스마트 자동차 네트워크의 보안취약점 분석 및 해결방안 마련★

김 진 묵*, 문 정 경**, 황 득 영***

요 약

4차 산업혁명 시대에 가장 주목 받는 기술 중에 하나로 스마트 자동차 분야에 대한 관심이 매우 높아지고 있다. 가까운 미래에는 스마트 자동차를 타고 원하는 곳으로 이동하는 것이 가능해질 뿐만 아니라, 인공지능 요소를 포함한 스마트 자동차가 스스로 갑작스런 자동차 사고를 회피할 수도 있다. 하지만 스마트 자동차 분야가 발전하면 할수록 보안 분야에서 발생할 수 있는 다양한 위험성은 증가하게 된다. 그러므로 본 연구에서는 스마트 자동차 네트워크에서 발생할 수 있는 보안 취약점들에 대한 이해를 바탕으로, FIDO와 속성기반 권한 위임 기법을 사용한 정보보호 기술을 스마트 자동차 네트워크에 적용함으로써 안전하고 보안성이 높은 제어 기술을 제공할 수 있게 하고자 한다. 제안한 연구방법은 안전한 스마트 자동차 제어 기술을 사용함으로써, 스마트 자동차 네트워크 환경에서 발생할 수 있는 보안 취약점들을 해결할 수 있음을 보였다. 뿐만 아니라 스마트 자동차 네트워크 분야에서 발생할 수 있는 보안 취약성들을 해결하기 위한 다양한 제안방법들을 향후 연구를 통해서 제안하고자 한다.

Smart Vehicle Security Vulnerability Analysis and Solution Support

Jin-Mook Kim*, Jeong-Kyung Moon**, Deuk-Young Hwang***

ABSTRACT

One of the most remarkable technologies in the era of the 4th industrial revolution is the interest in the field of smart cars. In the near future, it will not only be possible to move to a place where you want to ride a smart car, but smart cars, including artificial intelligence elements, can avoid sudden car accidents. However, as the field of smart automobiles develops, the risks are expected to increase. Therefore, based on the understanding of security vulnerabilities that may occur in smart car networks, we can apply safe information security technology using FIDO and attribute-based authorization delegation technique to provide smart car control technology that is safe and secure. I want to. In this paper, we show that the proposed method can solve security vulnerabilities by using secure smart car control technology. We will further study various proposals to solve security vulnerabilities in the field of smart car networks through future research.

Key words : Smart vehicle, FIDO, Attribute-based authentication, Security vulnerability, Analysis

접수일(2018년 7월 30일), 수정일(1차: 2018년 9월 23일), 게재확정일(2018년 9월 29일)

★ 본 논문은 2016년도 강원대학교 대학회계 학술연구조성비로 연구하였음(관리번호-620160028).

* 선문대학교 IT교육학부

** 가천대학교 소프트웨어중심대학

*** 강원대학교삼척캠퍼스 컴퓨터공학과(교신저자)

1. 서 론

스마트 자동차 시장이 급격하게 발전하고 있다. 특히 무인 자동차 분야에 대한 관심과 기술 개발이 빠르게 진행되고 있는 실정이다. 이런 스마트 자동차 환경은 기존의 자동차와 달리 자동차 소유자의 허락을 받아서 인공지능 프로그램이 대신 자동차를 운전하게 할 수도 있고, 실시간으로 수집된 교통 상태 정보를 참고해서 우회도로를 찾아 빠르게 운전할 수도 있다. 이처럼 스마트 자동차 편리해질 것이다. 뿐만 아니라 자동차 운전을 할 수 있는 자격증을 소지하지 못한 여성이나 어린 아이들도 안전하게 집까지 귀가할 수 있게 된다.

하지만 스마트 자동차 네트워크가 발전함으로써 여러 가지 기존에 발생하지 않았던 위험한 상황들도 나타날 것이다. 예를 들어, 자동차 소유자가 알고 있는 비밀번호를 공격해서 스마트 자동차를 훔치거나, 스마트 자동차 소유자만이 접근할 수 있는 특별한 권한이 있는 서비스에 원격으로 접속하여 범죄에 악용할 수도 있다.

특히, 스마트 자동차 네트워크가 갖고 있는 보안 취약점들이 무엇인지 알아내어 교통사고나 범죄가 일어날 가능성이 있는 문제들을 해결하기 위한 수단과 정책을 미리 마련해야만 한다. 국내에서는 2017년 7월, 정부 주도로 KISA가 주축이 되어 스마트 자동차 보안 취약점 분석에 착수하였다. 하지만 현재까지 보안 취약점 조사 및 분석이 진행되고 구체적인 대응방안 등이 마련되지 못한 실정이다.

그러므로 본 논문에서는 스마트 자동차 네트워크에서 발생할 수 있는 보안 취약점들을 8가지로 구분해 보았다. 여러 가지 다양한 보안 취약점들 중에서 본 연구에서는 가장 시급하다고 판단한 스마트 자동차 사용자에 대한 인증방법에 대해 제안하였다. 그리고 두 번째로 스마트 자동차 자체에 대한 인증 방법으로 스마트 자동차에 탑재한 CM OS 보드의 하드웨어 정보를 활용한 식별정보를 생성해서 하드웨어 인증 기법을 제안하고자 한다.

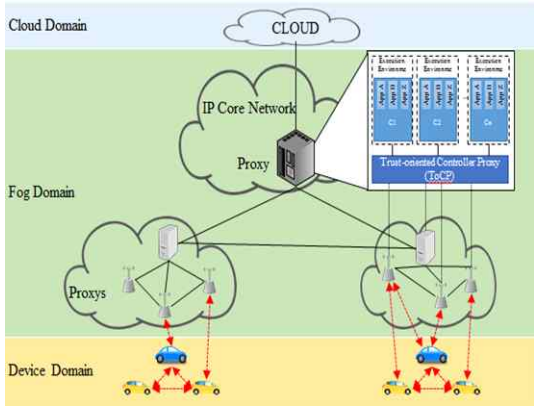
본 논문에서 우리가 제안한 하드웨어 기반 스마트 자동차 식별 알고리즘을 사용하면 빠르고 안전하게 스마트 자동차에 대한 인식 및 식별이 가능하다. 뿐만 아니라 스마트 자동차에 대한 위치 추적 같은 민감 정보에 접근하기 위해서는 사용자 인증을 거친 자동차 소유자와 경찰 기관 등에만 제공할 수 있는 대리 인증 기법 등에도 활용할 수 있을 것으로 생각한다.

본 논문의 구성은 다음과 같다. 2장은 관련 연구로 C-ITS(Cooperative Intelligent Transport System)를 참조한 스마트 자동차 네트워크 환경과 스마트 자동차 네트워크 환경에서 발생 가능한 보안 취약점들에 대해서 설명한다. 3장은 제안하고자 하는 보안성과 권한 위임이 기능을 갖는 스마트 자동차 네트워크 환경에 대해서 제안하였다. 4장은 제안한 보안성과 권한 위임 기능을 갖는 스마트 자동차 네트워크 환경이 보안 취약성에 안전하게 동작할 수 있음을 보이고자 분석하였다. 마지막으로 결론을 기술하였다.

2. 관련 연구

2.1 스마트 자동차 네트워크 환경

ISO TC204에서 제시한 C-ITS는 차량과 기반 간 및 차량과 차량 간의 고속 무선 통신을 기반으로 개방형 플랫폼으로 운영된다.



(그림 1) 스마트 자동차 네트워크 구조도

운전자와 도로 사용자에게 교통사고 발생을 경고하여 교통 안전 수준을 한 단계 끌어 올렸다[11]. 그림 1은 스마트 자동차 네트워크 환경의 구조에 대해서 간략하게 나타내고 있다. 그림 1에서 나타낸 바와 같이, C-ITS 기반의 스마트 자동차 네트워크 환경은 3단계로 구성된다. 1 레벨인 스마트 장치 계층은 스마트 자동차와 이에 탑재된 다양한 센서 장치, 통신 장치, 제어 장치들로 구성된다. 2 레벨인 포그 네트워크 계층은 주변의 센서들이 자체 통신을 할 수 있는 여러 개의 프록시 단위 통신망들과 이들을 통합 관리하기 위한 한 개의 제어 네트워크로 구성된다. 그리고 최고 상위 계층인 클라우드 계층에서는 제어 네트워크들로 구성된 상위 계층으로 제어 네트워크들에 대한 통합 관리와 의사 결정을 신속하게 지원 가능하도록 구성된다.

CEN TC278 WG16과 함께 작업하는 ISO TC 204 WG1 및 WG18은 C-ITS의 표준 정의를 수립하는데 집중했다. 지금까지 표준으로 정의된 문서들은 대부분 유럽을 중심으로 이루어졌다. C-ITS의 표준 정의는 스마트 자동차 네트워크에 대한 안전성, 시스템 연속성, 효율성 및 편의성 향상을 목표로 하고 있다. 특히, ITS의 전반적인 구성과 동작 환경에 대해서 정의하고, ITS에서 동작하는 개체들 간의 정보 공유 및 대응 촉진을 통해 위험 정보 또는 권장 사항을 제공하고 있다[12].

차세대 인텔리전트 트래픽 시스템에 필요한 컴퓨팅 인프라를 구축하려면 처리 노드라고 하는 전용 컴퓨팅 장치를 네트워크에 배치해야만 한다. 예를 들어, 특수 라우터는 패킷을 전달할 수 있을 뿐만 아니라 일반 응용 프로그램과 관련된 컴퓨팅도 처리할 수 있다. 더욱이 맞춤형 컴퓨팅 인스턴스를 제공할 수 있는 유사 프로그램 인터페이스도 제공해야 한다[13].

2.2 스마트 자동차 네트워크에서 발생 가능한 보안 취약점들

<표 1> 스마트 자동차 네트워크에서 발생 가능한 대표적인 보안취약점들

취약점	설명
회선 도청 및 정보 유출	- 프록시 서버 혹은 교통 센터에 불법 접근을 통한 센서 정보 수집 - 블루투스 및 무선 통신에 대한 스니핑 공격을 통한 데이터 유출 - 차량의 통신 장치에 의한 정보 유출
개인 정보 침해	- 차량에 저장된 정보(차량 상태정보, 소유자 정보와 같은 개인 정보)를 유출한 후 이에 대한 분석 - 차량 운전 이력 정보를 유출한 후 이에 대한 분석을 통해 개인의 행동 정보를 분석
데이터 위/변조	- 블루투스 및 무선 통신을 통한 데이터 위조 및 변조 - 차량의 시동 및 문 잠금과 같은 자동 제어 장치에 정보에 대한 위/변조
명의 도용	- 개인 식별 정보(인증 정보)에 대한 불법 접근, 복사, 신분 위장 공격
서비스 거부 공격	- 무의미한 정보를 무선 및 블루투스 통신망에서 합법적으로 여러 차례 전송을 통해서 정상적인 서비스가 불가능하도록 하는 공격
물리적 공격	- 자동차 메모리 장치의 전압을 분석하는 것과 같은 물리적 유형의 공격
위치 추적	- 사용자의 ID를 이용하여 위치 정보 및 주행 기록 정보를 추적
퍼지 공격	- 스마트 자동차나 통신 시스템이 갖는 물리적 범위를 넘치거나 부족하게 공격하여 시스템 오류가 발생하도록 함 - 스마트 자동차나 통신 시스템에서 전송하지 않은 정보를 보낸 것처럼 속여서 오류가 발생하도록 함

참고문헌 13에서 정리한 바와 같이 표 1은 스마트 자동차 네트워크 환경에는 8가지 대표적인 보안 취약점들이 존재한다. 그 중에서도 스마트 자동차 내부에 설치된 화이트 박스 덮어쓰기 공격에 대한 보안 취약점, 자동차 자체에 대한 하드웨어 식별 체계와 사고 발생 시 권한 위임을 통한 원격 제어, 스마트 자동차에 대한 서비스 거부 공격도 심각한 문제를 발생할 수 있다.

더욱이 해커는 원격에서 스마트 자동차의 이동 상태 정보를 취득해서 위치 추적공격을 할 수도 있고, 자동차를 정상적으로 운전할 수 없게 하는 서비스 거부 공격을 일으킬 수도 있다.

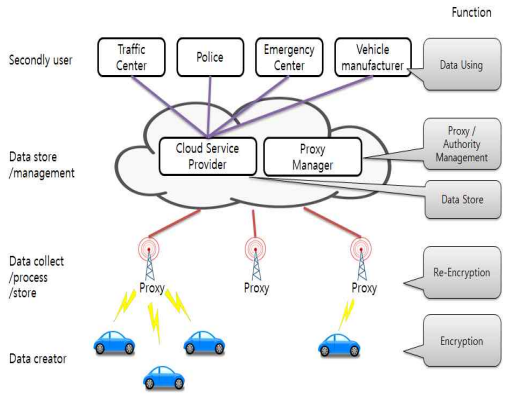
본 연구에서는 개인정보 침해(자동차 자체 정

보, 사용자 인증 정보)와 명의 도용에 위협에 대한 해결 방법을 중심으로 연구하고자 한다. 뿐만 아니라 회선 도청 및 정보 유출을 막을 수 있는 방법에 대해서도 제안하고자 한다.

3. 제안 모델

3.1 안전한 스마트 자동차 네트워크 모델

스마트 자동차 네트워크 환경에서 특정 차량을 추적할 수 있고, 비상시 스마트 자동차에 원격 제어가 가능한 모델을 제안하고자 한다[14]. 제안 모델에서는 신뢰할 수 있는 제 3 자에 프록시 서버를 설치하여 위치 추적이 가능하다. 그림 2는 본 연구에서 제안하고자 하는 속성 기반 권한 위임이 가능한 스마트 자동차 네트워크 모델을 나타내었다[15].



(그림 2) 제안하는 스마트 자동차네트워크 모델

그림 2에서 나타낸 제안 모델은 4계층 구조이다. 데이터 생성 계층은 스마트 자동차들로 구성된다. 데이터 수집 및 처리 계층은 프록시 서버들로 구성된다. 3계층인 데이터 저장 및 처리 계층은 클라우드 서비스 제공업자들의 네트워크이다. 최상위 계층인 2차 사용자 계층은 경찰서, 소방서, 자동차 생산자, 교통관제 센터로 구성된다.

스마트 자동차에 의해서 생성된 수집 데이터들을 스마트 교통 신호 장치에 설치된 네트워크 수집 장치를 통해서 수신할 수 있다. 현재 개인 정보와 같은 중요한 데이터는 기밀성을 보장하기 위해서 암호화를 수행해서 전달하게 한다. 궁극적으로 이렇게 수집된 데이터들을 클라우드 서비스를 통해서 분산 저장한다.

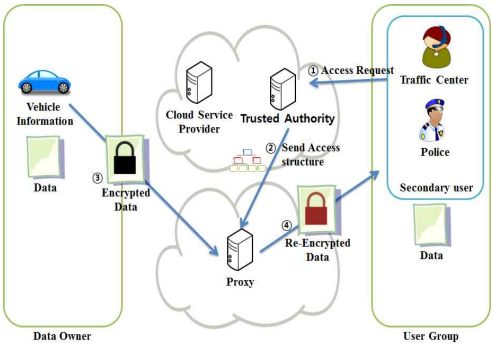
저장된 데이터는 2 차 사용자의 목적에 따라 분류되어 사용할 수 있다. 스마트 교통망 환경에서 차량으로부터 수집된 데이터들은 대부분이 그 크기가 방대하고 비정형적인 데이터들이 대부분이다. 그러므로 일반적인 클라우드 컴퓨팅 환경에서는 실시간 처리가 어렵고 네트워크 처리 지연 시간이 발생하는 문제를 가지고 있다. 따라서 스마트 시그널링 장치들은 프록시 기능을 수행하며, 센싱 데이터의 수집 및 저장뿐만 아니라 프로세싱 기능까지 갖는다.

실시간 처리가 필요한 특정 차량을 추적하는 경우와 마찬가지로 프록시 처리는 재 암호화를 제공하여 보조 사용자 (예 : 경찰차, 구급차)가 데이터를 복구할 수 있도록 구성한다. 즉, 2 차 이용자인 경찰이나 소방대원 등은 차량 정보를 관리하는 행정 기관이 추적할 특정 차량의 해독 권한을 먼저 취득하고, 암호화된 자동차 정보 혹은 자동차 소유자에 대한 개인 정보를 해독할 수 있는 권한을 위임받을 수 있다. 즉, 차량 데이터 생성자는 정보를 전달하기 전에 제3의 신뢰기관(행정 기관)의 공개키로 전송하고자 하는 데이터를 암호화한 후 전달하도록 설계하였다. 이렇게 암호화된 데이터는 공개키의 쌍이 되는 비밀키를 가진 신뢰기관만이 해독할 수 있다. 뿐만 아니라 경찰이나 소방대원과 같이 현장에서 활동하는 신뢰기관과 유사한 권한을 갖는 사용자도 권한을 위임 받아서 신뢰기관의 비밀키로 암호화된 데이터를 해독한다.

3.2 속성기반 사용자 인증을 통한 접근제어

그림 3은 제안한 속성기반 권한 위임 모델의 처리 과정을 보여주고 있다. 제안 모델에서 사용하는 암호화 기술은 기존의 신뢰기관만 가질 수 있는 사용자 권한 위임 기법을 사용해 경찰이나 소방대원이 스마트 자동차를 사용 가능하다. 이를 위해서 제안 모델에서는 4단계로 구성된 권한 위

임 처리 절차를 갖는다.



(그림 3) 속성기반 권한위임 모델

이에 대해서 자세히 설명하면 아래와 같다.

1 단계 : 통신센터 직원이나 경찰 등의 통신요청 - 통신 센터 직원이나 경찰, 소방대원 등이 신뢰기관 서버에게 자동차 정보에 대한 조회나 처리를 위해서 통신을 요청한다.

2 단계 : 신뢰기관 서버와 프록시 사이의 통신요청 전달 및 처리 - 신뢰기관 서버는 정상적인 통신에 대해서 프록시에게 정보 요청 및 전달을 수행한다.

3 단계 : 프록시와 스마트 자동차 사이에서의 사전 정보 수집 및 처리 과정 - 스마트 자동차들은 사전에 프록시에 주기적으로 신뢰기관이 배포한 공개키를 사용해서 프록시에 상태 정보를 전송해서 처리 및 저장해 둔다.

4 단계 : 프록시 서버와 정보 요청자 사이의 인증 확인 및 정보 재암호화를 통한 전송 - 프록시 서버는 정보를 요청한 사용자의 권한을 속성 기반으로 확인하고, 정상적인 사용자임이 확인된 경우에만 스마트 자동차로부터 주기적으로 수집된 정보들을 재-암호화해서 전달한다.

제안 시스템은 4 단계의 처리절차를 통해서 사용자에 대한 신분 인증, 자동차 차체에 대한 인증, 속성기반 권한 위임, 데이터 암호화, 재-암호화 및 전송이 안전하게 수행한다.

3.3 FIDO(Fast IDentity Online) 기반의 차체 인증기법

제안 모델에서는 FIDO를 기반으로 자동차 차체에 대한 인증을 추가로 실시하고, 차량 사고 발생이나 도난과 같은 상황에서도 원격 제어가 가능하도록 하고자 한다. 뿐만 아니라 자동차 도난 사고 상황에서 오용을 방지할 수 있도록 하고자 한다.

이를 위해서 먼저 자동차를 구입 후 곧바로 정당한 자동차 사용자는 자신이 자동차의 올바른 사용자임을 증명하기 위한 소유 증명 작업을 실시한다. 이를 위해서 자동차 소유자는 제 3 자의 신뢰할 수 있는 기관에 자동차 차대 정보와 함께 자신의 지문 정보를 등록한다. 이렇게 등록된 소유자의 지문 정보는 자동차를 원격 제어나 위치 추적 등에 있어서 사용할 수 있도록 권한을 위임할 수도 있게 한다. 일반적으로 이런 기능은 자동차를 사용하는 경우에는 자동차의 문을 열거나 시동을 걸고자 하는 때도 이용할 수 있을 것이다.

하지만 자동차 소유자가 주행하는 동안 의료사고가 발생하거나 자동차 소유자가 지정한 사용자가 사무실 밖에 있을 때와 같이 특별한 상황에서는 경찰이나 소방대원과 같은 사람이 자동차문을 열거나 시동을 끄고자 할 때 권한을 위임하도록 하여서 원격 제어가 가능하게 한다.

4. 제안모델 분석

앞서 연구 제안 단계에서 밝힌바와 같이 스마트 자동차 네트워크에서 발생 가능한 10가지 정도의 다양한 취약점들 중에서 본 연구에서는 아래의 3가지 사항에 대해서 높은 관심을 가지고 있다. 뿐만 아니라 이를 해결할 수 있는 스마트 자동차 네트워크를 구성하기 위한 모델을 제안하였다.

본 연구에서 제안한 모델이 앞서 기술한 보안취약점들에 대해서 얼마나 안전할지 검토해 볼 결과를 적는 것으로 연구의 결과를 가늠해 보았다.

4.1 기밀성

본 연구에서 제안한 모델은 국제 표준인 AES-256 암호 알고리즘을 사용한 암호화와 복호화를 적용함으로써 스마트 자동차로부터 수집된 정보를 스마트 신호등이나 프록시 서버, 신뢰기관에 전달하기 위해서 사용하도록 하였다. 이를 통해서 수집된 자동차 위치 정보, 교통 정보 등에 대한 기밀성을 보장할 수 있다. 뿐만 아니라 이를 통해서 중간자 공격에 대해서도 안전함을 보장할 수 있다.

4.2 무결성

제안 모델에서는 전송된 데이터에 대한 무결성을 보장하기 위해서 국제 표준인 MD5 알고리즘을 사용해서 무결성을 보장할 수 있도록 설계하였다. 이를 통해서 중간자 공격이나 위.변조 공격으로부터 데이터가 무결함을 보장할 수 있다.

물론 최근의 컴퓨팅 파워나 처리 능력을 고려한다면 SHA-256과 같은 고 성능의 무결성 알고리즘을 적용할 수도 있으나, 스마트 자동차와 통신하는 교통 신호등이나 정보 수집에 사용하는 센서 장치들을 고려해서 MD5를 사용하도록 설계하였다. 향후 연구에서는 이를 개선하도록 노력할 것이다.

4.3 재-사용 공격

제안 모델에서는 MD-5 알고리즘을 사용해서 스마트 자동차로부터 수집된 정보들을 여러 대의 교통 신호등을 거쳐서 프록시 서버로 전송하도록 설계하였다. 이 과정에서 앞서 사용된 비밀키나 시간값, 위치값 등을 재-사용하는 것을 방지하기 위해서 MD-5 해쉬값을 생성할 때, 자체적으로 시간값을 해쉬화해서 포함하도록 설계하였다. 이를 통해서 재-사용 공격이 불가능하도록 하였다.

이외에도 앞서 설명하였던 다양한 스마트 자동차 네트워크에서 발생 가능한 보안 취약점들에 대한 제안 모델의 안전한지 여부를 단순하게 비교. 정리한 것을 표 2에 나타내었다.

<표 2> 제안 모델의 보안취약점 분석

Security item	Support
Uni-directionality	○
Data-confidentiality	○
Non-Interaction	○
Intransitively	○
Re-encryption control	○
Master key security	○
User/Attribute revocation	○
Multi-use	X
Collusion prevention	△
Man-in-the-Middel attack	△

표 2에서 나타내고 있는 바와 같이 다양한 보안 취약점 들 중에서 제안 시스템은 다중 사용자 공격에는 취약할 것으로 예상된다. 뿐만 아니라, 충돌 회피와 중간자 공격에는 다소 취약하나 안전성만을 제공할 수 있다.

5. 결 론

본 논문에서는 속성 기반 암호화 알고리즘과 FIDO 기반 사용자 인증 구조를 사용하여 스마트 자동차 네트워크 환경에서 발생할 수 있는 8 가지 보안 취약점들에 대해서 해결 방안을 제시하였다.

스마트 자동차 네트워크 환경에서 발생할 것으로 예상되는 8 가지 취약점들 중에서 대표적인 3 가지 보안 취약점에 대해서는 완벽하게 보장할 수 있음을 보였다. 첫째, 자동차 소유자가 자신의 자동차를 정확하게 증명할 수 있도록 하는 사용자 인증 서비스를 제공할 수 있다. 두 번째로 교통경찰이나 구급대원이 자동차 소유자에게 소유 권한을 위임 받아서 스마트 자동차의 교통사고나 절도와 같은 위급 상황에서도 유연하게 처리할 수 있도록 하였다.

이외에도 제안한 연구 모델에서는 앞으로 더욱 많은 향후 연구를 수행할 것이다. 제안모델에 대한 일부 구현 및 시뮬레이션만이 시행되었으며, 향후 이를 위한 좀 더 많은 실험과 시뮬레이션을 통한 실험 결과를 제시하고자 한다.

참고문헌

[1] Gartner, "Predicts 2010: Social Software Is an Enterprise Reality", Dec., 2009.

[2] Final report of the Social Web Incubator Group, http://www.w3.org/2005/Incubator/ socialweb /wiki/FinalReport, W3C

[3] Open Mobile Alliance(OMA), "White Paper on Mobile Social Network work Item Investigation", May 16, 2011.

[4] Jeremiah Owyang, "The Future of the Social Web", Forrest Research, April 27, 2009.

[5] Ed H. hi, "The Social Web: Reaearch and Opportunities", Computer, Vol. 41, Issue 9, pp.88-99, Sept., 2008.

[6] Won Kim, Ok-Ran Jeong, Sang-Won Lee, "On social Web sites", Information Systems, Vol, 35, Issue 2, pp. 215-236, April, 2011.

[7] John G. Breslin, Alexnadre Passant, Stefan Decker, "The Social Semantic Web", Springer, 2010, ISBN: 978-3-642-01171-9

[8] Jeremiah Owyang, “A Collection of Social network Stats for 2010:, http://j.mp/dnXxlz

[9] Yoo-jin Lee, Seung-Jin Kwak, “A Study on the Activation of Social Network Service of University Libraries”, 18th Korea Information Management Society, 2010.

[10] Chen Xu., Fenfei. Ouyang, and Heting Chu, “The Academic Library Meets Web 2.0: Applications and Implications”, The Journal of Academic Librarianship, 35(4), pp. 324-331, 2009.

[11] Hong, K., Lillethun, D., Ramachandran, U., Ottenwälder, B. and Koldehofe, B., Mobile fog: A programming model for large-scale applications on the internet of things. In Proceedings of the second ACM SIGCOMM workshop on Mobile cloud computing, ACM 2013;15-20.

[12] LOKE, Seng W. The internet of flying-things: Opportunities and challenges with airborne fog computing and mobile cloud in the clouds. arXiv preprint arXiv:1507.04492, 2015.

[13] 이명렬, 박재표, 스마트카 정보보안 침해위협 분석 및 대응방안 연구, 한국산학기술학회논문지, 제18권 제3호, pp.374-380, 2017.

[14] You-Jin Song, Jin-Mook Kim, Characterization of privacy based on context sensitivity and user preference for multimedia context-aware on IoT, Multimedia Tools and Applications (2018), https://doi.org/10.1007/s11042-018-6103-5, 2018.

[15] Hyung-Jong Cha, Ho-Kyung Yang, Jin-Mook Kim, You-Jin Song, A Study on Data Processing for Application of Vehicular CPS in Fog Computing Environment, Advanced Science Letters, Vol. 23, No. 10, pp. 10379-10383, 2017.

[저 자 소 개]

김 진 묵 (Jin-Mook Kim)
1998년 2월 : 배재대학교 전자계산학과(이학사)
2000년 2월 : 배재대학교 컴퓨터공학과(공학석사)
2006년 2월 : 광운대학교 컴퓨터과학과(공학박사)
2006년 9월 ~ 2008년 2월 : 선문대학교 컴퓨터공학과 연구교수
2006년 9월 ~ 현재 : 선문대학교 IT교육학부 부교수

관심분야 : 정보보호, 네트워크 보안, 사용자 인증, 빅-데이터 분석
E-Mail : calf0425@sunmoon.ac.kr

문 정 경(Jeong-Kyung Moon)
1993년 2월 : 배재대학교 원예학과(학사)
2006년 2월 : 단국대학교 인터넷정보학과(공학석사)
2013년 2월 : 공주대학교 컴퓨터공학과(공학박사)
2012년 3월 ~ 2월 : 선문대학교 IT교육학부 계약교수
2018년 3월 ~ 현재 : 가천대학교 소프트웨어중심대학 초빙교수

관심분야 : 클라우드 컴퓨팅, N-스크린, 네트워크, 정보보안, 빅데이터 분석
E-mail : jkmoon@gachon.ac.kr

황 득 영 (Deuk-Young Hwang)
1988년 2월 : 광운대학교 전자계산학과(이학사)
1990년 2월 : 광운대학교 전자계산학과(공학석사)
1999년 2월 : 광운대학교 전자계산학과 (공학박사)
1990년 3월 ~ 1994년 2월 : 전주 기전대학교 전자계산학과 조교수
1994년 3월 ~ 현재 : 강원대학교 삼척캠퍼스 컴퓨터공학과 교수

관심분야 : 프로그래밍 언어, 컴파일러, 정보보안, 빅-데이터 분석, 소프트웨어 공학
E-mail : dyhwang@kangwon.ac.kr