

# A STUDY ON BIG DATA BASED NON-FACE-TO-FACE IDENTITY PROOFING MODEL

<sup>1</sup>HEEGYUN YEOM, <sup>2</sup>DAESON CHOI, <sup>3</sup>KWANSOO JUNG, <sup>4</sup>SEOKHUN KIM

<sup>1</sup>Professor, Daejeon University, Department of Computer Engineering, Korea

<sup>2</sup>Professor, Kongju National University, Department of Medical Information, Korea

<sup>3</sup>Professor, Howon University, Department of Cyber Security, Korea

<sup>4</sup>Professor, Paichai University, Department of Electronic Commerce, Korea

E-mail: <sup>1</sup>yeom@dju.kr, <sup>2</sup>sunchoi@kongju.ac.kr, <sup>3</sup>ksjung@howon.ac.kr,

<sup>4</sup>vambition@daum.net (Corresponding Author)

## ABSTRACT

Online service providers are increasingly considering the adoption of a variety of additional mechanisms to supplement the authentication security provided by conventional password verification. Recently, the authentication and authorization methods using the user attribute information have been used for various services. In particular, the need for various approaches to non-face-to-face identification technology for online user registering and authentication are increasing demands because of the growth of online financial services and the rapid development of financial technology. However, non-face-to-face approaches can be generally 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. Thus, we propose a big-data based non-face-to-face Identity Proofing model that verifies identity on online based on various and large amount of information of user. The proposed model performs identification of various attribute information required for the identity verification level. In addition, the proposed model can be quantified identity proofing reliability as collects and verifies only the user information required for assurance level of identity proofing.

**Keywords:** *Non-Face-To-Face, Authorization, Identity Proofing, Big Data*

## 1. INTRODUCTION

In recent years, FinTech has been leading the financial services industry. Such a convergence trend of finance and technology is rapidly growing around the world, creating destructive innovation and added value to the financial market through ICT. Traditional financial institutions have used offline face-to-face systems to provide users with the reliability and security essential to financial services. On the other hand, FinTech companies are leading innovation in financial services by introducing a new type of financial business model that is different from existing financial transaction methods based on advanced technology. Among these technological innovations, online professional financial institutions and non-financial institutions are leading innovations to provide users with various financial services based on non-face-to-face systems. Also, as the user authentication technology such as FIDO (Fast IDentity Online) [3] is advanced recently, the time of Identity proofing is shifted from the local to the remote location, and thus the importance and reliability of Identity

proofing are more emphasized. In order to respond to these changes, the Korean Financial Services Commission has recently issued guidelines for Identity proofing non-face-to-face personal information. Recently, the convenience and reliability of the supplementary information have been improved because the service providers of the online collect and utilize various information of the user in order to provide the customized service. For this reason, SNS authentication technology using Big data, which is a lot of information of users, is being studied in the authentication technology field. Big data based authentication technology such as SNS authentication extracts attribute information required for authentication based on a large number of data and is used for user authentication and ID theft detection through a process of confirming this information from the user. Since the SNS authentication information extraction and verification process is similar to the identity proofing process for verifying the attribute information of the user, it can be applied to the non-face identification method. In this paper we propose a large data base that verifies user attributes in order

to provide high accuracy of Identity proofing based on TTA.KO-12.0292 [2] and International Standard X.1254 [4] To-face Identity proofing model. The proposed identity proofing model divides the user attribute information into the identification information and the auxiliary information, and confirms a plurality of attribute information required for the identity verification level. In this way, the proposed model can classify the identity verification level of granularity and quantify the identity verification reliability by collecting and verifying the information required for the guarantee level. This proofing model can be used not only for identification but also for ID theft detection. In addition, since the proposed model only requires attribute information that can confirm the level of the user assurance required for the service, it provides efficiency in service aspect and convenience in user aspect. The composition of this paper is as follows. Section 2 introduces the related research, and Section 3 explains the detailed description and verification method of the proposed identity proofing model. Section 4 describes the implementation and evaluation of the proposed model, and Section 5 describes the conclusions of this study.

## 2. RELATED WORK

### 2.1 Overview of Identity Proofing

#### 2.1.1 Overview

Identity proofing is a process that identifies whether a person is a person or not through a specific method [5, 6]. This is sometimes used in combination with the term Identity proofing. Identification as defined in national standards is a process by which an Identity proofing and verification body gathers information and verifies its identity [1] to identify the identity of an entity with a certain assurance level. In this paper, we define the concept of identifying a specific user entity as Identity proofing.

#### 2.1.2 Reference Standards

ISO / IEC and TTA are actively pursuing domestic and international standardization processes related to identity proofing. First of all, ISO / IEC 29115 [7] provides 4 levels of assurance as an international standard, and it covers the process of authentication threats and controls, assurance level standards, related terms, related subjects, and entity authentication. ISO / IEC 29003 [8] presents three levels of identity proofing and requirements, including Identity proofing

objectives, identification information, related terms, related entities, and Identity proofing processes[5]. In Korea, the TTA established a standard (TTAK.KO-12.0292) [2] for domestic guidelines for identity proofing management. This standard is applicable to the identity proofing management guidance of financial institutions providing Internet financial services and defines online identity verification methods and grades based on international standards (ISO / IEC 29003) and domestic guidelines[1, 2].

#### 2.1.3 Identification Means

The identity means refers to a procedure for confirming that the identity is authenticated by using the identification information given by the identity verification organization to the user and the secret information that the user only knows or holds. A means for verifying that a subject requesting a service or information is the user himself or herself and verifying the user is a means of identifying the user[9]. This identity verification means consists of an identification that identifies who the subject is, authentication to authenticate the subject, and an authorization step to grant system resources to the subject. It is a requirement[10]. Depending on the nature of the identity verification method, various methods are applied depending on whether they are face-to-face or non-face-to-face, electronic / resident registration number provision. In Korea, identity verification is performed using various methods such as I-PIN, official certificate, mobile phone authentication, etc. based on domestic laws[11].

### 2.2 Big Data based User Authentication

The research that verifies user identification information or user authentication by utilizing big data may be used as verification technology of auxiliary attribute information for identity proofing[20]. In particular knowledge - based authentication and trust - based authentication which analyze user 's social data and verify user' s attributes are actively researched on Facebook and Google.

#### 2.2.1 Social Authentication

Existing sns authentication schemes utilize social knowledge to authenticate users or utilize mutual trust among users [17,18,20]. Specifically, the most-studied method of the previously proposed knowledge-based social authentication method mainly performs user authentication based on a user-posted picture on an online social network

(OSN) site [19,21,22]. Also, a method of identifying the user and generating related questions by analyzing the user's personal information, location information and behavior was also proposed [23,24,25]. In addition, in the case of the trust-based authentication method, many researches are conducted on a system that identifies a user or performs authentication using a trust relationship between users[26,27,28,29,30]. Further, in an attempt to replace the password Google recently proposed a method of determining the level of authentication based on a calculated confidence score based on several factors related to user activity and usage patterns[31].

**2.3 Non- face-to-face Identity Proofing**

In the case of an Internet bank or a new FinTech service Identity Proofing is performed on a non-face-to-face basis for online service registration [1, 6]. However, the non-face-to-face method is relatively weaker than the face-to-face method in terms of risk such as impersonation of others. Therefore, in order to enhance the safety of the non-face-to-face method in Korea, it is obligatory to double check two out of 4 non-face-to-face identity proofing methods and to check multiple elements by applying additional confirmation method [2, 12].

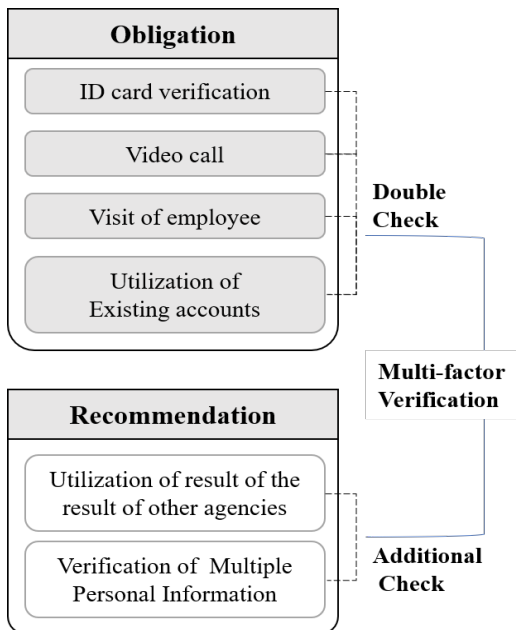


Figure 1: Authentication factors for the non-face-to-face identity proofing [2]

Figure 1 shows multiple (more than two) element verification methods to ensure the accuracy of real-name verification of non-face-to-face verification methods. Using these diverse identity proofing tools

at various levels of validation, you can perform stronger, non-confidential self-identification online.

**2.4 Identity Information**

Identity proofing is the process of verifying an entity based on various information. The user attribute information used in this process greatly affects the proofing reliability of identity proofing. The identity proofing is largely composed of identification attribute information and auxiliary attribute information.

An identification attribute is information that is used to uniquely identify an entity in one context by combining one or more pieces of identification information. In addition to the identification attribute information, the auxiliary attribute is the attribute information necessary to support the identity proofing process and indicates the relationship or association between the information subject and the identity information [2]. Table 1 shows examples of typical Identity proofing attribute information.

Table 1: An example of identification information [2]

Definition	Example of identification information
Identification Attribute	name, birthday, address, phonenumber, birthplace, resident registration number, email, bio information etc.
Corroborative Attribute	Other names, relationships and associations, reference numbers for identity evidence, information about the identity evidence provided, etc.

The Identity proofing assurance level associated with reliability is a three-level rating in ISO / IEC 29003 and a four-level rating in ISO / IEC 29115 [5, 7, 8]. In this study, we refer to the 4-step Level of Identity Proofing (LoIP) proposed in the national identification management guidance standard. The identity proofing assurance level and the objective of each grade are shown in Table 2.

Table 2: A level of identity proofing [2]

Description	Objective
LoIP0-Non Confidence	<ul style="list-style-type: none"> <li>No identification method is required. (using ID or Password)</li> </ul>
LoIP1-Low Confidence	<ul style="list-style-type: none"> <li>Identity is unique within context</li> </ul>
LoIP2-Medium Confidence	<ul style="list-style-type: none"> <li>Identity is unique within context</li> <li>the entity to which the identity pertains exists</li> <li>Information entity is weakly associated with identity</li> </ul>
LoIP3-Very High Confidence	<ul style="list-style-type: none"> <li>Identity is unique within context</li> <li>the entity to which the identity pertains exists</li> <li>Information entity is strongly associated with identity</li> </ul>

Identity proofing the three criteria for determining the assurance level are defined as follows.

- Uniqueness: The subject's identity is unique.
- Existence: The identity of the subject exists.
- Connectivity: The identity of the subject is associated with the subject of information within that context.
- Connectivity: The identity of the subject is associated with the subject of information within that context.

### 3. NON-FACE-TO-FACE IDENTITY PROOFING MODEL

The non-face-to-face identity proofing model provides simplicity and security to prove the identity of a person online without having to prove themselves offline. In order to provide higher accuracy of identity proofing in accordance with the domestic and foreign policy situation which recommends using multiple methods together, considering the complement of non-face identification method, Is a non-face-to-face identification model. This chapter describes the identity proofing model and explains the user's big

data collection method and identity proofing verification algorithm.

#### 3.1 Big data based non-face-to-face identity proofing model

The identity proofing method proposed in this paper is a method of identifying users by verifying uniqueness, existence, and connectivity which are the criteria for identity assurance level based on a plurality of user identity verification attribute information.

In addition, to prevent the unintentional collection of user information, the proposed method collects and analyzes only the user attribute information according to the identity verification level required by the online Non-face-to-face service. As a result, the identity proofing information provider verifies the attribute information provided by the user in order to perform the granular identity proofing required by the service to be used by the user, evaluates the guarantee level of the attribute information, and provides the service provider with identity proofing results. The proposed model basically consists of an identity proofing information provider (IDP) that performs identity proofing with the user, a trust information server (TIS) that verifies the user's trust information, user data (registration and creation information) A Secondary Information Server (SIS), and a Service Provider (SP) that provides services to users. Figure 2 shows the components and service concept diagram of the proposed model.

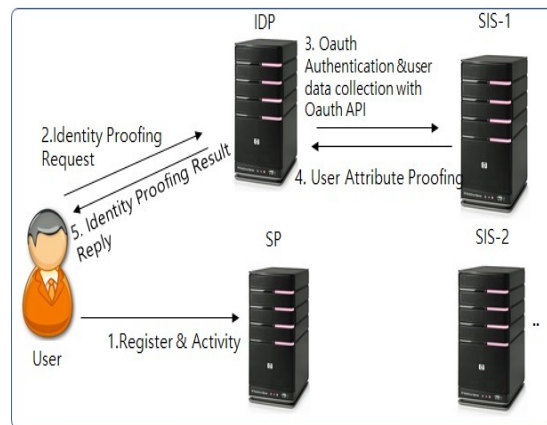


Figure 2: A concept of Big Data based identity proofing model

#### 3.2 Identification information collection

In order to prevent the user from collecting the attribute information of the user indiscriminately, the proposed method requires only the attribute

information required for the service requested by the user and can receive the input directly. Alternatively, the proposed method uses the Open API based authentication protocol such as OAuth (Structured / Unstructured) registered and generated by the user. User identity information required for each identity proofing assurance level is divided into basic verification attributes and extended verification attributes for the assurance level evaluation. The detailed data and the collection method of the verification attribute are shown in Table 3.

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.)

In order to use the non-face-to-face online service, the user only needs to provide the IDP with the attribute information necessary for evaluating the identity proofing grade requested by the service provider. Level 0 and Level 1 can be entered directly by the user or provided with attribute information through an auxiliary information source. And level 2 can be provided with various user attribute information from the auxiliary information source under the user's approval. Finally, level 3 can receive the attribute information

of the trust information directly from the user or submit a copy. As a result, the proposed method collects user data segmented according to the identity proofing class and uses it to verify the identity proofing assurance level by using it for attribute verification.

### 3.3 Verification attribute

The non-face-to-face identity proofing method proposed in this paper verifies identity proofing in four steps in order to provide verification efficiency and reliability of user attribute information, referring to domestic and international standards. identity proofing Table 4 shows the detailed verification criteria according to the assurance level.

Table 4: Verification criteria by LoIP

Classification	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)

Non-face-to-face identity proofing the type of verification method and the concrete application method first collect identification information for user's uniqueness verification and use unreliability information to determine uniqueness, existence and connectivity. Then, we perform knowledge - based verification that the user knows the information for access rights to the auxiliary information source, verify the existence and weak connection of the user by checking the information of the auxiliary information source and the registered and collected user attribute information. Also, the base-based verification is used to verify whether a user has a mail account or a mobile terminal by using a temporary authentication number value. Finally, feature-based verification is used for verifying the connectivity by requesting only the information that can be generated by the user or by performing a query response based on the collected user's data to additionally verify the existence and strong connection of the user. Attribute information to be verified at each identity proofing level is defined as shown in Table 5.

Table 5: Verification Attribute By LoIP

Classification	Basic Verification Attribute
LoIP0	ID
LoIP1	Identification Information (resident registration number, email, cellular phone number)
LoIP2	LoIP1 + Corroborative information
LoIP3	LoIP1 + LoIP2 + Authoritative information (registration card, passport information, driver license)
Classification	Expansion Attribute Verification
LoIP0	None
LoIP1	Name, age, birth date, sex, area, etc.
LoIP2	User attribute information in corroborative sources (detailed address, workplace, school, friend information, post, photo, etc.)

LoIP3	Possession-based attribute information, feature-based attribute information
-------	---

4. IMPLEMENTATION AND VERIFICATION OF PROPOSED MODEL (EVALUATION)

4.1 Implement non-confidential identity verification model

The big data based non-face-to-face identity proofing model proposed in this paper is used to evaluate the identity proofing assurance level of Big Data based on the online standards based on domestic and international standards on identity management. In order to implement and verify this paper uses user 's social big data as auxiliary information and user' s resident registration information as trust information. The proposed model consists of five kinds of objects such as user, IDP, TIS, SIS, and SP. First, the IDP collects attribute information from the user to perform identity proofing verification of the user. The method of collecting the attribute information is performed by a method of directly inputting by the user and a method of allowing the user to collect information by sharing the information from the auxiliary information source. Figure 3 shows the process of collecting user's attribute information and social information in IDP.

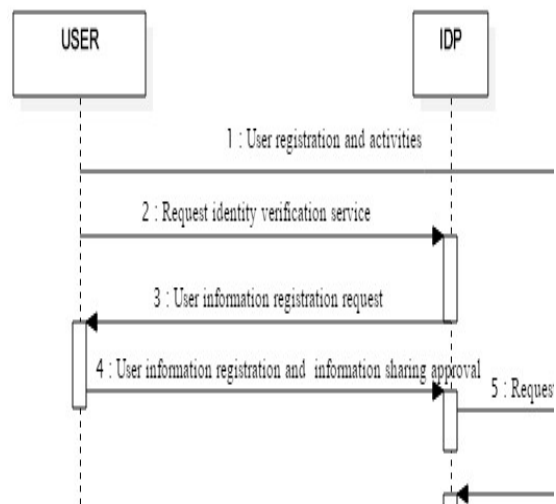
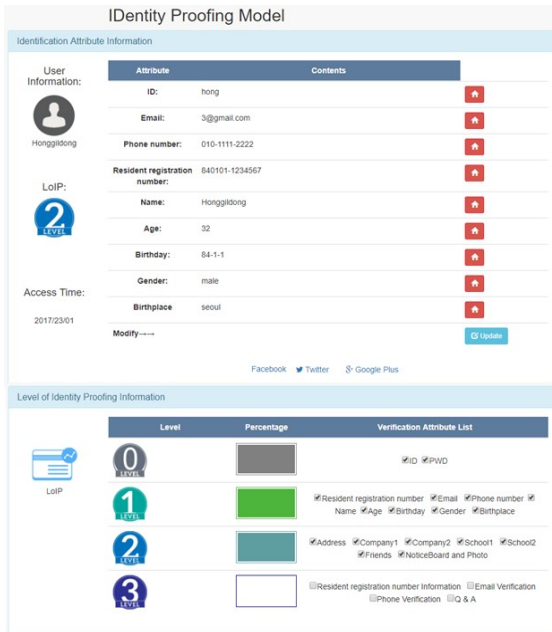


Figure 3: A Procedure For Collecting User Identification Attribute Information

Through the above procedure, the IDP performs identity proofing verification using the collected attribute information of the user. Figure 4 is a result

screen of IDP in which the user inputs the attribute information directly in order to evaluate the identity proofing assurance level or verifies the identity proofing information by sharing the information from the auxiliary information source through the social login. Identity proofing Attribute verification evaluates the identity proofing assurance level based on the identity proofing attribute information collected at the IDP.



The screenshot shows the 'Identity Proofing Model' interface. It is divided into two main sections: 'Identification Attribute Information' and 'Level of Identity Proofing Information'.

**Identification Attribute Information:** This section displays user details for 'Honggildong'. It includes fields for ID (hong), Email (3@gmail.com), Phone number (010-1111-2222), Resident registration number (840101-1234567), Name (Honggildong), Age (32), Birthday (84-1-1), Gender (male), and Birthplace (seoul). There are 'Modify' and 'Update' buttons at the bottom.

**Level of Identity Proofing Information:** This section shows four levels of verification:

Level	Percentage	Verification Attribute List
0	0%	ID, PWD
1	25%	Resident registration number, Email, Phone number, Name, Age, Birthday, Gender, Birthplace
2	50%	Address, Company1, Company2, School1, School2, Friends, NoticeBoard and Photo
3	75%	Resident registration number Information, Email Verification, Phone Verification, IQ & A

Figure 4: An Example Of User Information For Identity Proofing

#### 4.2 Analysis and evaluation of non-face-to-face identity proofing model

For the analysis and evaluation of the proposed method, we collected and evaluated the data of 10 users using the account information of five experiment participants using Facebook, which is a social network service (SNS) and five virtual users created for the experiment. Experimental results show that the proposed method evaluates users' reliability information and assurance level and the evaluation result is influenced by the number of user information Figure 5.

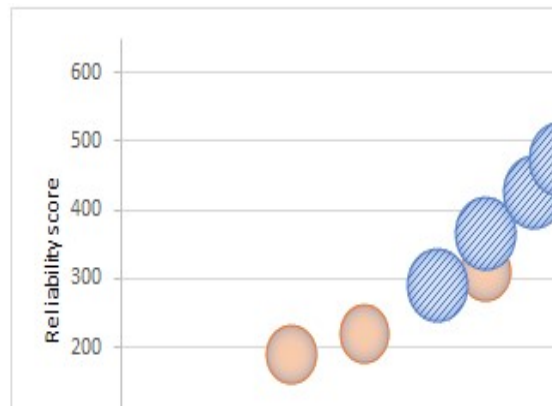


Figure 5: Analysis Result Of The User Identity Proofing

In the experimental results, the level 1 class that guarantees uniqueness was acquired by all the experimenters because only the basic identification information can be satisfied. However, some users who did not register their own information in SNS provider among SNS providers were not able to acquire the second grade because the level 2 class had to satisfy existence and weak connection with uniqueness. And among the users who acquired the second grade, all the users who performed the trust information and the possession based verification procedures were able to obtain the third grade. Overall, users who have proven identity proofing up to grade 3 provided an average of 16.8 user information to IDP. However, the number of subjects participating in the experiment and the amount of data are small, so additional experimentation is required to ensure the reliability of the verification results.

#### 4.3 Case Study

Traditional identity verification focuses on identification similar to authentication. However, since this method is insufficient to identify a user, various identification methods have been proposed based on recent social network service user information and friends list a method of identifying a user's identity by a query response method has been proposed. As the FinTech service expands, it is recommended to use a stronger identification method that is complemented by a combination of identity verification standards and various identity verification methods required by the government. thus, a method of confirming the identity of a user using a plurality of pieces of personal information provides information for determining a user's identity by calculating a reliability (score) based on the information of the user.

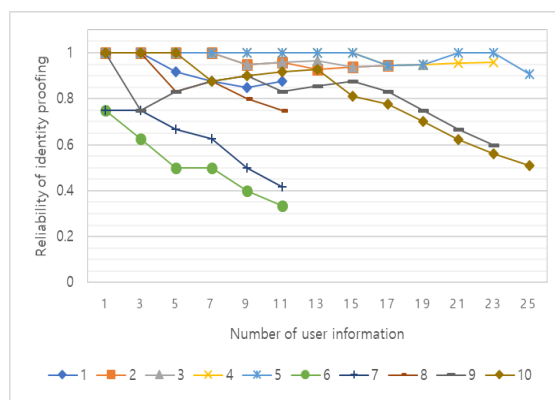


Figure 6: Reliability Of Identity Proofing On The Impact Of The Number Of User Information

Figure 6 shows the confidence score calculated by evaluating the user's information. According to the experimental results, the reliability of actual users (1 to 5) is maintained over 90% even if the amount of information increases. However, the reliability of a virtual account (6 to 10) does not match the information you enter, so the more information you need to check, the less stable it is. As a result, it can be proven through experiments that the proposed method is suitable for use as a proof of identity by providing a reliability score that can identify a user using a plurality of pieces of information.

#### 4.4 Discussion

Existing social network authentication is a way to verify the identity of people you know. This method is used in emergencies where critical identification means are not available because people can not identify themselves. Existing methods responded to emergencies through e-mail, Q & A inquiry methods and customer center. e-mail is insufficient to satisfy security, and the registration query response method is problematic in that a third party can guess the response and the customer center is costly and vulnerable to social engineering attacks [9]. In order to solve these problems, a method of verifying multi-channel authentication and complex attribute information has been proposed and demanded. The proposed method is a proposed secondary authentication method for multi - channel based identification. To ensure the accuracy and reliability of your identity verification, we identify your identity based on your social data and identify your properties. The proposed method differs from the various identification methods using user information based on various user information (big data), the result of user's identification can be evaluated as reliability value rather than approval and rejection, which plays a complementary role in

multi-channel authentication and multiple factor verification. Therefore, Identification Based on the identity information that the system has assessed, you can gain the accuracy of your identity verification, generate trusted information that can be used to prevent identity theft, and provide the benefit of providing information to other service providers.

#### 5. CONCLUSION

This paper proposes a new non-face-to-face identification technology that minimizes the risk of non-face-to-face identification technology and improves reliability one of the technologies required for the development of Fintech services and online financial services. The key content of the proposed method is a big data based identity verification technology that collects information of the identity verification agent online from the information source and verifies the identity of the user. We also proposed a model for sharing information about assurance to provide other service providers with identity verification information.

Future research will be conducted on strong identification technology based on strong data that uses dynamic information in addition to the static attribute information used in the non-face identification technique proposed in this paper.

#### ACKNOWLEDGMENTS

This work was partly supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (B0717-16-0139, Security Technologies for Financial Fraud Prevention on Fintech) and the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (2016R1A4A1011761).

This work was supported by the research grant of Pai Chai University in 2017.



**REFERENCES:**

- [1] H.Y. Youm, K. H. Kim, and S. H. Kim, "Guideline on Identity Proofing Management", *TTA Journal*, Vol. 167, 2016, pp.78-82.
- [2] TTA Standard, "Guideline on Identity Proofing d
- [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, 2015, pp.65-69.
- [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, Dec. 2015, pp.1503-1514.
- [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, 2015, pp.28-46.
- [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, Aug. 2004, pp.347-352.
- [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, Dec. 2015, pp.59-88.
- [12] Financial Services Commission, "A Rationalization of Real Name Verification on the Account Opening", May. 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*, Oct. 2006, pp.167-178.
- [14] P. Hanacek, K. Malinka, and J. Schafer, "e-Banking security –A comparative study", *IEEE Aerospace and Electronic Systems Magazine*, Vol. 25, No. 1, Jan. 2010, pp.29-34.
- [15] NIST Special Publication, 800-63-2 Electronic Authentication Guideline
- [16] OAuth 2.0[Online], Available: <https://oauth.net/>
- [17] N. Alomar, M. Alsaleh, A. Alarifi, "Social authentication applications attacks defense strategies and future research directions: A systematic review", *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1080-1111, 2nd Quart. 2017.
- [18] R. W. Reeder and S. Schechter, "When the password doesn't work: Secondary authentication for Websites", *IEEE Security Privacy*, Vol. 9, No. 2, Mar./Apr. 2011, pp. 43-49.
- [19] S. Jain et al., "New directions in social authentication," in *Proc. USEC*, San Diego, CA, USA, 2015.
- [20] Upal Mahbub and Rama Chellappa, "PATH: Person Authentication using Trace Histories", *UEMCON 2016*, New York, USA.
- [21] U. Mahbub, S. Sarkar, V. M. Patel, and R. Chellappa. Active user authentication for smartphones: A challenge data set and benchmark results. In *Biometrics Theory, Applications and Systems (BTAS)*, 2016 IEEE 7th Int. Conf., Sep. 2016.
- [22] L. J. Shepard, W. Chen, T. Perry, and L. Popov, "Using social information for authenticating a user session," U.S. Patent 8 910 251, Dec. 9, 2014.
- [23] E. M. Underwood, J. E. Sullivan, and R. McGeehan, "Social age verification engine", U.S. Patent 8 671 453, Mar. 11, 2014.
- [24] M. J. Puflea, "System and method for location-aware social networking authentication", U.S. Patent 13 537 585, Jun. 29, 2012.
- [25] N. Z. Gong and D. Wang, "On the security of trustee-based social authentications," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 8, pp. 1251-1263, Aug. 2014.
- [26] S. Schechter, S. Egelman, and R. W. Reeder, "It's not what you know, but who you know," in *Proc. SIGCHI Conf. Human Factors Comput. Syst. (CHI)*, Boston, MA, USA, 2009.
- [27] "Facebook introducing trusted contacts." (2013). [Online]. Available: <https://www.facebook.com/notes/facebook-security/introducingtrusted-contacts/10151362774980766>, Accessed on Oct. 9, 2015.



- [28] L. Li, X. Zhao, and G. Xue, “Searching in the dark: A framework for authenticating unknown users in online social networks”, in Proc. Glob. Commun. Conf. (GLOBECOM), Anaheim, CA, USA, 2012, pp. 714–719.
- [29] “Google plans to bring password-free logins to android apps by year-end.” (2016). [Online]. Available:  
<http://techcrunch.com/2016/05/23/google-plans-to-bring-passwordfree-logins-to-android-apps-by-year-end/>, Accessed jun. 16, 2016.