연구논문 정보화정책 제23권 제1호, 2016년 봄호, pp.56~73

사물인터넷 신뢰 연구와 시사점: EU FP7을 중심으로

윤 영 석*, 조 성 균**, 이 현 우***

요 약 IoT (Internet of Things)는 기기, 사람, 이들의 데이터를 연결하여 새로운 비즈니스 기회를 제공할 것으로 예상된다. 그러나 신뢰가 결여된다면 IoT (Internet of Things)가 제안하는 가치는 달성될 수 없다. IoT는 끊임없는 연결을 추구한다는 측면에서 사람, 사물과 같은 연결 대상에 대한 신뢰가 전제되어야 한다. 그러나 현재까지 진행된 IoT 연구의 대부분은 플랫폼과 어플리케이션 개발에 집중되어 있어 신뢰할 수 있는 연결과 상호작용에 대한 논의는 상대적으로 부족하다. uTRUSTit, ABC4Trust, Inter-Trust, COMPOSE, SMARTIE와 같은 유럽의 FP7 ICT 연구 프로그램은 이러한 간극을 해소하고자 하는 연구들이다.

본고에서는 이들 프로젝트의 목적과 연구 방향을 소개하고 논의하였다. 각각의 연구가 취하고 있는 접근은 조금씩 상이하지만 이들 연구의 공통점은 신뢰할 수 있는 연결을 통해 프라이버시와 안전을 모두 담보하고자 하는 것이다. IoT의 기대를 충족시키기 위해서는 국내에서도 연결된 사물들에 대한 신뢰 연구가 필요한 시점임은 분명하다.

주제어: 신뢰, 사물인터넷, 유럽, FP7

Researches on Trust in IoT and Implications: Focusing on EU Framework Programme 7 (FP7)

Yoon Young Seog, Seng-Kyoun Jo, Hyun-Woo Lee

Abstract The Internet of Things (IoT) is expected to provide new business opportunities by connecting devices, persons, and their data. However, the value proposed by IoT cannot be realized without trust. As IoT premises on the seamless connections, it should guarantee trust among the connected persons and things. However, there is lack of relevant discussion on how to achieve trustworthy connections and interactions because most of academic studies have mainly focused on the development of IoT platforms and applications. To fill the gaps, recent EU-funded projects such as uTRUSTit, ABC4Trust, Inter-Trust, COMPOSE, and SMARTIE have been conducted under the FP7-ICT Framework Programme.

This paper presents and discusses each project's purpose and approach. Although their approaches are somewhat different from each other, all of them dedicate to achieving both privacy and security by providing the trustworthy connections. It seems to be clear that Korea also needs more academic and practical contribution in terms of researches, to implement "trust" among connected things, which will eventually satisfy what really IoT is expected for.

Keywords: Trust, IoT, EU, FP7

2016년 1월 29일 접수, 2016년 1월 29일 심사, 2016년 3월 2일 게재확정

* 한국전자통신연구원 초연결통신연구소 연구원
** 한국전자통신연구원 초연결통신연구소 선임연구원
*** 한국전자통신연구원 초연결통신연구소 책임연구원

Ⅰ. 서 론

Internet of Things(IoT)란 지능화된 사물들(Things)이 연결되어 형성되는 네트워크에서 사람과 사물, 사물과 사물 간에 상호 소통하고 상황인식 기반의 지식이 결합되어 지능적인 서비스를 제공 하는 인프라로 정의된다(표철식 외, 2013: 3). 따라서 IoT 기술은 사물들 간의 연결을 전제로 한다는 측면에서 연결되는 대상이 신뢰할 수 있어야 한다.

학술적 관점에서 신뢰는 다양한 개념으로 이해되고 있지만, "특정 관계가 있는 한 당사자(Trustor)가 다른 당사자(Trustee)에 대해 그(Trustor)에게 중요한 특별한 행동을 할 것이라는 기대에 근거하여 다른 당사자(Trustee)의 행동이 야기할 위험을 감수할 의사(Willingness to Take Risk)"라는 정의(Mayer, et al., 1995: 712)가 가장 넓게 받아들여지고 있다. 비대면 환경이라는 특징을 가진 전자 상거래에서 신뢰는 거래 의향, 브랜드 충성도, 재구매 의향, 구전 의향 등의 소비자 인지와 행위를 설명하는 핵심 변인으로 이해되어 왔다(Chaudhuri, et al., 2011: 81~93; Corbitt. et al., 2003: 203~215; Sirdeshmukh, et al., 2002: 15~37; Hong, et al., 2011: 469~467; Ranaweera, et al., 2003: 82~90).

이러한 신뢰의 개념은 IoT의 맥락에서도 중요한 의미를 가진다. 왜냐하면 IoT 환경은 다양한 기기, 응용서비스의 연결과 이들 사이에 발생하는 상호작용을 전제하고 있어 사용자들이 위험(Risk)과 불확실성(Uncertainty)을 경험할 가능성을 내제하고 있기 때문이다. 따라서 이러한 위험과 불확실성을 감수하고 사용자들이 연결을 허용하고 일련의 행위를 수행하기 위해서는 신뢰가 담보되어야 한다. 그러나 어떻게 신뢰를 정의하고 측정하고 분석하고 활용할지에 대한 논의는 이제 막 시작되는 단계이다(김호원, 2014: 38).

IoT 환경에서 신뢰의 필요성이 대두됨에 따라 유럽 FP7의 uTRUSTit, ABC4Trust, Inter-Trust, COMPOSE, SMARTI와 같은 프로젝트들이 최근 종료되었거나 진행 중에 있다(uTRUSTit, 2012b; ABC4Trust, 2015b; Inter-Trust, 2015; COMPOSE, 2015; SMARTIE, 2015b). 각 프로젝트의 연구 기간 및 예산을 정리하면 〈표 1〉과 같다. 유럽 FP7프로그램 (7th Framework Programme for Research and Technological development)은 2007년부터 2013년까지 총 533억 유로가 투입된 범 유럽차원의 R&D 공동 연구개발 프로그램으로 유럽의 과학기술 기반 강화와 기술 경쟁력 확보를 목적으로 한다. 7차 프로그램 종료 후 지금은 FP8(2014~2020)이 진행 중에 있다. 본 고는 이들 프로젝트의 목표와 연구 내용 및 접근 방향을 살펴보고 의미 있는 시사점을 제공하고자 한다.

Ⅱ. uTRUSTit

1. 연구 배경과 목적

〈표 1〉 신뢰 관련 주요 FP7 연구 프로그램

프로젝트 명	연구 기간	연구 예산 (유로)
uTRUSTit (Usable TRUST in the Internet of Things)	2010. 9.~2013. 9.	3,289,859
ABC4Trust (Attribute-based Credentials for Trust)	2010.11.~2015. 2.	13,063,511
Inter-Trust (Interoperable Trust Assurance Infrastructure)	2012.11.~2015. 4.	5,241,746
COMPOSE (Collaborative Open Market to Place Objects at your SErvice)	2012.11.~2015.10.	7,406,084
SMARTIE (Secure and sMArter ciTIEs Data Management)	2013. 9.~2016. 8.	4,862,363

출처: uTRUSTit, 2012b; ABC4Trust, 2015b; Inter-Trust, 2015; COMPOSE, 2015; SMARTIE, 2015b.

일반적으로 어플리케이션의 정보의 보안(Security) 속성은 숨겨져 있어 사용자들이 이해하기 어렵다(Dumortier, et al., 2012: 568~569). 다시 말해 사용자들은 어떤 어플리케이션 또는 사물이 인터넷에 연결되는지, 어떻게 이들이 연결되는지, 어떠한 정보가 전달되는지, 누가 이 정보를 전달받는지에 대해 정확히 할 수 없다. 따라서 응용 서비스들이 점차 유비쿼터스화 되고 일상생활에 스며들게 되는 IoTs 환경에서 사용자들의 보안과 신뢰에 대한 정보 습득 과정은 보다 복잡해지고 어려워질 수밖에 없다(Dumortier, et al., 2012: 568~569).

이러한 문제 해소를 위해 uTRUSTit(Usable TRUST in the Internet of Things) 프로젝트는 사용자가 쉽게 이해할 수 있는 IoT 단말과 서비스에 대한 신뢰 정보를 제공하는 소프트웨어 개발을 목적으로 한다. 구체적으로는 인증 및 인가 방식, 연결 네트워크의 형태, 개인정보 보호 정책, 저장 기간, 정보 취득 기관 등 보안(Security), 개인 정보(Personal Information)에 관계된 정보를 시각화하여 사용자가 연결 대상에 대한 신뢰 정보를 보다 쉽게 파악하도록 하는 것이 목적이다. 이 프로젝트에는 유럽 6개국에서 6개 산·학·연이 공동 참여하였다.

2. 주요 연구 내용 및 결과물

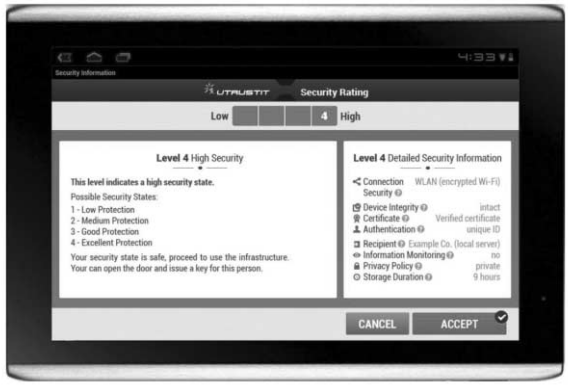
uTRUSTit는 TFT(Trust Feedback Tool)라는 유저 인터페이스를 제공한다. TFT는 사용자와 연결된 IoT 단말에 대한 신뢰 정보를 표현하는 어플리케이션이다. TFT는 단말에서 수집되는 데이터를 바탕으로 단말과 관련된 신뢰 정보를 시각화하여 제공한다. 수집되는 정보는 개인 정보의 이용 범위, 정보 저장 기간, 연결 방식 등이며 이를 토대로 사용자들은 4가지 단계의 보안 등급을 설정할 수 있다(〈그림 1〉 참조). 4단계로 구분한 이유는 중립을 의도적으로 배제하여 사용자의 판단을 보다 존중하기 위해서이다(uTRUSTit, 2012: 27).

만일 사용자들이 TFT를 4단계로 설정하면 사용자 정보 보호 수준을 최대로 높이는 것이고, IoT 기기는 각 단계에서 정의하고 있는 수준 이상의 개인 정보를 응용 서비스가 요청하면 서비스 연결을 거부한다. 〈그림 2〉는 TFT 등급을 4단계로 설정한 경우에 사용자에게 전달되는 화면을 나타내며, 사용자들은 이러한 정보를 확인하고 네트워크 주소, 전화번호, 위치, 이름 등의 개인 정보를 감출 수 있다.

uTRUSTit는 스마트홈, 스마트 오피스, 전자투표 서비스 시나리오를 제안하였으며(uTRUSTit, 2011:

출처: uTRUSTit, 2012a: 27

〈그림 1〉 TFT의 보안 등급 시각화



출처: uTRUSTit, 2013: 29~30

〈그림 2〉 TFT의 구동 방식 예

6~29), 각각의 시나리오는 파생된 하부 시나리오를 가진다. 일례로 스마트 홈 서비스 시나리오는 출입 관리 및 통제, 분실키 등록 철회 및 신규 키 발급, 약품 관리 및 위기 상황 대처, 위치 기반 응급 상황 조기 대처라는 4개 하부 시나리오를 포함하고 있다(uTRUSTit, 2011: 6~29).

3. 연구 의미와 시사점

이 연구는 IoT에서 신뢰를 주제로 하는 최초의 프로젝트라는 측면에서 새로운 연구 영역을 개척하였다는 중요한 의미를 가진다. 그러나 이 프로젝트는 몇 가지 한계점을 가진다. 첫째, IoT는 사람과 사물의 다양한 관계를 상정하고 있으나, 이 연구는 사물의 신뢰만을 다루고 있다. 즉, 사람에 대한 신뢰와 사람간의 관계는 반영하고 있지 않다. 둘째, 이 연구는 연결되는 대상이 요청하는 정보의 수동적 시각화에 국한되어 있다. 다시 말해 보안과 신뢰에 대한 제한된 정보의 시각화에 집중하고 있어 연결 대상이 내포하고 있는 다양한 위험 요소와 동적 변화를 반영하고 있지 않다. 그러나 네트워크 연결 방식, 인증 방식, 개인 정보 모니터링, 개인 정보 보호 정책을 일반 사용자들이 쉽게 이해할 수 시각화하여 이용자의 프라이버시 보호 권한을 강화한 시도는 후에 등장한 다양한 프로젝트의 태동과 연구 방향에 영향을 미쳤다.

Ⅲ. ABC4Trust

1. 연구 배경과 목적

지금까지 사용자 인증을 위한 개인 정보는 개인의 프라이버시를 고려하지 않고 설계되어 왔다. 기술적 측면에서 개인 정보 보호 방식은 크게 패스워드 방식과 암호화 방식으로 구분할 수 있다. 그런데, 패스워드 방식은 사용자 인증을 통해 서비스 제공자에게 필요 이상의 정보가 전달되기 때문에 개인의 프라이버시를 보호하기에 적합하지 않다(ABC4Trust, 2011: 10~12). 예를 들어, 패스워드 방식의 인증 방식을 적용하고 있는 보험사는 카드사와의 정보 연동을 통해 특정인의 초콜릿 구매가 빈번하다는 점을 파악할 수 있다. 이러한 경우 보험 계약자의 비만 가능성이 높

아짐을 유추한 보험사는 가입자의 보험료를 인상시킬 수 있으며, 이는 사용자의 원치 않은 개인 정보의 유출에서 비롯된 것이다(ABC4Trust, 2015b).

ABC4Trust(Attribute-based Credentials for Trust)는 어플리케이션 구동을 위해 필수적인 최소 정보만을 전달하여 개인 정보 보호를 담보하는 동시에 신뢰할 수 있는 안전을 담보하고자 하는 것이 목적이다. 개인 정보 보호와 안전을 동시에 충족시키기 위해 ABC4Trust는 속성 기반 자격에 대한 레퍼런스 아키텍처인 Privacy-ABCs를 제안하고 구현하였다. ABC4Trust는 총 7개국 12개의 산·학·연이 참여하여 진행하였으며 Nokia, IBM, Microsoft 등의 국제적 기업도 참여하였다.

2. 주요 연구 내용 및 결과물

ABC4Trust의 결과물인 Privacy ABCs(Privacy-preserving Attributed-based Credentials)의 특징을 정리하면 〈표 2〉와 같다.

가장 중요한 특징은 사용자들이 개인 속성의 일부만을 선택하여 서비스 제공자에게 전달할 수 있다는 것이며, 분리되어 전달된 일부의 개인 속성 정보는 결합될 수 없다. 이는 privacy-ABCs가 하나의 보안키와 복수의 공개키 방식을 채택하였기 때문에 가능한 것이다. 이 공개키는 익명(Pseudonyms)으로 지칭된다 (ABC4Trust, 2015a: 18).

폭넓게 적용되고 있는 기존의 암호키 방식은 사용자들이 하나의 쌍으로 구성된 보안/공개키를 생성하여 인증하는 방식인 반면, Privacy-ABCs는 하나의 보안키와 복수의 공개키 방식을 사용한다. 쌍으로 구성된 보안/공개키 생성 방식에서의 자격 증명은 공개키의 서명과 속성으로 자격 증명이 이루어지므로 사용자 인증(Certificate)을 토대로 사업자는 이 사용자에 대한 신원 식별을 통해 다양한 정보 취득이 가능하다.

그러나 Privacy-ABCs에서의 자격 증명은 사용자의 비밀키와 속성으로 이루어지기 때문에 사용자가 선택한 일부 속성 정보만이 서비스 제공자에게 전달되어 서비스 사업자는 사용자가 접근을 허락한 제한된 정보에만 접근 가능하다.

익명은 링크가 불가능하다. 사용자들은 하나의 비밀키를 바탕으로 서로 다른 익명을 생성함으로써 다양한 응용 서비스에서 그 목적에 맞도록 이용할 수 있고, 이 익명은 연결이 불가능하기 때문에 사업자가 데이터 연결과 추론을 통해 개인에 대한 정보를 추가적으로 획득할 수 없다. 조사자(Inspector)는 신뢰할 수 있는 인증기관으로 토큰의 의미를 구분해 낸다. 폐지기관(Revocation Authority)은 발급된 사용자 인증을 파기하여 더 이상 자격(Credential)이 토큰을 생성하지 못하도록 한다. 또한 자격증명은 서비스 종료 후 폐지되어 사용자가 원치 않는 정보 보관은 봉쇄된다.

정리하면, Privacy-ABCs 방식은 복수 공개키 기반의 자격증명 방식을 이용하여 사업자에게 개인 정

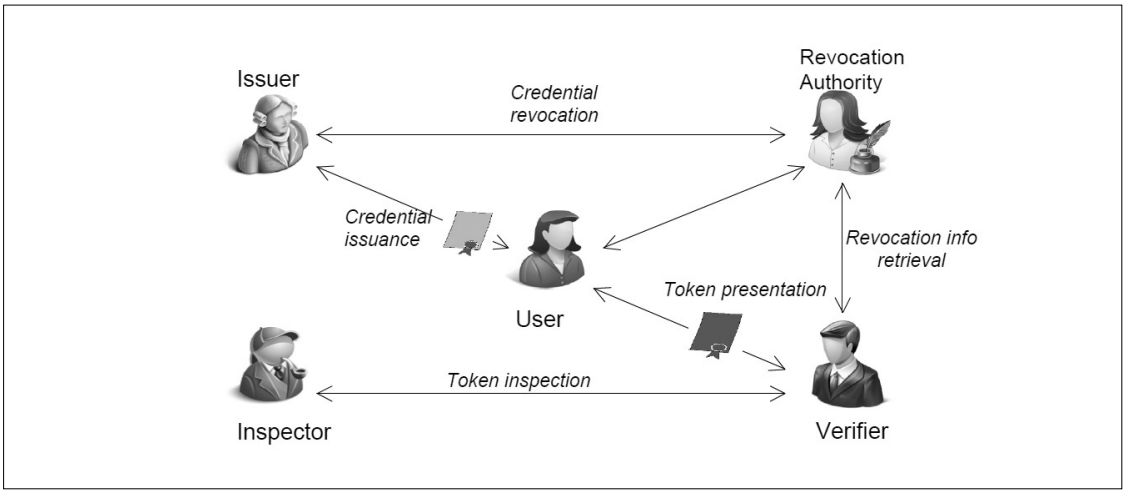
〈표 2〉 Privacy-ABCs의 주요 특징

특징	내 용
속성의 선택적 공개 (Selective disclosure of Attributes)	사용자들은 개인 속성을 감출 수 있으며, 필요한 정보만 공개 가능 일례로 사용자는 자신이 학급에 속한 학생임을 익명 상태로 증명할 수 있음
비연결성 (Unlinkability)	다른 표현 토큰 (presentation token)은 연결될 수 없음 증명자 (Verifier)는 사용자의 다른 공개키를 추적할 수 없음
조사 (Inspection)	조건부 자격증명 사용
폐지 (Revocation)	폐지 권한에 의한 자격 증명

보의 일부만을 전달한다. 따라서 Privacy-ABCs 방식을 채택한다면, 서비스 제공자들은 사용자에 대한 일부 정보만을 확인할 수 있고, 단일키를 통한 사용자 정보 링크가 불가능하기 때문에 사용자의 프라이버시는 보다 강화된다. Privacy-ABC의 참여자와 인증과정은 〈그림 3〉과 같으며 각각의 역할은 〈표 3〉과 같다.

Privacy-ABCs가 실제 환경에 적용될 수 있고, 유의한 효과를 보일 수 있음을 입증하기 위해 ABC4Trust는 두 가지 파일럿 테스트를 진행하였다(ABC4Trust, 2012: 19~61). 첫 번째 파일럿 테스트는 그리스의 파트라스 대학에서 익명성 기반의 강의 평가 시스템에 적용되었다. 〈그림 4〉와 같이 Privacy-ABCs 기술을 통해 학생들은 강의 평가에 있어 익명성을 보장받는다.

두 번째 파일럿 테스트는 스웨덴의 Norrtullskolan 학교에서 privacy-ABCs 기반의 학교 내 소셜 네트워크 플랫폼이 구축되고 평가되었다(ABC4Trust, 2012: 19~61). 이 플랫폼은 채팅 커뮤니티, 정치 토론, 개인 건강 상담, 문서 공유 기능을 제공한다. 각



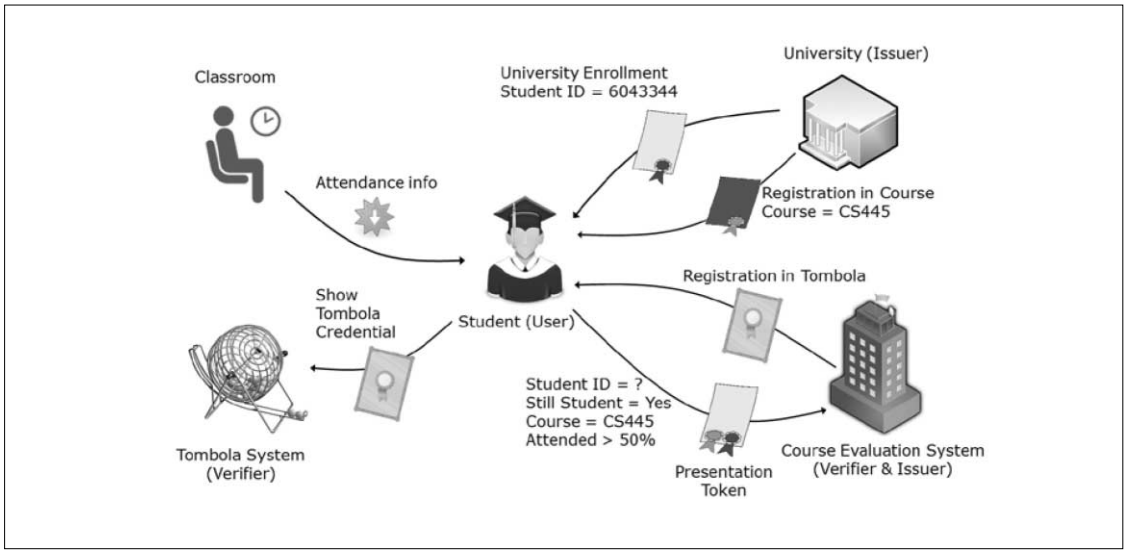
출처: ABC4Trust, 2015a: 7~9

〈그림 3〉 Privacy-ABCs 인증 과정과 참여자

〈표 3〉 Privacy-ABCs의 참여자의 역할

참여자	역 할
발급자 (Issuer)	Privacy ABCs 키 발급
사용자 (User)	Privacy-ABCs 발급키 저장 최소한의 속성 정보만으로 증명자에게 신용 증명서 (credential)과 속성 (attribute)를 가지고 있음을 표현토큰 (presentation token)을 보냄으로써 증명
증명자 (Verifier)	사용자 제공 증거가 정책 (presentation policy)에 부합하는 지 확인
폐지기관(Revocation authority)	발급자 요구에 의해 신용증명서 폐기 이 경우 이 증명서는 더 이상 표현토큰 생성에 더 이상 이용되지 못함
조사자 (Inspector)	인식된 속성 값 또는 다른 형태의 암호화된 속성값을 밝힘

출처: ABC4Trust, 2015a:7~9



출처: ABC4Trust, 2012: 19~61

〈그림 4〉 익명성 기반 강의 평가

각의 기능 단위별 서비스에 대해 Privacy-ABCs는 익명성이 담보되는 사용자 인증이 가능함을 보였고, 공개 속성을 토대로 확인된 사용자에게 각기 다른 권한을 제공함을 보였다. 예를 들면 시험결과, 성적, 개인 성취 계획 등 민감한 서류에 대한 접근 권한은 사용자 인증 과정을 토대로 구분된다. 또한, 학생들은 공개되는 속성을 선택할 수 있다. 예를 들면, 학생들은 이름, 성별, 나이 등에 대한 속성 정보를 자율적으로 선택하여 공개할 수 있다.

3. 연구 의미와 시사점

이 연구는 정보 보호 관점에서 신뢰 문제를 접근하였고, 선택적 속성 공개를 통한 사용자 인증을 토대로 사용자의 프라이버시 강화를 추구하였다. 따라서 사용자들이 원치 않는 개인정보의 노출과 활용이 사전 차단될 수 있다.

그러나 이 연구는 사용자 관점에서만 발생하는 신뢰 문제를 다루고 있다는 한계를 가진다. 즉, 사용자의 개인 속성 정보의 보호는 다루고 있으나 사용자가 소유 또는 연결한 기기의 신뢰는 다루고 있지 않다. 따라서 다양한 IoT 디바이스가 연결을 시도하고 정보를 요청하는 IoT 환경에의 적용은 한계를 가진다. 또한, 인증 이후 단계에서 발생할 수 있는 신뢰기만 행위와 이에 따른 조치는 포함하고 있지 않으며 평판 정보와 같은 동적 신뢰 정보의 변화는 반영되어 있지 않다.

Ⅳ. Inter-Trust

1. 연구 배경과 목적

IoTs, 클라우드 기술, 모바일 컴퓨팅 기술과 같은 웹 기반 소프트웨어 아키텍처는 보안(Security)에 취약하다(Inter-Trust, 2013c: 11~12). 또한 서로 다른 소프트웨어 시스템간의 경계가 점차 사라지고 있고, 네트워크와 서비스는 개방형 구조를 토대로 설계되고 구현됨을 요구받고 있다. 따라서 이질적 네트워크와 다양한 통신 단말로 구성된 시스템간의 상호 호환 이슈는 발생할 수밖에 없으며, 이러한 과정에서

신뢰는 담보되어야 한다. 서로 다른 보안 정책을 가질 수밖에 없는 이종 시스템간의 정보 교환을 위해 Inter-Trust(Interoperable Trust Assurance Infrastructure)는 보안정책 협상이라는 개념을 제안하였다(Inter-Trust, 2013c: 13~14).

이 프로젝트의 목적은 이질적인 네트워크와 기기에 존재하는 서비스와 어플리케이션의 신뢰를 담보하기 위해 동적이고 가변적인 프레임워크를 개발하는 것이다(Inter-TRUST, 2013c: 13~14). 이를 위해 각 기기와 시스템 간에 존재하는 보안 정책간의 관리, 강화, 협상을 허용하여 요구되는 보안 수준을 충족시켜 상호운용성(Interoperability)을 보장하고자 한다. 이 프로젝트에는 유럽 5개국 10개 산·학·연이 공동 참여하였다.

2. 주요 연구 내용 및 결과물

유비쿼터스 컴퓨팅, M2M, IoT로 대변되는 미래 통신 환경에서는 이종 기기와 플랫폼이 공존하고 다양한 네트워크로 연결되므로, 다양한 기기와 서비스에서의 정보 교환을 위해서는 신뢰 프레임웍이 필요하다(Inter-Trust, 2013b: 6~10). 이를 위해 Inter-Trust는 서로 다른 보안 정책을 가지고 있는 다양한 단말과 시스템의 상호 운용 보장을 위해 협상을 토대로 양측 모두 받아들일 수 있는 보안 정책을 도출하도록 설계되었다.

보안 정책의 협상과정을 구체적으로 살펴보자. a 시스템과 b 시스템이 존재하고 각 시스템에는 단말 A와 B가 연결되어 있다고 하자. Inter-Trust는 A의 보안 정책을 먼저 모델링한다. 단말 A와 B의 상호 연동을 위해 A와 B는 커뮤니케이션 모듈을 통해 보안 정책을 1차적으로 협상한다. 관점 생성기(Aspect Weaver)는 협상 정책에 따라 동적으로 보안 정책을 짜 맞춘다. 이를 통해 도출된 보안 정책은 코드화되어 삽입되는데, 양측의 보안 정책을 만족시키는지, 어플리케이션에서 요구한 보안 수준과 부합하는지 등을 조사하고 검진한다. 이후 지속적인 보호와 환경 변화 대응을 토대로 제안된 보안 정책의 신뢰성을 증진시켜 상호호환성을 보장한다.

Inter-Trust는 연구 개발 결과물의 실효성을 증명하기 위해 전자 투표와 차량-차량/차량-인프라 통신 서비스 시나리오를 제안하고 파일럿 테스트를 진행하였다(Inter-Trust, 2014: 44~62).

3. 연구 의미와 시사점

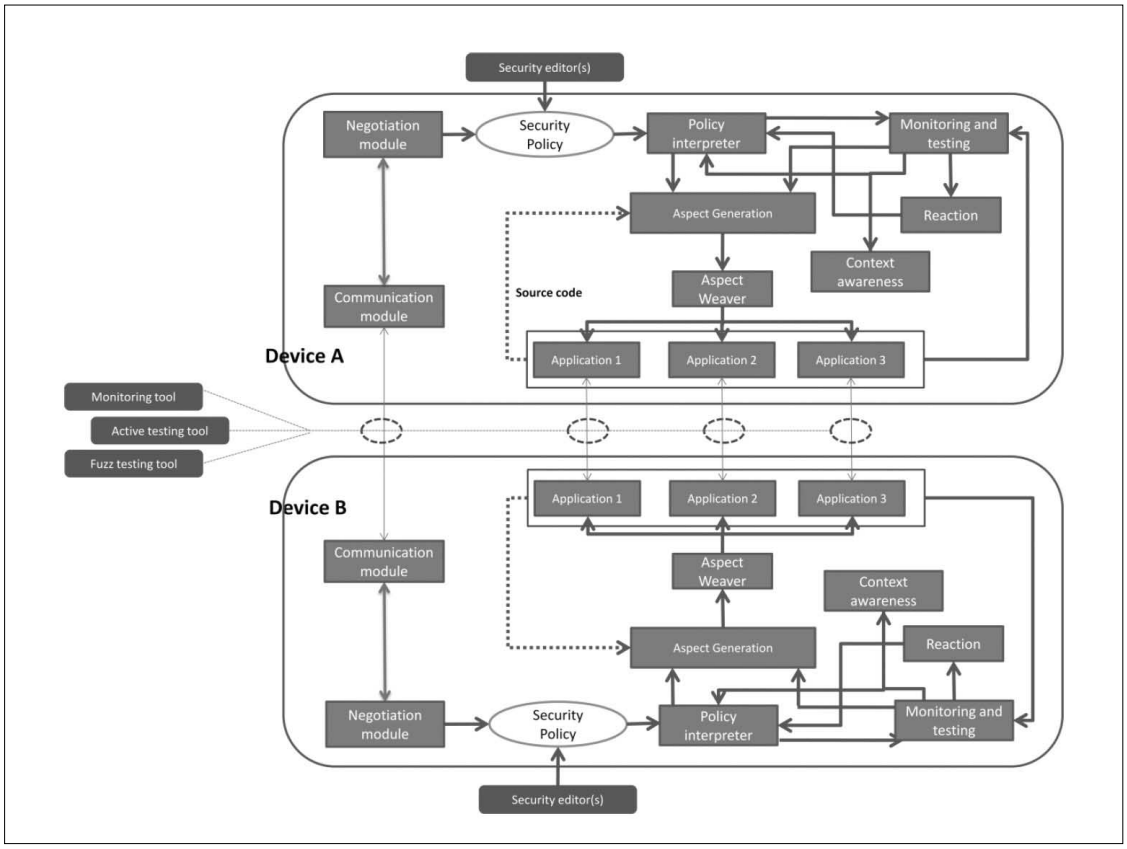
Inter-Trust는 앞에서 논한 두 프로젝트와 달리 이기종 시스템간의 정보 교환에서 발생하는 신뢰 문제를 다루었고 보안 정책의 협상이라는 방법으로 접근하였다는 측면에서 분명한 의미를 가진다. 이 연구는 서로 다른 시스템간의 연동을 위해 보안 정책의 모델링, 협상, 추출, 실행, 관찰, 대응의 과정을 통해 확보되는 프레임워크를 제안하였다. 이러한 접근은 보안 레이어가 소프트웨어의 다른 레이어와 분리될 수 있기 때문에 보다 높은 유연성을 가질 수 있다.

그러나 이 연구는 신뢰할 수 있는 연결이 협상을 통해 담보될 수 있고 합의될 수 있다 전제에서 출발하고 있으나, 다양한 신뢰 요소의 존재와 신뢰의 동적 특징을 상기해본다면 다양한 신뢰 이슈를 완전히 해소시키기는 어렵다. 또한, 이 연구는 보안 정책의 상호 호환에만 집중하여 해킹, 분실 등과 같은 신뢰 이슈를 다루고 있지 않다. 또한 이용자 관점에서 발생하는 문제를 다루지 있지 않다. 즉, 믿을 수 없는 이용자의 시스템 접근은 원천적으로 막을 수 없고, 시스템간의 보안 정책 협상에 집중하고 있어 사용자 관점의 개인정보 보호 문제를 직접적으로 다루고 있지 않다.

Ⅴ. COMPOSE

1. 연구 배경과 목적

IoT 플랫폼을 개발하기 위한 다양한 시도가 있었



출처: Inter-Trust, 2013a: 10~12

〈그림 5〉 Inter-TRUST 시스템 구조

으나, 이들 대부분은 "구현"에만 집중하여 이용자에게 가치를 제공하는 "전달"에 실패하고 있어 IoT의 가능성을 제대로 실현하지 못하고 있다(COMPOSE, 2014a: 11~13). COMPOSE(Collaborative Open Market to Place Objects at your SErvice) 프로젝트는 시장 지향적 관점에서 실질 세계와 가상 세계를 연결하는 새로운 서비스의 출현을 촉진하는 IoT 플랫폼을 개발하는 것을 목적으로 한다. COMPOSE는 스마트 기기와 서비스와 어플리케이션이 거래되는 개방형 시장의 개념을 제안하였으며, 이 시장에서는 Internet of Content(IoC), Internet of Service (IoS)의 사물(Thing)들이 거래되고 연결될 수 있다. COMPOSE는 IBM Israel 주관으로 총 6개국 12개의 산·학·연이 공동 참여하였다. 특히 참여기관 중에는 EVRYTHNG도 포함되어 있는데, EVRYTHNG은 IoT 기술과 표준을 주도하고 있는 IoT 플랫폼 업체이다.

2. 주요 연구 내용 및 결과물

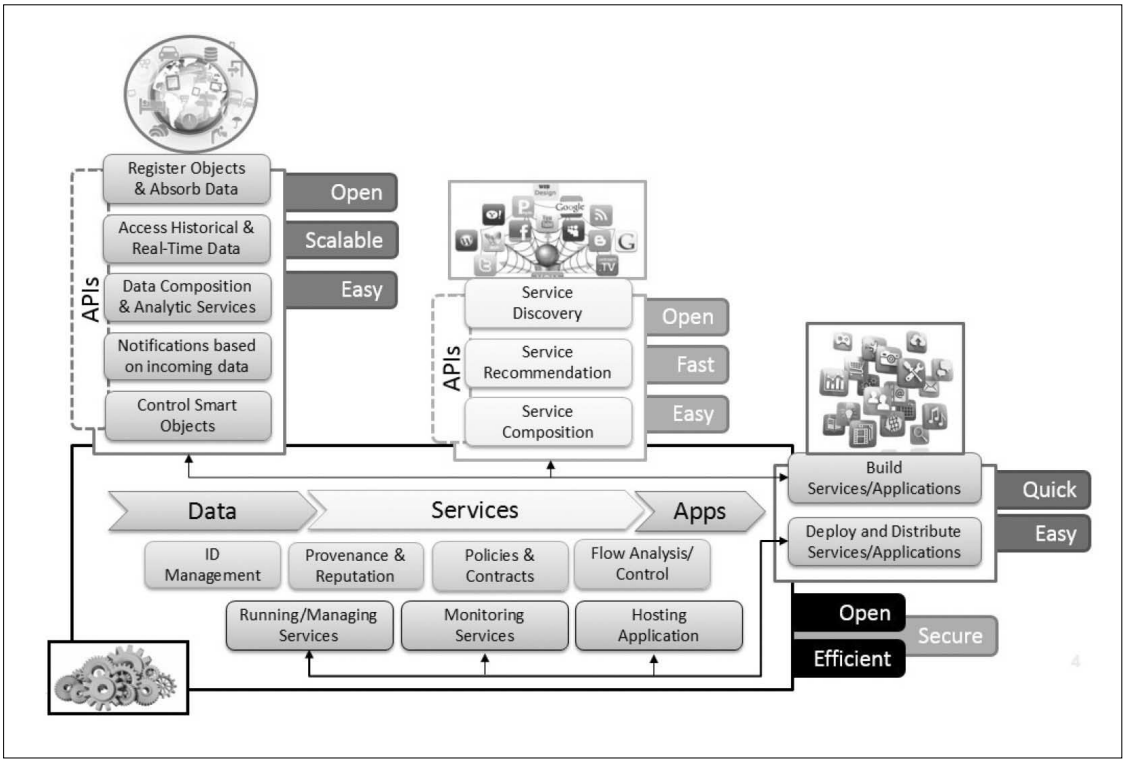
COMPOSE는 실질, 가상의 객체 (Objects)를 웹상에 존재하는 객체로 표현하고, 이들 객체를 거래를 할 수 있는 시장 기반 IoT 플랫폼을 개발하는 것을 목적으로 한다. 〈그림 6〉은 COMPOSE의 구조와 기

능의 핵심 특징을 나타낸 것이다.

COMPOSE가 제공하는 시장은 상호 연결된 객체들이 개방형 시장에서 쉽게 공유되고 통합되어 IoT, IoC, IoS의 융합과 거래가 발생하는 시장이다. 간단히 말해 이러한 접근은 앱 스토어와 매우 유사하다. 즉, 거대한 거래 시장이 존재하고 이 시장에서 개발자들은 API, SDK와 같은 공개된 자원을 바탕으로 다양한 응용 서비스를 효율적으로 개발하여 판매할 수 있으며, 사용자들은 이 시장에서 IoT 응용 서비스를 이용할 수 있다.

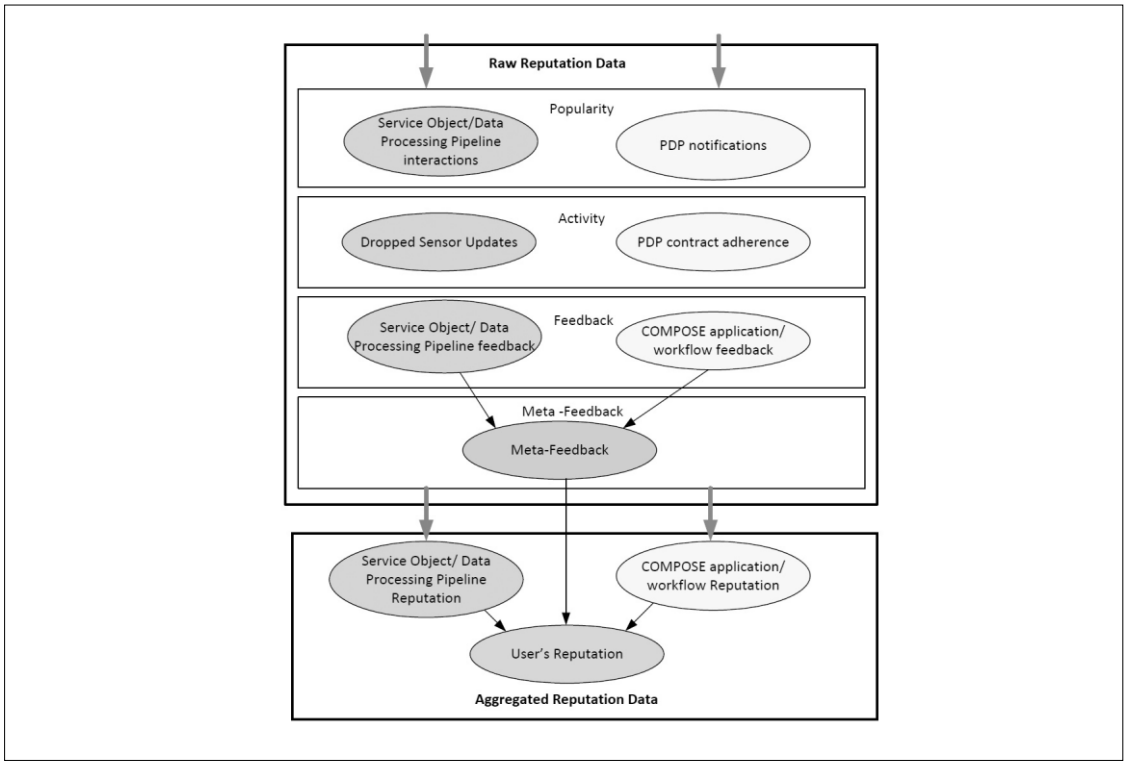
COMPOSE는 이러한 거래가 가능한 시장이 구동될 수 있도록 스마트 객체들을 표준화된 서비스로 가상화하는 접근을 채택하였다. 이를 위해서는 거래의 안전을 담보하고, 프라이버시 보호가 가능한 데이터 수집과 배포, 지식 산출이 가능해야 한다. 따라서 시장 참여자들의 거래 효율성 확보를 위해 스마트 객체의 발견과 동적 서비스 구성이 핵심 사안이 된다. 이를 위해 COMPOSE는 평판 관리 기능을 제공하고 있다. 사용자들이 과거사용 경험과 지식이 없더라도 어플리케이션과 서비스 객체가 높은 평판을 가진다면 신뢰를 형성할 수 있고 이를 통해 어플리케이션을 이용할 수 있기 때문이다. COMPOSE에 적용된 평판 시스템은 사용자로부터의 피드백 뿐 아니라 각 개체(Entity)가 제대로 동작하는지에 대한 모니터링 정보를 활용한다. COMPOSE는 〈그림 7〉과 같이 사용자 피드백, 인기도 (Popularity), 활동성 (Activity)이라는 세 가지 차원에 대한 평판 정보를 서비스 객체와 COMPOSE 어플리케이션에서 추출하여 평판 값을 추정한다.

사용자 피드백, 인기도, 활동성에 대한 평판 정보는



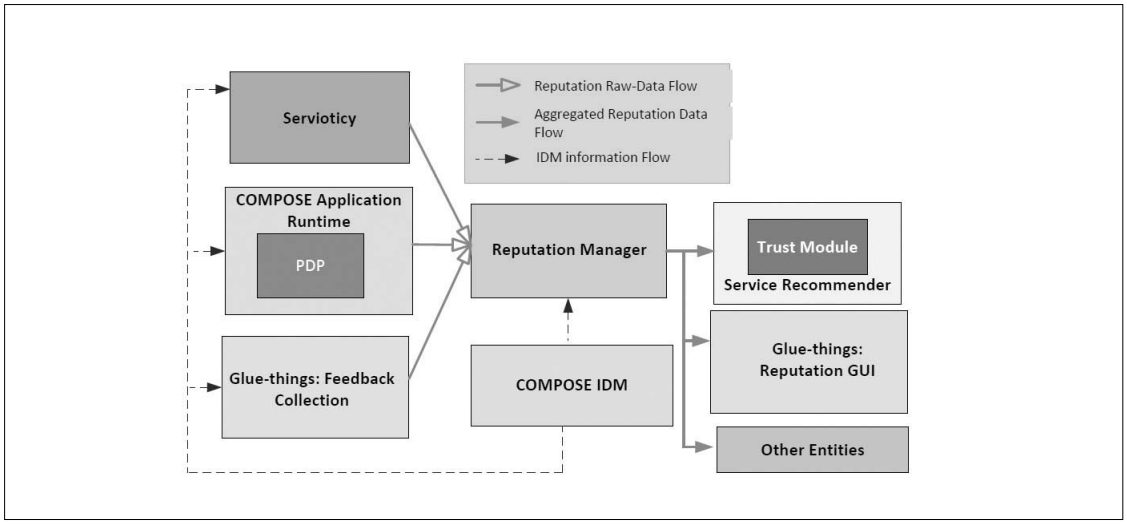
출처: COMPOSE, 2014c: 33~34

〈그림 6〉 COMPOSE의 구조와 핵심 특징



출처: COMPOSE, 2014b: 8~10

〈그림 7〉 COMPOSE의 평판 정보 분석 과정



출처: COMPOSE, 2014b: 16~17

〈그림 8〉 COMPOSE의 평판 관리 정보 흐름

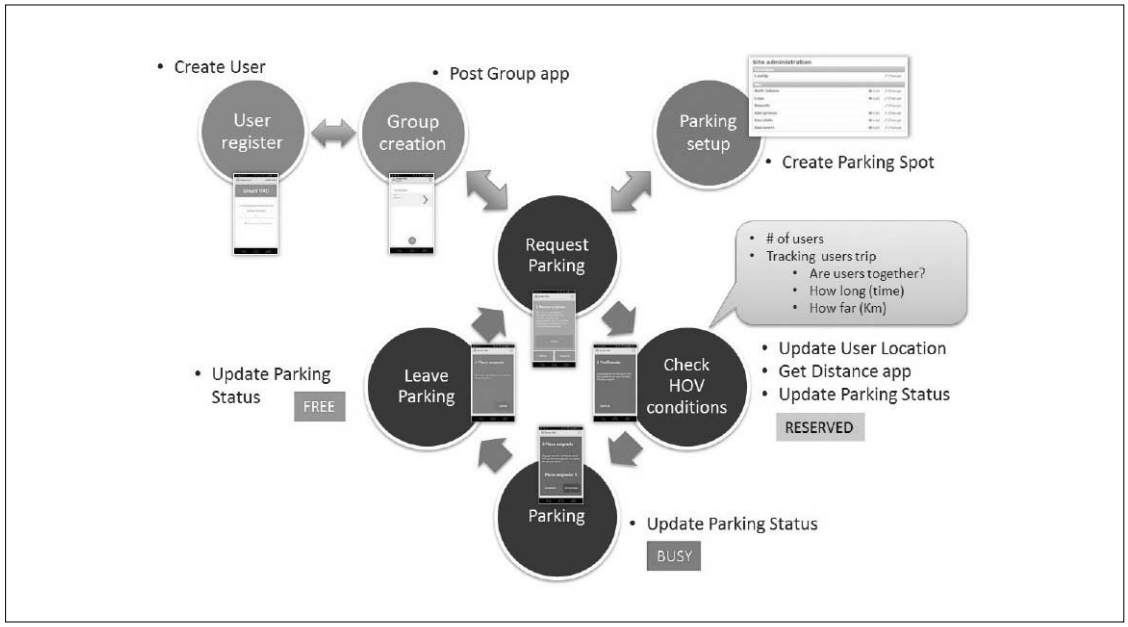
로우 데이터로 취합되어 평판 관리자(Reputation Manager)가 통합된 평판 값을 계산하고, 이는 서비스 추천자(Service Recommender)에 포함된 신뢰 모듈(Trust module)에 전달된다(〈그림 8〉). 신뢰 모듈은 이 정보를 토대로 COMPOSE 응용 서비스들의 랭킹 정보를 추출해 낸다. 랭킹 정보는 사용자들의 서비스와 객체 선택을 위한 의사 결정에 이용될 수 있다. 또한 COMPOSE는 보안과 평판 정보 관리와 사용자 피드백 정보 참조를 위해 ID 관리 기능을 탑재하고 있다.

COMPOSE는 스마트 시티(Smart City), 스마트 공간(Smart Space), 스마트 영역(Smart Territory) 3개의 서비스 시나리오를 제안하였다 (COMPOSE, 2014d: 8~61). 이중 스마트 시티는 바르셀로나의 오픈 데이터, 센서 정보 등을 이용하여 거주민을 위한 서비스를 제공하고 있다. 스마트 시티는 교통 혼잡 완화를 위해 자동차 공유(카 쉐어링) 서비스를 응용 분야로 설정하였다. 자동차 소유주는 동일 경로를 통해 이동하는 다른 사람들과 자동차를 공유하는 그룹을 생성하여 자동차를 공유하여 교통비를 분담할 수 있다. 스페인 Tarragon대학의 750명의 직원과 학생들이 카 쉐어링 서비스에 참여하고 있다.

3. 연구 의미와 시사점

COMPOSE는 시맨틱 웹 기술을 바탕으로 물리적으로 존재하는 객체를 가상화하여 객체로 표현함으로써 다양한 IoT 단말과 응용 서비스의 거래, 조립을 가능케 하였다. 이를 위해 가상화된 객체의 등록, 검색, 평판 관리에 있어 신뢰 개념을 접목하였다.

COMPOSE는 비즈니스와 시장에 대한 고민과 배려가 확연히 들어나는 시장 지향적 접근을 시도한다는 다른 연구와 차별성이 있다. COMPOSE는 SDK와 개방형 API를 지원하여 외부 개발자의 생태계 참여를 통해 플랫폼 경쟁력을 확보하고자 한다는 측면에서 앱 스토어와 매우 유사한 전략을 취하고 있다.



출처: COMPOSE, 2014d: 8~29

〈그림 9〉 COMPOSE의 카 쉐어링 기능 흐름

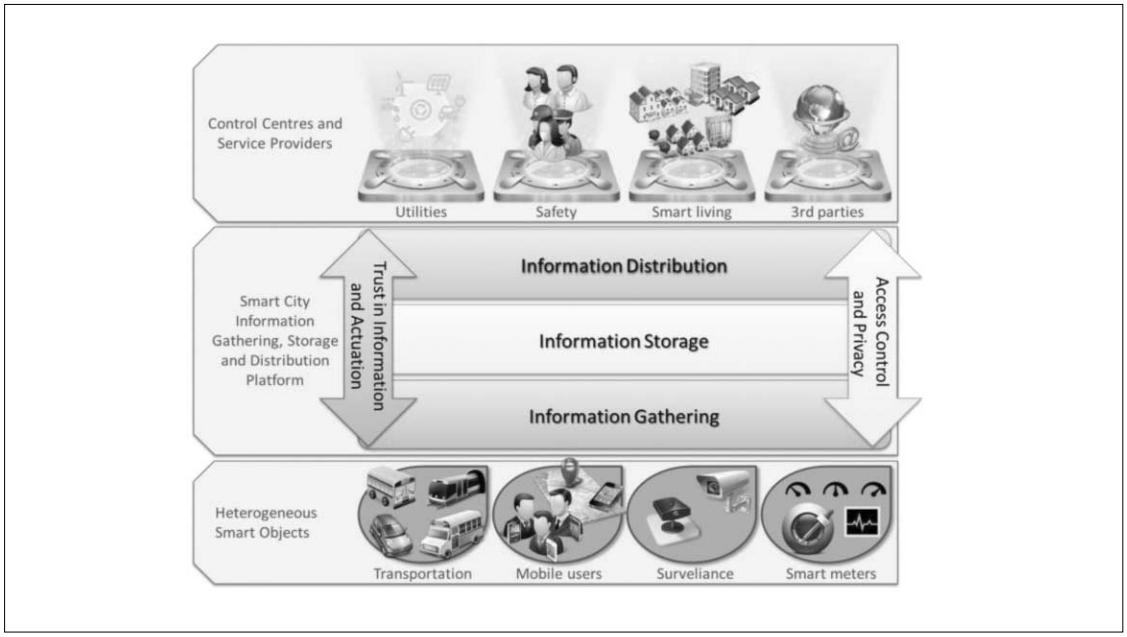
그러나 COMPOSE 프로젝트는 새로운 IoT 플랫폼을 제안한 것이므로, 다른 IoT 플랫폼과의 상호 연동 이슈가 존재할 수밖에 없다. 플랫폼 경쟁력을 확보하기 위해 양쪽 시장에 존재하는 참여자들에게 충분한 참여 동기를 제공해야 한다. 일례로 플랫폼 경쟁력 확보에 실패한 삼성 바다, 블랙베리와 같은 전철을 밟지 않기 위해서는 초기 시장 선점 및 임계 가입자 규모 확보가 반드시 필요하다.

Ⅵ. SMARTIE

1. 연구 배경과 목적

높은 도시 거주 비율(80%이상), 도심의 노후된 인프라, 삶의 질 개선에 대한 요구로 인해 스마트 시티의 필요성이 대두되고 있다. 스마트 시티는 기존 도시를 개선하여 도시의 효율성을 제고하고 데이터를 활용하여 새로운 가치를 창출하고자 하는 접근이다(SMARTIE, 2013: 3~10).

IoT, 빅 데이터 기술의 도래로 다양한 형태의 데이터가 도시 내에서 생산되고 있다. 그러나 IoT 단말과 이용자 간의 데이터 교환 과정에서 보안, 개인 정보, 신뢰 문제는 발생할 수밖에 없다. 이러한 문제를 해소하기 위해 SMARTIE(Secure and sMArter ciTIEs Data Management)는 스마트 시티에서 발생하는 대용량 이종 정보를 안전하고 신뢰할 수 있게 전달하는 분산 프레임웍을 개발하고자 한다. 안전하고, 신뢰할 수 있고, 믿을 수 있는 IoT 시스템을 이용하는 것은 스마트 시티와 관련된 도시 거주민, 사업자, 도시 행정관청 등 다양한 이해관계자들에게 큰 편익을 제공할 수 있다. 또한, 다양한 정보원천으로부터 수집된 정보의 통합 및 관리를 통해 데이터의 연결과 연동이 가능하다면 새로운 가치를 제공할 수 있을 것이다(SMARTIE, 2013: 3~10). SMARTIE 프로젝트에는 유럽 4개국 7개 산·학·연이 참여하여 진행하고 있다.



출처: SMARTIE, 2014b: 10~11

〈그림 10〉 SMARTIE의 개요

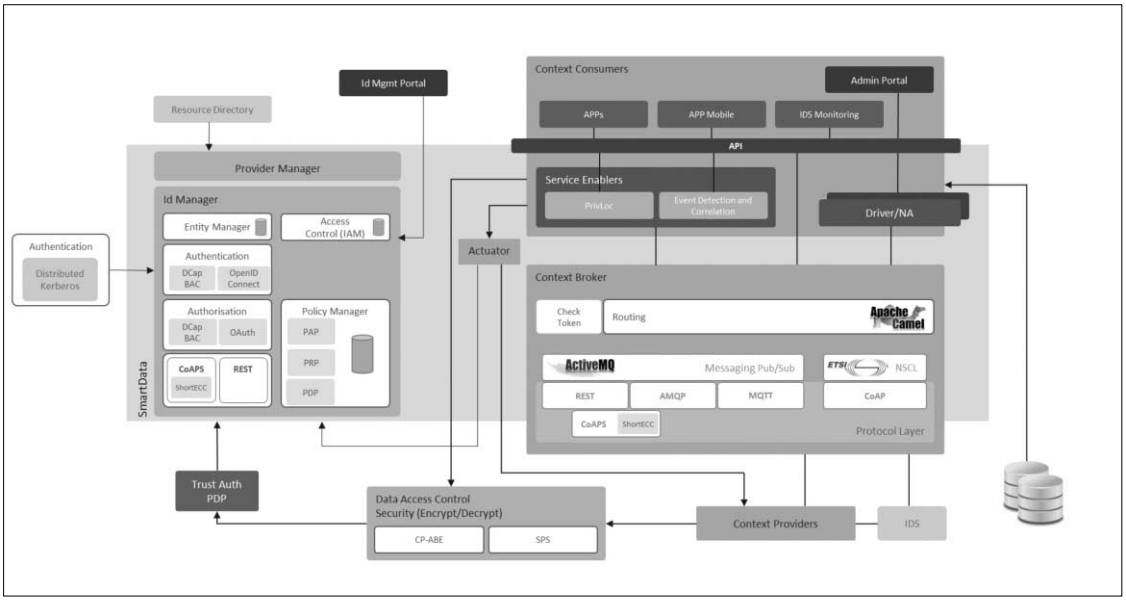
2. 주요 연구 내용

SMARTIE는 도시에 산재한 데이터들을 취합, 저장하여 도심 거주민의 안전과 편리를 위해 가공된 데이터를 적재적소에 제공하는 플랫폼 개발을 목적으로 한다. 〈그림 10〉은 SMARTIE 프로젝트의 개념을 도식화 한 것이다.

SMARTIE IoT 플랫폼은 IoT-A 프로젝트에서 제안한 Architecture Reference Model (ARM) 모델을 바탕으로 설계되었다(SMARTIE, 2015a: 21~22). IoT-A 프로젝트는 2010년 1월부터 2013년 11월까지 수행된 FP7 프로그램으로 IoT 시스템 간의 상호호환을 위한 아키텍처 참조 모델을 도출하는 것을 목적으로 한 연구이다(IoT-A, 2011: 2~8). SMARTIE의 IoT 플랫폼 구조는 〈그림 11〉과 같다.

SMARTIE에서 다루고 있는 신뢰 이슈는 크게 세 가지이다(SMARTIE, 2014b: 10~12). 첫째, IoT 시스템에 연결된 디바이스의 신뢰 이슈로 이는 사이버 공격 및 IoT 디바이스의 도난으로 발생하는 문제를 다룬다. 둘째, 다양한 데이터 원천으로부터 수집된 데이터의 결합에서 발생하는 신뢰 이슈가 존재한다. 즉, 이질적 데이터의 결합과정에서 데이터의 무결성 문제, 센싱 데이터의 에러, 악의적 공격 등의 문제 등이 발생할 수 있다. 마지막으로, IoT 단말과 소비자 사이에서 신뢰할 수 있는 데이터 교환 이슈를 다룬다.

SMARTIE는 교통 트래픽 관리, 대중교통, 스마트 에너지 관리 3개의 시나리오를 제안하였다(SMARTIE, 2014a: 15~37). 교통 트래픽 관리 시나리오는 독일 프랑크푸르트에서 구현되었으며 교통, 기후, 센서, 비디오카메라, 외부 정보 등을 이용한 교통 흐름 정보 공유 및 관리가 시연되었다. 대중교통 시나리오는 세르비아의 베오그라드에서 진행되었으며 여행객을 대상으로 가상현실과 접목하여 스마트 대중교통 정보를 제공하였다. 마지막으로 스마트 에너지 관리는 스페인의 Murcia 대학에서 진행되었으며, IoT 기기를 토대로 대학 전력 소비가 효율적으로 관리가 가능함을 보였다.



출처: SMARTIE, 2015a: 21~22

〈그림 11〉 SMARTIE IoT 플랫폼 구조

3. 연구 의미와 시사점

도시에 산재한 비실시간 공공 데이터의 공개와 활용은 국내에서도 적용되어 있다. 그러나 실시간 센싱 데이터를 응용한 공공 IoT 서비스 및 플랫폼 개발이 진행되고 있다는 점은 큰 의미를 지닌다. 수많은 센서를 통해 축적되는 실시간 데이터를 공공의 편익 증진을 위해 활용하고자 하는 이 연구는 관심을 가지고 지속적으로 살펴볼 필요가 있다. 즉, 데이터의 개방과 활용을 토대로 새로운 가치를 창출하는 시대라는 거시적 패러다임을 의미할 뿐 아니라 신뢰할 수 있는 데이터를 활용한 실시간 IoT 응용 서비스의 출현이라는 측면에서 SMARTIE를 살펴볼 필요가 있다. 안전, 개인정보 보호, 신뢰를 고려한 IoT 플랫폼 개발을 목적으로 하는 SMARTIE는 아직 진행 중이므로 연구의 한계를 논의하는 것은 유보하는 것이 타당하다.

Ⅶ. 요약 및 시사점

전자상거래 영역에서 신뢰에 대한 연구는 서비스, 제품 공급자에 대한 신뢰로 주로 소비자 행동에 미치는 영향과 신뢰가 소비에 미치는 인지적 구조에 대한 이해를 넓히는 연구가 주류를 이루어 왔다. 그러나 IoT 영역에서의 신뢰는 공급자 뿐 아니라 연결 대상, 주변 환경 및 맥락에 대한 신뢰라는 보다 확장된 개념으로 접근되어야 타당하다. 신뢰 정보가 IoT 생태계 참여자들에게 제공되어야 안전한 연결, 개인 정보의 보호, IoT에서의 거래를 촉발시킬 수 있으며, 나아가 혁신적인 서비스의 출현을 기대할 수 있기 때문이다.

본고는 유럽 FP7에서 수행된 프로그램 중 IoT에서의 신뢰를 담보하기 다양한 프로젝트를 살펴보았다. 각 연구의 접근 방향은 조금씩 다르지만, 연구의 목적에는 일관된 공통점들이 존재한다. 첫째, IoT의 무한한 가능성을 실현하기 위해 신뢰 개념을 IoT에 접목할 필요성이 있음을 강조하고 있다. 둘째, 이들 연구는 개인 정보 보호와 안전이 적절한 균형을 유지할 필요가 있음을 지적하고 있다. 왜냐하면 안전을 담보하기 위해 너무 많은 개인 정보를 요구하는 것은 합당치 않고, 반대로 개인 정보 보호를 위해 안전을 도외시할 수기 때문이다. 다시 말해, 개인정보 보호가 보장되는 가운데 데이터 분석을 통해 신뢰할 수 있는 연결과 안전을 담보하고자 시도하고 있다. 특기할만한 점은 FP7에서 수행된 이들 연구에서는 개인정보 보호의 무게 비중이 보다 높다는 점이다. 셋째, 이들 연구는 모두 사회과학적 분석이 포함되어 있고, 이는 신뢰라는 개념의 정의와 분석, 측정을 위해 인문사회학적 시각을 수용하고 있다.

각각의 프로젝트에서 다루고 있는 신뢰의 영역과 접근 방향의 차이는 〈표 4〉와 같이 요약될 수 있다. 각 프로젝트가 정의하고 있는 신뢰의 개념과 적용 영역은 분명한 차이가 있다. 일례로 uTRUSTit는 사물간의 신뢰에 집중하고 있는 반면, 시장 지향적

〈표 4〉 FP7 IoT 신뢰 연구별 신뢰 영역과 접근방법의 차이

프로젝트	신뢰 진단/해소영역			접근방법
	사람	사물	관계	
uTRUSTit		○		정보 시각화
ABC4TRUST	○			비밀키/인증서 관리
Inter-TRUST		○		보안 정책 협상
COMPOSE	○	○	○	시장 지향적 플랫폼
SMARTIE	○	○		안전한 플랫폼

이고 개체들 간의 거래를 허용하고 있는 COMPOSE는 신뢰 분석 대상을 사람, 사물, 관계를 모두 포함하고 있다.

본고는 비교적 새로운 연구라 할 수 있는 IoT에서의 신뢰라는 주제로 유럽 FP7에서 수행중이거나 완료된 프로젝트들을 살펴보았다. 그러나 본고는 이제 막 시작단계에 접어든 위 프로젝트들의 개념과 접근을 정리한 것으로 향후 보다 심도 있는 분석과 관찰이 필요하다. 본 연구의 한계를 정리하면 다음과 같다. 첫째, 본고는 거시적 관점에서의 국내 IoT 연구 방향성은 제시하고 있으나 정책 목표와 구체적인 방향은 담고 있지 않다. 국내 IoT의 연구 현황을 점검하고 이를 토대로 구체적 정책 목표를 제안하는 것은 본고의 범위에서 벗어나기 때문이다. 이에 대한 연구는 후속 연구로 남겨둔다. 둘째, 이 연구에는 신뢰의 구체적 적용 영역, 사업자와 공급자의 시각차이, 신뢰 정보의 수집 및 취합 방법과 이에 따른 차이, 주요 성공 요인 등 다양한 관점에서의 분석은 포함하고 있지 않다. 이는 이제 막 시작된 IoT내 신뢰 연구의 사례가 충분치 않고 아직 본격적인 상용 서비스가 존재하지 않기 때문이다. IoT 생태계 관점에서 참여자의 이해득실과 참여 동기를 분석한 연구가 향후 필요하다. 셋째, 유럽 뿐 아니라 다양한 국가에서 수행중인 관련 연구를 탐색하여 접근 방향의 차이를 확인할 필요가 있다. 이 역시 본고의 범위에서 벗어나기 때문에 이에 대한 연구는 후속 연구로 남겨둔다.

IoT 시장의 성장과 그 잠재력에 대해서는 큰 이견이 없다. 점차 성숙되어가는 IoT 환경에서 본 연구가 국내 ICT 정책 및 연구 방향에 시사하는 바는 크다. 소비자 측면에서는 IoT 연결로 인한 이득이 연결 과정에서 발생할 수 있는 불확실성과 위험보다 커야 IoT를 받아들일 것이다. 따라서 IoT시장의 본격적 개화를 위해서는 신뢰할 수 있는 연결을 제공할 수 있어야 한다.

국내 역시 IoT 응용 서비스의 확산과 소비자 저변 확대를 위해 신뢰 관점에서 IoT를 살펴보고 이를 접목한 연구가 절실히 필요한 시점이다. 이를 위해서는 학제 간 연구를 통해 신뢰에 대한 충분한 이해를 토대로 연구가 진행되어야 할 것이다. 일례로 IoT 환경은 이용자, 단말, 관계, 상황 정보 등 복합적인 정보가 신뢰를 결정짓는 요소가 되므로 어떻게 신뢰를 정의하고 추출하고 분석하는지에 대해서는 다양한 학문의 시각과 방법론이 결합되어 논의되어야 할 것이다. 또한, 신뢰 추출 과정에서 발생할 수 있는 개인정보 유출 방지 방안, 생태계 구축 전략, 제도적 이슈 해소 방안 등이 함께 모색되어야 할 것이다. 나아가, 개인 정보 보호와 안전 한쪽에 치우치지 않는 균형 있는 정책이 마련되어야 할 것이다.

■ 참고문헌

김호원 (2014). "사물인터넷 환경에서의 보안/프라이버시 이슈." 「TTA 저널」, 153: 35~39.

표철식·강호용·김내수·방효찬 (2013). "IoT(M2M) 기술 동향 및 발전 전망." 「한국통신학회지」, 30(8): 3-10.

ABC4Trust (2011). "ABC4Trust D2.1 Architecture for Attribute-based Credential Technologies - Version 1." https://abc4trust.eu/download/ABC4Trust-D2.1-Architecture-V1.2.pdf (Retrieved Oct 22, 2015).

ABC4Trust (2012). "ABC4Trust D5.1 Scenario Definition for both Pilots: ABC4Trust." https://abc4trust.eu/download/ABC4Trust-D5.1-Scenario-Definition.pdf. (Retrieved Oct 22, 2015).

ABC4Trust (2015a). "R2.1 Privacy-ABC Technologies, Personal Data Ecosystem, and Business Models: A feasibility study report: ABC4Trust." https://abc4trust.eu/download/R2.1%20-%20PDE%20and%20ABC%20Review%20V1.0.pdf (Retrieved Dec 4, 2015).

ABC4Trust (2015b). "ABC4Trust."

https://abc4trust.eu/(Retrieved Oct 18, 2015).

Chaudhuri, A. & Holbrook, M. B. (2001). "The Chain of Effects from Brand Trust and Brand Affect to Brand Performance: The Role of Brand Loyalty." *Journal of Marketing*, 65(2): 81-93.

COMPOSE (2014a). "D1.2.2 Final COMPOSE architecture document: COMPOSE." http://www.compose-project.eu/sites/default/files/publications/D1.2.2%20-%20Final%20COMPOSE%20architecture.pdf (Retrieved Dec 10, 2015).

COMPOSE (2014b). "D5.3.1 Reputation Management Report: COMPOSE." http://www.compose-project.eu/sites/default/files/publications/D5.3.1%20-%20Reputation%20management%20report.pdf (Retrieved Dec 12, 2015).

COMPOSE (2014c). "D7.2.1 Business Modeling Analysis: COMPOSE." http://www.compose-project.eu/document/d721-business-modeling-analysis (Retrieved Dec 9, 2015).

COMPOSE (2014d). "D7.3.2 Use Cases Implementation - Final Version: COMPOSE." http://www.compose-project.eu/document/d732-use-cases-implementation-%E2%80%93-final-version (Retrieved Nov 13, 2015).

COMPOSE (2015). "COMPOSE." http://www.compose-project.eu/ (Retrieved Nov 11, 2015).

Corbitt, B. J., Thanasankit, T. & Yi, H. (2003). "Trust and e-commerce: a study of consumer perceptions." *Electronic Commerce Research and Applications*, 2(3): 203-215.

Sirdeshmukh , D., Singh, J. & Sabol, B. (2002). Consumer Trust, Value, and Loyalty in Relational Exchanges. *Journal of Marketing*, 66(1): 15-37.

Dumortier, J. & Vandezande, N. (2012). "Trust in the proposed EU regulation on trust services?" *Computer Law & Security Review*, 28(5): 568-576.

Hong, I. B. & Cho, H. (2011). "The impact of consumer trust on attitudinal loyalty and purchase intentions in B2C e-marketplaces: Intermediary trust vs. seller trust." *International Journal of Information Management*, 31(5): 469-479.

Inter-Trust (2013a). "D.2.3.1 INTER-TRUST Approach and Framework Specification (first version)." http://inter-trust.lcc.uma.es/documents/10180/15714/INTER-TRUST-T2.3-IT-DELV-D2.3.1-ApproachAndFrameworkSpecification-First-V1.0/51c97210-be53-4e49-827f-d4e666ded4bf (Retrieved Dec 19, 2015).

Inter-Trust (2013b). "D2.4.1. Market analysis (first version)." http://inter-trust.lcc.uma.es/deliverables (Retrieved Dec 3, 2015)

Inter-Trust (2013c). "Inter-trust D2.2.1 Gap and Standards Analysis First Version." http://inter-trust.lcc.uma.es/documents/10180/15714/INTER-TRUST-T2.2-UMU-DELV-D2.2.1-GapStandardsAn-First-V1.00.pdf/dcc886d8-1824-4973-8e73-2a91c7a3f85e (Retrieved Nov 1, 2015).

Inter-Trust (2014). "Inter-TRUST D3.3 Guidelines for Deployment." http://inter-trust.lcc.uma.es/documents/10180/15714/INTER-TRUST-T3.4-SCYTL-DELV-D3.3-GuideDeploy-V1.00.pdf/e4218bab-c76e-440e-9f9d-e4e1d96a510b (Retrieved Oct 21, 2015)

Inter-Trust (2015). "Interoperable Trust Assurance Infrastructure" http://inter-trust.lcc.uma.es/ (Retrieved Oct 17, 2015).

IoT-A (2011). "D1.2 - Initial Architectural Reference Model for IoT: IoT-A." http://www.iot-a.eu/public/public-documents/d1.2/view (Retrieved Dec 2, 2015)

Mayer, R. C., Davis, J. H. & Schoorman, F. D. (1995). "An Integrative Model of Organizational

Trust." *The Academy of Management Review*, 20(3): 709-734.
Ranaweera, C. & Prabhu, J. (2003). "On the relative importance of customer satisfaction and trust as determinants of customer retention and positive word of mouth." *Journal of Targeting, Measurement and Analysis for Marketing*, 12(1): 82-90.
SMARTIE (2013). "SMARTIE D2.2 Requirements." http://www.smartie-project.eu/publication_deli.html. (Retrieved Oct 19, 2015).
SMARTIE (2014a). "D2.1 Use Cases: SMARTIE." http://www.smartie-project.eu/download/D2.1-Use%20Cases.pdf (Retrieved Dec 8, 2015).
SMARTIE (2014b). "D3.1 Components for secure information gathering and storage: SMARTIE." http://www.smartie-project.eu/download/D3.1-Components_for_secure_information_gathering_and_storage_Final.pdf (Retrieved Nov 14, 2015).
SMARTIE (2015a). "D5.1 Integration and Validation Plan: SMATIE." http://www.smartie-project.eu/download/D5.1-Integration%20and%20Validation%20Plan.pdf (Retrieved Dec 9, 2015).
SMARTIE (2015b). "Welcome to SMARTIE Project." http://www.smartie-project.eu/ (Retrieved Dec 9, 2015).
uTRUSTit (2011). "D.2.2 Definition of User Scenarios: uTRUSTit." http://www.utrustit.eu/ (Retrieved Sep 3, 2015)
uTRUSTit (2012a). "uTRUSTit D2.7 Updated Design Guidelines on the Security Feedback Provided by the Things." http://www.utrustit.eu/ (Retrieved Sep 4, 2015).
uTRUSTit (2012b). "uTRUSTit Deliverables." http://www.utrustit.eu/ (Retrieved Sep 2, 2015).
uTRUSTit (2013). "uTRUSTit D2.8 Final UI-Guidelines for the Trust Feedback Provided by the IoT." http://www.utrustit.eu/ (Retrieved Sep 1, 2015).