보안성을 갖춘 NFC 통신 및 생체정보 기반의 운전자 인증 및 차량 제어 시스템 제안

Suggestion of Secure Driver Authentication and Vehicle Control System based on NFC Communication and Biometric Information

저자 (Authors)

박태환, 서화정, 임지환, 김호원

Tae-hwan Park, Hwa-joeng Seo, Ji-hwan Lim, Ho-won Kim

출처 (Source)

한국정보통신학회논문지 22(4), 2018.4, 700-707 (8 pages)

Journal of the Korea Institute of Information and Communication Engineering 22(4), 2018.4, 700-707 (8 pages)

발행처 (Publisher)

한국정보통신학회

The Korea Institute of Information and Communication Engineering

URL

http://www.dbpia.co.kr/Article/NODE07423606

APA Style

박태환, 서화정, 임지환, 김호원 (2018). 보안성을 갖춘 NFC 통신 및 생체정보 기반의 운전자 인증 및 차량 제어 시스템 제안. 한국정보통신학회논문지, 22(4), 700-707.

JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 22, No. 4: 700~707, Apr. 2018

보안성을 갖춘 NFC 통신 및 생체정보 기반의 운전자 인증 및 차량 제어 시스템 제안

박태환[1] · 서화정[2] · 임지환[2] · 김호원[1*]

Suggestion of Secure Driver Authentication and Vehicle Control System based on NFC Communication and Biometric Information

Tae-hwan Park[1] · Hwa-joeng Seo[2] · Ji-hwan Lim[2] · Ho-won Kim[1*]

[1*]School of Electrical and Computer Engineering, Pusan National University, Busan, 46241 Korea
[2]Department of IT, Hansung University, Seoul, 02876 Korea

요 약

자동차는 편리한 운송 기반 시설로써 우리생활에 폭넓게 활용되고 있으며, 운전자에 의해 차량의 모든 동작이 결정된다는 특징으로 운전자에 대한 적합한 인증이 중요하다. 특히 음주운전에 따른 다양한 사고로 인해 음주 시동 잠금장치 장착제도에 대한 도입 논의가 활발하며, 이러한 음주 시동 잠금장치 장착에 있어서 많은 비용과 시간이 소모된다는 단점이 있다. 장애인 및 국가유공자인 운전자에 대한 할인 혜택 제공에 있어서 사용자의 불편함 해소를 위한 적합한 사용자 인증이 필요한 상황이다. 이러한 문제점을 해결하고자 본 논문에서는 사용자의 스마트폰을 이용한 NFC 통신과 생체정보 기반의 운전자 인증을 통한 음주운전 방지, 장애인 및 국가유공자 혜택을 제공하는 효율적인 차량제어 및 사용자 인증 시스템을 제안하고자 한다.

ABSTRACT

Vehicles are used in daily life as convenient transport, it is important to authenticate driver because vehicles are controlled by driver. Especially, in these days, there is a discussion on introduction of Driving Under the Influence car-starting locking device installation for preventing accidents caused by Driving Under the Influence of alcohol, these car-starting locking device installation requires a lot of money and time. Suitable user authentication for solving user's inconvenience during the disabled and men of national merit to receive discount benefits is needed. In this paper, For solving these problems, we propose the efficient vehicle control and user authentication system for preventing driving under the influence and providing the disabled and men of national merit benefit based on driver authentication by using user's smartphone NFC communication and user's biometric information.

키워드 : 사용자 인증, 생체 정보, NFC 통신, 차량 제어

Key word : User Authentication, Biometric Information, NFC Communication, Vehicle Control

Received 3 January 2018, **Revised** 1 February 2018, **Accepted** 30 March 2018

*** Corresponding Author** Ho-Won Kim(E-mail:howonkim@pusan.ac.kr, Tel:+82-51-510-1010)
School of Electrical and Computer Engineering, Pusan National University, Busan, 46241 Korea

Open Access http://doi.org/10.6109/jkiice.2018.22.4.700 pISSN:2234-4772

Ⅰ. 서 론

자동차는 사용자를 안전하고 편안하게 원하는 위치로 운송해주시는 기반 시설로써 일상생활에 많이 사용된다. 하지만, 운전자에 의해 자동차의 모든 동작이 결정되는 특징으로 인해 자동차 운전자에 대한 적합한 인증이 필요하다. 이러한 자동차의 특징으로 인해 운전자의 음주운전 시, 운전자와 보행자 모두에게 위험한 사고로 이어질 수 있기 때문에 최근 이를 근절하기 위한 음주 시동잠금장치 장착 제도에 대한 도입 논의가 활발히 이루어지고 있다. 이와 더불어 국내의 장애인 및 독립유공자, 국가유공자에 대한 관련 법률에 의해, 법률의 대상자들에게 주어지는 주차 및 통행료 할인 혜택의 경우, 지문 인증을 통한 운전자 인증을 위한 추가적인 감면 인식기 설치 및 4시간 경과 시 재인증이 필요한 구조로 되어 있어 인식기 설치비용 및 사용자의 불편성 등과 같은 문제점을 가지고 있다. 이러한 문제를 해결하기 위해 운전자 편의성을 고려한 운전자 인증을 통한 사회적 공적 자금 낭비를 방지할 필요가 있다. 이를 보완하기 위해, 기존의 FIDO (Fast IDentity Online) 인증과 NFC 기반 출입 시동 등이 있지만, 물리적 탈취 및 오용 가능성이 높으며, 소유자 중심의 키 공유 방식이라는 문제점을 가지고 있다. 본 논문에서는 이러한 문제점을 해결하고자 NFC 통신과 생체정보 기반의 운전자 인증을 통한 차량 제어 시스템을 제안하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서 음주운전 측정 및 방지 기법과 사용자 인증 및 차량 제어에 대한 연구 동향에 살펴보며, 3장 본론에서는 제안 기법과 제안기법에 대한 평가에 대해 살펴본다. 마지막 4장에서 본 논문의 결론을 맺고자 한다.

Ⅱ. 관련 연구 동향

본 장에서는 음주 운전 측정 및 방지 관련 연구와 사용자 인증 및 차량 제어 관련 연구 동향에 대해 살펴본다.

2.1. 음주 운전 측정 및 방지 관련 연구 동향

본 절에서는 음주 운전 측정 및 방지 관련 연구 동향에 대해 살펴본다. 2016년 11월에 교통과학연구원에서는 음주 시동잠금장치 기술 동향과 해외 음주 시동잠금장치 도입 추세 및 관련 기술 적용 방법과 도입 가능성에 대해서 제시하고 있다[1]. 현재 음주측정에 사용되는 검지 방식은 크게 3개로 나누어질 수 있으며, 반도체 방식의 경우, 응답성이 우수하고 저렴한 가격의 장점을 가지지만, 외부 요인에 따라 정확도의 변화가 크다는 단점이 있으며, 전기 화학식의 경우, 정밀도는 높지만, 응답성이 떨어지는 단점을 가지고 있다. 마지막으로 비분산형 적외선식은 장기간 안정적 측정이 가능하나, 차량 환경으로의 적용에 있어서 어려움이 있다는 단점이 있다 [1]. 해외의 경우, 2011년 7월부로 유럽의회에서는 모든 차량의 음주 시동잠금장치의 의무적 장치를 이행하도록 하고 있으며, 프랑스의 경우, 2010년 이후, 캐나다는 1990년 앨버타주를 시작으로 현재 11개 주 및 준주에서 음주 시동잠금장치 프로그램과 음주 운전위반자에 대한 일정 기간의 의무 탑재를 시행하고 있다. 미국의 경우, 2016년 기준 25개 주에서 모든 음주 운전자에 대한 시동잠금장치 설치를 의무화하고 있다 [1]. 관련 기술 적용 방법 및 도입 가능성과 관련하여 (1) 대리 시동 등 부정 사용 방지 기술, (2) 시스템 보안 기술, (3) 긴급 시 음주 시동잠금장치 해제 기술, (4) 불법개조 방지 기술, (5) 음주측정 기술에 대한 적용 방식과 국내 도입 가능성에 대한 의견이 있었으며, 실제 음주 시동잠금장치를 통해 음주 운전의 재범률 감소 효과가 인정되고 있다[1, 2]. 이와 관련하여 삼성전자는 미국에서 내장형 스마트폰 음주측정기에 대한 특허 출원을 하였으며, 향후 삼성전자의 스마트폰에 적용하고자 하며 이와 관련된 애플리케이션까지 개발을 완료한 상태이다 [3]. 이와 유사한 사례로 2012년 미국 경찰에서 실제 이용하는 '필드 소브라이어티 테스트' 기반으로 아이폰/아이패드용 음주운전 방지 애플리케이션이 등장하였었다 [4].

2.2. 사용자 인증 및 차량 제어 관련 연구 동향

본 절에서는 사용자 인증 및 차량 제어와 관련된 최신 연구 동향에 대해서 살펴본다. 사용자 인증 기법과 관련하여 스마트폰과 스마트워치를 활용한 사용자 인증 기법 연구 [5] 가 있으며, 스마트폰에서 많이 사용되는 안드로이드 환경에서의 보안 위협과 보호 기법에 대한 연구 결과 [6] 가 있다. 이처럼 최근 스마트폰 및 PC 환경 상의 사용자 인증 및 보안에 대한 연구가 활발히 이루어지며, 이에 따라 스마트폰 및 PC 환경상에서의

간편한 금융 거래를 위해, FIDO (Fast IDentity Online) 프로토콜을 많이 사용한다 [7]. FIDO 프로토콜은 사용자 인증 토큰과 공개키 등록 과정과 사용자 인증 과정으로 구성되며, 사용자의 생체 정보를 활용하며, 사용의 편리성이 있다는 장점이 있다[7]. 하지만 이러한 FIDO 프로토콜은 개인별 금융 서비스에 초점이 맞춰져 있어서 제3자와의 거래 및 통신에 있어서 사용 불편성을 가지고 있다. 다음으로는 차량 간 통신 기반의 V2X 환경에서의 보안 관점에서 IEEE 1609.2를 중심으로 한 보안구조 및 차량용 PKI 시스템 구축 연구 결과가 있으며 [8], 올해 현대 자동차 그룹에서는 스마트폰의 NFC 통신을 활용하여 차량용 출입 시동 시스템을 구축하였다 [9]. 해당 시스템은 사용자의 스마트폰을 통한 사용자 인증과 NFC 기반의 차량 출입 시동이 가능하며, 이를 위한 웹 기반의 사용자 등록 및 인증 구조를 가지며, NFC 카드키 기반의 제 3자의 차량 출입 시동이 가능하게 하였다. 하지만 해당 시스템에서는 NFC 카드키의 도난, 오/남용과 같은 물리적 보안 취약성이 발생할 수 있으며, NFC 카드키를 가진 이에 대한 사용자 인증이 어렵다는 측면이 있으며, 음주운전 방지 및 장애인/국가유공자 혜택과 같은 차량에서의 응용서비스 연계성을 가지지 못하고 있다. FIDO 환경 상에서의 다중 생체 정보를 사용한 인증 방법에 대한 연구 결과 [10]가 있으며, 해당 논문에서는 FIDO에서 사용되는 주요 생체 정보 인식 기술 중 지문 인식의 장점으로 저렴한 비용으로 도입이 가능한 특징이 있으며, 신뢰도, 안정도 측면에서 높다는 장점을 가지지만, 지문 인식 장치에 습기가 있는 경우, 인신 오류율이 높아지며, 복제가 가능하다는 단점 등이 있으며, 홍채 인식의 경우, 홍채가 훼손되는 경우를 제외하고는 복제할 수 없으며, 통계학적으로 높은 정확도와 안경을 착용한 상태에서도 인식할 수 있는 특징을 가진다. 얼굴인식 기술의 경우, 2차원 정보 기반의 인식 기술은 정확도가 낮지만 저렴하다는 장점을 가지며, 3차원 영상의 경우, 높은 정확도를 가지지만, 큰 비용이 든다는 단점을 가지고 있다. 음성인식 기술의 경우, 복제할 수 없다는 장점을 가지지만, 음성 특징 추출 장치에 의한 인식률 차이 발생 문제와 사용자의 건강 상태 (감기 혹은 후두염으로 인한)에 따른 음성적 특징이 변경될 수 있다는 단점을 가진다. 앞서 설명한 바와 같이 다양한 생체 정보 인식 방식에 있어서 각각의 장/단점을 가지며, 본 논문에서는 이러한 다양한 생체 정보 인식 방식에 대해 생체 정보 인증토큰 목록 방식 기반의 사용자 선택 방식을 통한 운전자 등록/인증 및 차량제어 시스템을 제안하고자 한다.

Ⅲ. 본 론

본 장에서는 앞선 최신 연구 동향에서의 문제점을 해결하는 제안 기법에 대한 소개 및 평가에 관해 설명한다.

3.1. 제안 기법

본 논문에서 제안하고자 하는 기법은 크게 (1) 사용자 등록 과정과 (2) 사용자 인증과정으로 나누어질 수 있으며, (2) 사용자 인증과정의 경우, 공통부분과 차량 주인의 음주 운전에 따른 대리운전기사 운전 상황으로 나누어질 수 있다. 그리고 이러한 사용자 등록 및 인증 과정과 더불어 음주 운전 방지를 위한 기법 또한 제안하고자 한다.

3.1.1. 사용자 등록 과정

본 논문에서 제안하고자 하는 기법의 사용자 등록과정에서는 등록하고자 하는 사용자의 스마트폰과 제안 기법에서 사용되는 인증기관 (Certification Authority, CA)과의 통신을 통해 이루어진다. 먼저 사용자의 등록을 위해, 사용자는 인증기관 (CA) 에게 운전자 등록 요청을 전송하게 된다. 이후, 인증기관에서는 자신이 처리할 수 있는 인증토큰 목록 (지문, 얼굴인식, 홍채 인식 등의 생체정보 인증 토큰 목록)을 사용자에게 전달함과 동시에 사용자의 공개키 (PU_{usr})를 요구한다. 인증기관의 인증토큰 목록과 공개키 요구를 받은 사용자 (운전자)는 자신의 스마트폰에서 처리가 가능한 인증 토큰을 선택하여, 해당되는 생체정보 기반 인식 및 인증을 통해, 자신의 개인키 (PK_{usr})와 공개키 (PU_{usr})를 생성한다. 이후, 사용자는 자신의 개인키를 기반으로 자신의 공개키, 사용한 인증토큰정보, 운전자 유형 (차량 주인, 대리기사 등의 운전자 유형을 의미), 장애인/국가유공자관련정보 (장애인/국가유공자인 경우, 관련 정보를 포함, 아닌 경우에는 NULL로 표기)를 연결한 데이터에 대한 전자 서명한 결과와 자신의 공개키를 인증기관 (CA)에 전달한다. 인증기관 (CA)은 사용자로부터 사용자의 공개키 정보와 사용자의 개인키로 전자 서명된 데

이터에 대한 검증 이후, 해당 사용자의 정보를 등록한다. 이후, 사용자의 공개키 정보와 사용자의 개인키로 전자 서명된 데이터의 연결된 정보에 대해 인증기관의 개인키 (PK_{CA})로 전자 서명한 데이터와 인증기관의 공개키 정보 (PU_{CA})를 사용자에게 전달함으로써 사용자 등록과정이 끝나게 되며, 그림 1은 사용자 등록과정의 순서를 나타낸다.

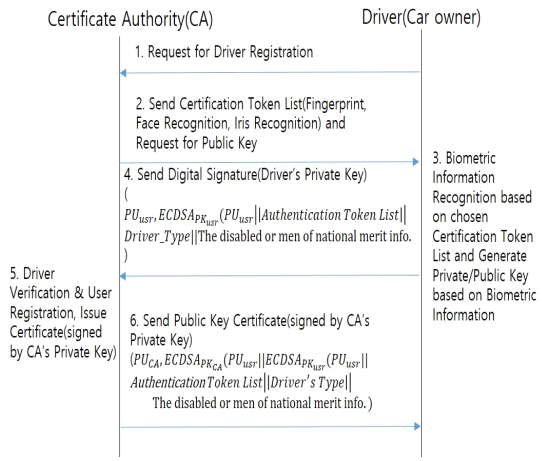

Fig. 1 User Registration of the Proposed Method

3.1.2. 사용자 인증 과정 (공통)

앞선 3.1.1.에서는 제안 기법의 사용자 등록 과정에 대해 살펴보았다. 본 절에서는 사용자 등록 과정 이후, 장애인/국가유공자 인증과정을 포함한 사용자 인증 과정의 공통적인 부분에 관해 설명한다. 해당 과정에서는 인증하고자 하는 사용자, 사용하고자 하는 차량의 운전자 인증을 위한 ECU 간의 NFC 통신 기반의 통신과 차량의 운전자 인증을 위한 ECU와 인증기관 간의 통신으로 구성된다. 사용자의 인증을 위해, 사용자는 먼저 사용하고자 하는 차량의 운전자 인증을 위한 ECU에 운전자 인증 요청 (운전자의 공개키 정보 포함)을 시도한다. 사용자로부터 운전자 인증 요청을 받은 차량의 운전자 인증을 위한 ECU는 운전자의 공개키를 사용하여 Nonce와 인증토큰 목록을 암호화하여 전달한다. 이후 사용자는 차량의 운전자 인증을 위한 ECU로부터 전달받은 인증토큰 목록 중 자신이 인증기관에 사용자 등록 시 사용한 인증 토큰 방식을 선택하여 인증하게 되며, 인증 완료 여부에 따라 Nonce를 처리하며, Nonce 처리 결과와 자신이 사용한 인증토큰 정보의 연결한 데이터에 대해 사용자의 개인키로 전자 서명한 후, 자신의 공개키 정보와 함께 차량의 운전자 인증을 위한 ECU로 전달한다. 이때, 전자서명을 하고자 하는 데이터의 종류는 크게 2가지이며, 음주 운전 측정의 필요 유무에 따라 나누어질 수 있다. 음주 운전 측정이 필요한 경우에 대해서는 3.1.4절에서 상세히 설명하고자 하며, 음주 운전이 필요하지 않은 경우, 사용자는 자신의 운전자 유형과 장애인/국가유공자 정보의 연결한 데이터를 앞서 말한 공통적인 부분 (Nonce 처리결과||인증토큰) 뒤에 연결하여 전자 서명을 진행한 후, 전송하게 되며, 음주 운전 측정이 필요한 경우, 운전자 유형과 음주측정결과를 공통적인 부분 뒤에 연결하여 전자 서명 처리 후, 전송하게 된다. 관련 정보를 전달 받은 차량의 운전자 인증을 위한 ECU는 운전자의 공개키 정보에 대해 자신의 개인키 (PK_{ecu})로 암호화하여 자신의 공개키 정보와 함께 인증기관 (CA)에게 운전자의 공개키 인증서를 요청한다. 운전자의 공개키 인증서 요청을 받은 인증기관은 사용자의 공개키 정보를 통해, 해당 운전자의 공개키 인증서와 인증기관의 공개키를 차량의 운전자 인증을 위한 ECU에 전달한다. 이후, 차량의 운전자 인증을 위한 ECU는 인증기관으로부터 전달받은 운전자의 공개키 인증서를 기반으로 관련 정보의 인증과정을 거친 후, 인증 결과를 운전자에게 전송한다. 이때, 인증 결과는 (1) 인증 완료||시동 가능, (2) 인증 완료||시동 불가능(음주운전의 경우), (3) 인증실패로 크게 3가지로 나눌 수 있다. 인증 결과가 (2) 에 해당하면 인증을 요청한 사용자의 음주운전 시도에 해당하며, 음주 운전을 막고자 추후 과정이 필요하며, 관련 과정에 대해서는 3.1.3.절에서 설명한다. 그림 2는 장애인/국가유공자 인증과정을 포함한 사용자 인증 과정의 공통적인 부분의 순서를 나타낸다.

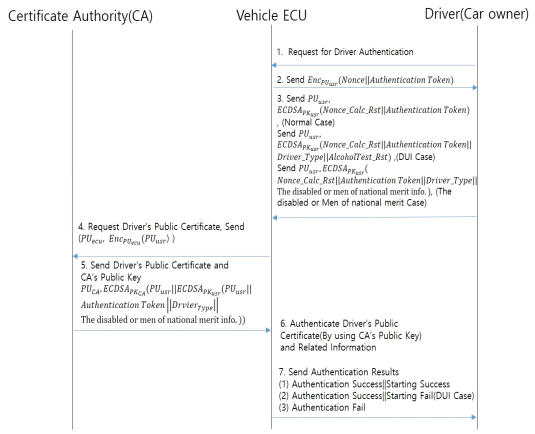

Fig. 2 User Authentication(Common) of the Proposed Method

3.1.3. 사용자 인증 과정 (대리운전)

본 절에서는 앞선 3.1.2절에서의 사용자 인증 결과가 (2) 인증 완료||시동 불가능에 해당하면 추후 적인 과정 및 대리운전기사 인증과정에 관해 설명한다. 사용자 인증 결과가 (2) 인증 완료||시동 불가능에 해당하면 자동적으로 사용자 스마트폰의 대리운전기사 호출 애플리케이션을 실행함과 동시에 현재 위치를 기반으로 대리운전기사를 호출하게 된다. 호출한 후, 대리기사 배정 완료 시, 배정된 대리기사의 공개키 및 공개키 인증서 (인증기관으로부터 이미 발급된 공개키 인증서)를 전송받아 사용자의 개인키로 전자 서명하여 차량의 운전자 인증을 위한 ECU로 전달하게 된다. 이후, 배정된 대리운전 기사가 차량에 탑승한 후, 탑승한 차량에 앞서 설명한 3.1.2. 절에서의 사용자 인증과정과 같은 과정의 사용자 인증 절차를 진행하며, 3.1.2절의 과정을 통해 인증기관으로부터 전달받은 대리운전기사의 공개키 정보 및 공개키 인증서와 사용자(차량 주인)로부터 전달받은 대리운전기사의 공개키 정보 및 공개키 인증서 간의 비교 과정과 현재 대리운전기사의 위치 정보를 포함하여 인증 요청 (앞선 3.1.2절의 인증과정에서 위치 정보만 추가됨)함으로써 현재 차량의 운전석에 탑승한 사람이 대리운전기사임을 확인할 수 있도록 하였다. 이러한 과정을 통한 인증 결과를 대리기사에게 전달하여 차량 시동 및 제어를 할 수 있도록 하여 음주 운전을 막을 수 있도록 하였다. 하지만 대리운전기사에 대한 운전자 인증과 앞선 3.1.2절에서의 운전자의 장애인/국가유공자 인증 완료 이후, 타인으로의 운전자 변경과 같은 운전자 변경이 발생할 수 있으며, 이에 대한 대응 방안이 필요하다. 이와 관련된 대응방안은 3.1.4절에서 자세히 설명하고자 한다. 그림 3은 3.1.2절의 인증결과가 음주운전인 경우, 대리운전기사에 대한 인증과정을 포함한 추후 과정에 대한 순서를 나타낸다.

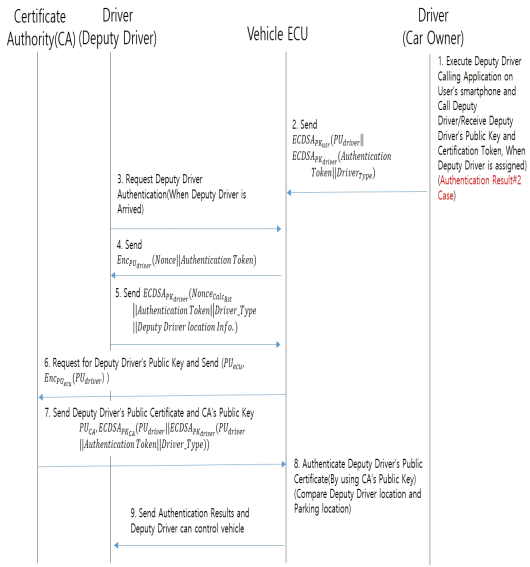

Fig. 3 User Authentication(Driving Under the influence of alcohol) of the Proposed Method

3.1.4. 운전자 변경 및 음주 운전 방지 기법

본 절에서는 앞서 설명한 3.1.2절과 3.1.3절에서 발생할 수 있는 사용자 인증 후, 운전자 변경 및 음주 운전 방지를 위한 기법에 관해 설명한다. 먼저 앞서 설명한 3.1.2절과 3.1.3절에서의 사용자 인증과정은 사용자 (차량 주인 및 대리운전 기사)의 차량 탑승 후, 차량의 문이 닫힌 상태에서 진행되며, 사용자 인증 완료 후, 바로 차량 엔진 점화를 통한 차량 제어를 시작하지 않고, 운전자의 안전을 위해, 안전벨트 착용 여부 확인 후, 안전벨트 착용 후 차량 제어가 가능하도록 한다. 이때, 차량의 탑승 인원 확인을 위해서 차량의 개폐되는 문의 개수 및 탑승 인원 증가에 따른 차량 진동을 응용하여 확인할 수 있도록 하였다. 이후 차량 주행 중 차량 정차 시, 현재 차량의 위치와 목적지 비교와 차량의 문 개폐 여부를 확인한다. 이때, 차량 주인이 운전하는 경우, 차량

문이 1개 이상 열릴 시, 대리운전 기사가 운전하는 경우, 차량 문이 2개 이상 열릴 경우, 운전자에 대한 사용자 재인증 요구를 통해, 사용자 초기 인증 이후, 운전자 변경을 통해 발생할 수 있는 음주운전 및 타인의 장애인/국가유공자 혜택을 방지할 수 있도록 관련 기법을 설계하였다.

3.2. 제안 기법 평가

본 장에서는 본 논문에서의 제안기법과 기존 연구 간의 평가 내용 및 결과에 관해서 설명하고자 한다. 제안기법의 특성 평가를 위해, 기존의 연구인 FIDO 프로토콜 방식 [7] 과 현대자동차의 스마트폰 NFC 출입 시동 시스템 [9] 과 비교 분석을 진행하였다. 비교 평가 결과는 표 1과 같다. 기존의 FIDO 프로토콜 방식 [7] 의 경우, 사용자의 생체정보 기반으로 보안성을 제공하며, 다양한 응용 서비스와의 연계성을 통해, 최신 다양한 분야에서 활용되고 있지만, 사용자 개인의 생체정보를 사용한다는 측면에서 제 3자에 대해 사용 연계성은 제공하지 않는다는 단점을 가진다. 현대자동차의 스마트폰 NFC 출입 시동 시스템 [9] 의 경우, 사용자의 생체정보 기반이 아닌 NFC 카드키 방식으로 차량 출입 및 시동을 제어하는 시스템이다. 해당 시스템에서는 제3자를 위한 NFC 카드키 양도 방식으로 제3자에게 차량의 출입 및 제어 권한을 위임 또는 양도할 수 있지만, 보안적 측면에 있어서 NFC 카드키 도난 시 보안 문제 및 차량 탈취 등의 문제가 발생할 수 있으며, 해당 시스템은 차량 출입 및 시동 제어에 초점을 맞춘 상태로써, 다른 응용 서비스와의 연계성을 고려하지 않고 있다. 표 1에서의 제안기법 평가를 통해, 본 논문의 제안기법은 기존의 생체정보 기반의 사용자 인증 프로토콜에서의 단점인 제 3자의 인증 및 서비스 연동 불가능을 해결하며, 이를 통한 생체정보 기반의 사용자 등록/인증과 제 3자(대리운전 기사)에 대한 인증이 가능하며, 가장 최근의 사용자 인증 및 차량 제어 시스템인 현대 자동차의 스마트폰 NFC 출입 시동 시스템이 가지고 있던 웹 사이트 기반의 사용자 등록 및 인증과 제 3자에 대한 권한 부여 시 발생할 수 있는 물리적 탈취 및 오/남용의 문제를 해결할 수 있었으며, 더 나아가 음주운전 방지와 장애인/국가유공자 차량 혜택과 같은 응용 서비스 연계와 사용자의 효율성 확보에서의 장점을 가진다는 것을 확인할 수 있다.

Table. 1 Comparison Results among the Proposed methods and previous works

	FIDO Protocol [7]	Smart phone NFC Access Starting System [9]	Proposed Method
Third-Party Use Connectivity	X	O	O
Providing Security	O	X	O
Using Biometric Information	O	X	O
Application Service Connectivity	O	X	O

표 2에서는 기존 연구와 제안 기법 간 가지는 장, 단점에 관해 설명하며, 이를 통해, 제안 기법이 기존 연구에서의 단점인 제 3자에 대한 서비스 제공 및 보안 취약성 문제를 해결한다는 것을 확인할 수 있다.

Table. 2 Pros and Cons among the Proposed methods and previous works

	Advantage	Disadvantage
FIDO Protocol [7]	• Using Biometric Information • Providing Security • Application Service Connectivity	• Not Supoort 3rd Party Use Connectivity
Smart phone NFC Access Starting System [9]	• Supoort 3rd Party Use Connectivity	• Security Vulnerability
Proposed Method	• Using Biometric Information • Providing Security • Application Service Connectivity • Supoort 3rd Party Use Connectivity	-

Ⅳ. 결 론

본 논문을 통해 최근 사회적으로 논의되고 있는 음주 시동잠금장치와 관련하여 스마트폰과 NFC 통신을 활용하여 사용자 생체정보 기반의 사용자 등록, 사용자 인증 기법 및 음주운전 방지 기법을 제시하였다. 이를

통한 운전자의 음주 운전 방지, 장애인/국가 유공자의 경우, 인증을 통한 관련 혜택을 효율적으로 받을 수 있는 기법을 제안하였으며, 제안 기법을 통해, 제 3자의 인증을 통한 안전한 차량 제어권 이양 또한 가능하며, 기존 연구 대비 사용자의 사용 편리성 및 관련 서비스와의 연계성이라는 장점을 가진다. 향후, 본 논문에서의 제안 기법에 대한 추가적인 수정 보완을 통한 실제 차량 환경으로 응용 및 적용을 수행하고자 한다.

ACKNOWLEDGEMENT

This research of Taehwan Park was supported by the Energy Technology Development Program of the Korea Institute of Energy Technology Evaluation and Planning (KETEP), granted financial resource from the Ministry of Trade, Industry & Energy, Republic of Korea. (No. 20152000000170)

This research of Howon Kim was supported by a 2-Year Research Grant of Pusan National University.

This research of Hwajeong Seo was financially supported by Hansung University.

This work of Jihwan Lim was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2017R1C1B5075742).

References

[1] The Road Traffic Authority. Drinking Boot Lock Technology Trends [Internet]. Available: https://www.koroad.or.kr/cmm/fms/epkoroadFileDown.do?board_code=PRBBS_070&board_num=102126&file_num=173624.

[2] The Korea Times. There is a effect of Ignition Interlocking for Drunken Drivers [Internet]. Available: http://ny.koreatimes.com/article/20170913/1075803.

[3] Global Economic. Samsung Electronics Smartphone, transformed into guardian angel to prevent drunk driving [Internet]. Available: http://www.g-enews.com/view.php?ud=2017081609044053370 0af48a60a_1.

[4] The Korea Daily. iPhone Application for preventing driving u nder the influence, providing self test [Internet]. Available: ht tp://koreadaily.com/news/read.asp?art_id=1132420&referer=.

[5] H. J. Seo. "User Authentication Method Using Smartphine and Smartwatch," *Journal of the Korea Institute of Information and Communication Engineering,* vol. 21, no. 11, pp. 2109-2114, Nov. 2017.

[6] J. H. Jang, S. H. Han, Y. K. Cho, U. J. Choe, J. M. Hong, "Survey of Security Threats and Contermeasures on Android Environment," *Journal of Security Engineering*, vol.11, no.1, pp.01-12, Feb. 2014.

[7] S. R. Cho, D. S. Choi, S. H. Jin, H. H. Lee, "Passwordless Authentication Technology-FIDO," *Electronics and Telecommunications Trends*. vol. 29 no. 4, pp. 101-109, Aug. 2014.

[8] Y. S. Lee, S. G. Sim and D. S Kim. "Security technology for V2X communication". *Journal of The Korea Institute of Information Security and Cryptology*, vol. 24, no. 2, pp. 28-34, Apr. 2014.

[9] Hyundai Motor Group. The best clever method for opening car doors and Smartphone NFC Vehicle Access Starting System [Internet]. Available: http://blog.hmgjournal.com/Tech/smartphone-nfc-enter.blg?status=301.

[10] C. J. Chae, H. J. Cho, H. M. Jung, "Authentication Method using Multiple Biometric Information in FIDO Environment," *Journal of Digital Convergence,* vol. 16, no. 1, pp. 159-164, Jan. 2018.

박태환(Tae-Hwan Park)

2013년 2월 : 부산대학교 정보컴퓨터공학부 학사 졸업
2013년 3월~현재 : 부산대학교 전기전자컴퓨터공학과 석, 박사 통합과정
※ 관심분야 : 암호화 구현, IoT 디바이스 보안, 양자 내성 암호

서화정(Hwa-Jeong Seo)

2010년 2월 : 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월 : 부산대학교 컴퓨터공학과 석사 졸업
2016년 2월 : 부산대학교 컴퓨터공학과 박사 졸업
2015년 4월~5월 : 싱가포르 난양공대 인턴쉽
2016년 1월~2017년 3월 : 싱가포르 과학기술청 연구원
2017년 4월~현재 : 한성대학교 조교수
※관심분야 : 정보보호, 암호화 구현, IoT

임지환(Ji-Hwan Lim)

2014년 3월~현재: 한성대학교 IT 융합공학부 학부과정(3학년)
※관심분야 : 사이버보안, 암호화 구현, IoT, 블록체인

김호원(Ho-Won Kim)

1993년 2월 : 경북대학교 전자공학과 학사 졸업
1995년 2월 : 포항공과대학교 전기전자공학과 석사 졸업
1999년 2월 : 포항공과대학교 전기전자공학과 박사 졸업
2008년 2월 : 한국전자통신연구원 정보보호연구단 선임연구원/팀장
2008년 3월~현재 : 부산대학교 전기컴퓨터공학부 정교수
※관심분야 : 스마트그리드 보안, RFID/USN 정보보호 기술, PKC 암호, VLSI 설계, Embedded system 보안, IoT 보안, 블록체인 보안, 양자 내성 암호