JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 18, No. 1 : 11~17 Jan. 2014

스마트 전자정부 구현을 위한 보안 알고리즘 응용 제안

임광철[1] · 정영철[2*]

Proposed that Application of the Security Algorithm for Implement Smart m-Gov

Kwang-Cheol Rim[1] · Young-chul Choung[2*]

[1]Department of Mathmatics, Chosun University, Gwangju, 230-6610, Korea
[2]Department of Computer Engineering, Chosun University, Gwangju 230-7381, Korea

요 약

ICT 생태계의 동인으로 전자정부는 그 형태의 변화를 가져온다. 이에 따라 스마트 전자정부 구현을 위해서 정부는 m-Gov 서비스를 활성화 하고, 이를 위해 기술정책을 수립할 필요가 있다. 따라서 본 논문에서 스마트 전자정부 구현 모형을 제시하고, 안전한 m-Gov의 인프라 구성을 위해 양자암호 시스템을 서버보안에 응용할 수 있는 정보보안 기술정책으로서 보안 알고리즘을 제안한다. 이것은 결국 보안성, 안전성, 경제성이 확보된 대국민 및 기업에 대한 스마트 전자정부 서비스를 제공하는 행정이념을 추구하는 것이다.

ABSTRACT

As ICT Ecosystem does, electronic government changes in its form. Accordingly, in order to realize Smarter m-Gov, the governments need to vitalize m-Gov services and enact technology policy. Therefor, this manuscript suggests possible model of m-Gov realization and security algorithm as a technology policy which applies quantum cryptography system to server security for the construction of secured m-Gov's infrastructure. What the manuscript suggests seeks administrative ideas of Smarter m-Gov's services which contain security, stability, and economic feasibility for the benefits of nation and enterprises.

키워드 : ICT 생태계, m-Gov, 스마트 전자정부, 양자평문전송

Key word : ICT Ecosystem, Mobile Government, Smart Government, Quantum Plaintext Transport

접수일자 : 2013. 12. 26 심사완료일자 : 2014. 01. 02 게재확정일자 : 2014. 01. 10

*** Corresponding Author** Young-chul Choung(E-mail:kornet41@chosun.ac.kr, Tel:+82-62-230-6575)
Department of Computer Engineering, Chosun University, Gwangju 230-7381, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2014.18.1.11 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

ICT 기반의 정보화 사회는 다방면의 생태계를 변화시키고 있다. 전자정부도 마찬가지다. 거치성 PC 시대를 대체할 이동성과 소형의 편리성이 강조된 컴퓨팅 구현이 가능한 스마트기기 시대의 도래로 모바일 패러다임의 변화로서 유선에서 무선으로, 음성에서 데이터로의 사용자 패턴의 변화를 가져오고 있다. 또한 스마트기기 확산은 반도체, ICT 산업 등의 성장과 개인화된 스마트기기로 개인의 상황과 특성이 반영된 다양한 여가활동, 사회적 관계형성 등 국민생활에 급속한 변화의 유발을 보이며, 모바일 라이프 확산에 따라 m-Gov 행정서비스 수요가 증가한다.

정부・국민・기업은 기존 PC기반의 서비스를 이동성, 개방성, 다양성, 경제성 등을 지원하는 모바일기기 이용환경 변화를 보이고 있다. 이에 따라 스마트 시대에 걸 맞는 전자정부 패러다임의 변화가 요구된다. 따라서 대국민 및 기업의 정보화 환경변화에 따른 정부의 역할로서 스마트 전자정부 구현을 위한 m-Gov 서비스 활성화를 위해 새로운 전략을 수립할 필요가 있다.

본 논문은 스마트 전자정부의 구현을 위해서 전략수립의 대응책으로써 보안대책 모형을 네트워크, 단말, 서버보안의 세 부분으로 구조화하여 모형 프레임을 제시한다. 이 구조화된 모형모델을 기반으로 서버보안의 안전성을 위해 양자 평문전송 알고리즘의 안전성을 제안한다. 따라서 제안한 보안 알고리즘을 응용한 정부통합서비스센터의 안전성은 전자정부의 정보보안 관리 목적을 실현할 수 있음을 제고하고자 한다.

Ⅱ. 스마트 전자정부 전망

ICT 생태계 변화는 전자정부에도 예외가 아니다. 현재 우리나라는 전자정부 종합평가 세계 1위 국가로서 스마트 전자정부시대를 선도하기 위하여 기존의 PC 기반 전자정부의 패러다임을 모바일 기반으로 한 m-Gov의 생태계로 전환되고 있다.

2012년 국내 스마트폰 보급이 PC 보급을 역전시켰다. 2011년 3월에는 가입자 1,000만에서 2012년에 들어서면서 급속히 2,000만을 돌파하였다. 스마트폰의 보급·확산, 모바일 인터넷 활성화 등으로 인터넷 이용환경은 유선기반에서 무선기반으로 급속히 변화중이다. 2013년 11월 14일 Gartner가 발표한 보고서에 따르면, 2013년 3/4분기 기준 글로벌 스마트폰 판매량은 전년동기 대비 45.8% 증가한 2억 5,020만대를 기록, 글로벌 전체 휴대폰 판매량 중 55%를 차지한 것으로 집계 됐다[1].

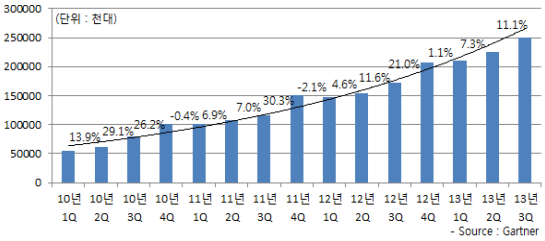

그림 1. 전세계 스마트폰 판매량 추이
Fig. 1 Sales Trend of Worldwide Smartphone

국내의 스마트폰 가입자는 2013년 4월 10일 기준으로 이동전화 가입자(5375만 여명) 중에 스마트폰 사용자는 약 3400만 여명에 이른다[2].

이에 따라 이동통신 환경의 생태계는 불가측하게 진화하고 있으며, 또한 무선 기반의 보안 취약성도 산재하고 있는 현실이다.

따라서 대국민 및 기업은 이동성과 내재성이 편리한 다양한 서비스를 요구하므로 정부는 이의 눈높이에 맞는 스마트한 m-Gov 서비스와 안전한 정보보호를 위한 스마트 전자정부 서비스 제공이 필요하다.

2.1. ICT 생태환경 변화

전 세계적으로 1990년대 PC 주도의 IT 활황에 이어서 2009년 아이폰 출시로 대한민국의 ICT 생태계의 패러다임은 유선에서 무선으로 사용자 패턴 변화를 가져왔다. 이에 따라 m-Life, m-Economy 시대의 개막이 시작되었다. 모바일통신 환경이 컴퓨팅을 위한 플랫폼으로 자리매김함에 따라, 다양한 형태의 컴퓨팅이나 애플리케이션을 가지고 있는 기기와 기능들이 모바일 환경으로 수용되는 것이 가능해졌다.

최근 급속하게 확산되는 스마트기기인 스마트폰, 태블릿 등은 모바일 환경에서의 컴퓨팅이 다양화되는 것으로도 해석할 수 있다[3]. 이에 따라 모바일 환경은 이동성, 개방성, 다양성, 경제성 등 이용환경의 변화로 대국민 및 기업은 행정서비스를 기존 PC 기반 서비스를

모바일로 전환을 요구하고 있다[4].

따라서 정부는 스마트한 전자정부 구현을 위해 새로운 디지털 시대에 대비하여 보다 안전한 정보의 커뮤니케이션을 위해서 행정시스템 변화에 유연함을 보여야 한다.

2.2. 전자정부 생태환경 변화

우리나라 전자정부법 제2조 1항에 의하면 전자정부는 정보기술을 활용하여 행정기관의 사무를 전자화함으로써 행정기관 상호간 또는 국민에 대한 행정업무를 효율적으로 수행하는 정부를 말한다.

전자정부법에 따른 정보기술의 진화는 불가측적이다. 따라서 새로운 디지털 시대의 진행으로 ICT의 생태환경은 전자정부에도 커다란 영향을 미치며 진행하고 있다. 이에 따라 새로운 형태의 스마트 전자정부로서 대국민 및 기업을 위해 기술적으로 보다 안전하고 유연한 행정개혁과 서비스 개선을 전략적 수단으로 m-Gov를 추진해야하며, 또한 행정부처 간에 유기적 협업이 수행되는 효율적인 준비가 있어야 한다.

2.3. 스마트 전자정부 역할

국가의 행정시스템을 혁신하기 위해서는 전자정부 서비스 공급자와 소비자 간의 동력엔진이 요구된다. 국가혁신은 기술적으로 보안성, 안정성, 유연한 확장성 등이 보장된 전자정부 통신네트워크를 구성하여 국가기관에게 품질이 보장된 정보통신 서비스를 제공함으로써, 정보공유 및 유통 활성화로 정부부처 간 협업형 전자정부 구축을 목표로 하고, 신기술 출현, ICT 생태환경 변화 등에 따른 국가기관의 신규수요를 효율적으로 수용할 수 있도록 유연한 확장성을 갖도록 해야 한다[5].

따라서 전자정부는 ICT를 기반으로 정부의 업무를 전자적으로 처리하여 행정의 효율성, 투명성을 증대시키고, 대국민 및 기업이 원하는 정보와 서비스를 언제 어디서나 이용할 수 있으며, 국정운영 과정에 개방・공유・참여할 수 있는 기회를 확대해 주어야 한다. 이에 따라 스마트 전자정부의 역할은 m-Gov 구현을 위해 정부운영 시스템을 개선과 함께 안전한 정보보안을 위한 정부기능의 질적 향상을 가져오는 혁신을 위한 핵심전략 수단이 요구되고 있다.

Ⅲ. 스마트 전자정부 모형구도

현재의 전자정부는 정부의 형태를 변화시키는 동인으로써 ICT 역할이 행정시스템에 반영되기 때문에 행정서비스가 공급자 중심에서 수요자 중심으로 변화 하면서 정부의 정보 노출에 심각한 현상이 현실화 되고 있다.

스마트한 m-Gov는 정부의 서비스를 유비쿼터스 5any 형태로 안전하고 빠르게, 그리고 쉽게 대국민 및 기업에 접근할 수 있어야 한다. 이에 따라 스마트한 전자정부 구현을 위해 정부는 대국민 및 기업을 위한 전자정부를 구현할 수 있는 m-Gov 서비스 활성화 전략수립이 필요하다[2].

따라서 본 논문에서는 그 활성화 방안으로 스마트한 전자정부 보안대책 모형구도를 (그림 2)와 같이 제안한다.

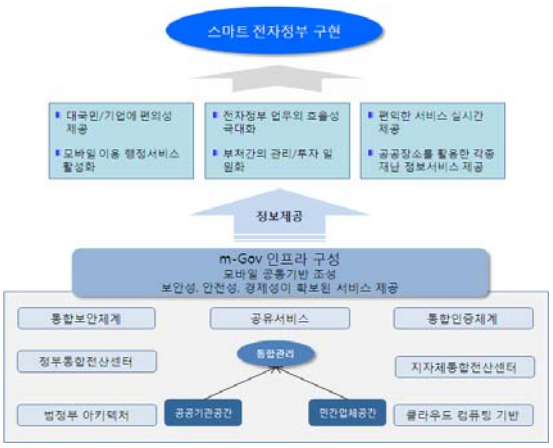

그림 2. 스마트 전자정부 구현 모형
Fig. 2 Model of Smart Government Strategy

정부는 m-Gov의 주요한 정책방향으로써 스마트 전자정부 구현을 위해서는 모바일 공통기반을 조성하고 보안성, 안전성, 경제성이 확보된 전자정부 서비스를 제공하기 위해 m-Gov의 전자적 보안 인프라를 구성하여 보다 안전한 정보를 제공하여야 한다. 이러한 인프라 기반의 제공된 정보의 정책과제 3가지를 제언하면 다음과 같다.

첫째, 대국민 및 기업에 편의성 및 모바일 이용의 행정서비스를 제공하여야 한다.

둘째, 전자정부 업무의 효율성을 극대화하고, 부처간의 관리 및 투자에 대한 일원화가 이루어 져야 한다.

셋째, 대국민 및 기업에 대한 편익한 서비스 정보를 실시간 제공하고, 각종 재난으로부터 정보서비스가 제공되어야 한다.

따라서 m-Gov 정책과제로서 전자정부의 보안성은 정부의 업무프로세스와 행정서비스 효율성을 위해 스마트기기 기반의 오피스 구축은 보안위협으로 부터 안전성이 담보되어야 하는 것이다. 이것이 전제될 때 대국민 및 기업에 대한 서비스의 질적 향상과 국가 경쟁력의 향상을 가져온다.

Ⅳ. 보안 알고리즘

4.1. 보안대책 모형 제안

Ⅲ절에서 제안된 정책과제에 따라 스마트 전자정부 구현은 보안성, 안전성, 경제성이 확보된 서비스 제공이어야 한다. 그러기 위해서 모바일 공통기반을 조성하여야 한다. 안전한 보안을 위한 m-Gov는 공통기반 시스템 플랫폼을 갖춰 암호화 기술을 적용하고, 민간 트래픽 분리를 통한 안전하고 실용적인 국가 무선망 이용제도를 마련하는 것이다. 이를 위해 모바일 네트워크, 단말, 서버 등의 서비스 전반에 대한 선제적인 범 m-Gov 서비스를 위한 보안 기술정책 전략이 필요하다.

따라서 안전한 행정서비스 실현을 위해 (그림 3)과 같이 전체적으로 안전성 있는 기술적 보안대책 모형프레임을 제안한다.

그림 3. 보안대책 모형 프레임
Fig. 3 Strategy Frame of Security Measure

제안된 보안대책 모형프레임은 먼저 네트워크 보안에 있어서 기존의 모바일 플랫폼에 VPN 서버를 구축한다. VPN은 암호화 인증과 같은 기술을 이용할 수 있도록 IPSec에서 사용하는 AH(Authentication Hear)와 ESP(Encapsulation Security Payload)를 일반 IP 패킷에 확장하여 사용한다. IPSec과 같은 IP 계층의 보안기술은 네트워크 기반의 어떤 서비스나 애플리케이션도 보호할 수 있으며 원격사용자, 라우터, 방화벽 등을 수정하지 않고도 구현할 수 있다는 장점이 있다[6]. 그러므로 네트워크는 암호화 통신 및 인증 시스템에 의해 정보보호가 가능하다.

단말보안은 Security Sublayer는 IEEE 802.16 및 TTA에서 제정한 표준으로 PHY, MAC을 기술하고 있는데, MAC은 시스템 접속, 대역폭, 할당, 연결 설정 및 관리 기능을 담당한다. 이런 MAC 중에서 최하위에 보안기능을 제공하는 Security Sublayer로 정의되는데, 이는 단말 및 사용자 인증, 세션 및 데이터 암호화를 위한 키 생성과 교환, 암호화된 데이터의 송수신, 메시지 무결성 검증기능 부분으로서 구성되어 있는 것을 활용하는 m-Gov 기술전략으로 보안이 가능하다[7].

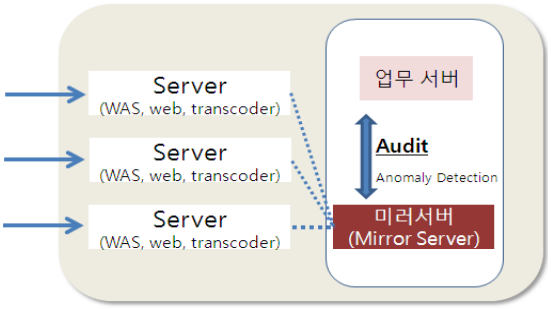

그림 4. 서버 프레임
Fig. 4 Server Frame

현재 서버보안(통합센터 보안)은 네트워크 보안의 시스템과 통합하여 이용되고 있는 실정이다. 정부통합서비스센터는 대국민 및 기업에 대한 서비스 제공을 위한 전자정부 서비스이기 때문에 현실적으로 개방화 되어 있는 상태이므로 유무선 통합망을 경유한 모바일 공통 플랫폼 서버에의 접속으로 내부경로의 해킹방어에는 한계를 가진다.

따라서 보다 안전한 통합센터 보안을 위해 (그림 4)와 같은 서버 이중화를 통한 서버를 분리하여 보다 철저한 안전망을 구축해 업무서버에서 Mirror Server를 두고 철저한 검사를 이루기 위한 이례적인 탐지를 상시

로 하여야 한다[8].

4.2. 보안 알고리즘 제안

제안된 보안대책 모형의 서버보안에 있어서 철저한 보안이 더욱 안정적으로 응용되기 위해서 보안 알고리즘 응용이 요구된다. 전자정부 서비스가 모바일 공통 기반을 조성하고 보안성, 안전성, 경제성이 확보된 전자정부 서비스를 제공하기 위해 m-Gov의 인프라를 구성하여야 한다. 인프라 구성에 있어 단말, 네트워크, 서버보안의 기반으로 형성되는 것이다.

(그림 4)의 서버 이중화를 통한 서버분리로 보다 철저한 안전망을 구축해 업무서버에서 Mirror Server를 두고 철저한 검사를 이루기 위해서 양자암호 시스템을 개선한 이중 광자전송을 이용한 사용자 비밀평문교환 구현 알고리즘(양자평문전송 알고리즘)을 응용한다. 양자평문전송 알고리즘은 기존의 양자암호 알고리즘이 키 전송 프로토콜로써 BB84 프로토콜과 E91 프로토콜을 사용하여 양자암호시스템을 이용하였지만, 제안한 알고리즘은 양자 비밀키를 이용하여 송신자와 수신자의 동기화된 비밀키로 각자의 관용키를 형성하고 이를 이용한 암호와 복호가 이루어지는 원리를 이용한다. 양자 비밀 평문전송 프로토콜의 공격관점에서 보면 전송되는 데이터는 가로채기에 대한 정보의 노출을 최소화 하여야 하고 정보 도청자의 위장 인증을 바로 감지 할 수 있어야 한다.

양자평문전송 알고리즘은 Intercept-resend 도청방식과 MiTM(Man in the middle) 공격에 대한 안전성을 볼 때, Intercept-resend 공격에 대한 안전도는 (표 1)에서와 같이 엘리스가 보내는 128비트의 큐빗 상태에 대해 전위 64비트의 확인 과정을 통해 확률적 안전도를 확보할 수 있다.

만약 중간 공격자에 의한 데이터 가로채기가 발생한다면 각 비트별 $\frac{1}{4}$의 확률로 오류가 생성된다. 이를 64비트의 병렬데이터로 환산하면 $(\frac{1}{4})64$의 확률로 일치하게 되므로 공격이 불가능하다. MiTM 공격에 대하여 악성 공격자의 위장 데이터 교환은 공개채널에서 엘리스와 밥의 상호 이차인증으로 실질 사용자의 존재성을 확인 할 수 있기 때문에 공격이 불가능함을 확보한다.

양자평문전송 알고리즘은 BB84 프로토콜과 E91 프로토콜의 양자 얽힘에 의해 공격자의 유무를 판단하고 공격 징후에 대처하는 형식을 사용하여 One-time Pad와 같은 안전도가 확보된다[9].

(표 1)과 (표 2)의 One-time Pad를 병합적으로 양자화된 데이터를 후진 비트열로 저장・전송하면 1라운드 데이터열은 검출필터의 난수성에 의해 보내고자 하는 평문의 절반을 양자암호 알고리즘으로 안전하게 전송되고 평문의 나머지 절반은 2라운드 데이터에 의해 양자암호 알고리즘으로 전송된다.

두 표에서와 같이 1라운드 데이터와 2라운드 데이터를 EX-OR 연산으로 병합하면 온전한 평문이 된다. 이것은 양자암호의 안전도를 승계하면서 평문전송이 원활히 이루어지는 것이다.

공격자에 대한 사용자 인증은 기존 BB84 프로토콜

표 1. 이중광자 평문전송 1라운드 데이터 흐름도
Table. 1 1round data flowchart of double poton transform

		1	2	3	4	···	60	61	62	63	64	65	66	67	68	···	124	125	126	127	128
엘리스	송신비트	0	1	1	0	···	1	1	0	0	0	1	0	0	1	···	1	0	1	0	0
	필터	⊕	⊗	⊕	⊗	···	⊕	⊗	⊕	⊕	⊕	⊕	⊗	⊗	⊕	···	⊕	⊗	⊗	⊕	⊗
	상태	|↕〉	|↗〉	|↔〉	|↖〉	···	|↔〉	|↗〉	|↕〉	|↕〉	|↕〉	|↔〉	|↖〉	|↖〉	|↔〉	···	|↔〉	|↖〉	|↗〉	|↕〉	|↖〉
밥	검출	⊕	⊕	⊕	⊕	···	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	···	⊕	⊕	⊕	⊕	⊕
	관측	|↕〉	|↕〉			···	|↔〉		|↕〉				|↕〉	|↕〉		···				|↕〉	|↕〉
	비트	0	0	1	0	···	1	1	0	1	1	1	0	0	1	···	1	0	1	0	0
일치		T	F	T	F	···	T	F	T	T	T	T	F	F	T	···	T	F	F	T	F
원타임		0		1		···	1		0	0	0	1			1	···	1			0	

- 공개채널에서 엘리스 전송필터와 전위 64비트 공개
- 공개채널에서 밥의 전위 64비트 검출필터와 검출 데이터공개
- 후위 검출 64비트 저장

표 2. 이중광자 평문전송 2라운드 데이터 흐름도
Table. 2 2round data flowchart of double poton transform

		1	2	3	4	···	60	61	62	63	64	65	66	67	68	···	124	125	126	127	128
엘리스	송신 비트	1	1	0	1	···	1	0	1	1	0	1	0	0	1	···	1	0	1	0	0
	필터	⊕	⊗	⊕	⊗	···	⊕	⊗	⊕	⊕	⊕	⊕	⊗	⊗	⊕	···	⊕	⊗	⊗	⊕	⊗
	상태	|↔〉	|↗〉	|↕〉	|↗〉	···	|↔〉	|↖〉	|↔〉	|↔〉	|↕〉	|↔〉	|↖〉	|↖〉	|↔〉	···	|↔〉	|↖〉	|↗〉	|↕〉	|↖〉
밥	검출	⊗	⊗	⊗	⊗	···	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	···	⊗	⊗	⊗	⊗	⊗
	관측		|↗〉		|↗〉	···		|↖〉					|↖〉	|↖〉		···		|↖〉	|↗〉		|↖〉
	비트		1		1	···		0					0	0		···		0	1		0
일치		F	T	F	T	···	F	T	F	F	F	F	T	T	F	···	F	T	T	F	T
원타임			1		1	···		0					0	0		···		0	1		0

- 엘리스가 전위 랜덤64비트와 후위 동일 64비트 전송
- 밥의 ⊗ 검출기 검출 후 전위 64비트 공개
- 엘리스의 전위 64검출비트와 데이터 공개
- 밥의 후위 64 비트 저장 후 1라운드 저장 64비트와 or 연산 시행

의 안전도를 승계함으로서 안전함이 입증되었고, 백도어(Backdoor)에 대한 공격법이 연구되고 있기 때문에 공격에 대한 안전성은 이미 확보 되었다고 볼 수 있다. 현재 기술적으로 양자화된 데이터의 양을 원활히 수행할 수 있을 만큼의 전송능력이 완성되지 않은 실정이다.

향후 양자전송이나 양자컴퓨터의 발전은 양자화된 평문전송의 사용이 급진적으로 확대될 것으로 기대된다. 따라서 이와 같은 안전한 보안 알고리즘을 서버보안의 프레임 적용에 응용된다면 전자정부의 안전성은 더욱 확보될 것이다.

따라서 제안 알고리즘의 응용으로 m-Gov의 행정서비스는 무선 보안의 취약성이 더욱 부각되고 있는 현실에서 대국민 및 기업에 대한 전자정부 서비스로서 정보보안의 안전성을 더욱 갖추는 것이 효율성, 경제성 있는 국가경쟁력의 가치척도라 할 수 있다.

Ⅴ. 결 론

ICT 생태계는 지금도 불가측적으로 진화되고 있다. 이에 따라 스마트 시대에 맞는 전자정부 패러다임의 변화는 대국민 및 기업에 대한 전자정부 행정서비스를 제공하는 기회인 것이다. 이를 위해서 정부는 끊임없이 정책적으로 연구 투자하고, ICT의 급속한 발전에 따른 유선기반 e-Gov에서 m-Gov로 변화된 이동성, 개방성, 다양성, 경제성 등을 수용할 수 있는 새로운 요구사항에 대비하여야 한다.

따라서 본 논문에서 대국민 및 기업의 정보화 환경 변화에 따른 정부의 역할로서 스마트 정부 구현을 위한 m-Gov 서비스 활성화를 위해 보다 안전한 m-Gov 보안대책 서비스 전략을 수립하고, 이의 대응책과 m-Gov 정책과제로 스마트한 전자정부 보안대책 모형모델과 양자평문전송 알고리즘 응용을 제안 하였다.

특히 안전성 있는 기술적 보안대책 모형 프레임과 구체적으로 서버, 네트워크, 단말보안 프레임을 갖춘 구조에서 제안된 보안 알고리즘을 서버보안에 응용하여 안전한 스마트 전자정부 구현이 가능함을 논거 하였다.

결론적으로 본 논문은 스마트 전자정부 구현을 위한 보안 알고리즘 응용 제안의 논제 활용가치로 인해, 정부의 혁신과 대국민 삶의 질을 향상시킬 수 있는 행정의 궁극적인 목적 실현의 최적 수단으로 활용되어 보다 안전한 정보보호의 행정이념을 추구하는 민주적 가치가 구현되기를 기대한다.

REFERENCES

[1] Gartner, Gartner Says Smartphone Sales Accounted for 55 Percent of Overall Mobile Phone Sales in Third Quarter of

2013 ; Barcelona, Spain, November 14, 2013. Available: http://www.gartner.com/newsroom/id/2623415?fnl=search

[2] Y. C Choung, Y. G Bae, “m-Gov Strategy and Policy Challenges ICT Ecosystem Changes,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 17, no. 7, pp. 1532-1536, July. 2013.

[3] H. R Kang, Others. “Mobile broadband and mobile biz model,” KISDI: Basic Research 12-7, pp. 157-158, Dec. 2012.

[4] *Government Strategy Seminar based on Smart phone, “e-government(M-Gov)* Policy Direction according to Spread of mobile,” Ministry of Security and Public Administration, Republic of Korea: Jun. 2010.

[5] Y. C Choung, Y. G Bae, “Research of convergence application services in u-Gov,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 11, no. 6, pp. 1048, Jun. 2007.

[6] M. Y Lee, Other. *Network Security Technology of Next Generation*, Life & Power Press, 2004.

[7] L. Nuaymi(c), “Possible Research Axis in Radio Resource Management,” Telecom Bretagne, Rennes, Lisbon: pp.13, Feb. 2008.

[8] C. S Park, “Security measures for implementat of Secure mobile service,” *Government Strategy Seminar based on Smart phone*, Seoul Womens University, Republic of Korea: Jun. 2010.

[9] J. Z Seol, K. C Rim, “Using Double Photon Transmission of Quantum Cryptography, ”*Journal of the Korea Institute of Information and Communication Engineering*, vol. 17, no. 8, pp. 1859-1863, August. 2013.

임광철(Kwang-cheol Rim)

2000년 조선대학교 대학원 이학석사
2006년 조선대학교 대학원 이학박사
현재 조선대학교 수학과 외래교수
※관심분야 : 응용수학, 정보보안, 양자암호, 암호학

정영철(Young-Chul Choung)

1987년 조선대학교 행정학과 학사
2003년 조선대학교 전자공학과 석사
2007년 조선대학교 정보통신공학과 박사
현재 제이앤아이코리아 연구소장, 조선대학교 컴퓨터공학부 외래교수
※관심분야 : 정보통신정책, 전자정부, 네트워크 보안, 융복합 응용