Journal of KIIT. Vol. 17, No. 5, pp. 129-136, May 31, 2019. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2019.17.5.129

IoT 환경에서 GDPR에 부합하는 개인정보수집 동의 절차

이구연*[1], 방준일**, 차경진***, 김화종*[2]

GDPR Compliant Consent Procedure for Personal Information Collection in the IoT Environment

Goo Yeon Lee*[1], Junil Bang**, Kyung Jin Cha***, and Hwa Jong Kim*[2]

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No. 2018-0-00261, IoT 환경에서 일반개인정보보호규정에 부합(GDPR Compliant)하는 개인정보 관리 기술 개발)

요 약

센서 등 많은 IoT 디바이스들은 화면출력 및 입력장치 등이 결여된 경우가 많아 개인정보보호법이나 GDPR 등에서 요구하는 개인정보수집 동의 절차를 만족시키기 어려워, 해당 비즈니스 분야 발전에 법적인 걸림돌로 작용하고 있다. 본 연구에서는 법적인 요건을 만족하는 IoT 시스템에서의 개인정보수집 동의 절차를 설계한다. 설계된 방식에서는 먼저 사용자의 개인정보가 암호화된 상태로 수집되며, 이후 데이터 수집 서버와 사용자 에이전트 사이에 개인정보 수집을 기반으로 연관을 맺음으로서 암호화된 내용을 복호화 한다. 이러한 연관 동의 과정에서 사용자 에이전트는 데이터 수집 서버의 개인정보수집 약관 등을 이해하고 복호화키를 제공한다. IoT 시스템에서의 이러한 방식의 개인정보수집 동의 절차는 GDPR 등의 법령에서 정하는 투명성, 자율성 등의 요건을 만족함으로서 개인정보를 취급하는 IoT 비지니스 분야의 발전에 크게 기여할 것으로 판단된다.

Abstract

Many IoT devices like sensors lack screen and input devices, thus making them hard to meet the consent conditions that GDPR requires. This is acting as a legal barrier for further advancement in the business field. In this paper, we designed the process for consent of personal information collection that meets the legal conditions. In this design, user's personal data is received in an encrypted form by data collecting server first. The encrypted personal data can be decrypted after associating with user agent based on the consent procedure of the collection of personal information. During the consent procedure, user agent understands the privacy policy about personal information collection and offers the key to decrypt the data. This kind of personal information collection agreement procedure will satisfy the transparent and freely given consent requirements of GDPR. Thus, we can speculate from here that the proposed procedure will contribute to the evolution of IoT business area dealing with personal information.

Keywords
GDPR, IoT, personal information, consent procedure, privacy policy

* 강원대학교 컴퓨터정보통신공학과 교수(*[1]교신저자)
- ORCID[1]: https://orcid.org/0000-0002-1769-6230
- ORCID[2]: https://orcid.org/0000-0002-3822-390X
** 강원대학교 컴퓨터정보통신공학과 대학원 석사과정
- ORCID: https://orcid.org/0000-0003-0582-1572
*** 강원대학교 경영대학 교수
- ORCID: https://orcid.org/0000-0001-8286-9284

· Received: Feb. 15, 2019, Revised: Apr. 25, 2019, Accepted: Apr. 28, 2019
· Corresponding Author: Goo Yeon Lee
Dept. of Computer Eng., Kangwon National University, Chuncheon, Korea,
Tel.: +82-33-250-6394, Email: leegyeon@kangwon.ac.kr

Ⅰ. 서 론

개인정보보호는 한국의 개인정보보호법[1]이나 유럽의 개인정보보호 규정(GDPR, General Data Protection Regulation)[2]-[4] 등에서 볼 수 있듯이 개인정보 수집 주체에게 개인 정보의 생명주기상 개인정보 생성, 수집, 저장, 처리, 폐기에 이르기까지 엄격한 절차의 준수 및 관리책임을 묻고 있다. 이러한 개인정보의 수집 및 처리 과정에서 가장 먼저 시행해야 할 절차는 수집시의 동의 절차이다.

일반적으로 개인정보 수집은 오프라인 및 온라인을 가리지 않고 다양한 영역에서 이루어지고 있다. 오프라인의 경우 우리는 신용카드 가입이나 통신서비스 가입, 또는 은행에서의 계좌 개설 등에서 개인정보 수집 및 동의에 관한 경험을 많이 하고 있다. 오프라인과 더불어 온라인상에서도 개인정보 수집이 많이 이루어지는데 인터넷상에서 컴퓨터나 스마트폰을 통하여 특정 사이트의 회원 가입이나, 온라인 쇼핑몰에서의 물품 구매 및 결제 시에 개인정보 수집 및 활용에 동의를 많이 한다. 위와 같은 개인 정보의 수집 절차의 준수는 법에 의하여 규제 및 감사를 받으며 이를 어기면 벌금이 부과된다, 우리나라 개인정보보호법의 경우 벌금은 대략 1천만원, 3천만원, 5천만원 등의 수준으로 개인정보 수집 주체가 다소 법적 절차를 소홀히 할 수 있는 여지가 있으나, 유럽의 GDPR의 경우 벌금의 액수가 전 세계 매출액의 4%까지 부과하게 되어 개인정보 수집 및 처리 절차의 적법성에 대한 철저한 대비를 하고 있다. 이러한 개인정보 수집에 대한 동의 절차는 오프라인 경우는 면대면으로 서류에 서명을 하게 되며, 온라인상에서도 컴퓨터나 스마트 폰의 화면을 통하여 개인 정보 처리 약관을 이해하고 이에 대한 동의 또는 거부 표시를 입력 장치를 통하여 수행함으로서 법적 절차를 준수하게 된다.

최근 많은 IoT 디바이스가 개발 및 상용화 되고, 이러한 IoT 디바이스들로 구성된 IoT 시스템이 구축되어 여러 분야에 적용됨에 따라 다양한 정보를 생성, 처리함으로서 우리 생활을 보다 윤택하고 편리하게 하고 있다. 개인화된 웨어러블 IoT 디바이스들의 경우 사람의 몸에 부착되어 여러 정보를 센싱하고 이를 게이트웨이를 통하여 부가적인 처리를 수행한다. 자이로 센서나 가속도 센서 뿐만 아니라 신체의 여러 건강 신호를 센싱하는 IoT 디바이스들은 신체의 이상신호를 바로 검출하여 긴급 의료 기관으로 전송할 수 도 있다. 가정 내의 자동화를 위한 IoT 시스템도 많이 개발되어, 가정 내의 여러 곳에 설치되고 있으며, 이는 주로 냉장고(터치기능 스크린 부착 냉장고), TV, 셋탑박스 또는 전용 접속장비 등을 게이트웨이로 하여 IoT 수집 정보 주체에게 정보를 전달한다. 가정 내의 온도 및 습도, 에너지 사용량, 각종 가전 제어, 불법 침입 감지, 원격 검침 등의 기능을 수행함으로서 우리의 생활을 훨씬 편리하게 한다.

위의 여러 IoT 시스템에서 생성되고 처리되는 정보는 개인과 관련이 없는 단순 정보도 있지만, 개인정보에 해당하는 경우가 많이 존재한다. 또한 개별적으로는 개인정보에 해당하지 않지만 여러 개의 정보가 결합되면 개인정보에 해당하는 경우도 있다. 이러한 경우 개인정보 관련 법령의 적용을 받게 되는데, IoT 시스템의 본질적인 제한된 자원으로 인하여 해당 법령의 준수가 쉽지 않은 경우가 발생한다. 특히 동의 절차의 경우 일반적인 컴퓨터나 스마트폰과는 달리 출력장치 및 입력장치가 존재하지 않는 제한된 기능을 가지고 있는 IoT 디바이스의 경우에는 개인정보수집 동의 절차에 관한 법령을 준수하기가 어렵다. 간혹 IoT 시스템이 설치되어 있는 영역에 들어갈 경우 한 쪽 벽에 개인정보 수집 약관을 게시하여 동의 절차를 갈음하고자 노력하는 경우가 가능하나 이는 GDPR 등에서 명시하고 있는 자유로운 선택(거부할 수 있는 권리) 및 투명성 (약관이 개인정보 제공자에게 쉽게 접근되고, 또한 이해하기 쉽도록 제공되어야함) 측면에서 보면 만족스럽지 못하여 법적 다툼의 여지가 존재한다.

그러므로 이러한 문제를 해결하기 위해서는 IoT 시스템에 특화된, 개인정보보호 법령에서 제시하는 개인정보수집시의 동의 요건을 준수하는 메카니즘의 연구 및 설계가 필요하다. 이에 본 연구에서는 IoT 상에서의 효율적이고 안전한 개인정보수집 동의 절차에 대한 연구를 수행한다.

II. 관련 연구

IoT에서의 개인정보 수집 동의에 관한 많은 필요성이 제기되었고, 여러 절차가 연구되었다. 하지만 지금까지 제안된 방법들은 적용도메인에 대한 특장점을 가지고 있는 반면, GDPR에서 요구하는 법적 요건을 부분적으로만 만족시키고 있는 상황으로, 아직까지 법령에서의 규정을 충분히 만족시키는 연구는 이루어지고 있지 않은 상황이다.

[5]의 연구에서는 IoT에서의 프라이버시, 동의(Consent) 및 인가(Authorization) 측면에서 해결해야 할 난제들에 대하여 논의하였다. 다양한 IoT 디바이스의 이질성 및 제한된 자원으로 인한 한계를 극복하는 문제, 디바이스의 아이덴터티 및 소유권, 그리고 사용자가 관리 가능한 프라이버시 정책들에 대한 도전 과제들을 제시하였다. [6]의 논문에서는 IoT 프라이버시 등을 위한 마스킹 기법을 활용한 프라이버시 및 유틸리티 정보의 보존 프레임워크를 제시하였다. 제안된 프레임워크는 협의 과정을 기반으로 IoT 데이터 취급 관리 과정에서 유틸리티와 프라이버시의 절충안을 찾기 위한 구조를 설명하였다.

[7]의 논문에서는 IoT 환경에서 사용자의 정책(Policy)에 기반을 둔 정보수집 동의 절차를 설계하였다. 정책은 사용자 및 서비스 공급자, 그리고 IoT 디바이스를 포함하는 스마트 디바이스와 상호 작용을 함으로서 개인정보를 취급한다. 정책 관리자(Policy Manager)는 정책 데이터베이스를 기반으로 사용자의 개인정보의 제공 여부를 PDP(Policy Decision Point)의 결정에 근거하여 PEP(Policy Enforcement Point)가 집행하는 프레임워크를 설계하였다. 이러한 방식은 데이터 소유자가 서비스 제공자에게 사전 가입해야 하고, 또한 스마트 시티나 스마트 홈처럼 기반 기설이 잘 갖추어져야 하는 단점이 있어 IoT 디바이스로부터 개인정보를 바로 수신하는 개인정보 수집 주체를 가정하고 있는 현행 법령체계의 적용에는 적당치 않다. [8]의 연구에서는 C-ITS(Cooperative Intelligent Transport Systems)에서 [7]의 연구의 정책에 기반한 정보수집절차 개념을 적용한 프레임워크를 제안하였다. 해당 연구에서 C-ITS는 차량 등에 탑재된 시스템으로 속도와 위치 정보 등을 브로드캐스팅하고, 다른 차량 및 도로 사이드에 설치된 무선 통신 스테이션과 통신을 수행한다. C-ITS에서 전달되는 정보들에는 다양한 개인 관련 정보들이 포함되어 있으므로, 정책기반으로 이러한 정보들의 전송 여부를 결정한다. 이 연구 또한 [7]의 연구와 마찬가지로 IoT 디바이스로부터 개인정보를 바로 수신하는 개인정보 수집 주체를 가정하고 있는 현행 법령체계의 적용에는 적당치 않다.

[9]에서는 스마트폰 및 주변의 저전력 블루투스(BLE, Bluetooth Low Energy) 디바이스를 이용한 동의 절차를 제안하였다. 본 연구에서는 PrivacyBat라고 하는 BLE 기반의 프레임워크에 프라이버시 선호 정도를 포함 시키고, 사용자가 프라이버시가 포함된 정보 취급시에 동의 여부에 대한 규정을 정의하였다. [10]의 연구에서는 IoT에서의 투명성을 제고하기 위한 방안을 제시하였다. 데이터 수집 장치의 존재를 감지한 경우 사용자는 IoT 디바이스와 연결된 스마트 폰 등을 이용하여 개인정보 수집 동의 절차를 수행하는 방안으로 Wi-Fi의 GAS(Generic Advertisement Service) 이나 블루투스의 GATT (Generic Attribute Profile) 규격을 통하여, 주위에서 제공 되어지는 서비스들에 대한 정보를 교환할 때 프라이버시 정책에 대한 내용을 수신하여 이해함으로써 직접적으로 선택을 할 수 있도록 하는 직접적인 방법과, 프라이버시 수집 정책이 있는 데이터베이스의 레지스트리(Registry)를 사용자가 접속하여 프라이버시 정보의 수집 여부에 대한 선택을 할 수 있는 등록기반 방법을 제안하였다. 해당 연구에서는 개인정보 수집 동의시의 투명성제고에 관한 원칙적인 방법을 제안하였으나, 상호 인증이나, 기밀성 등의 세부적인 절차에 대한 연구는 미비한 상황이다. [11]의 연구에서는 사물 인터넷 환경에서 개인정보 활용 시 GDPR을 만족하기 위한 개인정보 관리 프레임워크에 관한 연구를 수행하였으나, 법령의 요구조건을 만족하는 구체적인 절차 연구보다는 설계에 의한 프라이버시(Privacy by Design)에 추가적으로 신뢰를 추가하는 전략을 제시하였다.

일반적으로 개인정보 수집시의 동의 절차는 [12]에서 제시된 바와 같이 용이성, 유용성, 투명성 및 선택성 등의 요구조건이 필요하며, 이와 같은 조건들은 GDPR의 법령에 의하여 규정되고 있다. 이에

본 논문에서는 IoT 환경에서의 개인정보수집시에 법령에서 제시하는 동의 요구 조건을 준수하는 메카니즘을 연구하며, 이는 개인정보를 취급하는 IoT 비지니스 분야의 발전에 기여할 것으로 판단된다.

III. IoT 시스템에서의 개인정보 수집 동의 절차 설계

본 논문에서 연구된 IoT 시스템에서의 개인정보 수집 동의 절차의 개인정보흐름 및 처리 과정을 그림 1에 나타내었다.

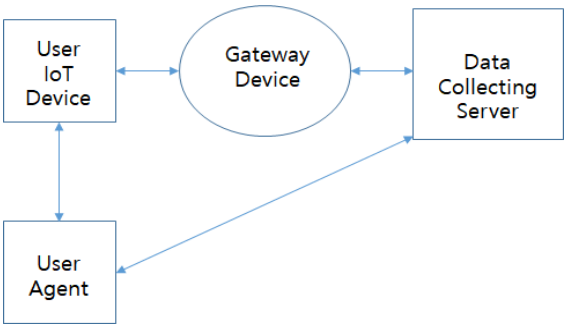

그림 1. IoT 시스템에서의 개인 정보 흐름
Fig. 1. Flow of personal information in IoT system

그림 1에서 개인 정보를 생성하는 사용자 IoT 디바이스와 개인정보를 수집하는 데이터 수집 서버는 게이트웨이 디바이스를 통하여 패킷 통신을 수행한다. 사용자 에이전트는 사용자 IoT 디바이스의 초기 설정 및 설정 갱신 절차를 수행한다.

본 논문에서 IoT 시스템의 개인정보 수집 및 이에 필요한 동의 획득 과정 설계는 초기화 설정 및 개인정보 수집 동의 절차 프로토콜 과정으로 이루어진다.

3.1 사용자 IoT 디바이스 설정

사용자 IoT 디바이스 설정은 사용자 에이전트에 의해서 이루어진다. 사용자 에이전트는 데스크탑 PC나 스마트 기기 등의 입출력 장치가 있는 디바이스를 통하여 이루어진다. IoT 디바이스의 설정에는 사용자 IoT 디바이스에서 사용될 암호화 및 무결성 기법들이 암호모음 형식으로 설정된다. 또한 해당되는 암호키들이 지정되고, 이후 주기적으로 또는 필요시에 갱신된다. 사용자 IoT 디바이스에서 사용되는 암호화 및 무결성 기법으로는 경량화 특성을 가지고 있어 제한된 용량의 시스템에서 많이 사용되는 타원곡선 암호화 기법을 사용할 수 있다.

3.2 사용자 IoT 디바이스 메시지 형식

표 1은 사용자 IoT 디바이스가 생성하는 개인정보(PII, Personally Identifiable Information)메시지 형식을 나타낸다.

표 1. PII 메시지 형식
Table I. PII Message format

Device ID (permanent or temporary)	
Sequence number	
Contact point (anonymous or identifiable) of PII owner	
Time stamp	
Cipher_suite$_0$, PubKey$_0$	
Cipher_suite for PIIs	
PII type 1	PII value encrypted with PubKey$_1$
PII type 2	PII value encrypted with PubKey$_2$
...	...
PII type n	PII value encrypted with PubKey$_n$

* PII : Personally identifiable information
* PubKey$_i$ and PriKey$_i$ are asymmetrically paired public key and private key

표 1의 메시지 형식에서의 각 항목의 설명은 다음과 같다.

- 디바이스 ID : 해당 IoT 디바이스를 구분할 수 있는 ID이다. 디바이스 ID는 영구적으로 사용할 수도 있고, 익명성을 강화시키기 위하여 자주 변경할 수 있는 임시적인 값을 사용할 수도 있다.
- 일련 번호 : 생성된 PII 메시지의 일련번호를 표시한다. 디바이스 ID와 더불어 일련번호는 해당 PII 메시지를 고유하게 구분할 수 있도록 한다.
- PII 소유자의 연락처 : 데이터 수집 서버가 개인정보 수집 동의를 획득하기 위하여 접촉할 수 있는 PII 소유자의 연락처를 나타낸다. 데이터 수집 서버는 IoT 디바이스로부터 PII 메시지를 수신하게 되면 수신된 PII 메시지내에 포함되어 있는 개인정보에 대한 수집 동의를 위하여 PII 소유자와 통신을 해야 하는데, 이 때 사용되는 연락처이다. 이 연락처는 이메일 주소나 각종 SNS 어카운트

도 가능하다. 이러한 연락처는 익명화 또는 비식별화되어 소유자를 구분할 수 없도록 할 수도 있으며, 개인정보 소유자의 성향에 따라 문제가 되지 않는 경우에는 식별 가능한 연락처를 사용해도 된다. 이 연락처를 통하여 데이터 수집 서버는 사용자 에이전트와 개인정보 수집 동의 절차 프로토콜을 진행한다.

- 타임 스탬프 : PII 메시지의 생성시간을 표시한다.
- $Cipher\_suite_0$, $PubKey_0$: 데이터 수집 서버가 개인정보 수집 동의 절차 및 개인정보 수집 획득을 위해 사용자 에이전트에게 보내는 메시지의 암호화에 사용되는 공개키 및 암호화 알고리즘을 표시한다.
- Cipher_suite for PIIs : PII 값을 암호화할 때 사용되는 암호화 알고리즘을 표시한다. 제한된 자원의 IoT 디바이스에 적당한 타원곡선 암호화 기법을 사용한다.
- PII 타입 : PII 메시지에 포함되어 있는 개인정보의 타입을 표시한다. 이름, 주소, 나이, 성별, 개인 연락처 및 각종 IoT 에서 측정되어 지는 생체 의료 정보, 위치 정보, 환경정보, 움직임 정보, 홈 유틸리티 사용 양 또는 패턴 정보 등이 가능하다. 현재의 연구 상태에서는 PII 타입 자체는 평문형태로 전송된다. 추후 보다 개인정보의 보호가 민감한 상태에서는 PII 타입의 비식별화 기능의 추가를 도입할 계획이다.
- $PubKey_i$로 암호화 된 PII 값 : PII 타입에 해당되는 값을 포함한다. 이 값은 공개키 $PubKey_i$로 암호화 되어 있어 이 값의 추출을 위해서는 해당되는 개인키 $PriKey_i$가 필요하다.
- $PubKey_i$와 $PriKey_i$: 타원곡선 암호화 기법에서의 공개키, 개인키 쌍을 나타낸다. PII 타입 i에 대한 공개키, 개인키 쌍인 $PubKey_i$, $PriKey_i$는 일정 기간 PII 타입 i에 대하여 연관되어 사용된다. 즉 데이터 수집 서버가 PII 타입 i에 대한 개인키 $PriKey_i$를 개인정보수집 동의 절차 프로토콜을 거쳐 확보한 경우, 이후 같은 IoT 디바이스에서 발생되는 PII 메시지의 PII 타입 i에 대하여서는 계속해서 복호화 하여 PII 값을 수집할 수 있다. 개인정보 소유자는 PII 타입 i에 대한 공개키, 개인키 쌍인 $PubKey_i$, $PriKey_i$를 일정 기간이 지난 후 또는 필요시에 갱신한다.

3.3 개인정보 수집 동의 절차 설계

그림 2는 본 연구에서 제안하는 IoT 시스템에서의 개인 정보 수집시의 동의를 받기 위한 절차를 나타낸다.

① One or more PII Messages : 사용자 IoT 디바이스는 공개키로 암호화된 PII 값들을 포함하고 있는 표 1의 형식을 갖는 PII 메시지를 생성한다.

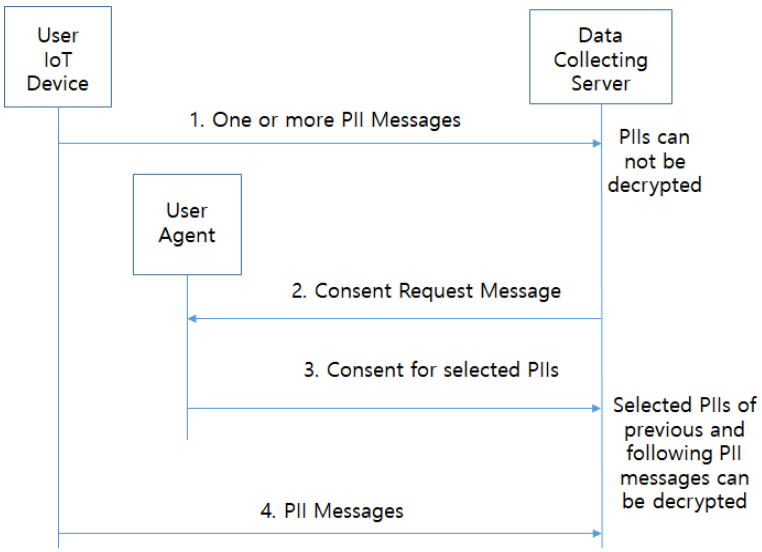

그림 2. IoT 시스템에서의 개인정보 동의 절차

Fig. 2. Consent procedure for personal information collection in IoT system

데이터 수집 서버는 사용자 IoT 디바이스로부터 생성된 한 개 또는 여러 개의 PII 메시지를 수령한다. 데이터 수집 서버는 수신한 PII 메시지에 대하여 데이터베이스의 연관(Association) 테이블을 검색하여 기존의 연관 연부를 체크한다. 연관이 되어 있는 디바이스로부터 온 메시지인 경우 연관 테이블의 해당 공개키들을 이용하여 PII 값들을 복호화함으로서 개인정보를 수집한다.

② Consent Request Message : 데이터 수집 서버는 PII 메시지가 기존에 연관이 되어 있지 않은 경우 PII 메시지안에 있는 소유자의 연락처로 동의 요청 메시지를 전송한다. 동의 요청 메시지는 다음의 항목을 포함하고 있으며, 공개키 $PubKey_0$로 암호화한다.

- ✓ 디바이스 ID, 일련번호, 타임 스탬프 : 사용자 에이전트는 이 항목들을 이용하여 해당 PII 메시지를 식별한다.
- ✓ 데이터 수집 서버의 인증서 : 인증서는 서버의 공개키를 포함하고 있으며, 사용자 에이전트는 이 인증서를 확인함으로서 데이터 수집 서버를 인증할 수 있다. 현재 상태에서는 사용자 에이전트는 서버의 개인키 소지 여부(POP, Proof of Possession of Private Key)를 수행하지 않으나, 추후에 사용자 에이전트와 서버 사이에 개인정보 협상 기능이 추가될 경우에는 POP 기능을 추가할 예정이다.
- ✓ 개인정보처리방침 문서 또는 이를 나타내고 있는 사이트의 링크 : 사용자 에이전트는 문서의 내용에서 또는 링크된 사이트를 통하여 개인정보에 대한 수집 항목 목록 및 이에 대한 처리 방침 등을 포함한 개인정보 수집 동의 약관을 확인하고 이해할 수 있다. 사용자 에이전트는 입출력 장치를 통하여 사용자에게 이를 보여주고, 사용자는 수집 항목 목록 중에서 수집을 허용하는 항목을 골라 체크하고, 필요한 동의 절차를 수행한다.

③ Consent for selected PIIs : 사용자가 수집에 동의한 개인정보 PII 항목에 대한 개인키 $PriKey_i$ 들을 데이터 수집 서버의 인증서에 포함되어 있는 공개키로 암호화하여 보낸다. 인증서의 개인키를 가지고 있지 않는 다른 서버의 경우 암호화된 $PriKey_i$ 들을 복호화 할 수 없으며, 인증서의 주체(Subject)에 해당하는 데이터 수집 서버만이 유효한 복호 절차를 수행할 수 있다. 데이터 수집 서버는 데이터베이스의 연관테이블에 새로운 연관을 만들고, 복호화한 개인키들을 연관테이블에 기록한다. 데이터 수집 서버는 이 키들을 이용하여 기존에 받은 PII 메시지 및 이어 도착하는 PII 메시지들의 선택된 PII type에 대하여 복호화를 수행하고, 개인정보 수집 및 처리를 할 수 있게 된다.

④ PII messages : 사용자 IoT 디바이스가 계속해서 생성하는 PII 메시지는 데이터 수집서버로 전달되어 처리된다.

Ⅳ. 개인정보 수집 동의 절차 분석

본 연구에서 제안하고 있는 IoT에서의 개인정보 수집 동의 절차는 개인정보보호법이나 유럽의 GDPR에서 규정하고 있는 개인정보수집 동의 절차를 만족한다. 데이터 수집 서버는 사용자 IoT 디바이스로부터 먼저 PII 메시지를 수령하나, 기존에 동의를 받지 않은 경우에는 암호화된 PII 값의 내용을 알 수가 없으므로 개인정보 수집이 안된 상태이다. 이는 암호화된 PII는 암호키가 없이는 현재의 암호해독 기술로는 알 수가 없으므로 암호화된 메시지를 가지고 있다고 해서 수집이 되었다고 볼 수가 없으므로 동의 절차가 없는 상태에서의 수집 제한의 법령 규정을 만족하게 된다.

이후 연관을 맺기 위해 사용자 에이전트에게 개인정보수집 및 처리 방침을 액세스할 수 있도록 함으로서 사용자는 개인정보 수집 및 처리 절차에 대하여 용이하게 숙지 할 수 있고 이해할 수 있도록 함으로서 개인정보보호법이나 GDPR에서 요구하는 투명성(Transparency) 조건을 만족할 수 있다. 또한 개인정보 수집 목록 중에서 사용자는 허용하고자 하는 개인정보 항목을 선택하여 데이터 수집 서버로 하여금 수집할 수 있도록 하며, 반면 선택되지 않은 개인정보 항목은 복호할 수 없도록 함으로서 개인정보 항목에 대한 자유로운 선택의 요건을 만족한다. 즉 IoT 디바이스로부터의 개인정보를 담은 PII 메시지들은 데이터 수집서버에 전달은 되나, 사

용자는 개인정보 항목에 대한 개인키를 제공하거나 또는 제공하지 않음으로서, 사용자가 동의하는 개인정보 항목에 대하여서만 수집을 허용한다.

본 연구에서 제안한 절차는 현대 암호학을 기반으로한 메시지 교환 절차로 이루어지므로, 본 제안의 유효성과 신뢰성은 현대 암호학의 안전성 및 신뢰성과 맥을 같이 한다. 그러므로 현대 암호학이 유효한 상태에서는 본 연구에서 제안하고 있는 IoT에서의 개인정보 수집 동의 절차는 법령에서 규정하고 있는 요건을 만족하는 동시에 동의 절차의 유효성과 신뢰성을 보장할 수 있게 된다.

V. 결 론

본 논문에서는 최근 이슈가 되고 있는 IoT시스템에서 개인정보보호법이나 유럽의 GDPR과 같은 개인정보보호법령에서의 규정을 만족하는 개인정보 수집시의 사용자 동의 절차를 설계하였다. 설계된 방식에서는 먼저 사용자 에이전트가 사용자 IoT 디바이스에 대한 초기화를 통하여 적용될 암호화 기법 및 암호키등을 설정하며, 이후 IoT 디바이스는 설정된 암호키를 이용하여 암호화된 개인정보를 생성 전송한다. 암호화된 개인정보를 수신한 데이터 수집 서버는 사용자 에이전트를 통하여 사용자에게 개인정보수집 및 처리방침에 대한 열람을 하도록 하고, 이어 원하는 개인정보 항목에 대하여서만 동의 절차를 진행하도록 한다. 동의 절차가 진행된 개인정보 항목에 대한 개인키를 수령한 데이터 수집 서버는 사용자 IoT 디바이스로부터의 암호화된 개인정보를 복호화하여 수집을 하게 된다.

위와 같이 본 논문에서 연구된 IoT시스템에서의 개인정보수집에 관한 동의 절차는 본 저자들의 지식의 범위 안에서는 법령을 충분히 잘 만족하는 최초로 제안으로 생각된다. 즉 이렇게 제안된 절차는 법령에서 규정하고 있는 투명성이나 자유로운 선택 요건 등을 충분히 만족하므로, 입출력장치의 제한이 있는 IoT 디바이스를 활용한 IoT 시스템이 기존의 응용 분야를 넘어서서 많은 개인정보를 수집하고 취급하는 고부가가치의 비즈니스 분야로 영역을 넓히는데 크게 기여할 것으로 기대된다.

References

[1] www.law.go.kr/lsInfoP.do?lsiSeq=195062&efYd=20171019#0000 : [accessed: Sep. 30, 2018]

[2] "Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)", European Commission, Jan. 2017.

[3] "Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", Official Journal of the European Union., May 2016.

[4] www.gdpr-info.eu : [accessed: Sep. 30, 2018]

[5] Cigdem Sengul, "Privacy, consent and authorization in IoT", 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), pp. 319-321, Mar. 2017.

[6] Arijit Ukil, Soma Bandyopadhyay, Joel Joseph, Vijayanand Banahatti, and Sachin Lodha, "Negotiation-based privacy preservation scheme in internet of things platform", SecurIT'12 Proceedings of the First International Conference on Security of Internet of Things, Kollam, India, pp. 75-84, Aug. 2012.

[7] Ricardo Neisse, Gianmarco Baldini, Gary Steri, Yutaka Miyake, Shinsaku Kiyomoto, and Abdur Rahim Biswas, "An agent-based framework for Informed Consent in the internet of things", IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, pp. 789-794, Dec. 2015.

[8] Ricardo Neisse, Gianmarco Baldini, Gary Steri, and Vincent Mahieu, "Informed consent in Internet of Things: The case study of cooperative intelligent transport systems", 23rd International Conference on Telecommunications (ICT), Thessaloniki, Greece, pp. 1-5, May 2016.

[9] Shi-Cho Cha, Ming-Shiung Chuang, Kuo-Hui Yeh, Zi-Jia Huang, and Chunhua Su, "A User-Friendly Privacy Framework for Users to Achieve Consents With Nearby BLE Devices", IEEE Access, Vol. 6, pp. 20779-20787, Mar. 2018.

[10] Claude Castelluccia, Mathieu Cunche, Daniel Le Metayer, and Victor Morel, "Enhancing Transparency and Consent in the IoT", IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, United Kingdom, pp. 116-119, Apr. 2018.

[11] Sooji Jeon, Jinhong Yang, Sungkwan Jung, and Chulsoo Kim, "A Study on the GDPR Compliant Personally Identifiable Information Management Technology for IoT Environment", 2018 Summer Conference of the Korean Institute of Communications and Information Sciences, pp. 1152-1153, Jun. 2018.

[12] Sun-Young Lee, "Analysis of User's Recognition for Personal Information Agreement and New Policy", Journal of KIIT, Vol. 12, No. 8, pp. 85-92, Aug. 2014.

저자소개

이 구 연 (Goo Yeon Lee)

1986년 : 서울대학교 전자공학과 (학사)
1988년 : KAIST 전기 및 전자 공학과(석사)
1993년 : KAIST 전기 및 전자 공학과(박사)
1993년 ~ 1996년 : 디지콤 정보통신 연구소
1996년 : 삼성전자
2004년 7월 ~ 2005년 2월, 2010년 1월 ~ 2011년 1월 : 미국 Cornell 대학교 Visiting Professor
2012년 8월 ~ 2014년 2월 : 강원대학교 IT 대학 부학장
1997년 ~ 현재 : 강원대학교 컴퓨터학부 교수
관심분야 : 데이터통신, 컴퓨터네트워크, 네트워크 보안, 차세대 인터넷, 이동통신, 네트워크 성능분석, 암호학, 정보보호관리체계

방 준 일 (Junil Bang)

2018년 8월 : 강원대학교 컴퓨터정보통신공학과 (공학사)
2018년 9월 ~ 현재 : 강원대학교 컴퓨터정보통신공학과 (석사과정)
관심분야 : 데이터분석, 머신러닝, 딥러닝, 네트워크 보안

차 경 진 (Kyung Jin Cha)

2011년 3월 : 호주 국립대학교(경영학박사)
2011년 3월 ~ 2014년 12월 : 계명대학교 경영정보학과 조교수
2015년 1월 ~ 현재 : 강원대학교 경영회계학부 부교수
관심분야 : 데이터분석, 정보보호, 스마트워크 등

김 화 종 (Hwa Jong Kim)

1982년 : 서울대학교 전자공학과 (공학사)
1984년 : KAIST 전기 및 전자과 (공학석사)
1988년 8월 : KAIST 전기 및 전자과(공학박사)
1988년 ~ 현재 : 강원대학교 컴퓨터정보통신공학과 교수
관심분야 : 데이터공유, 데이터분석, 인공지능, 머신러닝, 딥러