Research Article

A Study on the Utilization of MobileElectronic Notice Service using Korean Digital Identity Guidelines

Jong-Bae Kim
Department of Software Engineering, Sejong Cyber University, Seoul, Republic of Korea kjblove@hotmail.com

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: Recently, due to the spread of infectious diseases, the demand for services in a non-connected environment is increasing worldwide. Identifying the service counterpart in such a non-face-to-face environment has become the most important task.In this paper, we examine the status of overseas personal identification systems and explain the Korean digital identity guideline. Using the Korean digital identity guideline, it presents the application plan of mobile electronic notification service that has delivery and proof effect. For personal digital identity, Korea identifies citizens based on a registration number (RN) that is uniquely assigned at birth. However, if the RN is leaked or exposed, the problem of personal privacy invasion has emerged, and in the end, due to personal information protection issues, RNs cannot be collected unless required by law. Therefore, connecting information (CI) was utilized as a digital identity capable alternative to RN to clearly identify users online.CI has the advantage of being encrypted as a 1:1 match to the RN and not being able to identify an individual even if leaked.The mobile electronic notification service is designed to accurately deliver information to the target person in a non-face-to-face environment using CI.This service uses CI to identify the recipient of the electronic document, and after receiving identification from the personal identity proofing agency (PIPA), the service can be verified by reading the information.In this paper, we propose a method to easily provide information in the non-face-to-face era by presenting a method to apply to mobile electronic notification service (MENS) using Korean user identification guidelines.Through the proposed method, it can be confirmed that a system can be established to facilitate the mobile electronic notification service, which has the same effect as the delivery of information online and offline in the non-face-to-face era.

Keywords: Personal identity proofing service, mobile electronic notification service, connecting service, Korea digital identity guidelines**.**

1. Introduction

Due to the spread of infectious diseases that began in late 2019, the global offline market has contracted, and the demand for non-face-to-face services is rapidly increasing [1].Currently, OECD countries, including Korea, are demanding prohibition of large-scale gatherings, prohibition of gatherings, refraining from access to restaurants, and mandatory wearing of masks in public places to minimize the spread of infectious diseases.In particular, when accessing a specific place, users are required to provide personal information for future tracking.These causes are more aimed at preventing social chaos caused by disease and maintaining national security rather than protecting individual privacy.In Korea, users can be identified by collecting resident registration numbers (RN) consisting of 13-character numbers given to citizens when entering public places such as meeting places [2].

The Korean RN was started based on the ‘Resident Registration Act (1962)’, and the RN is also used as a means to identify the person without any other auxiliary means.Since 1975, the RN system has been established and is now universally used. However, as a result of checking through many years of personal information inspection, about 95% of 2,226 responding Internet providers collected user RNs, and 82% of them were collected through the Internet.As RN is used as an identification number, it also has the advantage of improving the convenience of administration and quality of service, but on the contrary, social unrest caused by personal information infringement accidents has increased.In particular, as it was investigated that more than 50% of the cases where RN was included in personal information leaked in a large-scale personal information infringement accident, an alternative RN method was developed to convert RN-based online services and spread to the present.The number of Internet users in Korea is about 436.36 million or 87.7% of the total [3].According to a government survey [4], the purpose of using the Internet is communication (e-mail, SNS, chat, Internet phone, etc.) 91.4%, data and information acquisition 89.4%, leisure activities (web radio, web TV, online games, etc.) 86.2%, operating homepages, etc. 44%, education and learning (online education, Wikipedia, etc.) 34.2%, and jobs and workplaces (job search, job-related online participation, etc.) 14.3%.In order to reduce the damage caused by the indiscriminate collection and misuse of RN, the Korean RN, Korea's ‘Information and Communication Network Act’ and ‘Personal Information Protection Act’ have been amended since 2012 to prohibit the collection of RN online and offline. In addition, the policy was changed to expand the service to verify the identity by equipping the RN alternative means and authentication system.Instead of RN, which can identify users, a system has emerged to identify users by using an identity verification method that can replace them. This system is not a 13-digit number system as information that matches RNs 1:1, and creates an identification system that can be changed.

In general, it is necessary to identify or authenticate a user for a secure online service.Until now, RN, which is a unique identification number assigned to users, has been used, but as collection was prohibited from 2012, a new user identification and authentication system was required.Identification is a process of verifying and authenticating that the user is an agreed upon according to a legitimate and reasonable procedure, and authentication is a process of verifying that the user is the real person through electronic information of online service users [5].In order to issue an alternative means of Korean RN, it is necessary to verify the identity of the person in a face-to-face or non-face-to-face manner.The face-to-face method is first checked by government and local governments, banks, and mobile telecommunication companies, and the non-face-to-face method is an online authentication method, which is used in services such as electronic finance and online transactions.As an alternative to RN, authentication methods can be classified into electronic/non-electronic media. Authentication methods through electronic media include I-PIN, accredited certificate, mobile phone authentication, and credit card authentication, and authentication through non-electronic media [6]. As a method, an identification card (resident registration card, driver's license, passport, etc.), a bankbook, or a credit card can be used.

In order to apply RN, which is a system that can identify users in Korea, as an identity verification method, which is a means to replace online, it is defined to have several suitable requirements.The Ministry of Information and Communication in Korea made appropriate standards in the 2005 ‘Guidelines for alternative means of RN on the internet’ to consider safety, convenience, and legal guarantees.The means of identity verification should have universality and uniqueness, the personal identity proofing agency (PIPA) should consider economic and legal feasibility (clarity of service), and the user should consider the versatility of the identity verification means and the reliability of the identity verification agency.

In order to create a Korean identification method, it is necessary to identify users at a face-to-face level and issue RN alternatives to them.Accordingly, the Korean government has established standards for designating anPIPA and institutionalized it to provide personal identity proofing services only when the required conditions are met.Since this personal identity proofing service also requires information that can identify users, the PIPA created connecting information (CI) that corresponds 1:1 with the user's RN and uses this CI to identify the user.As shown in Figure 1, the user provides his or her identity card to PIPA to receive identification and authentication, and is provided with identification information. The identity verification information is used as a means of presenting the identity to the internet service provider (ISP).

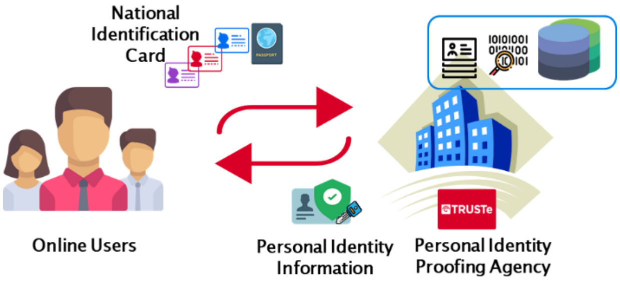
National Identification Card
PASSPORT
10101001
Online Users
Personal Identity Information
TRUSTe
Personal Identity Proofing Agency

Figure 1. Process of issuing personal identification informationthrough a PIPA

Due to the recent spread of infectious diseases, the use of CI for identification of online service users is increasing due to the rapid expansion of online services, and the requirements for using CI in offline services are increasing.In Korea, since 2019, the mobile electronic notification service (MENS) for administrative and public organizations has been implemented, allowing various types of information sent by public institutions to be received through mobile devices [7,14].MENS is a service that delivers information electronically as the existing paper-based mail delivery service requests a change to a non-face-to-face delivery service due to the spread of infectious diseases.Whereas traditionally paper-based mail services are used, MENS is a service that delivers text or push messages to users through electronic document replay providers.Advantages of using the MENS include: First, real-time confirmation of mailings, second, legal effect of electronic document distribution, third, prevention of damage due to loss, fourth, reduction of social costs used for paper mail, and fifth, time reduction. And there is an increase in efficiency.It is necessary to clearly identify users for MNES. In addition, the process of proving that users have received and viewed information accurately is also required.In order to meet these requirements, the use of CI provided by PIPA is a major requirement of Korean MENS.

In this paper, we introduce the current status of Korean-style non-face-to-face personal identification proofing service and propose a method of application to MENS using it.In order to meet the current situation where the demand for non-face-to-face services is increasing due to the spread of infectious diseases, the Korean MENS is a way to accurately transmit important information and prove reading by identifying and authenticating users.In this paper, in Chapter 2, we analyze the current status of overseas identity verification-related systems, and in Chapter 3, we analyze the status of Korean identity verification services. And in Chapter 4, we propose a mobile electronic notification service. Finally, a conclusion is presented.

2. Status of OverseasPersonal Identity Proofing Service

2.1 USA

The U.S. was introduced under the Social Security Act of 1935 to identify tax levies and taxpayers for social security. Since 1936, nine digits linking tax information, credit information, school records and medical records have been used as a personal security number (SSN).These SSN were expanded to include election registration, acquisition of driver's licenses, alien registration, and student registration, and are widely used in the private sector, such as credit card issuance applications, unlike the National Tax Service's handling of tax invoices through taxpayer numbers in 1961 [8].In the financial sector,SSNs and additional identification information (driver's license number, passport number and various other identification numbers) are collected and used for identification.However, in the case of a request for a social security number under the ‘Privacy Act of 1974’, prior notice is required by stipulating the need for submission, the legal basis for the request, the purpose of using the provided social security number, and the method of handling such rejection. The law sets regulations on the use and protection of numbers, and includes regulations on where to take responsibility in case of problems.Personally Identifiable Information (PII), which is used to identify or locate an individual, is used with other information [9, 10].It guarantees the free circulation of most information and has protection laws for each area in various fields.Moreover, according to the ‘The Patriot Act’, when an account is opened through a financial institution, basic information such as an individual's name and address and identification procedures such as social security number are mandatory, and online shopping malls, portals, and game sites It is common not to collect personally identifiable information on sites where electronic transactions are possible.In addition, online sites in the field of e-commerce and entertainment provide a service to sign up for a member using name, address, and payment information (if paid) as basic information for identification purposes.The National Institute of Standards and Technology (NIST) has developed a cyber identity authentication system since 2009, and each state has developed and used identity verification methods [11,15].For example, the Massachusetts Supreme Court ruled that zip codes were personally identifiable information under Massachusetts General Law. Accordingly, when purchasing items with a card at a mart or store, you can authenticate yourself through the PIN number.

2.2Canada

In Canada, Social Insurance Number (SIN) was introduced in 1964 for the identification of customers in the Canadian Pension Plan Administration and Canadian Employment Insurance Program, and in 1967 the Canadian Revenue Service began using it for tax purposes.It is used in 15 administrative tasks such as fines, income tax collection, and unemployment benefits. As a self-certification system, it can only be collected by specific administrative agencies or programs authorized by law, but there is no law prohibiting collection for purposes other than the purpose.However, when the Personal Information Protection Committee asks for a social insurance number, it asks for the law and purpose, and is notified to submit a petition if the service cannot be received due to the failure to provide a social insurance number.Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) regulates the collection, retention, use, and provision of personal information, which applies to the private sector [12].It stipulates that organizations or companies that require social insurance numbers must demonstrate the necessity of collection, and at this time, programs allowed to use social insurance numbers include immigration mediation assistance programs, income and health management programs, income tax objections and reversal decisions, Labor Adjustment Evaluation Committee, National Exposure Level Registry for Occupational Radiation Exposure, Regional and Aboriginal Housing Programs, Social Support and Economic Development Programs, etc.In addition, there is no need for identification procedures for sites that require identification in the financial, entertainment, and e-commerce fields of Canada.Online identity verification tools in Canada have a wide variety of features.In other words, how to use tools that individuals know themselves (password, personal identification number (PIN), account number, favoritecolor, pet name, etc.) and tools that the individual possesses (bank card, token, identification card, public key digital In a simple method using a certificate (public-key digital certificate, etc.), the person himself or herself or their actions (face image, iris recognition, voice recognition, gait, etc.) or other personal behavior information (e.g., specific computer account logon, specific Credit card usage information and web search record information) are also characterized by the diversity of identity authentication technologies that can be used for identity authentication.

2.3United Kingdom

The UK's laws for personal information protection include the EU Data Protection Directive, the Data Protection Act, and the Electronic Communications Act.According to these laws, the storage of personal information is only possible for a specific period with consent.GOV.UK Verify, as a key element of Digital Default, is applying an identity assurance program for the government's online service by providing the UK government's integrated authentication service, which has been branded as'GOV.UK Verify' [13].GOV.UK Verify is an integrated authentication service of the UK government, where the government does not directly verify an individual's identity online, but manages login information by selecting a user from among identity verification service providers.As of February 2017, seven organizations (Barclays, CitizenSafe, Digidentity, Experian, Post Office, Royal Mail, Secure Identity) have been certified and operated as identity verification service organizations.Each institution's identity authentication method is different, and the types of the method are increasing.The advantage of being secure is that the information entered by the user is not stored in one place or shared with no unnecessary information. This is an unknown way. Government services available through GOV.UK Verify include: IRS income tax verification, tax filing and other cleaning services, employment and person verification, financial transactions such as universal credit inquiries, and driver's license information verification at the Driver's License Office. It is being used for application and confirmation of government licensing and administrative work such as sharing.

2.4EU

Currently, the EU recognizes three types of digital signatures (all have legal effect), and this aims to guarantee the convenience of users by ensuring diversity of authentication systems and procedures.Specifically, identification through passport or ID card (Basic E-Signature), advanced E-Signature through a separate identification process, and Qualified E-Signature through a third-party credit service provider. Can be lifted.According to elDAS regulations, various electronic tasks processed between countries in the region, such as foreign university registration and access to electronic health records, can be safely carried out, and companies can save time and costs by simplifying administrative procedures, and convenience and flexibility when using government services. When using the online service, concerns about security and privacy exposure can be resolved by using the electronic ID of the relevant country.As can be seen from the inauguration process of IDAS and its purpose, it is necessary to look at it in terms of enhancing the convenience and diversity of methods for users' personal authentication procedures.In other words, it provides a new type of integrated authentication service while acknowledging the authentication procedures used in each country, and provides a way to deal with the cumbersome authentication procedures for each country in the European integrated market at once. Convenience is being emphasized.

3. Korean Digital Identity Guidelines

The guideline for the Korean identity proofing service stipulates how to identify using an alternative means without using a resident registration number.The alternative means of RN are to use the identification information (ID, mobile phone, etc.) and confidential information (PW, etc.) that the Korea Communications Commission (KCC) grants to users in the Standard on Designation of Personal Identity Proofing Agencies standard.Alternative means of RN include i-PIN, mobile phone, credit card, and public certificate.In Korea, ISPs indiscriminately stipulate a case where they must verify their identity online in order to minimize the need for personal identity proofing from online users.First, if there are special regulations in laws, second, if it is necessary for the operation of services provided by online operators, and third, it is limited to cases where it is necessary to protect the rights of users.At this time, it stipulates that identity verification on the Internet is performed in a safe and reliable way.In addition, when an ISP requests identification, the items of personal information to be collected, the purpose of use, the period of use and retention period, the purpose of collection or retention after the purpose of being provided has been achieved must be notified.

3.1 I-Pin

I-PIN (Internet Personal Identification Number: I-Pin) is a method of using identification ID and password after confirmation by the I-PIN issuing authority that allows users to use their identification information instead of the RN for membership and adult certification on the Internet.Figure 2 is a flow chart of I-Pin based identity verification service.

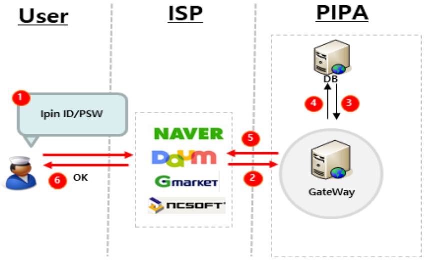

Figure 2. Flow of I-Pin based personal identity proofing service

3.2Public certificate

Public Key Infrastructure (PKI) is a security technology that ensures the confidentiality of transactions on the Internet while confirming the identity of the parties to the transaction. Public key cryptography is recognized as the most effective alternative for solving key distribution problems, providing various information protection functions such as authentication, non-repudiation, and digital signatures as well as confidentiality and integrity functions provided by symmetric key cryptography.When issuing an accredited certificate, it is a service that verifies the user's identity through an identity verification service agency and issues an accredited certificate. At this time, the creation of connection information, which is information identifying the person, is a structure created by the i-PIN organization.Figure 3 is a flow chart of the identity verification service based on public certificates.

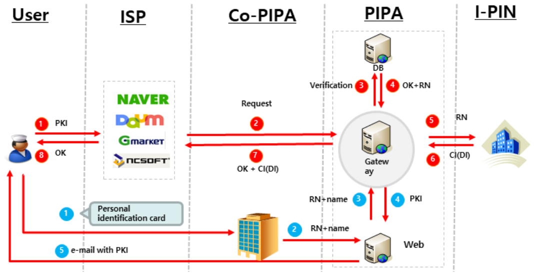

Figure 3. Flow of public certification based personal identity proofing service

3.3Mobile phone

For mobile phone authentication, enter the mobile phone number, date of birth, name, etc. in the website authentication window, and then enter the authentication number SMS sent to the phone to verify yourself in the corresponding authentication window.Due to the convenience of mobile phones, it is currently being used as the most common means of self-identification.Figure 4 is a flow chart of the identity verification service based on mobile phone.

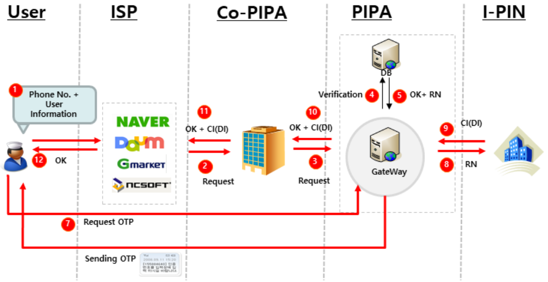

Figure 4. Flow of mobile phone certification based personal identity proofing service

3.4Credit card

Credit card authentication is a method of authentication using a credit card number, expiration date, and a password for identification.When providing a credit card-based identification service, the password for identification is not provided to the online business, but the first two digits of the password for identification are entered through ARS to identify the person.In the case of this method, it is not dependent on a specific medium such as a mobile phone, and the validity period of a credit card is proposed as 5 years, so it is used as a more secure means of identification.Figure 5 is a flow chart of the identity verification service based on credit card.

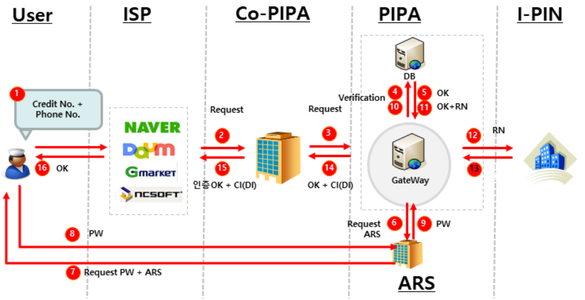

Figure 5. Flow of credit card based personal identity proofing service

4. Mobile Electronic Notification Service

The Korean mobile electronic notification service is a service that sends various guides or notices to subscribers of the document relay service provider through text/app push messages with registration effect instead of mail by public and administrative agencies.The registration effect refers to the use of a certified electronic address in accordance with the Electronic Documents Act to give an estimate of the facts of transmission and reception of electronic documents.By keeping the distribution certificate for proof of fact and forgery prevention of documents served in the process of distributing electronic documents in government agencies, it can secure reliability, prevent non-repudiation, and have legal effect.The sender and the receiver can confirm that the transmission and reception have been completed by authenticating the electronic address by the relay agency by transmitting it using a means called a certified electronic address. By providing the fact of distribution, they can be mutually verified.As described above, in the case of the existing mail notification service, the contents of the mail are scanned or copied and managed, and the details of the sending record are stored, and the sending company records and manages whether or not to receive it, and is used for proof of delivery and reception.By extending this inconvenience to a mobile-based notification service, it has the advantage of solving management difficulties and difficulties in handling.However, in the case of mobile notifications, various operators are performing distribution business based on electronic messages.For example, mobile phone text message transmission and app push message transmission are being used as electronic message transmission services.In such an electronic document distribution process, it is common for the sender and receiver to be different from each other in the electronic document transmission process.In this way, the notification information provided by public and administrative agencies to users can be viewed as a concept in which the sender becomes the public or administrative agency, and the user becomes the receiver.At this time, there is a limit to e-notification directly to users by public and administrative agencies.There is a limit that the recipient cannot recognize the electronic document receiving medium that only the person has access to.In other words, in the case of e-mails held by users, it is impossible to confirm the facts whether they are properly owned or whether the mobile phone number is owned by the user.This fact information is information that can be recognized by a communication service provider or an app service provider.Therefore, for the mobile electronic notification of public and administrative agencies, the user can be clearly identified through the matching process of the personal identification information held by the institution and the personal identification information held by the communication service provider.It is necessary to change to CI by providing the user's RN owned by the public institution to the identity verification institution.In addition, a process of transmitting the electronic document to the user is required after providing the CI to the electronic document relay service providers to identify the user.At this time, as in previous studies, CI also encrypts the CI as the user's unique identification information so that the identification information for the electronic notification service is shared, thereby suppressing the indiscriminate use of CI and protecting the user.Therefore, the requesting organization for sending the document transmits the RN and the name of the requesting organization to the relay. The identity verification agency converts the CI into encrypted CI and provides it. After that, the CI that the document relay service provider also has is converted into an encrypted CI, and it is used to identify the e-document sending company and user to provide a mobile e-notification service.Figure 6 is a flow chart of mobile electronic notification service processing.

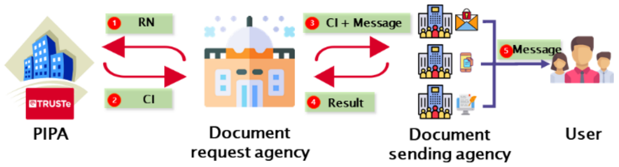

Figure 6. Flow of mobile electronic notification service

5. Conclusions

In this paper, we analysed the domestic and international status of identity verification services that identify and authenticate users non-face-to-face in online services.It can be seen that changes are being made so that online service providers can identify users when providing services while providing the personal information held by users to the minimum as possible for personal identity proofing services.In particular, the Korean digital identity guideline provides guidelines to protect the personal information of online service users by stipulating the standards for identity verification service, standards for designation of identity verification agencies, and the range of personal information provided to online businesses.It can be seen that there is an advantage of reinforcing personal information infringement and personal privacy protection by using RN, which is the existing unique identification information that can identify users, as CI.In other words, it can be seen that it is safer to protect users by using a CI encrypted with 64 bytes rather than an RN in a numeric format that can identify users.Using these CIs, electronic notification services are provided through smart phones.It can be seen that it is more effective to transfer to mobile than traditional paper-based notification service in terms of economic, temporal, and personal information protection.However, it is necessary to use CI for mobile e-notification service. CI is information that matches RN on a one-to-one basis, and in order to protect users, it is necessary to minimize the use of CI.Therefore, in order to identify users in the Korean mobile electronic notification service, the use of CI encrypted CI was used to strengthen user protection.It can be seen that there are various benefits by providing a mobile e-notification service by utilizing the CI provided by the identity verification agency designated according to the Korean digital identity guidelines.It can be seen that important information can be more safely delivered and verification of reading in the case of the recent rapid increase in the spread of infectious diseases due to the activation of the Korean mobile electronic notification service.

6. Acknowledgment

This work was supported by the Technology Innovation Program(20011675) funded By the Ministry of Trade, Industry & Energy (MOTIE, Korea) and the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT)(NRF-2020R1F1A106890011).

References

1. Mauro, T.; Floriano, D. R. (2020). COVID-19 in Italy: current stats, impact and ICT-based solutions. *IET Smart Cities*, 2(7), 74 –81.
2. Kim, J. B. (2019). A method to establish a personal identification and authentication integrated centerbased on the alternative means of resident registration number. *Proc. of Conf. Information and Control System*, 1, 212 – 213.
3. National Informatization White Paper. (2019). National Information Society Agency.
4. Digital Economy Life Survey. (2016). Korea Internet Security Agency.
5. Kim, J. B. (2017). Efficient Monitoring Method of Personally Identifiable Information on Images Exposed in the Web.*Journal of Internet Technology*, 18(7), 1573– 1585.
6. Kim, J. B. (2020). A Study on Differentiated Personal Proofing Service Based on Analysis of Personal Identification Requirements in Online Services.*Journal of the Institute of Internet, Broadcasting and Communication*, 20(2), 201– 208.
7. Kim, J. B. (2020). A Study on the Securing Technological Safety of Mobile Electronic Notification Service in Public and Administrative Agencies, *Journal of the Institute of Internet, Broadcasting and Communication*, 20(4), 1– 13.
8. Simson, G. (2000). Database Nation: The Death of Privacy in the 21st Century,O'Reilly.
9. Linda, W. (2007). The impact of personally identifiable information, *IT Professional*, 9(4), 62 – 64.
10. Yanjiang, Y., Xiaoxi, H., Feng, B., Deng, R. H. (2004). A smart-card-enabled privacy preserving E-prescription system, *IEEE Trans. on Information Technology in Biomedicine*, 8(1), 47 – 58.
11. NIST, (2015). NIST Requests Comments for Revising Its Electronic Authentication Guideline, NIST News.
12. Government of Canada, (2016). Social Insurance Number-Overview.
13. GOV.UK, (2016). Digital by Default Service Standard.
14. Chico, D. J. R., Sánchez, D. A. R. P., & García, D. M. J. (2019). análisiscomparativo del diferencial de preciosagrarios entre productores y consumidoreseneuropa, bajo criterios de seguridad alimentaria de abastecimiento. Cuadernos de Economía-Spanish Journal of Economics and Finance, 42(120), 268-278.
15. An, G., Wang, J., Yang, Y., & Du, X. (2019). A study on the effects to students' stem academic achievement with Chinese parents' participative styles in school education. Educational Sciences: Theory & Practice, 19(1).