KIPS Tr. Comp. and Comm. Sys.
Vol.6, No.10 pp.421~428 pISSN: 2287-5891

https://doi.org/10.3745/KTCCS.2017.6.10.421

A Study on Big Data Based Non-Face-to-Face Identity Proofing Technology

Jung Kwansoo† · Yeom Hee Gyun†† · Choi Daeseon†††

ABSTRACT

The need for various approaches to non-face-to-face identification technology for registering and authenticating users online is being required because of the growth of online financial services and the rapid development of financial technology. In general, non-face-to-face approaches can be exposed to a greater number of threats than face-to-face approaches. Therefore, identification policies and technologies to verify users by using various factors and channels are being studied in order to complement the risks and to be more reliable non-face-to-face identification methods. One of these new approaches is to collect and verify a large number of personal information of user. Therefore, we propose a big-data based non-face-to-face Identity Proofing method that verifies identity on online based on various and large amount of information of user. The proposed method also provides an identification information management scheme that collects and verifies only the user information required for the identity verification level required by the service. In addition, we propose an identity information sharing model that can provide the information to other service providers so that user can reuse verified identity information. Finally, we prove by implementing a system that verifies and manages only the identity assurance level required by the service through the enhanced user verification in the non-face-to-face identity proofing process.

Keywords : Non-Face-to-Face, User Authentication, FinTech, Big Data, Identity Proofing

빅데이터 기반 비대면 본인확인 기술에 대한 연구

정 관 수† · 염 희 균†† · 최 대 선†††

요 약

최근 온라인 금융서비스의 성장과 금융 기술의 급격한 발전으로 인하여 온라인에서 사용자를 등록 및 인증하기 위한 비대면 본인확인 기술에 대한 다양한 접근 방법의 필요성이 제기되고 있다. 일반적으로 비대면 방식은 대면방식에 비해서 많은 위협에 노출되어 있다. 따라서 최근에는 이런 위험성을 보완하고 보다 신뢰할 수 있는 비대면 본인확인 방법을 위해서 다양한 요소와 채널을 이용하여 사용자를 검증할 수 있는 정책과 기술이 연구되고 있다. 이러한 새로운 접근방법 중 하나는 다수의 사용자 개인정보를 수집하고 검증하는 기술이다. 따라서 본 논문은 사용자의 다양하고 많은 정보를 기반으로 온라인에서 본인확인을 수행하는 빅데이터 기반 비대면 본인확인 방법을 제안한다. 또한 제안방법은 서비스에서 요구하는 본인확인 등급에 필요한 사용자 정보만 수집하고 검증하는 세분화된 본인확인 정보관리 방법을 제안한다. 그리고 본 논문은 검증된 본인확인 정보를 사용자가 재사용할 수 있도록 다른 서비스 제공자들과 공유할 수 있는 본인확인 정보 공유 모델을 제안한다. 마지막으로 제안 방법이 비대면 본인확인 과정에서 강화된 사용자 검증을 통해서 서비스에서 요구하는 본인확인 등급만 검증하고 관리하는 시스템을 구현하여 실험 결과를 분석한다.

키워드 : 비대면, 사용자 인증, 핀테크, 빅데이터, 소셜 네트워크

1. 서 론

최근 금융서비스 산업은 금융(financial)과 기술(technology)을 결합한 핀테크(FinTech)가 변화를 주도하고 있다. 이러한 금융과 기술의 융합 트랜드는 정보통신기술(Information Communication Technology)을 통해 금융시장에 파괴적 혁신과 부가가치를 창출하며 전 세계적으로 급격하게 성장하고 있다. 일반적으로 전통적인 금융기관들은 사용자에 대해서 오프라인 대면시스템을 이용하여 금융서비스에 필수적인 신뢰성과 보안성을 확보해 왔다. 반면 핀테크 기업들은 첨단기술을 바탕으로 기존의 금융 거래 방식과는 차별화 된 새로운 형태의 금융 비즈니스 모델을 제시하며 금융서비스의 혁신을 이끌고 있다. 이러한 기술 혁신 중에서 온라인 전문금융기관과 비금

※ 이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원(No. B0717-16-0139, 핀테크 서비스 금융사기 방지를 위한 비대면본인확인 및 이상거래필터링기술)과 호원대학교 교내 학술연구비를 지원 받아 수행된 연구임.
† 정 회 원 : 호원대학교 사이버보안학과 조교수
†† 정 회 원 : 대전대학교 컴퓨터공학과 강의전담교수
††† 정 회 원 : 공주대학교 의료정보학과 부교수
Manuscript Received : March 2, 2017
First Revision : May 2, 2017
Accepted : July 10, 2017
* Corresponding Author : Choi Daeseon(sunchoi@kongju.ac.kr)

융기관들은 비대면 시스템을 기반으로 다양한 금융서비스를 사용자들에게 제공하려는 혁신을 선도하고 있다. 또한, 최근 FIDO(Fast IDentity Online)와 같은 사용자 인증기술이 고도화됨에 따라 본인확인 시점이 로컬에서 원격지로 옮겨가고 있으며, 이에 따른 본인확인의 중요성 및 신뢰성이 더욱 부각되고 있다. 이러한 변화에 대응하기 위해서 국내에서도 최근 국내 금융위원회에서는 비대면 본인확인 가이드라인을 발표하였으며, 인터넷 전문은행의 도입을 추진하면서 금융소비자의 접근 편의성을 높이기 위한 비대면 본인확인 방안을 금융기관에서 사용하도록 허용했다[1-3]. 이에 본 연구는 신원확인 관리에 관한 국내표준 TTAK.KO-12.0292[2]와 국제표준 X.1254[4]에 근거하여, 본인확인에 대한 높은 정확도를 제공하기 위해서 사용자 속성을 검증하는 빅데이터 기반의 비대면 본인확인 기술을 제안한다. 또한 본인확인 정보를 공유할 수 있는 모델을 제안한다.

2. 관련 연구

2.1 본인확인

1) 본인확인 개요

본인확인은 특정한 방법을 통해서 특정인이 본인인지 아닌지를 식별하는 과정으로 실명확인을 포괄하는 개념으로 사용한다[5, 6]. 이는 신원확인이라는 용어와 혼용되어 사용되기도 한다. 국내 표준에 정의된 신원확인은 신원확인 검증기관이 특정 보증 등급에 해당하는 실체에 대한 신원을 확인하기 위해 정보를 수집하고 이를 이용해 신원을 검증하는 과정이다[1]. 본 논문에서는 특정한 사용자의 실체를 확인하는 개념을 본인확인으로 정의하여 사용한다.

2) 본인확인 국내외 표준

본인확인과 관련된 국내외 표준화 과정은 ISO/IEC와 TTA에서 활발히 진행되고 있다. 우선 국제표준으로 ISO/IEC 29115[7]에서는 4단계의 보증레벨(Level of assurance)을 제시하며, 인증 위협과 이에 대한 통제사항, 보증레벨 기준, 관련 용어, 관련 주체, 실체 인증을 위한 프로세스 등을 제시한다. ISO/IEC 29003[8]에서는 3단계의 신원 확인 레벨(Levels of identity proofing)과 요구사항을 제시하며, 신원확인 목표, 신원확인 정보, 관련 용어, 관련 주체, 신원확인 프로세스 등을 제시한다[5]. 국내는 TTA에서 신원확인 관리를 위한 국내 지침에 대한 표준(TTAK.KO-12.0292)[2]을 제정하였다. 해당 표준은 인터넷 금융 서비스를 제공하는 금융기관의 신원확인 관리 지침으로 적용 가능하며 국제표준(ISO/IEC 29003)과 국내 지침에 근거해 온라인 신원확인 방법과 등급을 정의하며, 등급에 따른 기준을 제시한다[1, 2].

3) 본인확인 수단

본인확인 수단은 본인확인 기관이 사용자에게 부여하는 식별정보와 사용자만 알거나 가지고 있는 비밀정보를 기본적으로 사용하여 본인임을 확인하는 절차를 말한다. 또한 서비스 혹은 정보 등을 요청하는 주체가 사용자 본인임을 확인하고 이를 검증하는 사용자 인증을 위해 제공되는 수단을 본인확인 수단이라고 한다[9]. 이러한 본인확인수단은 주체가 누구인지를 밝히는 식별(identification), 주체를 증명하는 인증(authentication), 주체에 대한 시스템 자원을 허가하는 권한부여(authorization) 단계로 이루어지며, 이는 서비스를 제공받기 위한 필수적인 요구조건이다[10]. 본인확인 수단은 특성에 따라 대면/비대면, 전자적/비전자적, 주민등록번호 제공여부, 생체정보 제공여부 등에 따라 다양한 방법들이 적용되고 있다. 국내에서는 국내법에 근거하여 I-PIN, 공인인증서, 휴대전화 인증 등의 다양한 방법을 사용하여 본인확인을 수행하고 있다[11].

2.2 비대면 본인확인 방법

인터넷은행이나 새로운 핀테크 서비스에서는 온라인 서비스 등록을 위해서 비대면 방식으로 본인확인을 수행한다[1, 6]. 그러나 비대면 방식은 타인의 명의도용과 같은 위험성 측면에서 대면 방식보다 상대적으로 취약하다. 따라서 국내에서는 비대면 방식의 안전성을 제고하기 위해서 비대면 본인확인 방법 4가지 중 두 가지를 이중 확인 하도록 의무화하고 있으며, 추가적인 확인방법을 적용하여 다중요소를 확인하는 방법으로 권고하고 있다[2, 12].

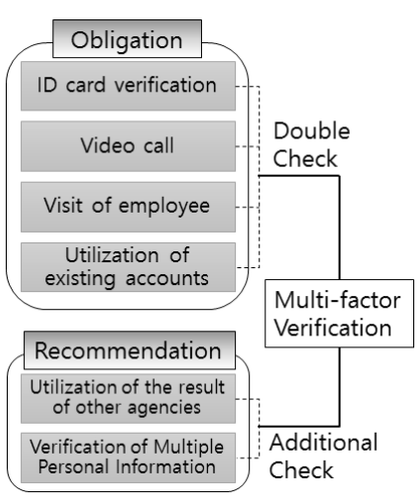


Fig. 1. Authentication Factors for the Non-Face-to-Face Identity Proofing [2]

Fig. 1은 비대면 확인방식의 실명확인 정확도 확보를 위한 다중(3개 이상) 요소 검증 방법을 보여준다. 이처럼 다양한 본인확인 수단을 여러 단계에서 검증에 활용하면, 온라인에서 보다 강화된 비대면 본인확인을 수행할 수 있다.

2.3 본인확인 정보

본인확인은 다양한 정보를 기반으로 실체를 검증하는 과정이다. 이 과정에서 사용되는 사용자 속성 정보는 본인확인의 검증 신뢰도에 많은 영향을 준다. 본인확인 정보는 크게 식별 속성 정보와 보조 속성 정보로 구성된다.

식별 속성은 하나 이상의 식별 정보가 결합되어 하나의 컨텍스트에서 실체를 유일하게 식별하는데 이용되는 정보이다. 그리고 보조 속성은 식별 속성 정보 외에 본인확인 과정을 지원하기 위해 필요한 속성 정보로 정보주체와 아이덴티티 정보와의 관계나 연관성 등을 나타낸다[2]. Table 1은 대표적인 본인확인 속성 정보의 예를 나타낸다.

Table 1. An Example of Identification Information [2]

Classification	An Example of Attribute Information
Identification Attribute	Alias, name, birthday, birthplace, address, phone number, resident registration number, email, bio information, etc.
Corroborative Attribute	Other names, relationships and associations, reference numbers for identity evidence, related information on the identity evidence provided, etc.

본인확인 검증 신뢰도와 관련된 본인확인 보증 등급은 ISO/IEC 29003에서는 3단계 등급을 ISO/IEC 29115에서는 4단계 등급을 제시하고 있다[5, 7, 8]. 본 연구에서는 국내 신원확인 관리 지침 표준에서 제안하는 4단계의 신원확인 보증 등급(LoIP, Level of Identity Proofing)을 참조한다. 본인확인 보증 등급과 각 등급의 목표는 Table 2와 같다.

Table 2. A Level of Identity Proofing [2]

Level	Objective
LoIP0 No Credibility	• No identification method is required. (using ID or password)
LoIP1 Low Credibility	• Identity is unique within context
LoIP2 Middle Credibility	• Identity is unique within context • Identity is existed in the information source. • Information entity is weakly associated with identity
LoIP3 High Credibility	• Identity is unique within context • Identity is existed in the authoritative source. • Information entity is strongly associated with identity

본인확인 보증 등급을 결정하기 위한 세부 기준은 다음과 같이 세 가지로 정의된다.

- 유일성: 주체의 아이덴티티가 유일하다.
- 존재성: 주체의 아이덴티티가 존재한다.
- 연계성: 주체의 아이덴티티가 해당 컨텍스트 내에서 정보주체와 연결된다.

3. 비대면 본인확인 검증 모델

비대면 본인확인 검증 모델은 오프라인에서 직접 자신을 증명하지 않아도 온라인에서 간편하게 본인을 증명하여 서비스를 제공받고 이용할 수 있도록 간편성과 보안성을 제공한다. 또한 비대면 본인확인 방법의 상호 보완성 등을 고려하여 복수의 방식을 함께 사용하도록 권장하고 있는 국내외 정책 상황에 맞게 보다 높은 본인확인의 정확도를 제공하기 위해서 다양한 사용자 신원확인 속성을 검증하는 빅데이터 기반의 비대면 본인확인 기술이다. 이번 장에서는 본인확인 검증 모델을 설명하고, 사용자의 빅데이터 수집 방법과 본인확인 검증 알고리즘, 그리고 본인확인 정보의 공유 서비스 모델을 설명한다.

3.1 빅데이터 기반 비대면 본인확인 검증 모델

본 논문에서 제안하는 빅데이터 기반 비대면 본인확인 방법은 다수의 사용자 신원확인 속성 정보들을 기반으로 신원확인 보증 등급을 위한 기준인 유일성과 존재성, 연계성을 검증하여 사용자를 식별 및 검증하는 방법이다. 또한 무분별한 사용자의 정보 수집을 방지하기 위해서 제안 방법은 온라인 비대면 서비스에서 요구하는 신원확인 등급에 맞는 사용자 속성 정보만을 수집하고 분석한다. 결과적으로 본인확인 정보 제공자는 사용자가 이용하려는 서비스에서 요구

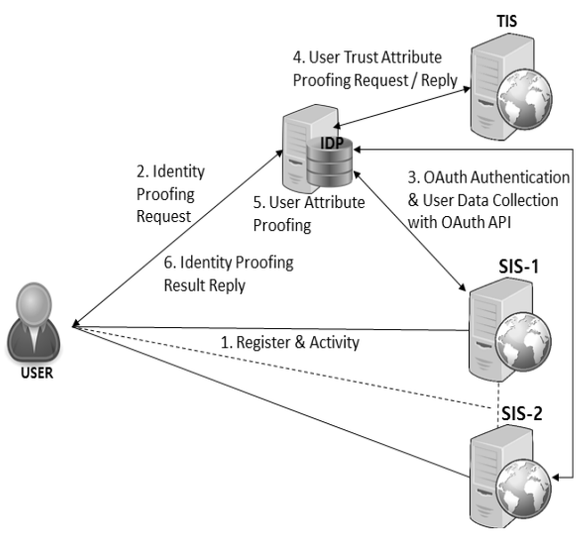


Fig. 2. A Concept of Big Data Based Identity Proofing Model

하는 세분화된 본인확인을 수행하기 위해서 사용자가 제공한 속성 정보를 검증하고 이에 대한 보증 등급을 평가하여 서비스 제공자에게 사용자의 신뢰성 정보인 본인확인 검증 결과를 제공한다. 제안 모델은 기본적으로 사용자와 본인확인을 수행하는 본인확인 정보 제공자(IDP: Identification Provider), 사용자의 신뢰 정보를 검증하는 신뢰 정보 소스(TIS: Trust Information Server), 사용자 데이터(등록 및 생성정보)를 제공하는 보조 정보 소스(SIS: Secondary Information Server), 그리고 사용자에게 서비스를 제공하는 서비스 제공자(SP: Service Provider)로 구성된다. Fig. 2는 제안 모델의 구성 요소와 서비스 개념도를 보여준다.

3.2 사용자의 본인확인 정보 수집 방안

제안 방법은 무분별한 사용자의 속성 정보 수집을 방지하기 위해서, 사용자가 요구하는 서비스에 필요한 속성 정보만을 사용자에게 요구하여 직접 입력 받을 수 있거나 OAuth[16]와 같은 Open API기반의 인증 프로토콜을 이용하여 소셜 네트워크에서 등록 및 생성한 다수의 사용자 데이터(정형/비정형)를 제공 받는다. 각 본인확인 보증 등급별 요구되는 사용자 속성 정보는 보증등급 평가를 위한 기본 검증 속성과 신뢰성 평가를 위한 확장 검증 속성으로 구분한다. 검증 속성에 대한 자세한 데이터와 수집 방법은 Table 3과 같다.

Table 3. Verification Attribute Information by LoIP

Level	Basic Verification Attribute	Expansion Verification Attribute
LoIP0	ID	-
LoIP1	Identification Information (resident registration number, email, cellular phone number)	Register Information (name, age, birthday, gender, country etc,)
LoIP2	LoIP1 + Corroborative information	User registration information and user creation information (profile, address, school, workplace, friends list, photo, etc.)
LoIP3	LoIP1 + LoIP2 + Authoritative information (registration card, passport information, driver license)	Responses to feature-based queries, requested creation information (posts, photos, location, etc.)

사용자는 비대면 온라인 서비스를 이용하기 위해서, 서비스 제공자가 요구하는 본인확인 등급을 평가받기 위해서 필요한 속성 정보들만 IDP로 제공하면 된다. 레벨 0와 레벨1은 사용자가 직접 입력하거나 보조정보 소스를 통해서 속성 정보를 제공받을 수 있다. 그리고 레벨2는 보조정보 출처로부터 다양한 사용자 속성 정보를 사용자의 승인아래 제공받을 수 있다. 마지막으로 레벨 3은 신뢰정보의 속성 정보를 사용자로부터 직접 입력 받거나 사본을 제출 받을 수 있다. 결과적으로 제안방법은 본인확인 등급에 맞게 세분화된 사용자 데이터를 수집하고, 이를 속성 검증에 사용하여 본인확인 보증 등급을 평가하고 신뢰성 정보를 생성하는데 활용한다.

3.3 본인확인 속성 검증 방안

본 논문에서 제안하는 비대면 본인확인 방법은 국내외 표준을 참고하여, 사용자 속성 정보의 검증 효율성과 신뢰성 제공을 위해서 본인확인을 4단계로 나누어 검증한다. 본인확인 보증 등급에 따른 세부 검증 기준은 Table 4와 같다.

Table 4. Verification Criteria by LoIP

Classifi-cation	Verification Criteria	Description
LoIP0	None	• Verify identifier(ID/PW) only in IDP
LoIP1	Uniqueness	• Verify the identification attribute information
LoIP2	Uniqueness, Existence, Weakly associativity	• Uniqueness and existence decision: Verify user attribute information from corroborative source • Existence and associativity decision: Confirm the existence of the identification information of LoIP1 from the authoritative sources
LoIP3	Uniqueness, Existence, strongly associativity	• Existence and associativity decision: Verify authoritative information from authoritative sources • Possession-based verification (ID, SMS, email) and feature-based verification (information creation, query response)

비대면 본인확인 검증 방법의 종류 및 구체적 활용방안은 우선 사용자의 유일성 검증을 위해서 식별정보를 수집하고 신뢰정보를 이용하여 유일성과 존재성, 연계성을 판단한다. 그리고 사용자가 보조정보 소스로의 접근 권한을 위한 정보를 알고 있는지 지식기반 검증을 수행하고, 보조정보 소스의 정보와 등록 및 수집된 사용자 속성 정보를 확인하여 사용자의 존재성과 약한 연계성을 검증한다. 또한 소지기반 검증은 사용자가 메일 계정이나 이동 단말기를 소지하고 있는지를 임시 인증번호 값을 이용하여 사용자의 강한 연계성을 검증하기 위해서 사용한다. 마지막으로 특징 기반 검증은 사용자만이 생성할 수 있는 정보를 요청하여 연계성을 검증하거나 수집된 사용자의 데이터를 기반으로 질의응답을

수행하여 사용자의 존재성과 강한 연계성을 추가적으로 검증하기 위해서 사용한다. 추가적으로 제안방법에서 공인기관인 신뢰정보 소스를 이용하는 검증절차는 각 기관에서 제공하는 검증 서비스 API를 활용할 수 있다. 또한 본인확인 등급별 기준 속성 검증 외에도 사용자의 신뢰도를 제공할 수 있는 보조적 평가항목으로 신뢰성 정보를 검증한다. 이를 위해서 각 속성들에 대한 검증 결과를 점수화 계산을 통해서 비대면 본인확인의 신뢰성 평가 정보를 제3자에게 제공한다. 이 정보는 각 서비스 제공자들이 보다 세분화되고 유연한 기준을 적용하여 본인확인 서비스를 자신의 서비스에 다양하게 적용할 수 있도록 지원한다. 이를 위해서 각각의 본인확인 등급(레벨)에서 검증하는 속성 정보들과 가중치 정보는 Table 5와 같이 정의한다.

Table 5. Verification Attribute by LoIP

Classifi-cation	Basic Attribute Verification	Weight
LoIP0	ID	0
LoIP1	Resident number (mandatory), email, phone number	w1 (50)
LoIP2	Subscription verification of an corroborative source, Confirm the existence of identification information in corroborative sources	w2 (50)
LoIP3	Verify authoritative information attributes	w3 (50)
Classifi-cation	Expansion Attribute Verification	Weight
LoIP0	None	0
LoIP1	Name, age, birth date, sex, area, etc.	w12 (w1/5)
LoIP2	User attribute information in corroborative sources (detailed address, workplace, school, friend information, post, photo, etc.)	w22 (w2/5)
LoIP3	Possession-based attribute information, feature-based attribute information	w32 (w3/2)

제안하는 본인확인 등급별 검증 속성을 점수화 하는 방법은 크게 두 가지로 나눈다. 첫 번째는 기본 속성 검증을 통해서 상기 언급된 등급별 세부 기준을 충족하는지 검증하여 본인확인 등급을 확정하는 방법이다. 두 번째는 확장 속성 검증을 통해서 각 등급의 추가적인 사용자 속성들을 점수화하여 신뢰성 정보를 생성하는 방법이다. 이를 기반으로 사용자의 본인확인 등급과 신뢰성 정보를 평가하는 본인확인 점수화 방법(scoring method of identification level)은 Equation (1), Equation (2)로 표현할 수 있다. 식에서 w_i은 속성별 가중치, b_n은 기본 속성 정보, e_n은 확장 속성 정보, P_LoIP_n은 각 등급별 검증 점수, P는 본인확인 등급의 종합 검증 점수를 나타낸다.

$$P\_LolP_n = (b_1 \times w_i + b_2 \times w_i + ...b_n \times w_i) + (e_1 \times w_{i2} + e_2 \times w_{i2} + ...e_n \times w_{i2}) \quad (1)$$

$$P = P\_LolP_1 + P\_LolP_2 + P\_LolP_3 \quad (2)$$

제안방법은 위에서 언급한 신뢰성 점수화 계산식을 통해서 사용자의 본인확인 등급 검증과 함께 추가적인 신뢰성 정보를 생성한다. 그리고 이렇게 계산된 속성 검증 정보를 사용자 및 온라인 서비스에게 제공하여 온라인 비대면 본인확인 서비스의 보다 세분화되고 유연한 신뢰성 정보를 활용할 수 있도록 지원할 수 있다.

3.4 비대면 본인확인 보증정보 공유 모델

비대면 본인확인 보증정보 공유 모델은 IDP에서 비대면 본인확인 과정을 통해서 본인확인 보증 등급과 신뢰성 정보를 생성하여 서비스 제공자에게 본인확인 보증정보를 제공하는 서비스 모델이다. 이런 서비스 모델은 온라인에서 핀테크와 같은 다양한 서비스 제공자가 신원확인 정보뿐만 아니라 사용자에 대한 신뢰할 수 있는 속성 정보를 이용하여 다양한 서비스를 제공하기 위한 정보 공유 방법으로 활용될 수 있다. 이와 같은 모델의 구성 요소와 기본 절차는 Fig. 3처럼 표현할 수 있다.

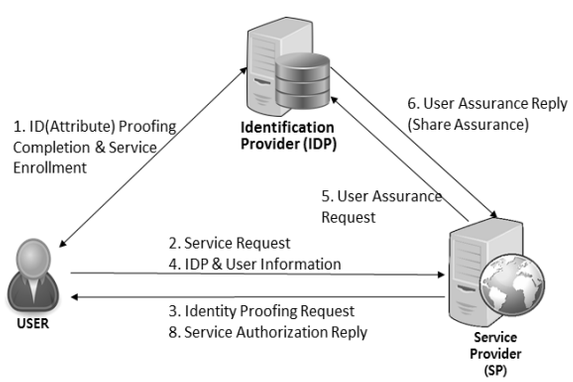


Fig. 3. An Identity Proofing Information Sharing Model

4. 제안 모델의 구현 및 검증(평가)

4.1 비대면 본인확인 검증 모델 구현

본 논문에서 제안하는 빅데이터 기반의 비대면 본인확인 서비스 모델은 신원확인 관리에 관한 국내외 표준을 근거로 온라인상의 모든 기관에서 활용할 수 있는 빅데이터 기반의 본인확인 보증 등급과 신뢰성 정보를 평가하고 이를 공유하는 신원확인 및 공유 서비스 모델이다. 이를 구현 및 검증하기 위해서 본 논문은 사용자의 소셜 빅데이터를 보조정보로 사용하고 사용자의 주민등록 정보를 신뢰정보로 사용하였다. 앞서 소개한 제안 모델은 사용자, IDP, TIS, SIS, SP

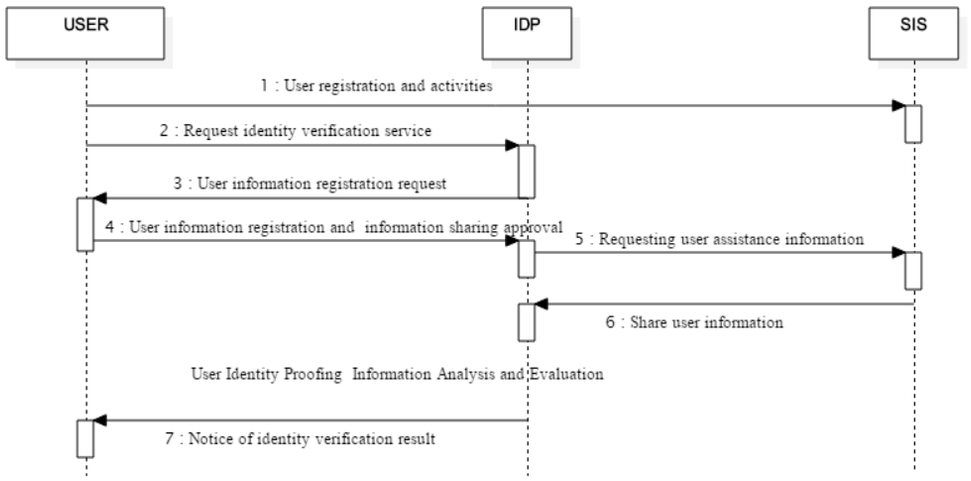


Fig. 4. A Procedure for Collecting User Identification Attribute Information

와 같이 크게 5종류의 개체로 구성된다. 우선 IDP는 사용자의 본인확인 검증을 수행하기 위해 사용자로부터 속성 정보를 수집한다. 속성정보의 수집방법은 사용자가 직접 입력하는 방법과 사용자가 보조정보 소스로부터 정보의 공유를 승인하여 수집하는 방법으로 이뤄진다. Fig. 4는 IDP에서 사용자의 속성정보와 소셜 정보를 수집하는 과정을 보여준다.

위와 같은 절차를 통해서 IDP는 사용자의 수집된 속성정보를 이용하여 본인확인 검증을 수행한다. Fig. 5는 IDP에서 사용자가 본인확인 보증 등급을 평가 받기 위해서 직접 속성 정보를 입력하거나 소셜 로그인을 통해서 보조정보 소스로부터 정보를 공유 받아 본인확인 정보를 검증한 결과화면이다. 본인확인 속성 검증은 IDP에서 수집된 본인확인 속성 정보에 기반으로 하는 본인확인 보증 등급과 신뢰성 수준을 평가한다. 이렇게 평가된 본인확인 정보는 서비스 제공자와 다른 IDP에 제공될 수도 있다.

Fig. 5. An Example of User Information for Identity Proofing

4.2 비대면 본인확인 검증 모델 분석 및 평가

제안방법의 분석 및 평가를 위해서 소셜 네트워크 서비스(SNS)인 페이스북을 이용하는 실험 참가자 5명과 실험을 위해서 생성한 가상의 사용자 5명의 계정정보를 활용하여 사용자 10명의 데이터를 수집하고 평가하였다. 실험을 통해서 제안 방법은 사용자들의 신뢰성 정보와 보증 등급을 평가 하였고, 평가 결과가 사용자 정보의 수에 많은 영향을 받는 것을 Fig. 6을 통해서 확인할 수 있다.

실험 결과에서 유일성을 보장하는 레벨 1등급은 기본 식별정보만 있으면 만족할 수 있기 때문에 실험자 전원이 획득하였다. 그러나 레벨 2등급은 유일성과 더불어 존재성, 약한 연계성을 만족시켜야하기 때문에 실험자 중에서 SNS 사업자에게 자신의 정보를 자세히 등록하지 않은 일부 사용자들이 2등급의 신뢰성을 획득하지 못하였다. 그리고 2등급을 획득한 사용자 중에 신뢰정보와 소지기반 검증을 절차대로 수행한 사용자들은 모두 레벨 3등급의 신뢰성을 획득할 수 있었다. 전체적으로 사용자의 신뢰성 점수는 평균 294점으로 계산되었으며, 3등급까지의 본인확인을 검증 받은 사용자들은 평균 16.8개의 사용자 정보를 IDP에 제공하였다. 하지만 실험에 참가한 피실험자의 수와 데이터의 양이 적어서 검증 결과에 대한 신뢰성 확보를 위해서는 추가적인 실험이 요구된다.

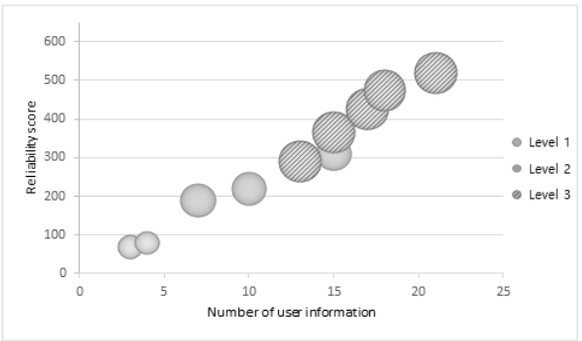


Fig. 6. Analysis Result of the User Identity Proofing

5. 결 론

본 논문은 핀테크 서비스와 온라인 금융서비스의 발전을 위해서 필요한 기술 중 하나인 비대면 본인확인 기술의 위험성을 최소화하고 신뢰성을 높일 수 있는 새로운 비대면 본인확인 기술을 제안하였다. 제안 방법의 핵심적인 내용은 온라인에서 본인확인 주체의 정보를 정보소스로부터 수집하여 본인을 확인하는 빅데이터 기반의 본인확인 기술로 국내외 표준을 참고하여 본인확인 보증등급뿐만 아니라 신뢰성을 보여주는 검증 점수도 평가한다. 또한 본인확인 보증정보를 다른 서비스 업자들에게 제공할 수 있도록 보증정보 공유 모델도 제안하였다.

향후 연구는 본 논문에서 제안한 비대면 본인확인 기술에서 사용한 정적인 속성 정보에 추가적으로 동적인 정보도 이용하는 강화된 빅데이터 기반의 본인확인 기술에 대한 연구를 수행할 예정이다.

References

[1] H. Y. Youm, K. H. Kim, and S. H. Kim, “Guideline on Identity Proofing Management,” *TTA Journal*, Vol.167, pp.78-82, 2016.

[2] TTA Standard, “Guideline on Identity Proofing Management,” TTAK.KO-12.0292, 2016.

[3] FIDO Alliance [Internet], https://fidoalliance.org/.

[4] X.1254 : Entity authentication assurance framework, May 2013.

[5] K. H. Kim, D. H. Yoo, S. H. Kim, B. J. Yoon, and H. Y. Youm, “Gap Analysis of ISO/IEC 29115 and ISO/IEC 29003 for Electronic Financial Services Environment in Korea,” *Review of Korean Society for Internet Information*, Vol.16, No.2, pp.65-69, 2015.

[6] K. Hong and K. Lee, “Advanced Mandatory Authentication Architecture Designed for Internet Bank,” *Journal of the Korea Institute of Information Security & Cryptology*, Vol. 25, No.6, pp.1503-1514, 2015.

[7] ISO/IEC 29115:2013, Information security - Security techniques - Entity authentication assurance framework.

[8] ISO/IEC 2nd CD 29003, Information security - Security techniques - Identity proofing.

[9] H. Yeuk, H. Yim, K. Lee, and K. Yim, “A Trend Analysis on Online Identity Verification methods,” *REVIEW OF KIISC*, Vol.25, No.6, pp.28-46, 2015.

[10] S. W. Lee, H. S. Kim, and K. Y. Yoo, “A Password - based Efficient Key Exchange Protocol,” *Journal of KISS : Information Networking*, Vol.31, No.4, pp.347-352, 2004.

[11] Y. J. Shin, S. H. Shin, J. Lee, and W. Han, “A Study on Improvement of Identification Means in R.O.K.,” *Journal of Korean Association for Regional Information Society*, Vol.18, No.4, pp.59-88, 2015.

[12] Financial Services Commission, “A Rationalization of Real Name Verification on the Account Opening,” 2015.

[13] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, “Forth-Factor Authentication: Somebody You Know,” in *Proc. 13th ACM Conference on Computer and Communications Security*, pp.167-178, Oct., 2006.

[14] P. Hanacek, K. Malinka, and J. Schafer, “e-Banking security - A comparative study,” *IEEE Aerospace and Electronic Systems Magazine*, Vol.25, No.1, pp.29-34, 2010.

[15] NIST Special Publication, 800-63-2 Electronic Authentication Guideline.

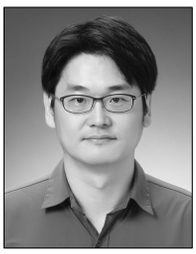
[16] OAuth 2.0 [Internet], https://oauth.net/.

정 관 수

e-mail : ksjung@howon.ac.kr
2007년 충남대학교 컴퓨터공학과(석사)
2007년~2009년 ETRI 연구원
2015년 충남대학교 컴퓨터공학과(박사)
2016년~현 재 호원대학교
사이버보안학과 조교수
관심분야 : IoT, 인증보안, 정보보호, 이동통신

염 희 균

e-mail : yeom@dju.kr
2002년 대전대학교 컴퓨터공학과(석사)
2007년 대전대학교 컴퓨터공학과(박사)
2012년~현 재 대전대학교 컴퓨터공학과
강의전담 교수
관심분야 : 클라우드 컴퓨팅, SW공학,
차세대 로봇, 빅데이터



최 대 선

e-mail : sunchoi@kongju.ac.kr
1997년 POSTECH 컴퓨터공학과(석사)
2009년 KAIST 전산학과(박사)
1999년~2015년 ETRI 인증기술연구실장
2015년~현 재 공주대학교 의료정보학과 부교수

관심분야 : 인증, 개인정보보호, 이상거래탐지, 의료정보보안, 머신러닝