J. Soc. Korea Ind. Syst. Eng Vol. 40, No. 3 : 116-122, September 2017
https://doi.org/10.11627/jkise.2017.40.3.116
ISSN : 2005-0461(print)
ISSN : 2287-7975(online)

Evaluation Criteria for Suitable Authentication Method for IoT Service Provider in Industry 4.0 Environment

Kwang Seob Jeong* · Sukjoo Bae** · Hyoungtae Kim***†

*Korea Trade Network (KTNET)
**Hanyang University Dept. of Industrial Engineering
***Woosong University Dept. of Business Management

4차 산업혁명 시대의 IoT 서비스 참여 주체에 대한 적합한 인증수단 선택을 위한 평가기준

정광섭* · 배석주** · 김형태***†

*한국무역정보통신(주)
**한양대학교 산업공학과
***우송대학교 경영학과

Advances in information technology, communication and network technology are radically facilitating digital convergences as the integration of human, equipment, and space in the current industry 4.0 era. In industry 4.0 environment, the vast amount of information with networked computing technology can be simultaneously accessible even in limited physical space. Two main benefit points out of these information are the convenience and efficiency in their online transactions either buying things online or selling online. Even though there exist so many benefits that information technology can create for the people doing business over the internet there is a critical problem to be answered. In spite of many such advantages, however, online transactions have many dysfunctions such as personal information leakage, account hacking, and cybercrime. Without preparing the appropriate protection methods or schema people reluctantly use the transaction or would find some other partners with enhanced information security environment. In this paper we suggested a novel selection criteria that can be used to evaluate the reliable means of authentication against the expected risks under on-going IoT based environment. Our selection criteria consists of 4 steps. The first step is services and risk identification step. The second step is evaluation of risk occurrence step. The third step includes the evaluation of the extent of damage. And the final step is the assessment of the level of risk. With the help of the above 4 step-approach people can systematically identify potential risks hiding in the online transactions and effectively avoid by taking appropriate counter actions

Keywords : Industry 4.0, Internet of things, Authentication, Evaluation criteria

Received 30 June 2017; Finally Revised 15 September 2017;
Accepted 18 September 2017
† Corresponding Author : gt4065b@gmail.com

1. 서 론

최근 정보통신 및 네트워크 기술의 급속한 발전 및 디지털 컨버전스의 확대로 그동안 기기 및 기능 중심으로 진행되던 디지털 컨버전스가 인간, 사물, 공간을 유기적으로 통합하는 차원에서 인간과 사물, 공간과 IT가 한데 어우러지는 사물인터넷 기반의 사회가 도래하고 있다. 사물인터넷 기술이란 서비스의 대상이 되는 인간 주변의 사물과 사물이 해당 서비스 대상자에게 최선의 서비스를 찾아내어 제공하기 위해 서로 실시간으로 통신 및 소통하는 능력을 기반으로 한다. 기술의 발전에 따라 컴퓨팅 기술은 기존의 단말기는 물론 일상적인 사물, 건물, 상품 등에도 내재화되며, 이들이 서로 네트워크화 될 수 있었기 때문에 사람, 사물, 공간의 네트워크화, 즉, 사물인터넷의 상상속의 사회가 현실 속에서 구현이 되고 있는 것이다. 이런 기술을 바탕으로 구축될 새로운 IT 서비스는 특성상 각 객체 간 정보가 자유롭게 이동하고 서비스간의 융・복합이 빈번하게 발생하며 한정되어 있던 물리적인 공간을 확장하고 보다 안전하고, 편리하고 쾌적한, 혁신적인 미래 모습을 열게 될 것이다. 이러한 새로운 기술로의 진보는 우리의 생활을 풍요롭게도 하지만 그 이면에는 인간의 기본 권리인 개인정보 유출 및 사생활 침해 문제가 도사리고 있다.

IoT 기술로 대변되는 4차 산업혁명 기반 사회의 특성으로 인해 필연적으로 개인의 사적인 정보공개를 요구하고 또 요구되는 개인정보는 단순한 정보가 아니라 생체인식을 통해 획득되는 바이오정보, 객체의 실시간 추적이 가능한 위치정보, 건강상태나 질병의 이력 등의 민감한 정보가 될 수 있는 것이 현실이다. 이에 따라 사생활 침해, 빅브라더에 의한 감시사회 심화, 해킹으로 인한 피해, 사이버 범죄 범람, 과도한 개인정보 수집 등으로 대표되는 수많은 부작용도 어렵지 않게 예상할 수 있다. 따라서 IoT 서비스에 참여하는 주체(개인 또는 기업)에 대한 신뢰성 있는 인증 방법이 제공되지 않는다면 서비스 전체에 대한 신뢰도가 저해되어 소비자들의 자발적인 IoT 서비스 참여 및 활용 의지를 떨어뜨리는 현상을 초래하게 되며 궁극적으로 미래 정보사회 전체의 위협으로 커질 수 있다. 이에 따라 본 연구를 통해 IoT 기반 환경하에서 예상되는 위험을 정리해보고 이에 대항할 수 있는 신뢰성 있는 인증수단에 대해 평가할 수 있는 평가기준에 대해 고찰해 보고자 한다.

2. 연구의 이론적 배경

2.1 인증의 개념

네트워크를 통한 비대면 방식의 전자적 거래는 시간과 공간을 초월하여 편이성, 효율성을 제공하여 새로운 거래 문화로 정착되었다. 그러나 온라인 거래는 많은 장점에 불구하고 개인정보 유출, 계좌 해킹, 사이버 범죄 등의 많은 역기능을 갖고 있으므로 보안에 대한 요구사항이 선결되어야 안정성을 확보 할 수 있다.

안전한 전자거래에 필요한 보안의 요소는 다음과 같은 항목들을 포함한다.

<Table 1> Categorization of Information Protection

Authentication Type	Descriptions
General Authentication	User Authentication Message Authentication
Integrity	Guarantees that Message is original without changes or forgery
Confidentiality	Guarantees that Message is accessible to authenticated users
Non-repudiation	Impossibility of Message Creation, Distribution or Receptions

인증에 대한 기존의 연구 중 가장 활발했던 내용은 기업이 제공하는 제품 및 서비스에 대한 인증제도에 대한 것이었다. 기업의 경쟁력 제고 및 소비자 보호차원에서 정부부처와 민간기관이 별도의 인증제를 운영하고 있으며 인증제도와 절차의 효율성 확보방안에 대한 체계적 논의가 진행되어 왔다[2, 4].

본 연구에서 인증은 사용자 인증을 의미하며 사용자 인증은 자체적으로 사용자가 수행하려는 어떤 활동으로부터 고립된 상황에 있는 특정한 사용자를 확인할 수 있게 한다. 사용자는 전형적으로 자신들의 식별번호를 기반으로 다른 활동을 수행하길 원하기 때문에 인증은 확실히 제한된 기능이며 흔히 혼동하는 권한 부여는 인증이 끝난 후에 이루어지는 절차이다[1].

2.2 인증수단의 분류

사용자 인증은 제공하는 방법에 따라 일반적으로 다음과 같이 분류된다.

<Table 2> Various Authentication Methods

Category	Authentication Methods
What You Know	Password, PIN, etc.
What You Have	Smart Card, Public Certification, OTP(OneTime Password), Mobile Device, Security Token, Radio Frequency Identification
What You Are	Personal Bio-information such as Palm Print, Iris, Face, Vein, DNA, Voice
What You do	Signature, Voice Identification

Single-Factor 인증은 위의 네 가지 인증수단 중에서 하나만 사용하는 방식이다. 일반적인 인증시스템은 하나의 인증수단만을 사용하고 있다. Multi-Factor 인증은 인증 과정에서 동시에 두 가지 이상의 방식을 사용하는 인증 방식이며 이는 신뢰성 및 시스템의 강도를 높여주어 침해 가능성을 낮춰준다.

예로 사용자ID 및 암호 기반의 인증을 사용하는 시스템인 경우, 기억기반 인증만 수행하는데 이를 소유기반(카드, 인증서)과 혼용하여 인증할 경우 더욱 강력한 인증을 제공할 수 있다. 확실히 Multi-Factor 인증은 사용자에게 인증 과정에서 보다 많은 작업을 요구하기 때문에 사용자를 번거롭게 만든다.

그러나 Multi-Factor 인증은 안정성에 있어서 위장 공격[1]을 더더욱 어렵게 만들어 안정성을 높여 준다.

2.3 인증 프로토콜의 위협과 공격

네트워크를 통해서 온라인 인증을 수행할 경우 다음과 같은 공격과 위협이 있을 수 있다.

<Table 3> Authentication Attack Type

Attack Type	Corresponding Results
Fishing	Authentication means leakage
Authentication message tapping	Authentication means leakage
Authentication message Reuse	illegal access to Service
Relying party(Service Provider) Camouflage	Authentication means leakage
Man-in-the-middle Attack	illegal access to Service
Session Hijacking	illegal access to Service
Social Engineering	Authentication means leakage

위와 같은 공격 및 위협에 대응하여 인증수단은 설계되어야 하며 각 대응 수단은 표준화되어 해당 표준을 준수한 인증수단은 사용자의 신뢰를 득할 수 있어야 한다.

호주 및 뉴질랜드 정부는 정치, 경제와 사회, 문화의 각 부문의 혁신과 이를 잘 연계하는데 IT를 적극적으로 활용하여 세계적으로 전자 정부를 선도하고 있다. 특히 뉴질랜드는 정부와 지역사회 간 발생하는 광범위한 온라인 거래에 대한 인증체계와 절차를 혁신적으로 관리하고 있다[3].

뉴질랜드 정부의 전자정부 프로그램 표준은 다음과 같이 인증 관련 표준을 제시하여 서비스 제공자가 참고할 수 있게 하였다[5].

1) 승인받은 사용자인 체 하여 시스템에 접근하려는 공격.

<Table 4> New Zealand e-Government Certification Standard

Standards	Purpose
Guide to Authentication Standards for Online Services	Provides a high-level overview of the NZ e-GIF authentication standards.
Evidence of Identity Standard	Specifies a business process for establishing the identity of government agency customers. Applies to offline as well as online services.
Authentication Key Strengths Standard	Specifies the authentication keys to be used for online authentication and protections necessary for the authentication exchange.
Data Formats for Identity Records Standard	Specifies data formats for a set of customer information data elements that government agencies may utilise in customer identity records.
Password Standard	Specifies requirements for passwords used for online authentication.
Other authentication key standards (to be developed)*	Specify the requirements for two-factor authentication keys used for online authentication.
Security Assertion Messaging Standard	Specifies messaging standards for communicating authentication assertions.

3. 연구의 방법

3.1 델파이 기법

1960년대에 Gordon과 Helmer에 의해 정형화된 델파이 기법은 현재의 상태에 대한 일반화 및 표준화된 자료가 부족한 경우, 전문가적인 직관을 객관화하는 예측의 방법으로 많이 사용되어 지는 기법이다. 델파이 기법은 추정하려는 문제에 관한 정확한 정보가 없을 때 다수의 의견이 소수의 의견보다 더 정확하다는 계량적 객관의 원리와 다수의 판단이 소수보다 정확하다는 민주적 의사결정의 원리에 근거를 두고 있다.

이러한 잇점을 토대로 평가기준을 개발하기 위하여 정책 델파이 기법을 활용하였다.

3.2 전문가 선정

델파이 기법에서는 표본 집단의 크기를 적정하게 결정해야 하는 것이 매우 중요한 과제이나 전문가 표본 집단의 크기 즉, 참가자의 수에 대해서는 명확한 규정이 없다. Ziglio(1996)에 의하면 10~15명의 소집단 패널만으로도 유용한 결과를 얻을 수 가 있다고 하였다[6].

이에 본 연구에서는 인증수단 선택을 위한 평가기준을 개발하기 위해 국내의 보안 및 인증전문가 10여명을 패널로 선정하였고 설문지 및 심화인터뷰를 통해 평가항목을 추출하고 항목별 가중치를 부여하였다.

먼저 1차 설문 및 인터뷰를 통해 비구조화된 설문지를 통해 대략적인 평가 절차에 대해 조사하였고 이를 기반으로 평가에 필요한 우선순위와 중요도를 선별하고 각 항목별 가중치를 구하여 최종 결과를 도출하였다.

4. 연구 내용

인증 관점에서 IoT 서비스의 위험 평가 절차는 다음과 같다.

Service identification and risk analysis	1. Identify the scope of the service to be risk assessed 2. Identify transactions and key information 3. Identification of hazards when no authentication means are applied
⇩	
Estimate the likelihood of a risk	1. Establishment of criteria for estimating likelihood 2. Estimation of the probability of occurrence of risk
⇩	
Estimate the amount of damage in case of danger	1. Establishment of standard for calculation of impact (Impact) 2. Estimate the damage level
⇩	
Risk Level Assessment	1. Estimation of risk level based on damage scale/ probability 2. Determination of final risk level based on risk level

<Figure 1> Steps of IoT Risk Evaluation

4.1 서비스 및 위험 식별 단계

IoT 서비스의 위험평가를 수행하기 앞서, 위험평가자와 서비스 제공자가 가장 먼저 수행해야 할 일은 위험평가 대상이 되는 서비스의 범위를 식별하는 일이다. 일반적으로 그 범위를 최소화 하는 것이 이상적이지만, 기본적 서비스 단위 또는 하나의 인증수단이 통용되는 범위를 위험평가의 최소 범위로 제한할 수 있다. 위험평가 범위를 식별한 후, 해당 서비스 범위 내에서 송・수신되는 트랜젝션 상의 주요정보를 식별해야 한다. 주요정보를 식별해야 하는 이유는 인증수단이 적용되지 않았을 경우, 비인가자 또는 비인가 기기・사물에 의해 해당 정보가 노출 및 위・변조될 가능성이 크기 때문이다. 주요정보가 식별되면 인증수단이 적용되지 않았을 경우를 가정하여 위험을 식별하고 위험 시나리오를 작성한다. 인증수단이 적용되지 않았을 경우에 발생하는 일반적인 위험의 형태는 다음과 같고, 위험 시나리오는 일반적인 위험형태를 근거하여 작성한다.

- 비인가자 또는 비인가 기기・사물을 통한 주요정보 노출
- 비인가자 또는 비인가 기기・사물을 통한 주요정보 위・변조

IoT 서비스에 적용하기 위한 인증수단을 선택하기 위해서는 먼저 해당 서비스의 위험수준을 평가해야 한다. 인증수단 적용은 비용과 사용자의 불편함이 동반되므로 서비스의 위험도를 파악하고 이에 맞는 수단이 선택되어야 한다. 위험평가 시 해당 서비스의 중요도 및 정보의 접근성 여부에 따라 다음과 같이 4가지로 인증 요구사항을 분류할 수 있었다.

<Table 5> Certification Requirements for Risk Level Classifications

Risk Level Classification	Certification Requirements	Rating
Low	password(8 characters or more)	4th
Middle	One-Factor authentication without password Enable authentication	3rd
High	two-factor authentication - use both password and OTP(one-time password) - Public Certification	2nd
Highest	- Use an authenticated certificate stored in HSM(Hardware Security Module)	1st

Risk Level 평가 시 표준 위험모델로 다음과 같은 수식을 사용하였다.

$$Risk\ Level = Likelihood \times Impact$$

어떤 사건에 대한 전체 위험도는 해당 사건의 발생가능성에 그 사건이 끼치게 되는 영향도의 크기를 곱한 것으로 계산한다는 것이다. 극도로 단순화된 위험도 계산 공식이지만 이 공식으로부터 우리는 위험도를 줄이기 위해서는 사건의 발생가능확률을 줄이거나 이 사건 발생으로 인한 영향을 최소화해야 한다는 직관적인 사실을 알 수 있다. 이러한 직관적 사실을 활용하여 <Table 6>에 제시된 것 같이 위험상황에 대한 평가 및 4가지 단계로 구분할 수 있다.

<Table 6> Risk Rating Based of Risk Level via Likelihood & Impact

		Likelihood	
		High	Low
Impact	High	Highest(1st)	Middle(3rd) or High(2nd)
	Low	Middle(3rd) or High(2nd)	Low(4th)

4.2 위험의 발생가능성(Likelihood) 산정

위험평가를 위한 서비스 범위 및 위험이 식별되면 위험평가자는 해당 서비스의 침해동기 및 서비스 환경을 종합적으로 고려하여 발생가능성 등급을 판단해야 한다. 발생가능성은 침해동기(Motivation) 및 서비스 환경(Environment)을 고려하여 <Table 7>과 같이 3가지 수준으로 구분할 수 있다.

<Table 7> Likelihood Level of Risks

	High	Middle	Low
Detailed Risk Explanations	- Big motivation for access - Easy accessibility	- Big motivation for access - Not Easy accessibility	- Small motivation for access - Easy accessibility

침해 동기는 대상 시스템이 제공하는 서비스의 중요도 및 보관하고 있는 정보의 중요성이 가장 큰 평가 기준으로 작용하며, 서비스 환경은 네트워크 이용 환경, 물리적 통제 등 통제 수단의 존재 여부, 불법적인 침해를 수행하기 위한 기술적인 난이도가 지표로 사용될 수 있으며 마지막으로 침해 발각 시 법적 처벌의 강도도 중요한 구분 지표로 사용될 수 있다.

<Table 8> Possible Outcomes of Each Risk Ratings based on Likelihood Level

Likelihood	Possible outcomes
Low	- Provide non-critical information about the service - Service environment that is accessible to unauthorized persons
Middle	- Provide critical information about the service - Service environment where access by unauthorized person is difficult
High	- This service provides important information - Service environment that is accessible to unauthorized persons

발생가능성의 세부 산정기준 정립 후, 사업주체는 식별된 위협에 대해 발생가능성을 산정한다. 발생가능성의 산정결과는 위협에 대한 발생가능성의 정도(높음, 보통, 낮음)가 된다.

4.3 위험발생 시 피해 규모 산정

위험평가자는 위험의 발생 가능성을 산정한 후, 실제 해당 위험이 발생한 경우를 가정하여 피해 규모와 피해 형태를 산정해야 한다. 피해 형태는 <Table 9>와 같이 "신뢰 및 명성의 훼손" 등 5가지로 분류하고, 각 피해형태에 따른 피해규모는 <Table 10>과 같이 3가지 등급(높음, 보통, 낮음)으로 정의한다.

<Table 9> 5 Types of Damage

Damage Types	Descriptions
Undermining trust and reputation	- Adverse effects on personal and corporate trust and reputation
Financial Loss	- Unfavorable impact on personal and corporate financial situation
Productivity Degradation	- Personal and corporate business productivity, efficiency, adverse impact on service utilization
Health and Safety Infringement	- Adverse impacts on personal and business health and safety
Violation of laws	- Adverse impacts on individuals and businesses that comply with legal requirements

피해규모의 세 가지 등급과 이를 구분하는 산정기준에 기반을 두어 위험평가자와 서비스 제공자는 서비스 환경에 적절한 피해규모 세부산정 기준을 도출해야 한다. 세부 산정기준은 서비스 제공자 및 서비스의 특성에 따라 추가·수정되어야 하며, 그 이유는 각 IoT 서비스별 서비스 제공자 및 서비스의 특성이 모두 상이하기 때문이다. 즉, 매출규모가 상이한 대기업과 중소기업, 서비스 성격이 상이한 공공기관과 일반기업체에게 동일한 세부 산정기준이 적용될 수 없기 때문이다.

<Table 10> Calculation Criteria for Damage Scale

Damage Types	High	Middle	Low
Undermining trust and reputation	Critical/ Long-term	Critical/ Short-term	Limited/ Short-term
Financial Loss	Disastrous/ Hard to Recover	Significant/ Hard to Recover	Trivial/ Easy to Recover
Productivity Degradation	Serious degradation of key functions, duration and scope	Significant degradation of key functions, duration and range	Decrease in key function, duration and scope
Health and Safety Infringement	Serious injury or death	Injuries requiring medical treatment	Injuries that do not require medical treatment
Violation of laws	A violation that could have a decisive influence on sentence	A violation that could have an influence on sentence	A violation that has no decisive influence on sentence

피해규모의 세부 산정기준이 정립된 후, 식별된 위험이 발생한 경우를 가정하여 피해규모를 산정한다. 피해규모의 산정 결과는 발생되는 피해형태(신뢰 및 명성의

훼손 등)와 피해형태 별 피해규모의 정도(높음, 보통, 낮음)가 된다.

일반적으로 기업에 미치는 피해의 규모는 사업적인 피해가 더 치명적이다. 사업적인 피해는 기술적인 피해로부터 발생하며 피해가 발생한 응용이 해당 기업에 얼마만큼의 중요도를 가지는 지에 따라 달라질 수 있다. 피해 규모는 일반적으로 해당 피해의 정도는 각 항목에 따라 0~9까지 수치화 할 수 있으며 각 항목별 세부적인 수치는 평가자에 따라서 달라질 수 있다.

4.4 위험수준 평가단계

IoT 서비스의 위험수준은 피해규모와 발생가능성을 고려하여 4가지 등급(최상, 상, 중, 하)으로 결정된다. 위험평가자는 <Table 11>과 같이 산정된 피해규모의 등급과 발생가능성의 등급을 곱하여 IoT 서비스의 위험수치를 산정한다. 위험수치의 산정결과는 계량화된 정수로 도출된다.

<Table 11> Calculation Criteria for Damage Scale

Category	Scale of damage	High	Middle	Low
Likelihood	Score / Weight	100	50	10
High	1	100×1 = 100	50×1 = 50	10×1 = 10
Middle	0.5	100×0.5 = 50	50×0.5 = 25	10×0.5 = 5
Low	0.1	100×0.1 = 10	50×0.5 = 5	10×0.1 = 1

note) the magnitude of the damage and the likelihood weights are adjustable by the risk assessor and the service provider.

위험수치가 계산되면 IoT 서비스의 최종 위험수준을 <Table 12>에 따라 평가하며 위험평가의 최종결과는 위험수준의 정도(최상, 상, 중, 하)가 되며 향후, 해당 위험수준에 따라 적절한 인증수단을 선택하여야 한다.

최종 위험 수치는 반올림을 통해 계량화된 정수로 만든 후에 위험수준의 정도를 평가한다. 위험평가의 최종결과는 위험수준의 정도에 따라 분류할 수 있으며 해당 위험수준에 따라 적절한 인증수단을 선택하여야 한다.

<Table 12> Estimate Final Risk Level of IT Service

Risk Figure	Risk Level	Remarks
76~100	Highest	Requires 1st level authentication method
51~75	High	Requires authentication method level 2 or higher
26~50	Medium	Requires authentication method level 3 or higher
1~25	Low	Requires authentication method level 4 or higher

note) risk figures can be adjusted by risk assessors and service providers.

5. 결 론

보이지 않는 컴퓨팅, IPV6 활성화를 통한 모든 장치의 네트워크화, 맥락인지 사물의 지능화, 무중단 컴퓨팅, 증강현실 등을 특징으로 하는 IoT 기술은 이용자의 경험을 중시할 것이며 사용자 친화적인 IT 환경을 조성할 것이고 IT 기기의 컨버전스 및 단순화, 지능화, 개인 맞춤, 모바일화를 제공할 것이다. 한편 이런 서비스를 위해 IoT 기반의 4차 산업혁명이 가져올 사회는 실시간 데이터를 수집하고 민감하고 포괄적인 개인정보를 수집할 것이며 이에 따라 프라이버시 및 침해의 위협도 크게 증가하리라 예상할 수 있다.

IoT 기술사회의 발전 및 확산에 발맞추어 연결될 객체를 인증하기 위한 인증수단을 살펴본 결과 적절한 인증수단을 선택하기 위해서는 제대로 된 위험평가가 최우선 과제라는 결론에 도달하였다. 실례로 보호하려는 정보보다 강한 인증수단을 선택하였을 경우 추가 비용 발생 및 과도한 인증수단 적용에 따른 사용자 불편이나 프로젝트 기간 연장 등의 위험이 있지만 보호하려는 정보보다 약한 인증을 택하였을 경우 법규의 위반, 해킹 피해, 프라이버시 침해 등 심각한 영향을 받을 수 있으며 이는 해당 서비스를 제공하는 기업의 신뢰 및 명성의 훼손, 추가 사업기회 손실, 피해 사용자들의 집단소송 등의 큰 피해로 이어질 수 있다.

그러므로 해당 서비스별 적절한 인증수단 선택을 위한 기준 제공은 IoT 환경 구축에 필수적인 항목이며 본 연구를 바탕으로 IoT 서비스 설계 및 서비스 제공자, 기기 제조업체등은 적절한 인증수단 선택에 참고가 되기를 바라며 향후 본 연구를 바탕으로 현재 구축되고 있는 4차 산업혁명에서의 스마트 팩토리나 사이버물리시스템 등에 적용된 인증수단이 적절한 수단인지에 대한 추가연구 등이 따라 준다면 IoT 기술시대의 적극적 선구자들에게 매우 유익한 정보를 제공하리라 생각된다.

References

[1] Calisle Adams, Steve Lloyd, Understanding PKI : Concepts, standards and deployment considerations, Infobook, 2003, p. 70.

[2] Cho, N.H., Woo, T.H., and Han, W.C., A Persent Views and Improvement policy of the Certification System in Korea, *Journal of Society of Korea Industrial & Systems Engineering*, 1999, Vol. 22, No. 51, pp. 211-220.

[3] Choi, K.J., A Study of Certification System for Ubiquitous Environment, Investigation Report to KISA, KISA-WP-2008-0022.

[4] Ko, H.W., A Study on State and Operation of Non-govern-

ment Certification in Korea, *Journal of Society of Korea Industrial & Systems Engineering*, Conference Preceeding, May 2007.

[5] New zealand Government, e-Government Guideline, chapter 3, 2005.

[6] Yoon, M.-S., A Three-round Delphi Study on the Roles and Competency Modeling of Secretaries, [Master's thesis], Ewha Womans University, 2000.

ORCID

Kwang Seob Jeong | http://orcid.org/0000-0001-8606-6999
Sukjoo Bae | http://orcid.org/0000-0002-9938-7406
Hyoungtae Kim | http://orcid.org/0000-0001-9506-9446