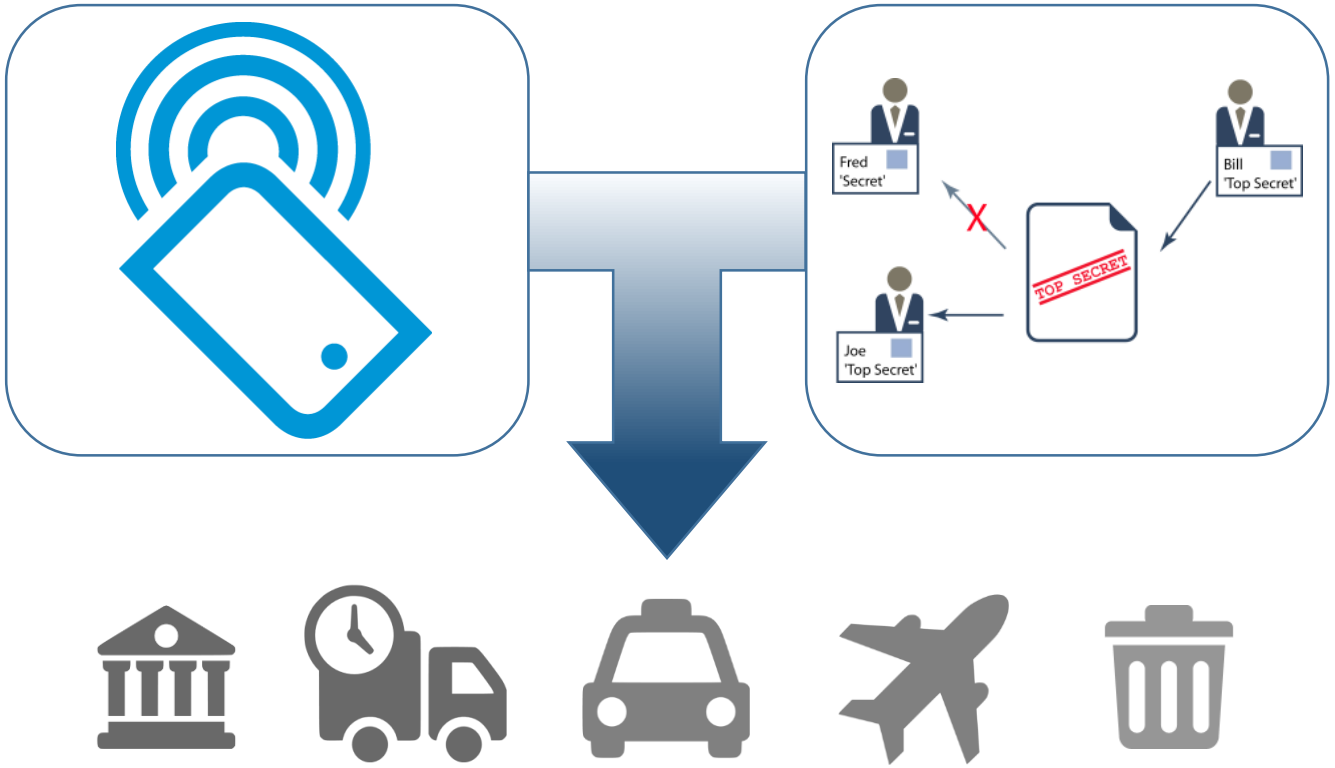
국가암호공모전 2015
(I-B 암호 활용 아이디어 제안)

역할 및 속성 기반 NFC 접근제어 기술
익명 및 필명 기반 프라이버시 보호 기술

INDEX

01 소개

- 높은 컴퓨팅성능과 다양한 통신 기능을 가진 스마트폰 보급
- 속성 기반 암호화 기술의 발전및 대중화로 인한 중요성 대두

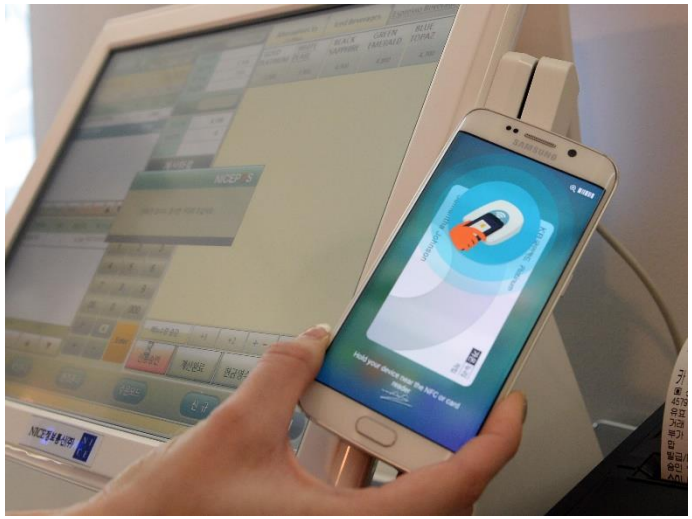


- **기존 서비스에 대한 역할 및 속성기반 NFC 접근 제어기술 제안**

02 기반기술

NFC(Near Field Communication)

- NFC(Near Field Communication)
  - 가까운 거리의 **무선통신**을 가능하게 하는 기술
  - **스마트폰**, 교통카드, 티켓 등 여러 서비스 분야에서 사용
  - 삼성 페이와 애플 페이와 같은 **핀테크**에 자주 이용
  - 보안 표준 적용으로 **안전한 통신**



NFC기술을 이용한 삼성페이와 에플페이

02 기반기술

RBAC(Role Based Access Control)

- RBAC(Role Based Access Control)
  - **역할 기반** 접근 제어 기술
  - 사용자(User), 역할(Role), 권한(Permission), 세션(session)으로 구성
  - 권한은 **정적**으로 할당 되어 한번 할당 되면 수정될 수 없음

속성	기능
사용자	하나 이상의 역할을 수행하는 객체, 하나 이상의 역할 수행
역할	접근 제어의 식별자와 권한 대입, 하나이상의 권한 가능
권한	자원에 대한 접근 권한과 접근 방법, 속성 추가 가능
세	권한을 활성화 시 여러 권한을 부여가

02 기반기술

ABAC(Attribute Based Access Control)

ABAC(Attribute Based Access Control)

- 속성 기반 접근 제어 기술
- 객체, 객체 속성, 주제, 주제속성, 권한, 인증 으로 구성
- 동적으로 속성이 할당 되며 실시간 환경에 적합

속성	기능
객체	하나 이상의 속성을 부여 받는 객체, 하나이상의 속성 가능
주제	접근 제어의 식별자와 권한 대입, 하나이상의 속성 가능
권한	자원에 대한 접근 권한과 접근 방법 및 수행 방법 정의
인증	객체 속성과 주제 속성 기반 수행 여부 판단

03 기존 서비스 및 제안 기법

택배 배달 시 NFC를 이용한 사용자 인증

- 택배 서비스는 구매 당사자에게 전달 되었는지 확인하는 과정이 중요
- 현재 택배 시스템은 수취인 인증절차가 대부분 생략 됨
- 수취인들이 간편하게 인증할 수 있는 수단 필요
- 스마트폰의 NFC 기능을 이용하여 택배 배달시 수취인 인증 제안
- 제3자에게 권한을 부여하는 속성 기반 모델 제안

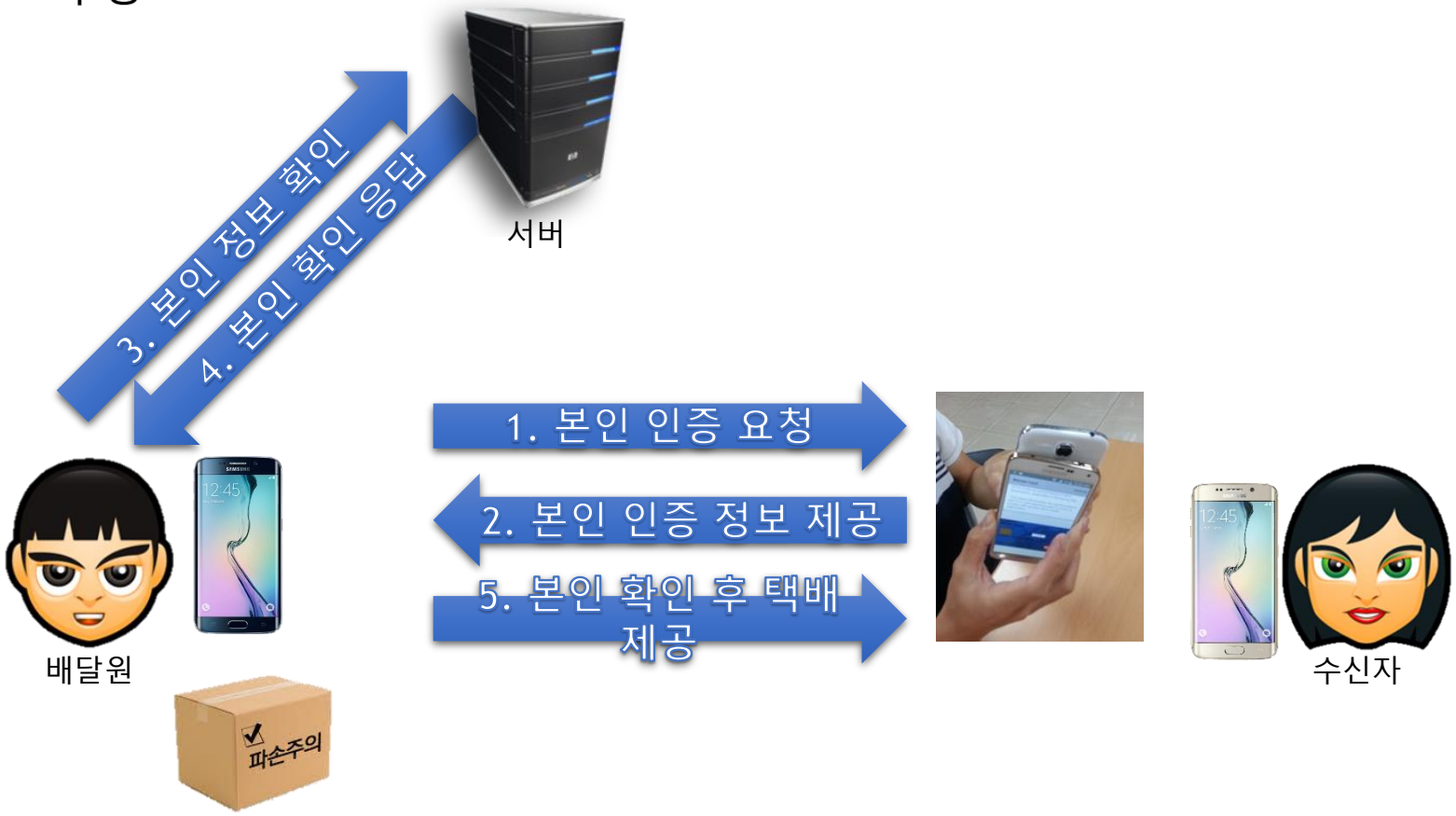
수취인 인증이 생략된 택배 수령

수취인 인증이 없는 무인 택배 보관함

03 기존 서비스 및 제안 기법

택배 배달 시 NFC를 이용한 사용자 인증

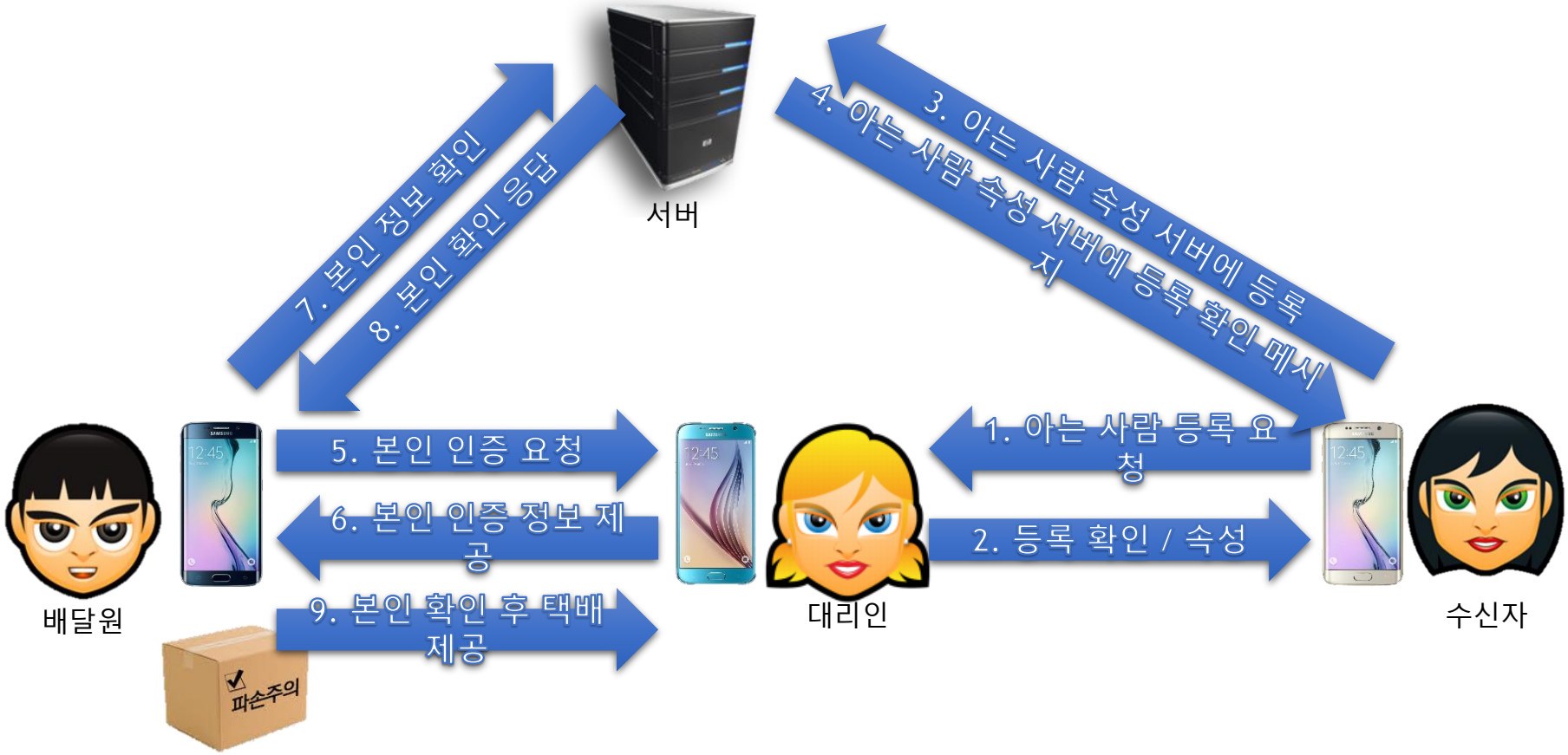
택배 서비스는 구매 당사자에게 전달 되었는지 확인하는 과정이 중요



03 기존 서비스 및 제안 기법

택배 배달 시 NFC를 이용한 사용자 인증

본인 부령 불가시, 속성을 부여 받은 대리인 수령



03 기존 서비스 및 제안 기법

NFC를 이용한 도서관 사용자 인증 및 대출 제어

- 도서관은 많은 사람들이 다량의 책을 대여 할수 있는 서비스를제공
- 많은 작업을 효율적으로 빠르게 처리해야 함
- 도서관 출입 및 도서 대출시 본인 인증 문제
- 상호 연동과정의 부족 및 암호화 되지 않은 불안전한 통신
- 도서관 전체 시스템 통합의 필요

도서 대출기를 이용한 불편한 대출

단순 1회성 사용자 인증을 통한 도서관 출입

03 기존 서비스 및 제안 기법

NFC를 이용한 도서관 사용자 인증 및 대출 제어

- 사용자 고유 정보 암호화를 통한 개인정보 보호
- NFC를 이용한 손쉬운 사용자 인증 및 인증 정보 기반 세션키 이용
- 세션키 바탕 통신 암호화로 안전한 통신 환경 제공

03 기존 서비스 및 제안 기법

도서관 내 NFC를 이용한 사용자 인증 및 대출 제어

실제 도서관에서 대출 과 **NFC**를 이용한 인증 및 대출 비교 실험

	입구	도서 검색	도서 선택	대출	출구	시간
기존	 학생증 을 통한 인증	 도서 검색기 이용	 도서 선택	 재 인증후 대출	 퇴장	8분 21초
NFC적용	 NFC를 이용한 인증	 스마트폰 도서 검색	 도서 선택	 NFC를 이용한 대출	 NFC를 이용한 퇴장	4분 40초

기존 도서 대출 시스템과 제안 하는 NFC를 이용한 인증 및 대출 비교

기존 도서 대출 시스템에 비해 약 3분 41초 가량 **절약**

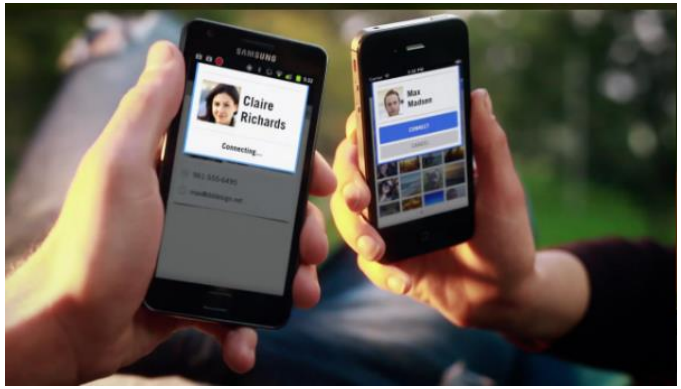
사람이 더 **많아 지는 시간**의 경우 더 많은 시간 절약 예상

03 기존 서비스 및 제안 기법

NFC를 이용한속성 기반 명함 교환

- 명함에는 공적인 정보(이름, 직책, 전화번호, 이메일 등)가 포함되게 됨
- 공적 정보가 악의적인 사용자에게 노출되어 프라이버시가 침해될 수 있음
- 기존 암호화 되지 않은 명함 교환 프로그램은 공격당하기 쉬움

안전하지 않은 명함 교환 방법



부채널 공격 혹은 해킹 공격에 취약한 명함 교환 방법

03 기존 서비스 및 제안 기법

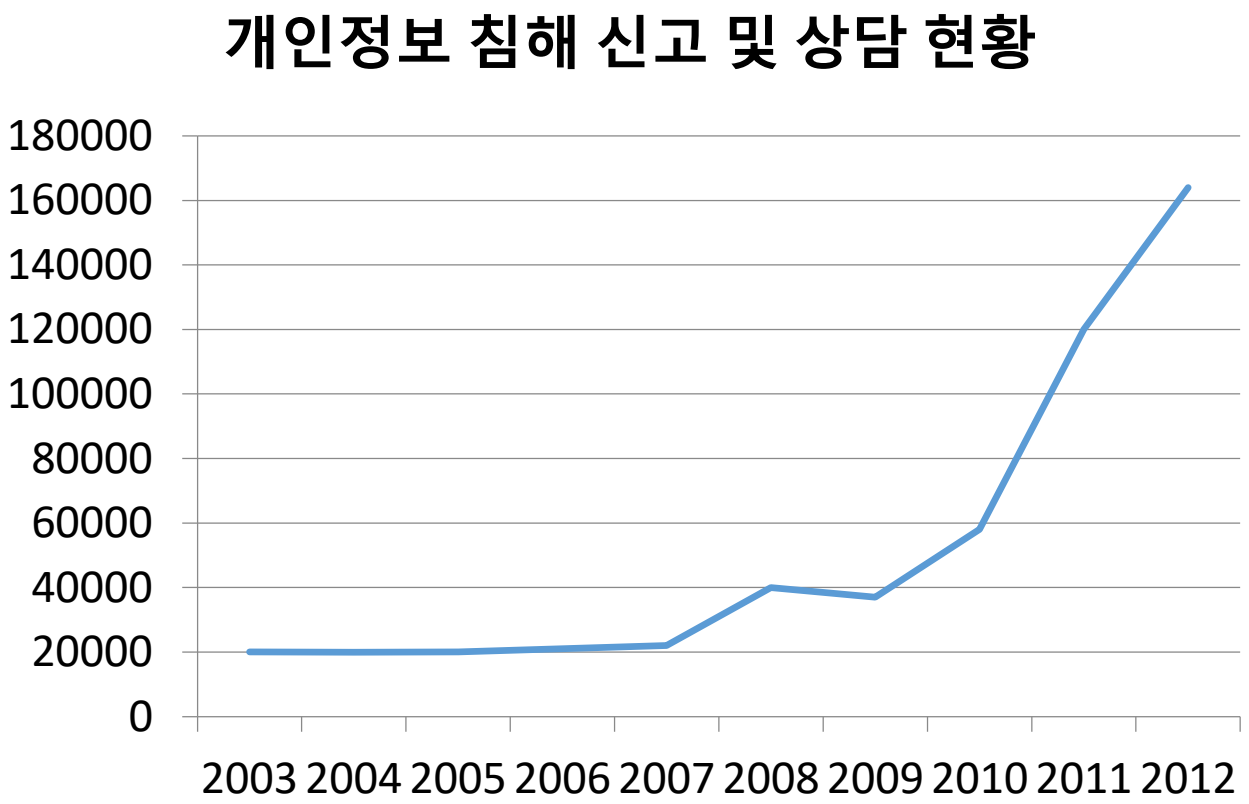
NFC와 얼굴 인증을 이용한 자동화 여권 심사

- 자신의 정보를 안전하고 빠르게 전달할 필요성의 대두
- 속성 기반 암호화 기법을 적용하여 명함을 관리
- 물리적인 명함의 정보노출 위험 방지

INDEX

01 소개

- 급속한 ICT 기술의 발전으로 인해 프라이버시 침해 증가



- **기존 서비스에 대한 프라이버시 보호 기법 제안**

02 핵심요소

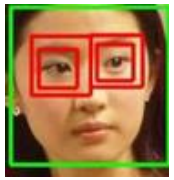
암호화 - 익명, 필명 마스킹

- 암호화 및 공개키 기반 구조를이용한 익명, 필명, 마스킹 처리
- 사용자의 프라이버시를 침해할 수 있는 핵심 개인정보를 암호화

RSA, ECC, AES

사용자 개인 정보 → 암호화 디바이스 → 익명, 필명, 마스킹 처리된 정보

익명, 필명, 마스킹화

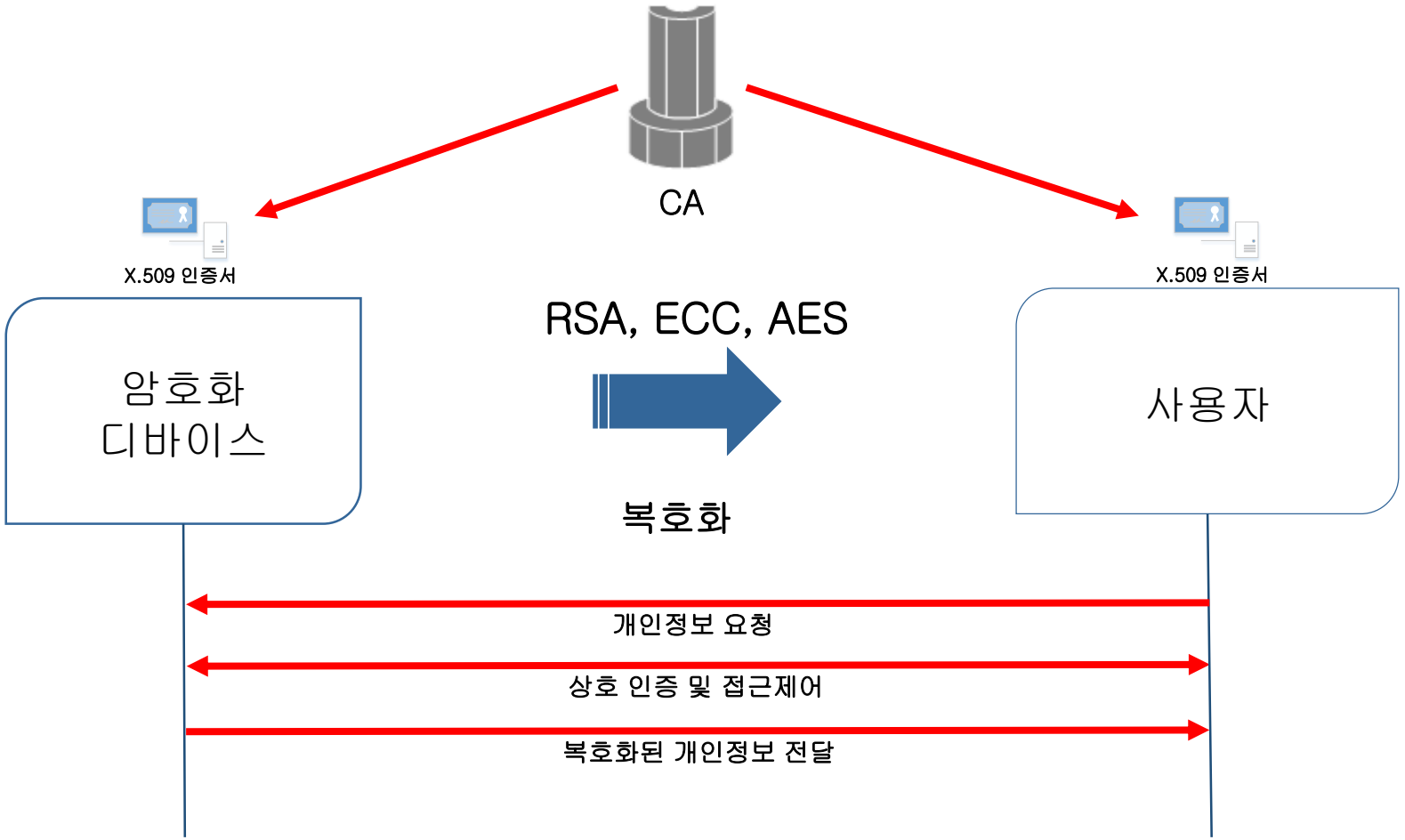
이름	: 홍길동
전화번호	: 010-1010-1010
카드 번호	: 1234-6789-3042-1234
사진	

이름	: 51237ab76c723d12
전화번호	: 1624ab6564d4f3d5
카드 번호	: dfdff65333abc7875
사진	

02 핵심요소

복호화 및 PKI

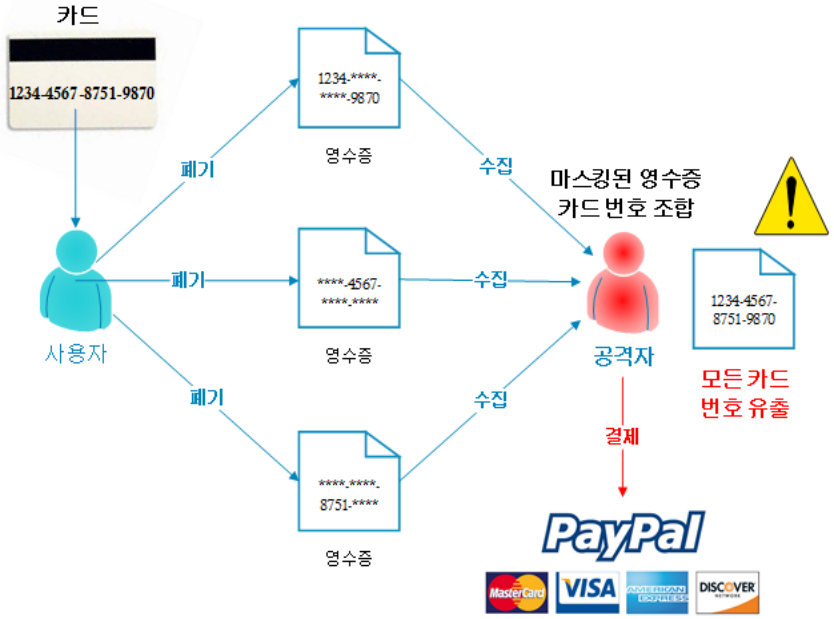
정당한 사용자만이 복호화를 통해 정보 식별 가능



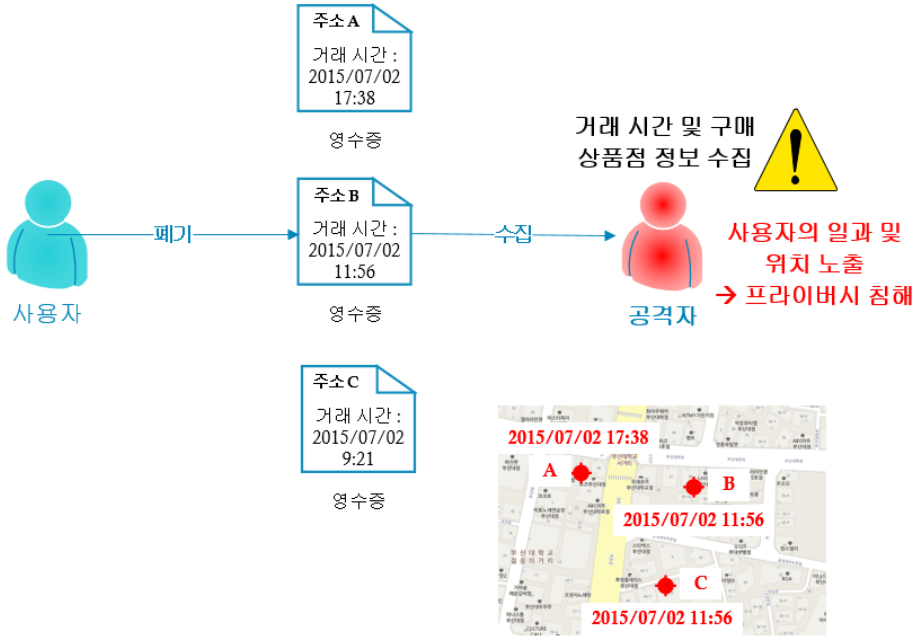
03 카드 결제 시스템

기존 기법의 문제점

- 영수증 : 거래에 대한 확인을 위해 다양한 정보 포함
- 대부분의 사람들은 영수증 관리 소홀
- 카드번호, 거래 시간, 구매 물품, 거래 장소, 회원 정보등의 정보 유출



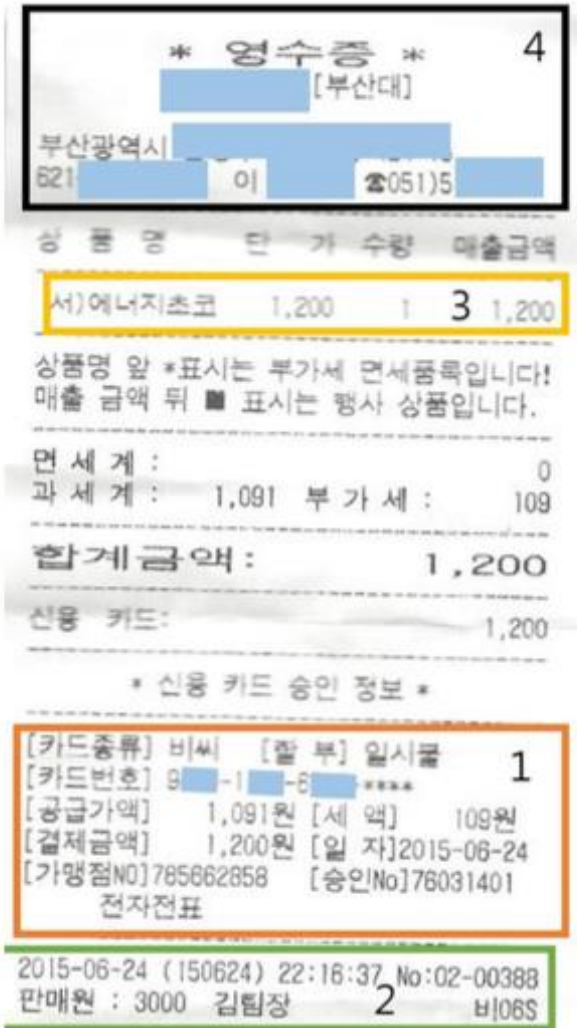
카드 번호 유출



거래 장소 및 시간 유출

03 카드 결제 시스템

유출된 정보



4. 거래 장소

3. 구매 물품

1. 카드번호

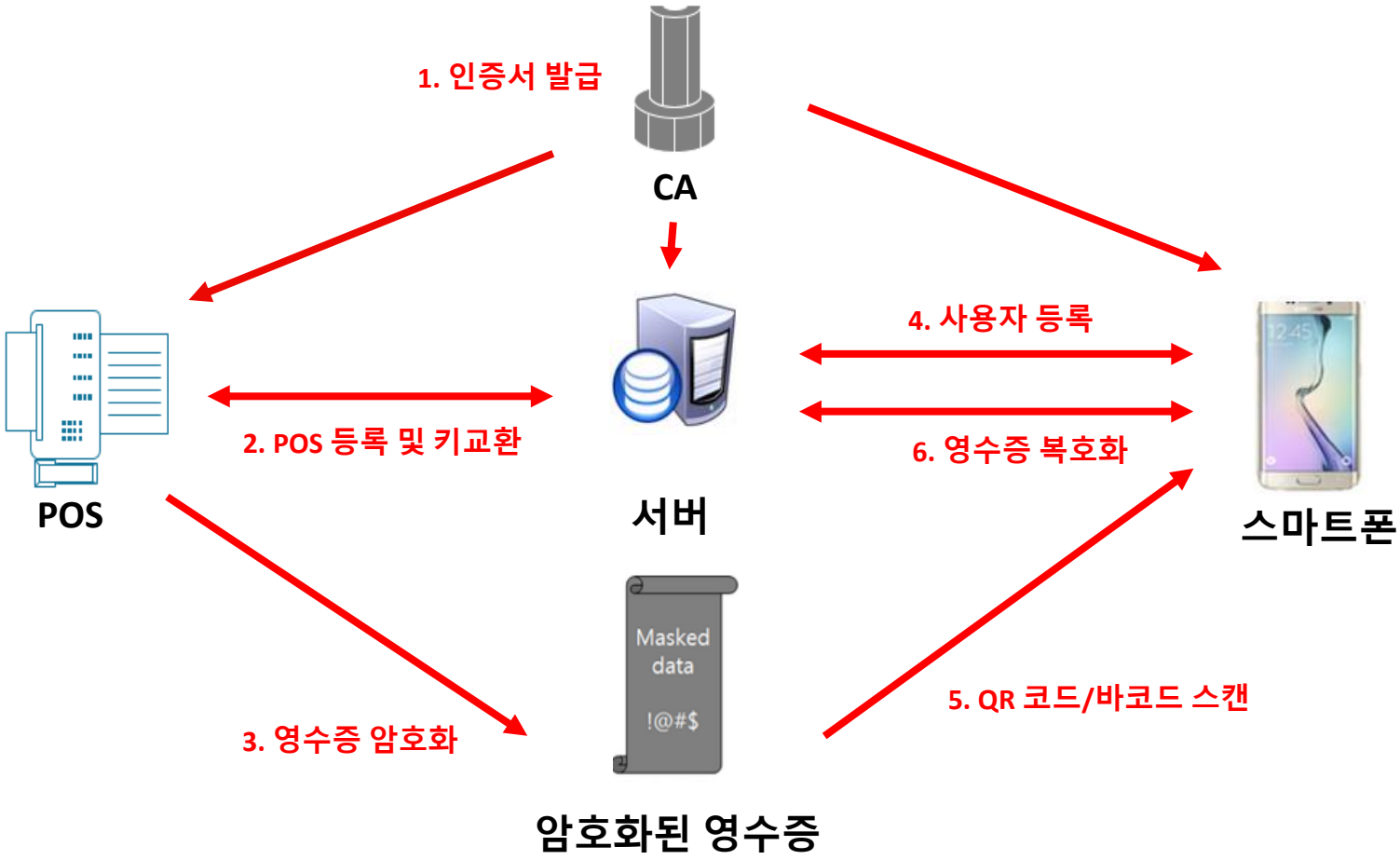
2. 거래 시간

5. 회원 정보

03 카드 결제 시스템

제안 기법

- 영수증을 출력하는 POS기를 통한 영수증 암호화
- 인증된 사용자에 대한 영수증 복호화 허용



03 카드 결제 시스템

기존 기법과 제안 기법의 비교

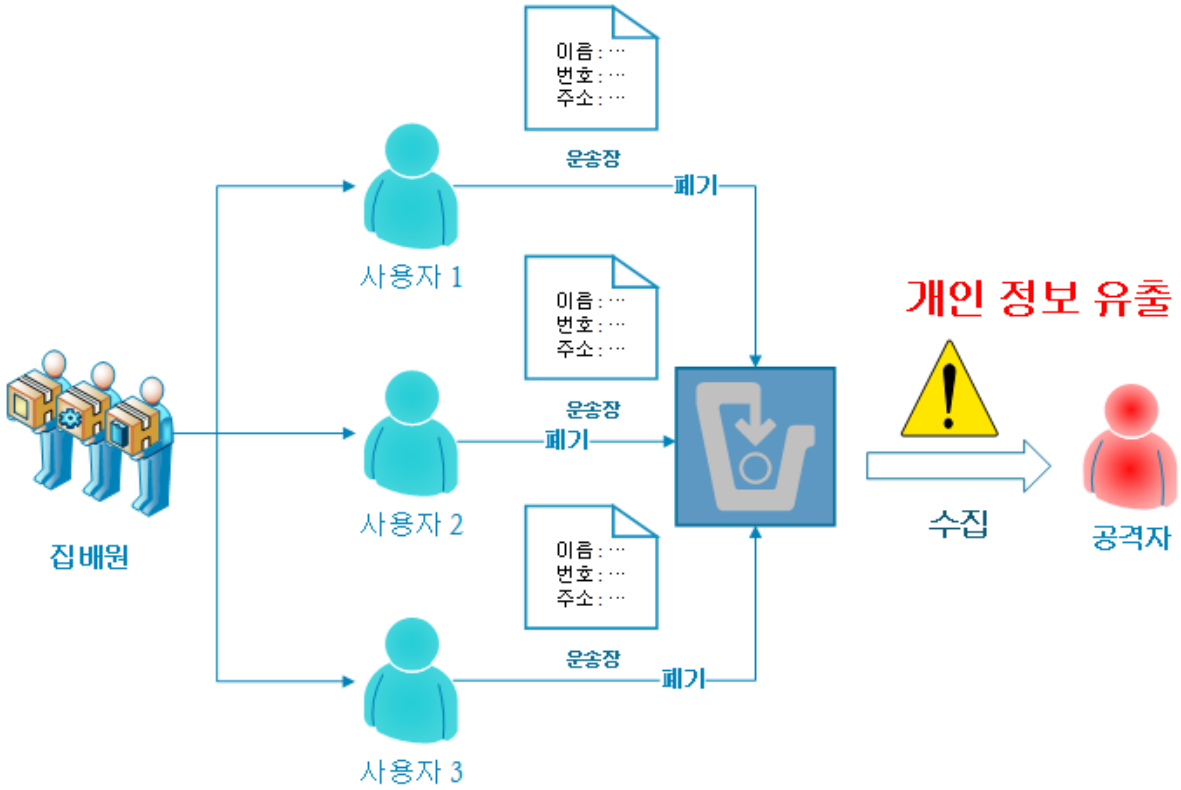
- 기존 기법에서는 거래 내용을 보다 확실 하는 것에 중점
- 제안하는 기법의 경우 중요 개인 정보에 대한 정보 은닉 기술 적용
- 금전적 피해 및 사용자의 프라이버시 보호 가능

	거래확인 기능	**정보 은닉**
기존 기법	O	X
제안하는 기법	O	O

03 택배 시스템

기존 기법의 문제점

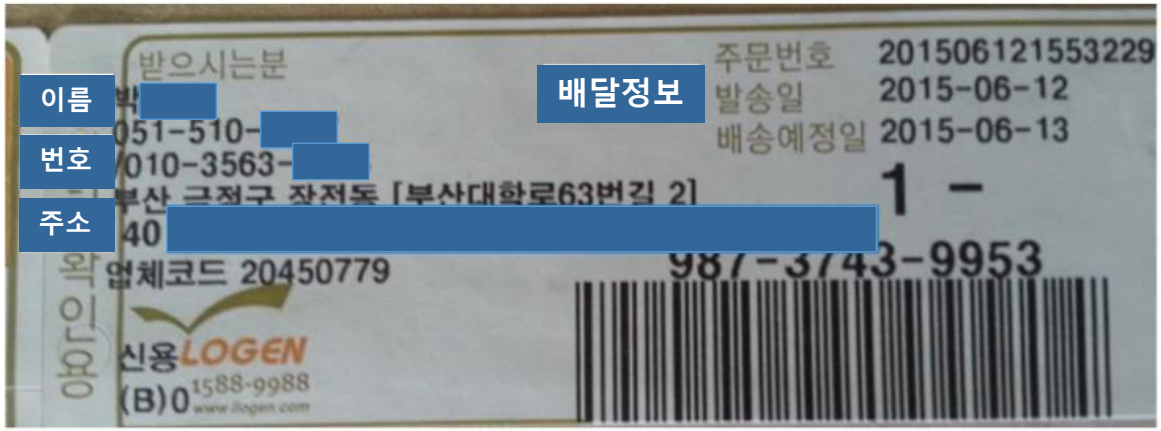
- 물건의 정확한 전달 및 구매자 확인을 위해 운송장에 중요 개인정보 입력
- 물품의 포장지에 부착된 운송장의 경우 관리에 소홀하기 쉬움
- 이름, 번호, 주소, 배달정보와 같은 민감한 개인정보가 유출



03 택배 시스템

유출된 정보

실제 운송장에 입력된 개인 정보



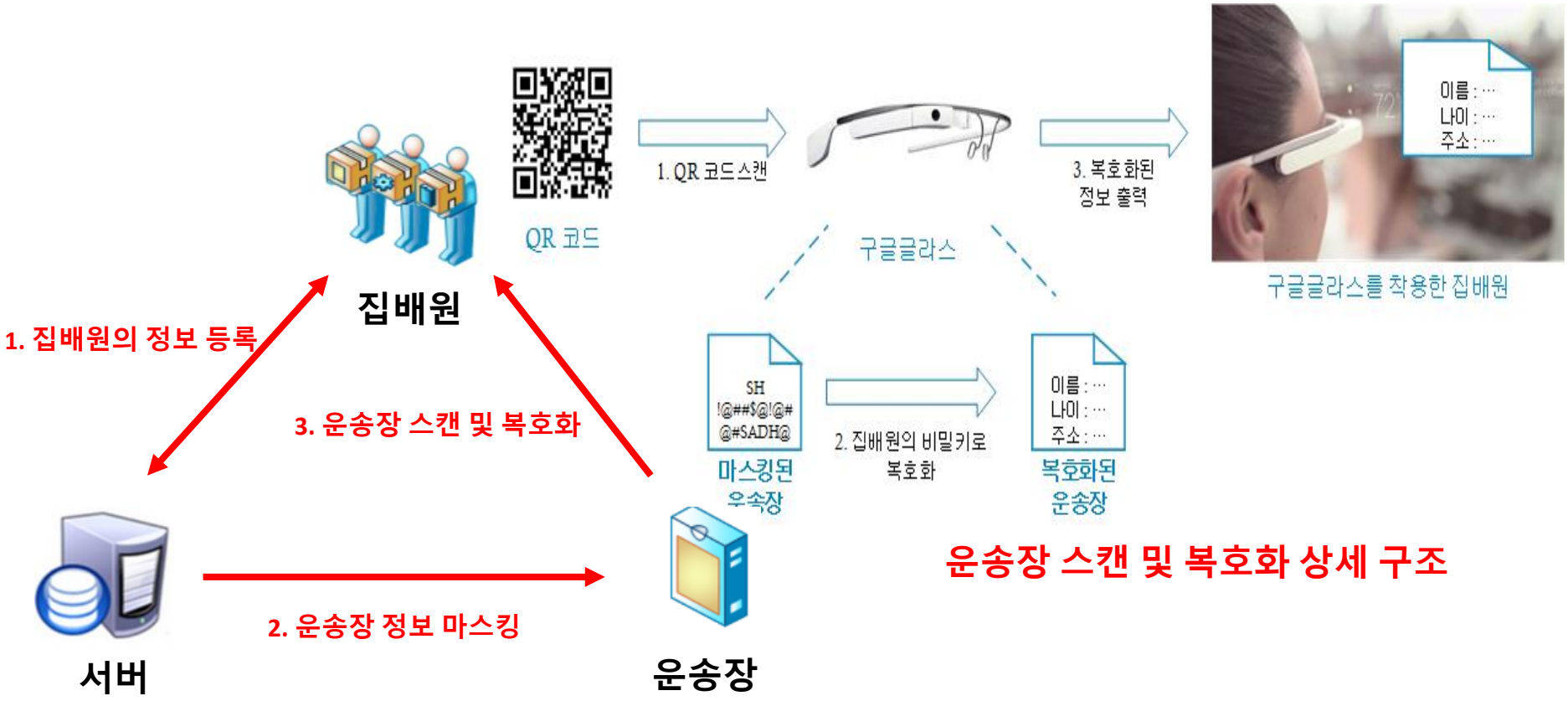
개선된 택배 시스템 - 안심 번호 서비스

번호를 제외한 주요 정보(이름, 주소 등)가 여전히 노출

03 택배 시스템

제안 기법

- 운송장의 주요 정보 암호화를 통한 프라이버시 보호
- 구글글라스를 이용한 정보 복호화



03 택배 시스템

기존 기법과 제안 기법의 비교

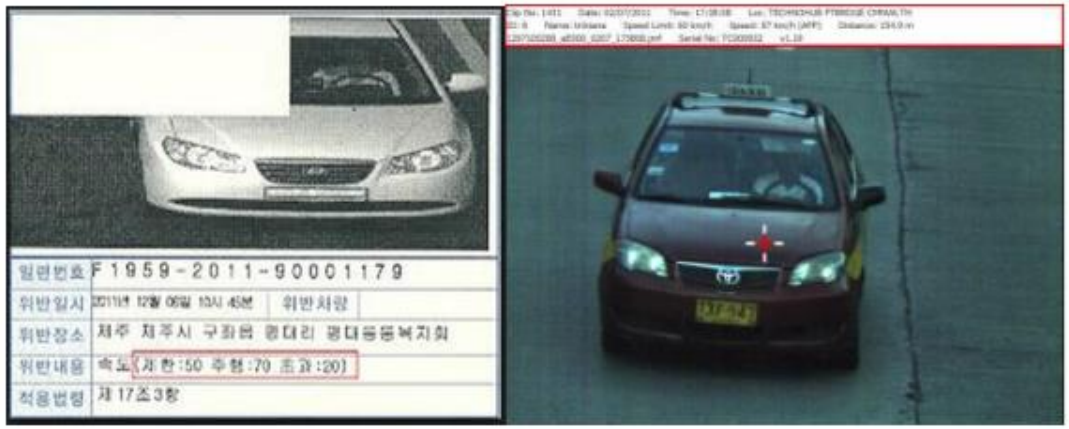
- 기존 기법은 집배원이 개인 정보를 확인하기 위한 별도의 장비가 필요 없음
- 운송장이 별다른 조치 없이 폐기될 경우 개인정보가 유출
- 제안 기법의 경우 집배원만이 확인 가능한 암호화된 코드를 운송장에 입력
- 사용자의 프라이버시 보호 가능

	배달 주소 확인	정보 은닉
기존 기법	O	X
제안하는 기법	O	O

03 속도위반 처리 시스템

기존 기법의 문제점

- 공무원이 직접 사용자의 중요 정보(얼굴, 동승자 등)를 마스킹



- 중간 처리 과정에서 중요 개인 정보가 유출 가능

NY중앙일보 > 뉴스 > 사회/정치 > 일반 기사목록 | 글자크기 +−

뉴욕주 차량국, 운전자 개인정보 팔았다

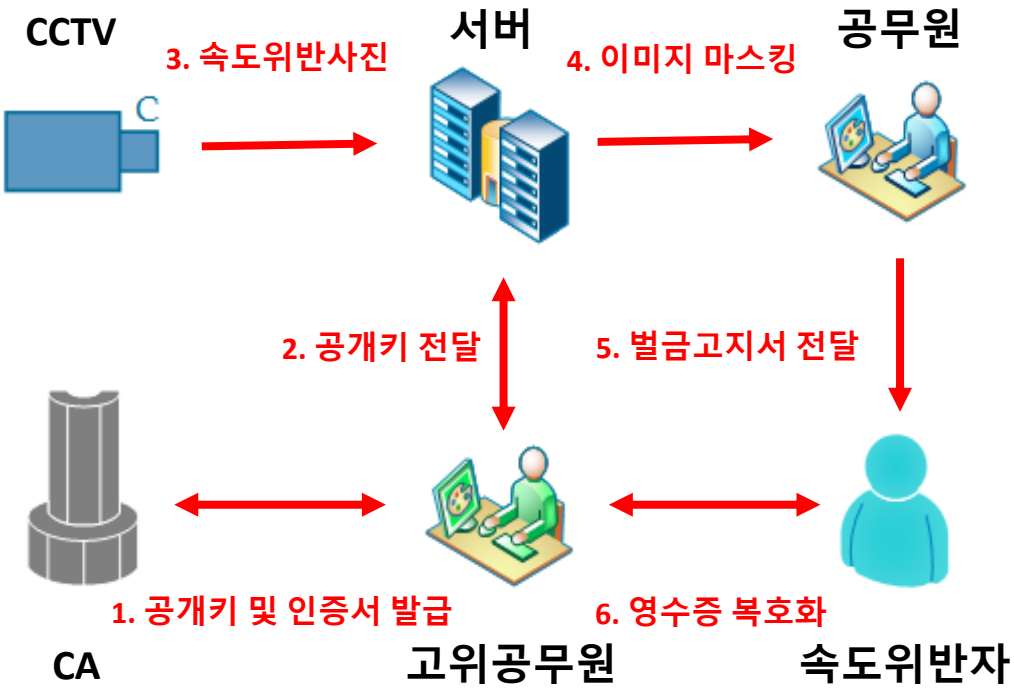
자동차 제조업체, 보험회사, 고용주 등에
CBS "지난해 6000만불 챙겨…연방법 위반"

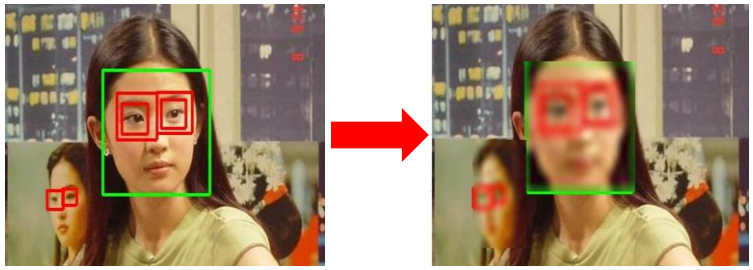
댓글 0 [뉴욕 중앙일보] 발행 2015/05/13 미주판 6면 기사입력 2015/05/12 21:53

03 속도위반 처리 시스템

제안 기법

- 고위 공무원(지역별)의 공개키를 이용한 암호화를 통해 이미지 마스킹
- 속도위반자의 요구가 있을 경우 고위 공무원의 개인키를 통해 복호화



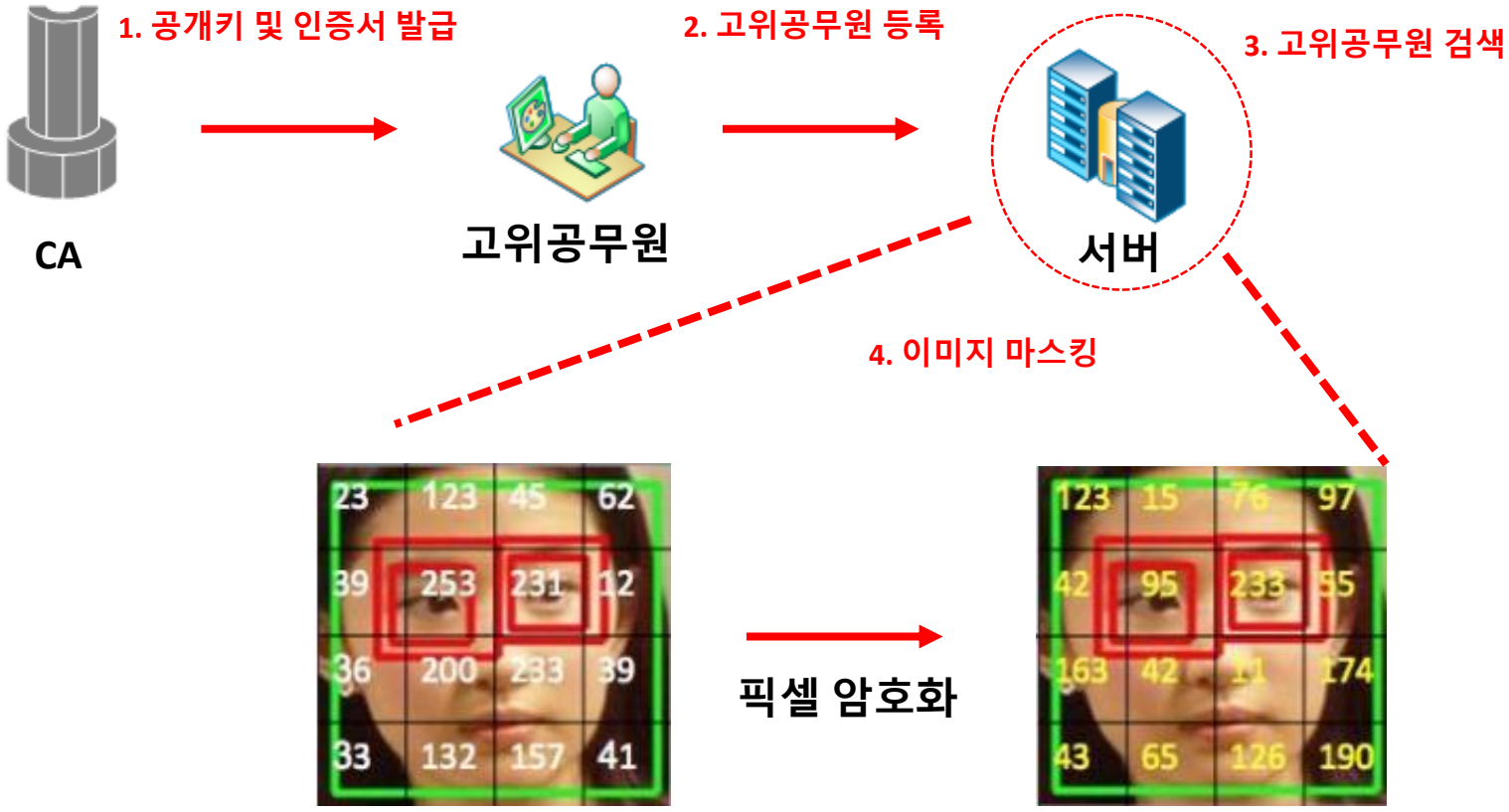


프로그램 기반 자동 마스킹

03 속도위반 처리 시스템

제안 기법

- 지역별 고위 공무원 공개키를 서버에 저장
- CCTV의 지역 정보를 통해 담당 고위 공무원의 공개키 검색



03 속도위반 처리 시스템

제안 기법 응용

- 안드로이드, iOS의 경우 사용자의 사진에 대한 시간, 장소별 정리 기능 제공
- 빅데이터 분석기술의 발달로 인해 프라이버시 침해 가능성 증가
- 얼굴인식을 통한 자동 마스킹 기술의 일반 사진에 적용
- 사진에 찍히는 타인에 대한 프라이버시 침해 예방

무보정사진

보정사진

03 속도위반 처리 시스템

제안 기법 응용

- 사진 촬영시 목표물 지정
- 목표물을 제외한 부분은 배경으로 설정
- 배경중에서 얼굴 인식을 통해 사람으로 인식된 부분 자동 마스킹

03 속도위반 처리 시스템

기존 기법과 제안 기법의 비교

- 기존 기법의 경우 촬영된 사진이 그대로 사용되어 프라이버시 침해 가능
- 제안하는 기법의 경우 자동 마스킹을 통해 이를 보완
- 서버단에서의 마스킹 처리를 통해 중간 단계 유출 방지
- 제안 기법을 응용할 경우 타인에 대한 프라이버시 침해 예방 가능

	사진 제공	프라이버시 보호기능	안전한 암호화 관리
기존 기법	O	X	X
제안하는 기법	O	O	O

04 결론

❑ **역할 및 속성 기반 NFC 접근제어 기술**

- ✓ 응용서비스에 대한 새로운 접근제어 및 관리 기법 제안
- ✓ 안전한 NFC 기술 및 속성/역할 기반 암호화 기법 적용을 통한 사용자 권한 조율
- ✓ 최신 IoT 기술과 암호의 적용한 기법 제시

❑ **익명 및 필명 기반 프라이버시 보호 기술**

- ✓ 기존의 다양한 으용서비스를 통해 침해되는 프라이버시 분석
- ✓ 암호학적 관점을 통한 해결 방안 제시
- ✓ 기존의 응용서비스보다 안전하고 편안한 응용서비스 제공 가능

감사합니다

THANK YOU