여 보안을 강화하는 만큼 편의성이 저하되는 부분이 불가피하게 생기게 된다. 그리고 이러한 불편한 점은 특히 물품 운송 과정에서 발생하게 된다.

기존 운송장은 개인 정보가 일부분이 가려져 있다고 하더라도 대부분 모든 운송장에서는 보내는 사람의 주소와 물품을 받는 사람의 주소는 있는 그대로 개방되어있다. 이는 물품을 운반하는 사람이 시각만을 통해서 운송장에 적혀있는 물품 운반 목적지를 확실히 알 수 있게 하는 매우 통상적인 방식이다. 그러나 본 논문에서 제안하는 방식에서는 스마트 글라스를 이용해서 물품이 배달되어야 하는 정보 등을 조회해야하기 때문에 물품의 운송지에 대한 정보가 매우 직관적으로 물품 운반자에게 전달이 되어야 한다. 이때 스마트 글라스라는 장치를 이용하는 만큼 일반적인 시각을 사용하는 것과는 다르게 더 고려되어야 하는 요소들이 존재한다. 특히 [그림 4-9]에서 볼 수 있는 것과 같이 스마트 글라스의 가장 큰 단점 중 하나로 여겨지는 시야 방해의 문제를 해결하면서도 동시에 물품에 대한 정보를 택배 기사에게 전달할 수 있어야한다.

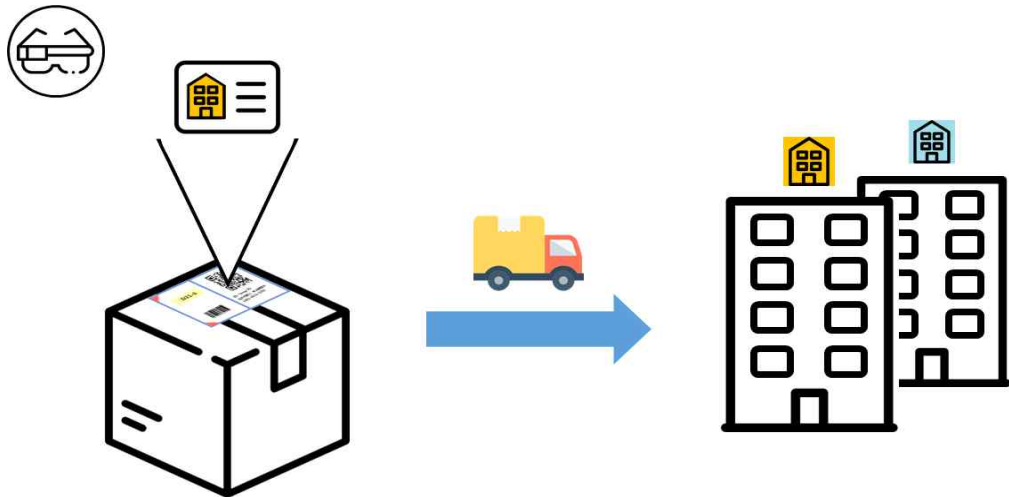


[그림 4-9] 스마트 글라스의 시야 방해 현상

HMD에 운송장의 정보를 직접 택배 운반자의 스마트 글라스에 띄우는 경우 많은 택배의 모든 정보를 띄울 수 없을 뿐만 아니라 일부만 띄우더라도 시야를 방해하게 된다. 이는 도로 상에서 운반함에 있어서 매우 불편한 인터페이스일 뿐만 아니라 차량 운전 도중에는 큰 사고로 이어질 수 있을 만큼의 위험한 일이다. 그렇기 때문에 택배 운반자의 시야를 가리지 않는 방식이 필요하다.

이를 위해서 본 논문에서는 스마트 글라스의 HMD에 직접적으로 운송장 정보를 띄워주는 방식이 아닌 AR 기술을 이용한 방식을 제안한다. 운송장에 대한 정보가 담겨 있는 QR 코드를 스마트 글라스로 스캔을 하게 되면 일반적인 시각을 사용하는 것과 동일하게 택배 운송장 바로 위로 운송장에 대한 정보가 뜰 수 있게 구현한다. 이를 통해 운반 도중에는 택배 운반자의 시야를 전혀 가리지 않고, 택배 물품의 운송장 위치를 스마트 글라스를 통해 볼 때에만 마치 일반 시야로 보는 것과 동일하게 직관적으로 운송장의 정보를 읽을

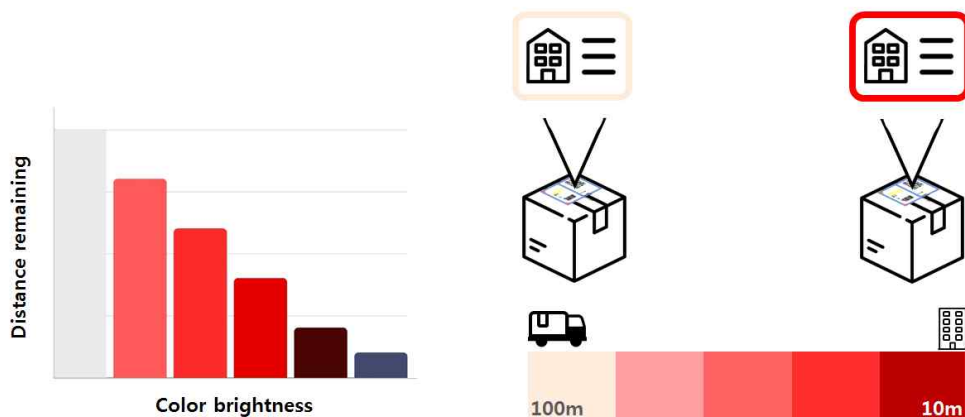
수 있게 된다. 뿐만 아니라 증강 현실 기술과 더불어 GPS 기술과 접목하여 스캔한 택배들이 배달되어야 하는 위치를 [그림 4-10]과 같이 색깔과 아이콘 등을 이용할 수 있다. 이를 통해 배달해야 하는 택배들의 목적지를 각 택배에 맞게 증강 현실로 구별해 표시하여 운반자가 배달해야 하는 위치를 더욱 직관적으로 알 수 있게 하여 운반의 효율성을 증가시킬 수 있다.



[그림 4-10] 증강 현실 활용 직관적 운송장 조회 및 운송 효율성 향상

증강 현실을 활용해 스마트 글라스를 사용하면서도 시야를 방해하지 않고 직관성과 운송 효율성을 높이는 방식과 더불어 운송하려는 위치에 대한 직관성을 더 높이는 방식을 제안한다. 앞서 택배가 운반되어야 하는 목적지에 증강 현실 기술을 이용하여 목적지를 표시할 것을 제안하였다. 이와 더불어 색깔의 밝기 및 명도를 활용하여 택배의 목적지 남은 위치에 대한 거리를 표기할 것을 제안한다. 택배 운반에 있어서 시간의 단축은 매우 중요하며 이를 위해서는 경로의 계산을 효율적으로 하는 것이 중요하다. 이를 위해서 목적지까지의 각 택배 물품의 남은 거리를 알 수 있으면 택배 운반을 함에 있어 효율성을 증가시킬 수 있다. 이를 위해 [그림 4-11]과 같이 각 택배 운송장의 QR 코드 위에 표시되는 운송장의 정보의 테두리에 색깔의 명도와 밝기를 이용해 남은 거리를 직관적으로 표시한다. 이를 통해 택배 물품을 하차할 때 가장 가까운 택배 목적지에 할당하는 택배부터 가장 멀리 목적지가 존재하는

택배까지 택배 운반자가 직관적으로 알 수 있으며 이를 통해 효율적으로 택배 운반 경로를 계산할 수 있다.



[그림 4-11] 색깔 밝기와 명도를 활용한 직관적 거리 계산

운송의 마지막 단계인 택배 수취인의 물품 수취 단계에서의 효율성 또한 고려해야 한다. 본 논문에서 현재까지 제안하는 방식에서는 현재 물품 수취인이 운송 받은 물품이 본인의 물품인지 확인하기 위한 방법으로는 운송장에 적힌 QR 코드를 QR 코드를 읽는 기능이 있는 스마트폰과 같은 기기를 이용해 운송장 정보 조회를 요청하는 방식이다. 이때 사전에 설정해 놓은 비밀번호를 통해 검증을 거친 후 운송장에 대한 정보를 확인할 수 있다.

이와 같은 방식은 등록되어 있는 스마트 글라스가 아닌 다른 QR 코드를 읽는 기기로 택배 운송장 정보에 접근하려고 했을 때 방지하기 위한 절차이며 또한 운송장 정보의 유출을 방지하면서 동시에 수취인이 정보를 확인할 수 있게 만들어 놓은 단계이다. 그러나 스마트폰 등과 같이 QR 코드를 읽을 수 있는 기기가 없는 상황에서도 본인의 물건인지를 확인해야 할 필요가 있다. 이를 위해 물품을 주문할 때 비밀번호뿐만 아니라 물건 수취인이 자신의 물건임을 확인할 수 있게 가명 또는 임시 ID를 지정할 수 있도록 하여 운송장에 표시한다. 이를 통해 운송장의 QR 코드를 읽지 않으면서 동시에 물건을 개봉할 필요가 없이 물품 주문자의 물건이 맞는지 확인할 수 있다. 물건의 내용 또한 알아야 할 필요에 대한 수요가 발생한다면 주문한 물건에 대한

대분류에 대한 표기 또한 할 수 있다. 예를 들어 의자를 주문한 경우 물품에 대한 표기를 가구와 같이 대분류로 설정해 QR 코드의 내용을 조회하지 않으면서 동시에 물건을 개봉하지 않아도 본인의 물건임을 확인하고 물품의 내용을 알 수 있도록 한다.

제 5 장 성능 평가

제 1 절 실험 환경

본 연구의 실험을 통해 기존의 택배 운송장 시스템과 비교하기 위해 기존 운송장 환경을 구현하기 위해 택배 업계에서 흔히 사용되는 운송장의 템플릿에 물품에 대한 정보와 보내는 사람, 받는 사람들의 정보를 작성하여 실제 운송장과 같은 환경을 구성하였다. 또한 제안하는 시스템에서 사용하는 QR 코드 방식의 운송장을 구현하여 두 운송장의 직관성, 보안성, 편의성 등을 비교하였다.

제 2 절 기존 시스템 평가

기존 택배 운송장 시스템은 크게 2가지 방식으로 나뉜다. 운송장의 모든 정보가 가려져있지 않고 전부 개방이 되어 있는 형식과 운송장에 적혀있는 정보의 일부가 특수 문자로 가려져 있는 형식으로 나뉜다.

전체 개방형 운송장의 특징은 일반적인 시야를 갖고 있는 모든 사람이 해당 정보를 읽을 수 있으며 운송장의 정보가 전혀 보호되지 않는다는 특징을 갖고 있다. 물론 장점으로 물품을 받는 사람과 물품을 배달해주는 기사 모두가 운송장에 대한 정보를 즉각적으로 파악할 수 있기 때문에 운송장 정보에 대한 직관성과 편의성이 높다는 장점을 갖고 있다. 일부 개방형 운송장의 특징으로는 전체 개방형과 마찬가지로 일반적인 시야를 갖고 있는 모든 사람이 접근할 수 있다는 점이 있으며 전체 개방형에 비하면 운송장 정보를 일부 가림으로써 정보 보호의 기능이 존재한다. 그러나 3장에서 말한 것과 같이 특정 대상의 운송장 정보 여러 개를 조합하면 원본 운송장의 정보가 나오기 때문에 개인 정보에 대한 보안성이 낮다. 물론 배달할 때에나 물건 수취인

이 운송장 정보를 파악하는 직관성이나 물품 전송 편의성은 개방형과 사실상 거의 동일하게 편리하다는 특징을 갖고 있다. 그러나 여전히 기존 택배 시스템에서 사용하는 개방형 방식의 운송장은 개인 정보 유출에 사실상 무방비한 상태라는 점은 동일하다.

제 3 절 제안 시스템 평가

기존의 시스템과 본 논문에서 제안한 시스템의 보안성 및 편의성 등을 비교 분석한다. 기존의 전체 개방형, 부분 개방형 그리고 제안하는 시스템의 방식의 특성을 정리하면 [표 5-1]과 같다.

[표 5-1] 기존 시스템과 제안 시스템 비교

	Conventional (Full disclosure)	Conventional (Partial disclosure)	Proposed
Information openness	Open to everyone with sight	Open to everyone with sight	Requires validation
Level of security	Very low	Low (Combination attack)	Very high
Intuitive of information	Very High	High	Medium
Information recoverability	No	No	Yes
Convenience of delivery	Very high	High	Medium

제안하는 시스템은 기존 전체 개방형과 일부 개방형에서 운송장의 정보를 텍스트로 표기하는 대신 QR 코드를 사용해 일반 시야로는 정보를 읽을 수 없게 설계하였기 때문에 일반적인 시야를 통한 정보 유출로부터 안전하였다. 또한 QR 코드에 대한 접근을 시도하더라도 미리 등록이 되어 있는 스마트 글라스가 아니라면 접근이 불가능하며 유일한 접근 방법은 비밀번호가 필

요하여 접근이 불가능했다. 정보에 대한 직관성은 현존하는 개방형 방식에 비해 떨어질 수 있으나 스마트 글라스를 사용하여 운송장 정보를 읽어 두 손이 자유로워질 수 있었으며 증강 현실 기술을 이용해 물품을 운송하는 기사 측면에서의 편의성을 보강되었으며 물품 수취인의 입장에서는 사전에 설정해 놓은 ID 등을 통해 본인의 물품인 것을 즉각 확인할 수 있었다.

제 6 장 결론 및 향후 개선 방안

코로나 사태로 인해 택배 이용 횟수가 그 어느 때보다 높아진 상황이다. 택배의 이용 횟수가 늘어나는 만큼 택배의 운송장을 통한 개인 정보 유출 현상 또한 같이 심각해지고 있어 이에 대한 보안 조치가 시급하다. 그러나 택배의 개인정보 유출을 방지하는 방식들은 여전히 개인 정보를 완전히 방어해주지 못하고 있다. 이에 본 논문에서는 운송장 정보를 QR 코드를 통해 보호하고 허가 받은 주체들만이 해당 정보에 접근할 수 있는 개인정보 유출 방지 기법을 제안하였다. 제안하는 방식을 통해 더 이상 개인 정보를 유출하려는 공격자는 일반 시각적 방식으로는 정보를 탈취할 수 없을 뿐만 아니라 QR 코드를 통해서도 허가가 되어 있지 않기 때문에 정보에 접근할 수 없게 된다. 또한 내부적인 접근 또한 블록체인을 통해 운송장 정보의 조회 사실을 관리하기 때문에 모든 접근 기록이 무결성이 보장된 상태로 기록이 된다. 이와 더불어 운송상에 효율성을 높이기 위해 QR 코드를 읽는 기기로 두 손이 자유로워 운반 효율성을 높여주는 스마트 글라스를 활용할 것을 제안하였으며 또한 스마트 글라스의 고질적인 문제인 시야 방해 문제를 증강 현실 기술을 통해 해결책을 제시하였다.

본 논문에서는 개인 정보 유출 문제에 대하여 일상생활에서 흔하게 사용되는 QR 코드 기술과 IT 기술들을 활용하여 문제를 해결하고자 하였다. 이와 같이 개인 정보 유출 방지를 위한 대안 방식으로 물리적인 접근뿐만 아니라 다양한 관점에서 개인 정보 보호에 대한 연구를 통해 미래 사회의 가장 중요한 재산 중 하나인 개인 정보에 대한 더 안전하고 발전된 방안을 찾을 수 있도록 지향되어야 할 것이다.

참 고 문 헌

1. 국외문헌

- Jo, Nam-sub (Seoul, KR) 2016 *Method of Confidentially Outputting Delivery Waybill, Server System Therefor and Agent System Therefor* United States K CLOUD CO., LTD. (Seoul, KR) 20160328763
- Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, and Edgar Weippl. 2010. QR code security. In *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia (MoMM '10)*. Association for Computing Machinery, New York, NY, USA, 430-435.
- Sarah Underwood. 2016. *Blockchain beyond bitcoin*. Commun. ACM 59, 11 (November 2016), 15-17.
- Gencer A.E., Basu S., Eyal I., van Renesse R., Sirer E.G. (2018) *Decentralization in Bitcoin and Ethereum Networks*. In: Meiklejohn S., Sako K. (eds) *Financial Cryptography and Data Security*. FC 2018. Lecture Notes in Computer Science, vol 10957. Springer, Berlin, Heidelberg.
- Martin Johansson and Mårten Pettersson. 2000. Eyes on the road—augmenting traffic information. In *Proceedings of DARE 2000 on Designing augmented reality environments (DARE '00)*. Association for Computing Machinery, New York, NY, USA, 147-148.
- Carmigniani, J., Furht, B., Anisetti, M. et al. *Augmented reality technologies, systems and applications*. Multimed Tools Appl 51, 341-377 (2011).
- A. Syberfeldt, O. Danielsson and P. Gustavsson, *Augmented Reality Smart Glasses in the Smart Factory: Product Evaluation Guidelines and Review of Available Products*, in IEEE Access, vol. 5, pp. 9118-9130, 2017.
- Furkan Tari, A. Ant Ozok, and Stephen H. Holden. 2006. *A comparison of perceived and real shoulder-surfing risks between alphanumeric*

and graphical passwords. In Proceedings of the second symposium on Usable privacy and security (SOUPS '06). Association for Computing Machinery, New York, NY, USA, 56-66.

Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. 2006. *Design and evaluation of a shoulder-surfing resistant graphical password scheme*. In Proceedings of the working conference on Advanced visual interfaces (AVI '06). Association for Computing Machinery, New York, NY, USA, 177-184.

2. 인터넷 자료

The Radio News. *6 billion unauthorized leaks of personal information over 10 years* [Internet]. Available: <http://www.jeonpa.co.kr/news/article-View.html?idxno=59734>

Security News. *Personal information accidentally leaked by delivery service* [Internet]. Available: <https://www.boannews.com/media/view.asp?idx=50589&page=1&kind=1>

CNET. *The smart glasses that could be ready for my eyes*[Internet]. Available: <https://www.cnet.com/news/the-smart-glasses-that-could-be-ready-for-my-eyes/>

CNA. *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>

ABSTRACT

Blockchain system for improving delivery efficiency and protecting personal information using smart glasses

Choi, Seung-Joo

Major in IT Convergence Engineering

Dept. of IT Convergence Engineering

The Graduate School

Hansung University

The importance of protecting personal information is getting more attention than ever. However, the courier system has not yet been able to keep up with this movement. The delivery box has a waybill with sensitive personal information about the recipient, such as name, phone number, and address, so anyone can easily steal personal information. In order to solve this problem, this paper proposes to deal with the contents of the waybill with QR code rather than text that any person with a normal eyesight can read. In addition, in order to prevent indiscriminate access to the QR code containing the information of the waybill, access to the information is limited to only the recipient and the smart glasses of the carrier which would be registered in advance in the blockchain network of the delivery system. In addition, in order to prevent personal information leaking from the malicious workers of the courier company

or the carrier with the access to the QR code information using the registered smart glasses, we also propose to record every access of the waybill information in the blockchain. Finally, in order to increase the efficiency of courier transportation, we propose to apply AR technology using the smart glasses. Lastly, we compare the difference between the existing courier system with the proposed one.

【Keyword】 Privacy, Blockchain, Smart Glasses, QR Code, AR