Journal of Digital Convergence
Vol. 16. No. 1, pp. 159-164, 2018

ISSN 1738-1916
https://doi.org/10.14400/JDC.2018.16.1.159

FIDO 환경에서 다중 생체정보를 이용한 인증 방법

채철주[1], 조한진[2], 정현미[3*]
[1]한국농수산대학 교양공통과, [2]극동대학교 에너지IT공학과, [3]한국과학기술정보연구원 슈퍼컴퓨터시스템개발실

Authentication Method using Multiple Biometric Information in FIDO Environment

Cheol-Joo Chae[1], Han-Jin Cho[2], Hyun Mi Jung[3*]
[1]Dept. of General Education, Korea National College of Agriculture and Fisheries
[2]Dept. of Smart & PhotoVoltaic Convergence, Far East University
[3]Dept. of Supercomputer System Development, Korea Institute of Science and Technology Information

요 약 생체정보는 저장, 암기, 손실 우려가 없고 도용이 불가능하다는 점에서 패스워드, PKI 등 기존 인증 방법의 대체 수단으로 주목받고 있지만, 개인정보 유출로 인한 프라이버시 침해가 발생한다. 이러한 취약점을 극복하고자 FIDO에서는 생체정보를 사용자 디바이스에 보존하여 인증하는 방식을 사용하여 서버에서의 개인정보 유출 문제를 해결하였다. 본 논문에서는 국내·외에서 활발히 연구되고 있는 FIDO 환경에서 사용할 수 있는 다중 생체정보 인증 방법을 제안한다. 다중 생체정보를 이용하기 위해 지문과 뇌전도 신호를 뇌지문 정보를 생성하여 이를 FIDO 시스템에서 사용할 수 있는 방법을 제안한다. 제안 방법은 현재 기존 2-Factor 인증 체계의 한계로 인한 문제점을 다중 생체정보를 이용한 인증으로 해결할 수 있다.

주제어 : FIDO, 생체정보, 다중 생체정보, 인증, 보안

Abstract Biometric information does not need to be stored separately, and there is no risk of loss and no theft. For this reason, it has been attracting attention as an alternative authentication means for existing authentication means such as passwords and authorized certificates. However, there may be a privacy problem due to leakage of personal information stored in the server. To overcome these weaknesses, FIDO solved the problem of leakage of personal information on the server by using biometric information stored on the user device and authenticating. In this paper, we propose a multiple biometric authentication method that can be used in FIDO environment. In order to utilize multiple biometric information, fingerprints and EEG signals can be generated and used in FIDO system. The proposed method can solve the problem due to limitations of existing 2-factor authentication system by authentication using multiple biometric information.

Key Words : FIDO, Biometric, Multiple Biometric, Authentication, Security

1. 서론

생체 인증 기술이란 고유한 생체정보를 이용하여 개인을 인증하는 기술로서, 출입국심사 및 출입통제 등 광범위한 분야에 적용되고 있으며 모바일 금융거래와 핀테크가 확산되면서 금융 분야에서 크게 부각되고 있는 기술이다. 현재의 인증 방법으로 PKI, OTP, 보안 토큰 등 다양한 기술들이 사용되고 있지만 최근에는 보관할 필요가 없고 이용이 편리한 생체 인증 기술이 크게 부각되고 있고 한편 사이버 침해사고, 전자금융사기 등 보안사고

*This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2017R1D1A1B03032876).
*Corresponding Author : Hyun Mi Jung(hmjung@kisti.re.kr)
Received December 6, 2017 Revised January 3, 2018
Accepted January 20, 2018 Published January 28, 2018

가 지속적으로 증가하고 있는 상황에서 기존 2-Factor 인증 체계의 한계 노출로 미국, 유럽 등 선진국은 제3자 공여 및 양도가 불가능한 생체 인증 체계로 전환을 추진하고 있다[1, 2]. 이러한 생체 인증에서는 개인의 생체정보를 이용하기 때문에 프라이버시 보호, 재사용성, 재전송 공격 방지 기술은 생체 인증 기술을 구현하는 것이 핵심이다.

최근 Microsoft, Google을 중심으로 FIDO의 보안인증 기술 검토하면서 스마트폰 제조업체 및 금융 관계 업체들도 생체 인증 기술 적용을 계획하고 있다. 또한 스마트폰을 이용한 생체 인증 기술 개발을 통해 시장을 선점하려는 경쟁이 활발하다. 기술 개발과 더불어 생체 인증 시장 규모도 2019년 61억5000만 달러(약 6조 2800억 원)로 확대될 전망이다. 생체정보 인증 기술은 주요 선진국 중심으로 활발한 연구개발이 진행 중에 있으며, 다중 생체 인식 인증 관련 세계 특허 출원 건수는 미국 8,221건 PCT 2,698건, 캐나다 623건, 한국 6건으로 선진국과의 격차가 크다[3]. 우리나라에서도 정부과제의 일환으로 지난 2015년 산학연 전문가로 구성된 표준연구회가 발족되어 국내·외 표준화 추진하고 있다.

이에 본 논문에서는 FIDO 환경에서 사용할 수 있는 다중 생체정보를 이용한 인증 방법에 대해 제안한다. 논문의 구성은 다음과 같다. 2장에서는 FIDO 기반 인증 기술, FIDO UAF(Universal Authentication Framework), FIDO U2F(Universal 2nd Factor) 방식에 대해 분석하고 3장에서는 FIDO 기반 인증에 사용되는 주요 생체정보 인증 기술에 대해 분석한다. 그리고 4장에 지문정보와 뇌전도 신호를 이용한 다중 생체정보를 이용한 인증 방법을 제안하고 5장에서 결론을 맺는다.

2. FIDO 기반 인증 기술

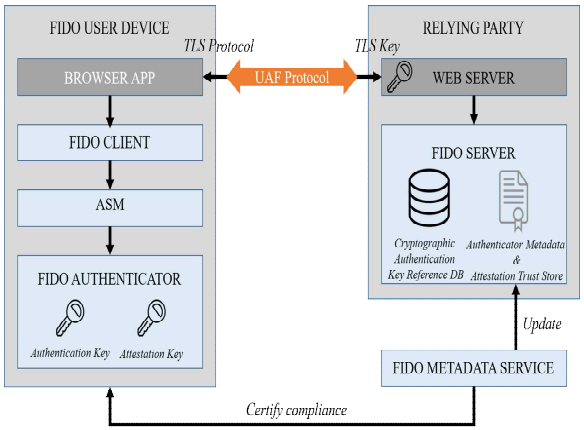
FIDO 인증 기술은 현재 사용자가 인증서 등과 같은 인증 수단을 소지하고, 패스워드와 같은 암호를 외우는 데서 발생하는 보안상의 문제점을 극복하고자 개발되었다. FIDO 인증 기술은 UAF 방식과 U2F방식을 제공한다. UAF 인증 방식은 기존의 ID/Password 인증 방식보다 보안이 강화된 개인의 생체 정보를 활용하는 표준이며, U2F는 ID/Password 인증 방식에 별도의 인증 장치를 추가적으로 사용하는 방식이다[4-7].

2.1 UAF 프로토콜

UAF 프로토콜은 사용자가 가지고 있는 디바이스에서 온라인 서비스와 연동하여 인증하는 기술이다. FIDO UAF 프로토콜에서는 사용자 디바이스를 이용하여 생체정보를 인식하게 되면 FIDO 서버에 접근할 수 있다. 그리고 사용자 디바이스에서 제공하는 보안 키를 입력하는 처리 절차를 가지고 있다. UAF 프로토콜 표준에서는 웹 서버, FIDO 서버, 사용자 디바이스 간에 연동되는 UAF 메시지를 정의하는 UAF Protocol Specification 등의 문서로 구성되어 있다. <Table 1>은 UAF 프로토콜 표준 리스트 및 표준에 대한 설명이다.

<Table 1> UAF v1.1 Specifications

UAF Specifications	Contents
FIDO UAF Architectural Overview	This overview document describes the various protocol design considerations in detail and also describes the user flows in detail.
FIDO UAF Protocol Specification	This document defines the message formats and processing rules for all UAF protocol messages.
UAF Application API and Transport Binding Specification	This document describes the client side APIs and interoperability profile for client applications to utilize FIDO UAF.
FIDO UAF Authenticator-specific Module API	This document defines Authenticator specific Modules and the API provided to the FIDO client by ASMs.
FIDO UAF Authenticator Commands	This document describes Low-level functionality that UAF Authenticators should implement to support the UAF protocol.
FIDO UAF APDU	This specification defines a mapping of FIDO UAF Authenticator commands to Application Protocol Data Units (APDUs) thus facilitating UAF authenticators based on Secure Elements.
FIDO Metadata Statements	This document defines the authenticator metadata.
FIDO Metadata Service	Baseline method for relying parties to obtain FIDO Metadata statements.
FIDO UAF Registry of Predefined Values	This document defines UAF-specific strings and constants.
FIDO Registry of Predefined Values	This document defines strings and constants applicable to various FIDO protocol families. See also FIDO UAF Registry of Predefined Values.
FIDO AppID and Facet Specification	This document defines the scope of user credentials and how a trusted computing base which supports application isolation may make access control decisions about which keys can be used by which applications and web origins.
FIDO ECDAA Algorithm	This document defines the direct anonymous attestation algorithm used in FIDO.
FIDO Security Reference	Provides an analysis of FIDO security based on detailed analysis of security threats pertinent to the FIDO protocols based on its goals, assumptions, and inherent security measures.
FIDO Technical Glossary	Defines the technical terms and phrases used in FIDO Alliance specifications and documents.



[Fig. 1] FIDO UAF High-Level Architecture

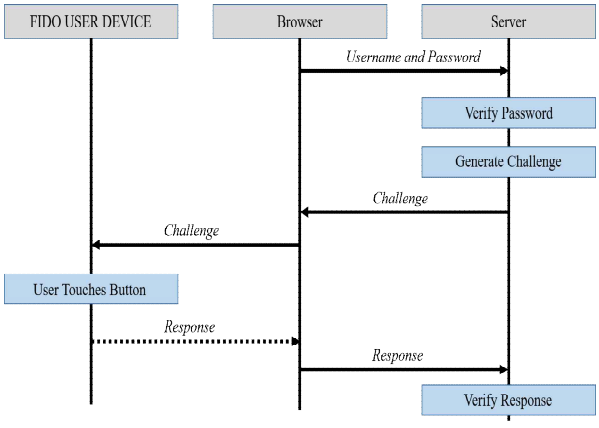
[Fig. 1]은 FIDO UAF High-Level 구조를 보여주고 있다. FIDO UAF에서 사용자 디바이스는 Browser APP, FIDO Client, ASM(Authenticator Specific Module), FIDO Authenticator, Authentication Key, Attestation Key로 구성되어 있다. FIDO UAF에서는 PKI 방식의 인증 기술을 사용하고 있지만 기존 PKI 방식과의 차이점은 사용자 디바이스 인증 모듈에 Attestation Certificate, Attestation Private Key가 설치되어 있다는 점이다. 사용자는 Public Key와 Private Key를 웹 서버에 전송할 때 서명뿐만 아니라 인증 모듈이 용도에 맞게 사용할 수 있게 한다. 사용자 등록 후 FIDO Server는 해당 FIDO Server와 디바이스 Authenticator에 Unique Secure Identifier를 할당하여 디바이스에 전송하고 서비스 연동에 해당 식별자를 이용하여 사용자를 인증한다.

2.2 U2F 프로토콜

U2F 프로토콜은 기존 인증 방법인 ID/Password 기반 인증 방식으로 1차 인증 한 후, 1회용 보안키를 저장한 USB 동글 또는 스마트 카드와 같은 별도의 디바이스를 이용하여 2차 인증하는 기술이다. U2G 프로토콜은 2-Factor 인증을 통해 기존 암호화 방식보다 좀 더 안전한 인증을 제공한다. U2F 프로토콜에서 사용자가 U2F 디바이스를 등록하면 사용자 U2F 디바이스는 Public Key와 Private Key를 생성하여 웹 서버에 Public Key를 전송한다. 사용자 인증을 위해 1차 인증 수행 후, 웹 서버는 전자서명을 이용하여 사용자가 장치를 소유하고 있는지를 확인한다. <Table 2>는 U2F 프로토콜 표준 리스트 및 표준에 대한 설명이다.

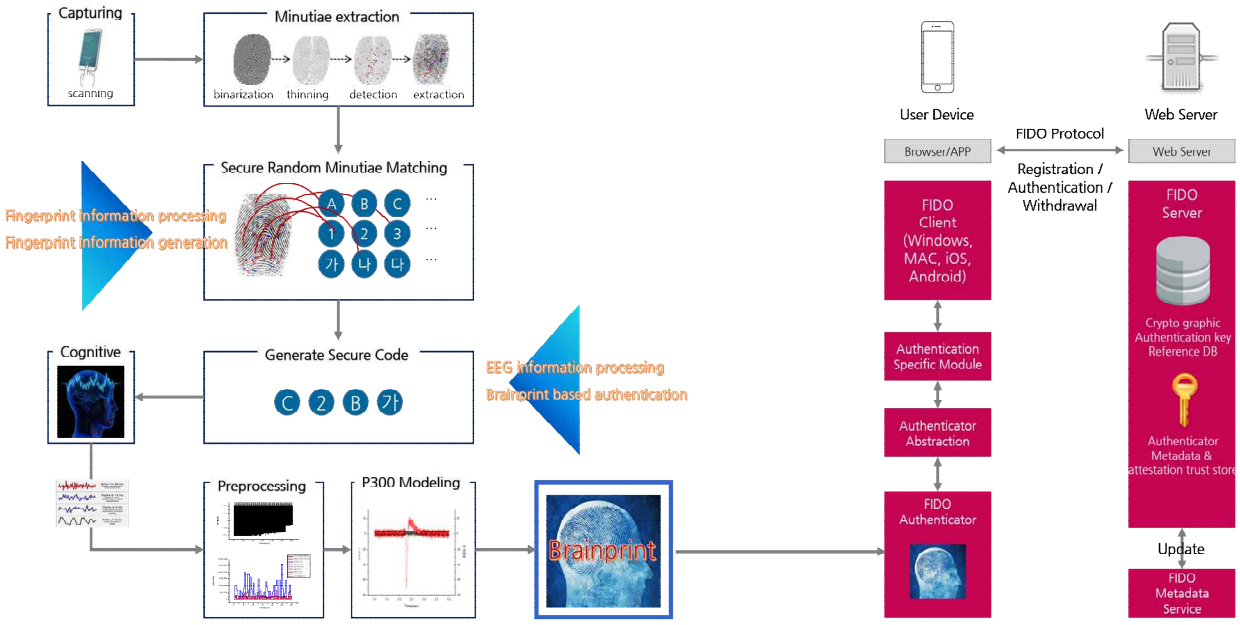
<Table 2> U2F v1.2 Specifications

U2F Specifications	Contents
FIDO U2F Architectural Overview	This overview document describes the various design considerations which go into the protocol in detail and describes the user flows in detail.
FIDO U2F Javascript API	This document describes the client side API in the web browser for accessing U2F capabilities.
FIDO U2F Raw Message Formats	This document describes the binary format of request messages which go from the FIDO U2F server to the FIDO U2F token and the binary format of the response messages from the token to the server.
FIDO U2F HID Protocol Specification	This document describes how messages sent from the FIDO Client to the USB U2F token are framed over USB HID.
FIDO U2F Implementation Considerations	This document describes implementation considerations and recommendations for creators of U2F devices and for relying parties implementing U2F support.
FIDO AppID and Facet Specification	The U2F protocol ensures that the origin foo.com can only exercise a key that was issued for foo.com by the U2F token.
FIDO Common Header Files	These header files define the values of symbolic constants and data structures referred to in the FIDO U2F Raw Messages document and the FIDO U2F HID Protocol Specification documents.
FIDO Bluetooth Specification	This document describes how the U2F protocol should be performed between a FIDO client and a Bluetooth Low Energy FIDO authenticator.
FIDO NFC Specification	This document describes how the U2F protocol should be performed between a FIDO client and an NFC FIDO authenticator.



[Fig. 2] FIDO U2F Basic Process Flow

[Fig. 2]는 FIDO U2F 기본 프로세스를 보여주고 있다. FIDO U2F에서의 사용자 인증 절차는 1차로 Username, Password를 FIDO Server에게 전송하여 사용자 인증을



[Fig. 3] System Structure of Authentication Method using Multiple Biometric Information in FIDO Environment

처리한다. 1차 인증 완료 후, 사용자는 USB 디바이스 버튼을 누르거나 태핑(Tapping)하는 방식으로 2차 인증을 수행한다. 이때 U2F 디바이스는 USB, NFC, Bluetooth 등 다양하게 응용될 수 있다.

3. FIDO 환경에서 주요 생체정보 인식 기술

생체정보 인증은 보안성, 편리성을 동시에 가지는 장점이 있으나, 생체정보를 인증하는 과정에서 서버에 생체정보를 저장하는 방식을 사용할 경우 개인정보 유출 취약점이 존재한다. 이러한 취약점을 극복하고자 FIDO에서는 생체정보를 사용자 디바이스에 보존하여 인증하는 방식을 사용하여 서버에서의 개인정보 유출 문제를 해결하였다.

3.1 지문 인식 기술

지문인식은 가장 널리 사용되고 있는 생체인식기술이다. 지문은 태어날 때의 모양이 특별한 일 없이는 변하지 않는다는 특징을 가지고 있으며, 간편하고 저렴한 비용으로 도입할 수 있다는 특징이 있다. 식별에 대한 신뢰도와 안정도에 있어서도 비교적 높은 것으로 평가되고 있다. 지문인식 기술은 일반적으로 특징점을 추출하여 비교하는 알고리즘으로 구성되어 있기 때문에 지문을 인식하는 장치에 습기가 있는 경우 오류 발생률이 높아진다[8-10].

3.2 홍채 인식 기술

홍채는 일란성 쌍둥이라도 서로 다른 것으로 알려져 있어 통계학적으로 DNA 분석보다 정확하다고 알려져 있다. 홍채는 유아기때 양쪽 모두 다르게 형성된다. 홍채 인식 기술은 적외선을 이용하여 홍채를 이미지 처리하여 등록한 후 이를 비교하는 방식을 사용한다. 이러한 홍채는 상처로 인한 홍채가 훼손되는 경우를 제외하고는 복제가 불가능하다는 특징이 있다. 또한 안경을 착용하는 경우에도 인식이 가능하다는 장점 때문에 많이 활용되고 있다[8, 9, 11].

3.3 얼굴 인식 기술

얼굴인식 기술은 개인의 얼굴을 등록하여 비교하는 방식을 사용한다. 얼굴을 인식하기 위해 사용하는 일반적으로 2차원이나 3차원 영상을 이용하거나 열화상 카메라를 이용하는 방식이 있다. 2차원 영상의 경우는 저렴한 비용으로 영상을 획득할 수 있지만 정확도가 낮다는 단점이 있고 3차원 영상의 경우 정확도가 높지만 비용이 많이 든다는 단점이 있다.[8, 9, 11, 12].

3.4 음성 인식 기술

음성인식 기술은 목소리 경로와 구강과 후두 모양에 의한 음성적인 특징을 이용하여 식별하는 기술이다. 이러한 음성적인 특징을 이용하기 때문에 타인의 목소리를 모방하는 방식으로는 복제가 불가능하다는 장점이 있다. 그러나 음성적인 특징을 추출하는 장치에 의해 인식률 차이 발생한다는 단점이 있다[8]. 또한 사용자가 감기에 걸렸거나 후두염에 감염될 경우 음성적인 특징이 변경될 수 있다는 단점이 있다[8, 9, 11, 12].

3.5 뇌전도 인식 기술

뇌전도를 이용한 생체정보 인식 기술은 특정 상황에 따라 반응하는 뇌전도를 이용하여 인식하는 기술이다. 특정 상황에 따라 뇌전도는 주파수와 진폭이 다른 파형으로 분류할 수 있다. Delta파는 0~4Hz의 파형으로 수면 상태일 때 발생, Theta파는 4~8Hz의 파형으로 졸리거나 깊은 명상일 때 발생, Alpha파는 8~12Hz의 파형으로 긴장이완이나 편안한 상태일 때 발생, Beta파는 15~30Hz의 파형으로 의식 활동이나 집중일 때 발생, Gamma파는 30~50Hz의 파형으로 외적으로 불안하거나 강한 스트레스상태에서 발생한다. 뇌전도 인식 기술을 사용하기 위해서는 잡음을 제거하여 사용하고 성능 분석을 위해 SVM 기계학습 등을 사용한다[13-16].

4. 다중 생체정보 인증 방법

논문에서는 3장에서 분석한 주요 생체정보 중 지문정보와 뇌전도 인식 기술을 이용한 다중 생체정보를 이용한 인증 방법을 제안한다. [Fig. 3]은 논문에서 제안하는 FIDO 환경에서 다중 생체 정보를 이용한 인증 방법을 보여주고 있다.

먼저 사용자 지문 인식을 위해 특징점과 랜덤번호를 매칭하여 보안 코드를 생성한다. 지문 정보를 추출하기 위해서 사용자 지문 10개 중 임의 개수를 입력 값으로 받는다. 입력 받은 지문의 특징점과 매칭하기 위해 시큐어 랜덤 함수를 이용하여 랜덤번호를 생성한다. 그리고 특징점과 랜덤번호를 매칭하여 보안 코드를 생성한다. 보안코드는 영문자, 숫자, 한글로 이루어져 있으며, 사용자가 보안코드를 인식하였을 때의 뇌전도를 측정한다. 뇌전도는 특정 개체를 인식하였을 때, P300 패턴이 발생하는 300ms 부근 신호를 패턴 처리하여 생성한다. 뇌전도 신호를 패턴 처리하여 뇌정보(Brainprint)를 생성하고 FIDO Authenticator에게 전달함으로써 사용자를 인증할 수 있다. <Table 3>은 FIDO 환경에서 다중 생체정보를 이용하여 사용자를 인증할 때, 다중 생체정보 생성 알고리즘이다.

<Table 3> Proposed Algorithm

Algorithm : Generate brainprint using multiple biometric information

let : $Fingerprint_{NO} \ni \{Fingerprint_{No1}, Fingerprint_{No2}, Fingerprint_{No3} \cdots, Fingerprint_{No10}\}$;
let : $SR_{NO} \ni \{1, 2, 3 \ldots 10, a, b, c, \ldots z, 가, 나, 다 \ldots 하\}$;

Function generate multiple biometric information()
    int i, j;
    for i=1 to 10 do
        NR_{NO} = Create random number;
        for int j=1 to 10 do
            SreureCode = ($Fingerprint_{NO}$ → NR_{NO});
        End
    Generate Brinprint = (brainwave → NR_{NO});
    End
    Rerurn all Brainprint;
End

제안한 알고리즘에서 뇌정보 값을 획득하기 위해서는 사용자 지문 값, 지문과 랜덤코드가 매칭된 보안코드, 보안코드를 인지한 뇌파정보 전부를 얻어야만 한다. 이는 단일 생체정보만을 이용했을 때 보다 공격복잡도가 증가한다. 또한 생체정보를 이용한 인증에서의 단점인 생체정보 유한성 문제를 해결할 수 있다는 장점이 있다.

5. 결론 및 향후 연구

생체정보는 저장, 암기, 손실 우려가 없고 도용이 불가능하다는 점에서 패스워드, PKI 등 기존 인증 방법의 대체 수단으로 주목받고 있지만, 개인정보 유출로 인한 프라이버시 문제 및 고정된 생체정보를 사용하게 되므로 재전송 공격에 취약한 문제점을 가지고 있다. 이러한 문제점을 해결하기 위해 논문에서는 프라이버시 및 재전송 공격에 강한 생체 인증을 위해 재사용 가능한 지문정보와 브레인프린트를 융합한 다중 생체 인증 기술을 이용한 인증 방법을 제안하였다. 향후 생체정보 인증 장비를 금융기관이 추가로 장착할 필요가 없는 FIDO 표준을 준용한 인증 시스템을 개발할 계획이다.

REFERENCES

[1] Costigan et al., "Behavioural Biometrics - A New Era of Security" The FinTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries, 2016.

[2] Jason Kim et al., "Standardization trend of non-face authentication technology based on telebio recognition", Review of Korea Institute Of Information Security And Cryptology, 2015.

[3] B. C Cho et al., "Technology Review on Multimodal Biometric Authentication", The Journal of The Korean Institute of Communication Sciences, 2015.

[4] https://fidoalliance.org/

[5] H. G. Cho et al., "A Methodology for the Improvement of Accredited Digital Certificate Integrating FIDO Biometric Technology and TrustZone", Journal of Digital Convergence, Vol. 15, No. 8, pp.183-193, 2017.

[6] H. W. Lee, "Current Status and Future Prospects of FIDO Authentication Technology", KFTC Payments Trends, Vol. 261, 2016.

[7] J. J. Kim and S. P. Hong, "Design of a Secure Biometric Authentication Framework Using PKI and FIDO in Fintech Environments", International Journal of Security and Its Applications, Vol. 10, No. 12, pp. 69-80, 2016.

[8] W. H. Choi, "A Study on Pament Method Utilizing Biometric Technology", Graduate School of Soongsil University, 2015.

[9] D. S. Han, "The Proposal for a Fingerprint Recognition Method for the Improvements of Security and the Use of each Application in FIDO Authentication", Graduate School of Soonchunhyang University, 2016.

[10] H. Y. Lee, J. G. Kim , "Quality Evaluation Model about Efficiency for Fingerprint Recognition System", Journal of Digital Convergence, Vol. 12, No. 6, pp. 215-221, 2014.

[11] G. H. Choi, H. M. Moon, S. B. Pan, "Biometrics System Technology Trends Based on Biosignal", Journal of Digital Convergence, Vol. 15, No. 1, pp. 381-391, 2017.

[12] H. J. Moon, M. H. Lee, K. H. Jeong, "Authentication Performance Optimization for Smart-phone based Multimodal Biometrics", Journal of Digital Convergence, Vol. 13, No. 6, pp. 151-156, 2015.

[13] G. J. Kim, J. S. Han, "Unsupervised Machine Learning based on Neighborhood Interaction Function for BCI", Journal of Digital Convergence, Vol. 13, No. 8, pp. 289-294, 2015.

[14] B.Gainmann et al., "Brain-Computer Interface, Revolutionizing Human-Computer Interaction", Springer, 2010.

[15] A.Nijholt et al., "Brain-Computer Interfacing for Intelligent System", IEEE Intelligent System, Vol. 23, No. 3, pp. 72-79, 2008

[16] J. W. Lee et al., "A Survey on Potential User's Needs and Demands for Brain Machine Interface(BMI) Technology Developments", Journal of Vocational Rehabilitation, Vol. 24, No. 3, pp. 5-25, 2014.

채 철 주(Chae, Cheol Joo) [정회원]

- 2009년 8월 : 한남대학교 컴퓨터공학과(공학박사)
- 2009년 9월 ~ 2013년 4월 : 한국전자통신연구원 선임연구원
- 2013년 4월 ~ 2016년 8월 : 한국과학기술정보연구원 선임연구원
- 2016년 9월 ~ 현재 : 한국농수산대학 교수
- 관심분야 : 정보보호, 바이오 보안, 네트워크 보안
- E-Mail : chae.cheoljoo@gmail.com

조 한 진(Cho, Han Jin) [종신회원]

- 1999년 2월 : 한남대학교 컴퓨터공학과(공학석사)
- 2002년 8월 : 한남대학교 컴퓨터공학과(공학박사)
- 2002년 8월 ~ 현재 : 극동대학교 에너지IT공학과 교수
- 관심분야 : 정보보호, 스마트폰 보안, 모바일 콘텐츠
- E-Mail : hanjincho@hotmail.com

정 현 미(Jung, Hyun Mi) [정회원]

- 2014년 2월 : 한남대학교 컴퓨터공학과(공학박사)
- 2012년 10월 ~ 현재 : 한국과학기술정보연구원 슈퍼컴퓨터시스템개발실 선임연구원
- 관심분야 : HPC, HPC 보안, 클라우드 컴퓨팅
- E-Mail : hmjung@kisti.re.kr