개인정보보호법을 준용하는 사물인터넷 플랫폼의 데이터 처리에 관한 연구

김효준, 송재승*, 박철수*
광운대학교, 세종대학교 정보보호학과 교수, 광운대학교 컴퓨터 정보공학부 교수
hyojun.kim@eglobalmark.com, jssong@sejong.ac.kr, parkcheolsoo@kw.ac.kr

A Study on privacy data processing in an IoT platform to comply with GDPR

Kim Hyo Jun, *Song Jae Seung, *Park Cheol Soo
KwangWoon Univ., Sejong Univ., KwangWoon Univ.

요 약

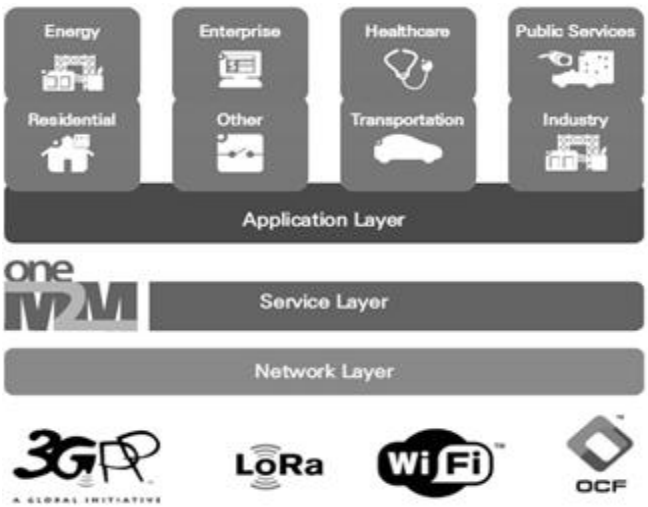
정보화 시대에 접어들면서 개인정보보호의 중요성이 강조되고 각국에서는 시민의 정보를 보호하기 위한 법령들이 시행되고 있다. 그중에서 유럽연합 (European Unio: EU)의 개인정보보호법인 일반데이터보호규정 (General Data Protection Regulation - GDPR)이 시행되면서 전 세계의 주목을 받고 있다. GDPR은 EU 시민의 개인정보를 취급하는 모든 기업 및 데이터 플랫폼에 적용된다. 이에 본 논문에서는 수많은 데이터를 자동으로 수집하는 사물인터넷 (IoT)의 특성을 고려하여 국제 사물인터넷 표준인 oneM2M 기반의 IoT 서비스 계층 플랫폼에서 GDPR 준용하며 개인정보 관련 데이터를 처리하기 위한 표준화 작업에 대하여 소개한다.

Ⅰ. 서론

유럽의 일반데이터보호규정 (General Data Protection Regulation - GDPR)에 의하면 개인정보란 식별된 또는 식별 가능한 자연인과 관련한 일체의 정보로서 개인을 나타내는 다양한 정보로 정의된다. GDPR은 이름, 주민등록번호, 사진뿐만 아니라 정보 사회의 도래로 새롭게 등장한 위치정보(GPS), 온라인 식별자 (IP, cookie), 유전정보, 몸무게, 키, 경제 수준, 신용, 종교, 문화, 사상도 개인정보로 취급한다. 각각의 정보는 개인을 식별할 수 없지만 두 개 이상의 정보가 결합하는 경우 개인을 식별할 수 있으므로 모든 정보가 안전하게 보호되어야 한다.

최근 사물인터넷(IoT)에 관한 연구가 세계 각국의 정부, 기업 등을 주축으로 활발히 진행되고 있다. IoT는 홈, 헬스케어, 스마트 팩토리, 자율 주행 등 산업 전반에 걸쳐 서비스되고 있고 일반적으로 나라, 제조업체별로 서로 다른 서비스 플랫폼을 사용하다 보니 사물인터넷 프레임워크 내에서 이질성과 파편화가 생겼다. 이러한 문제를 해결하기 위하여 oneM2M은 각국 표준화 기관들이 모여 글로벌 사물인터넷 서비스 플랫폼 표준을 개발하기 위해 2012년에 결성한 표준 협의체이다. 한국의 TTA를 비롯하여 미국의 TIA 및 ATIS, 유럽의 ETSI, 일본의 TTC 및 ARIB, 중국의 CCSA 그리고 인도의 TSDSI까지 총 8개의 지역 표준 개발 단체가 해당 국가별로 따로 표준을 개발하던 것을 멈추고, 전 세계적으로 하나의 사물인터넷 서비스 플랫폼 표준을 공동으로 개발하는 것을 목적으로 결성되었다. [그림 1]에서 보는 것처럼, oneM2M에서는 다양한 사물인터넷 응용 서비스를 지원할 수 있는 공통 플랫폼(Common Service Platform)을 정의하고 이에 대한 표준을 개발하는 것이 주된 목표다.[1]

2020년 IoT 디바이스에 연결된 센서의 수는 260억 개가 넘고, 그로 인해 생성된 데이터의 양이 기하급수적으로 늘어나고 있다. IoT 디바이스에서 생성된 정보는 IoT 플랫폼을 장착한 게이트웨이 및 서버로의 전송, 처리, 저장, 분석된다. 센서를 통해서 수집된 정보는 개인정보 또는 민감 정보를 포함할 수 있고, 직접적으로 개인정보를 포함하지 않더라도 이러한 단순 정보들이 모여 개인을 식별할 수 있으므로 GDPR에 적용을 받게 된다. 따라서, IoT 디바이스에서 측정되는 각종 데이터를 수집하고 관리하는 IoT 서비스 공통 플랫폼은 법령의 준수를 위한 개인정보 처리 메커니즘을 기본적으로 갖추어 제공하는 것이 필요한 상황이다.



[그림 1] oneM2M의 아키텍처

이에 따라, IoT 서비스 계층 플랫폼에 대한 사실상 국제 표준 단체인 oneM2M은 GDPR을 준용하고, 개인정보를 다루는 서비스에게 GDPR 등과 같은 법령에서 요구하고 있는 기능들을 제공하기 위한 신규 워크 아이템 (WI-0095, oneM2M System Enhancements to Support Data Protection Regulation - eDPR)을 승인하였고, 이를 기반으로 한 기술보고서 (TR-0062) 개발이 시작되었다.[2] 해당 워크 아이템에서는 여러 국가에서 시행 중인 개인정보보호를 위한 법령 및 관련 기술들을 살펴보고, IoT 서비스에서 GDPR을 준용하는 데 필요한 요구사항들을 도출하며, 이를 플랫폼에서 지원하기 위한 핵심 이슈 및 공통기능에 대한 표준 개발을 진행 중이다. 본 논문에서는 TR-0062에 대한 분석 내용에 대해 설명한다.

Ⅱ. 본론

GDPR은 개인정보의 처리에 대한 개인의 보호 및 개인정보의 자유로운 이동에 관한 규정이다. GDPR은 유럽연합에 거주하는 시민을 보호하기 위해

유럽연합 역내에서 사업을 하는 모든 조직 및 기관뿐만 아니라 유럽연합의 시민에 대한 정보를 수집, 처리, 저장하는 유럽연합 역외의 조직에도 적용되기 때문에 전 세계적으로 많은 기업이 GDPR에 주목하고 대응하기 위한 내부 데이터 보호에 힘을 쏟고 있다.

GDPR은 개인정보의 범주를 재확립하고 개인정보 처리자에게 비식별 조치 (Pseudonymization & anonymization)와 암호화 (Encrytion) 등을 사용하여 정보를 보호할 것을 권유한다. 또한, GDPR은 기업마다 개인정보처리자 (Controller) 와 수탁처리자 (Processor) 를 두어 최신 기술을 이용하여 보안 수준을 높일 것을 요구한다. 이외에도 GDPR은 개인정보 삭제권, 처리 제한권, 개인정보 이동권, 반대권 등의 신규 권리추가 및 기존 권리 명확화를 통하여 GDPR 이전의 개인정보보호 지침 보다 정보 주체의 권리를 확대 · 강화하였으며, 개인정보처리 활동의 기록, 개인정보처리 원칙, 개인정보 영향평가, Data protection by design and by default 등의 내용을 통하여 기업의 책임성을 강화하였다.[3]

GDPR은 전문 총 173개항, 본문 총 11장 9₤개 조항으로 이루어져 있다. 99개의 조항 중 oneM2M 플랫폼의 구조와 특징을 고려하였을 때 시스템에 영향을 줄 수 있는 조항의 경우 분석을 통해 IoT 플랫폼에서 공통적으로 제공이 필요한 기능들에 대한 요구사항이 도출되어야 한다.[4] 예를 들어, GDPR에서는 다음과 같은 조항을 포함하고 있다.

- 잊혀질 권리 (Right to be forgoten): GDPR의 17 및 19번 조항에 따르면 정보 주체는 프로세서에게 개인정보에 대한 삭제를 요청할 수 있고, 해당 데이터는 지체없이 삭제되어야 한다고 규정하고 있다.
- 비식별조치 : 제4조 5항에서 가명처리, 즉 추가적인 정보의 사용 없이 개인을 특정할 수 없도록 개인정보를 처리하도록 정의하고 있다.

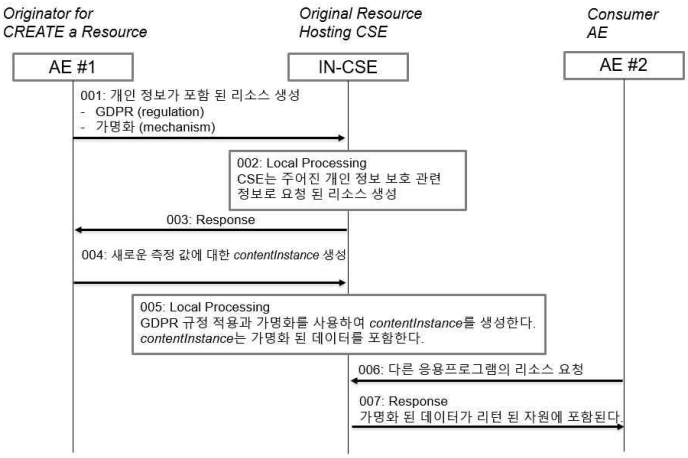
이러한 조항들은 시스템적으로 지원하기 위해서는 사용자 또는 사물인터넷 기기로부터 수신되는 데이터가 개인정보 관련 데이터인지에 대한 식별이 이루어져야 하며, 개인정보의 경우 시스템에서 데이터의 소유자로부터 처리에 대한 동의가 명시적으로 이루어질 수 있도록 하는 기능이 플랫폼의 한 기능으로 제공이 되어야만 한다.] 또 개인정보처리 전반에 걸쳐 개인정보 규정 및 데이터 처리기술에 대한 정보가 제공되어야 한다. 이를 위해 oneM2M 표준에서는 개인정보에 대한 식별 정보를 비롯하여 여러 추가 정보 (법령 종류, 가명화 방법 등)와 이를 처리 및 저장하기 위한 리소스 추가 및 관리가 필요하다.

[표 1]은 oneM2M에서 GDPR 준용 데이터 처리를 위해 필요로 되는 attributes와 내용을 보여준다. 해당 속성들은 GDPR 적용을 위해서 기본적으로 필요한 정보들을 리소스의 속성으로 만들 경우 추가할 수 있는 예를 보여주고 있다.

[표 1] oneM2M에서 GDPR 처리를 위해 추가 가능한 속성 예제

Attribute Name	Description
privacyRegulation	데이터에 적용될 규정 (GDPR, PIPA, etc..)
privacyIndication	개인정보보호 규정 적용 여부
privacyProcessing Rule	데이터에 적용될 기술 (가명화, 익명화 등)
privacyTechniques	가명화 및 익명화의 세부 기술 정보
privacyBlock	데이터 내 개인정보 위치 식별
privacySubject	개인정보보호 규정의 적용을 받는 리소스

[그림 2]은 oneM2M에 GDPR 관련 속성들이 추가되었을 경우 어떠한 절차를 거쳐서 사물인터넷 센서에서 측정된 개인정보 관련 데이터가 oneM2M 플랫폼에서 어떻게 처리 · 저장되는지와 저장된 데이터에 대해서 다른 응용 프로그램의 요청이 오면 어떻게 처리되는지 보여주고 있다.



[그림 2] 가명화 및 익명화 처리 절차

최초 사물인터넷 어플리케이션인 AE가 개인정보를 포함하는 데이터를 저장하기 위해 관련 리소스를 사물인터넷 플랫폼의 공통기능 제공 엔티티인 CSE에 생성하며 필요한 정보들을 리소스의 속성에 추가한다 (스텝 001~003). 이후 생성되는 개인정보들은 contentInstance라는 리소스에 저장이 되는데 이때 저장되는 리소스의 개인정보 유무를 확인하고, 익명화나 가명화 처리가 필요할 경우 속성에 명시된 방법에 따라서 데이터를 처리하게 된다 (스텝 004~005). 제3의 어플리케이션에서 (AE#2) 개인정보에 대한 검색 요청이 올 경우, CSE는 가명화 또는 익명화 처리된 데이터를 AE#2에 전달하게 된다 (스텝 006~007). 즉, 개인정보를 관리하는 리소스에 액세스할 수 있는 다른 IoT 응용 프로그램은 가명화 또는 익명화된 데이터만 볼 수 있다.

Ⅲ. 결론

4차산업혁명 시대를 맞이해서 다양한 산업들이 데이터 중심으로 이동함에 따라 사물인터넷 플랫폼에서 데이터의 중요성이 강조되고 있다. 유럽 외에도 한국, 미국, 일본 등 전 세계에서 개인정보보호에 대한 인식이 강화되고 관련 법령이 발의됨에 따라 사물인터넷 표준에서도 각 나라의 다양한 법령을 준수할 수 있는 기능 지원의 확장이 필요하다.

사물인터넷 플랫폼 관련 표준을 개발하는 국제 표준 단체인 oneM2M에서는 한국 업체들의 주도하에 한국의 개인정보보호법(PIPA)을 시스템적으로 지원할 수 있는 기능에 대한 표준을 개발하기 위해 워크 아이템을 Release 5의 일환으로 제안하고 승인시킴으로써 국제 표준에서 개인정보보호 처리를 위한 기능 표준화를 선도하고 있다. 개인정보법령을 지원하는 표준이 완성될 경우 oneM2M 표준은 데이터 처리의 보안성을 인정받아 스마트시티를 비롯하여 의료 등 보다 다양한 분야로 확산될 수 있을 것으로 기대된다.

ACKNOWLEDGMENT

본 연구는 광운대학교 소프트웨어 융합대학의 지원을 받아 수행된 연구임.
교신저자: 세종대학교 송재승 교수, 광운대학교 박철수 교수

참 고 문 헌

[1] oneM2M, https://www.onem2m.org/
[2] oneM2M Technical Report, TR-0062 https://member.onem2m.org/static_Pages/others/WPM-pages/TR-TS_List.htm
[3] GDPR, https://gdpr-info.eu/
[4] Swetina, J., Lu, G., Jacobs, P., Ennesser, F., & Song, J. (2014). Toward a standardized common M2M service layer platform: Introduction to oneM2M. IEEE Wireless Communications, 21(3), 20-26.