The Journal of Digital Policy & Management 2013 Oct; 11(10): 403-409

미정부의 빅데이터를 위한 보안정책

홍진근*
백석대학교 정보통신학부*

The Security Policy for Big data of US Government

Jinkeun Hong*
Div. of Information and Communication, Baekseok University*

요 약 본 논문은 미국 정부의 빅데이터 정책과 보안 이슈에 관해 고찰하였다. 빅데이터 R&D 이니셔티브 전략과 계획, NITRD 프로그램, 정부기관의 빅데이터 전략을 소개하였고, 또한 미군에서 빅데이터 운용환경, 군사 작전에 사용되는 빅데이터 정보, 주요 연구기관과 주제, 보안가이드라인 등에 대해 살펴보았다.

주제어 : 보안정책, 빅데이터, 군사작전, NITRD, OSTP

Abstract This paper review about big data policy and security issue of US government. It is introduced Big data R&D initiative strategy and plan, NITRD program, and big data strategy of government. It is presented operation environment of big data in US government, big data information for military operation, major research organization and topic, security guideline and so on.

Key Words : Security Policy, Big data, Military Operation, NITRD, OSTP

1. 서론

오바마 정부는 백악관 산하 과학기술정책실(OSTP)가 주관이 되고, 6개 연방기관이 주도적으로 참여하여, 빅데이터 접근 수집 관리에 요구되는 소요기술 및 방법 전반에 대한 '빅데이터 R&D 이니셔티브(2012. 3. 28)' 전략 수립 및 계획을 추진해 가고 있다[1-3]. 일반적으로 빅데이터는 거대 데이터(정형, 비정형)를 수집하며 특정 패턴을 도출하여 수집된 데이터에 대한 예측 분석을 실시한다. 이에 대한 정의는 맥킨지, IDC, 위키피디아, 가트너 등이 정의해오고 있다.

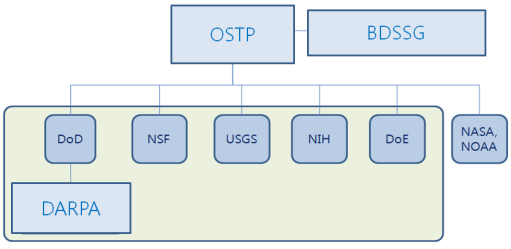
NITRD(Networking and Infomation Technology R&D) 프로그램은 미 정부 다부처, 다기관이 참여하는 IT R&D 프로그램으로 ICT 기술과 관련된 협업체계와 연구 필요성 인식에 따라 구성이 되며, 7개 프로그램의 영역 가운데 관심주제인 빅데이터, 무선 스펙트럼 연구개발이 영역이 있다. 최근 미 대통령의 2014년 NITRD 재정투자 규모가 39.68억불에 이를 것으로 밝힌 바 있으며, 프로그램의 10개 분야 가운데 하나인 CSIA(사이버 보안과 정보보증) 분야 또한 8억 3백만달러(2012년 6억5천3백9십만달러)를 투자할 계획이다.

미 정부가 추진하는 빅데이터와 보안문제는 국가 보

Received 23 August 2013, Revised 25 September 2013
Accepted 20 October 2013
Corresponding Author: Jin-Keun Hong(Baekseok University)
Email: jkhong@bu.ac.kr

ISSN: 1738-1916

안 환경에서 현재 직면하고 있는 빅데이터 보안 문제가 무엇인지, 국가차원에서 보안 문제를 해결하기 위해 빅데이터 접근을 통해 연방정부가 어떤 일을 해야 하는지, 국가 보안 전략을 수립하고자 할 때 빅데이터와 관련된 유일하거나 상이한 일이 무엇인지, 빅데이터와 함께 국가 보안에 직면한 문제를 해결하기 위한 현재 정부가 추구해야할 솔루션은 무엇인지 등을 토대로 물음이 제기되고 있다. 그러므로 미 정부의 빅데이터 보안 전략은 곧 보안-전망-국제질서, 국방-외교-경제-개발- 국토안보-정보-통신-인적 측면에서 총체적으로 접근하고 있다.



[Fig. 1] USA big data R&D initiative

현재 미 정부가 발표한 2014 NITRD 재정 투자계획은 다음과 같다.

〈Table 1〉 NITRD 2014 budget

Government	2012	2014
NITRD	38.1B$	39.69B$
DARPA	4.89B$	4.186B$
DHS	54.4M$	76.5M$
DoD	772.3M$	881.5M$
DoE	497.7M$	541.2M$
NIST	97.1M$	143.7M$
NSF	12.163B$	12.274B$
CSIA	6.539B$	8.3B$
HCI&IM	775.6M$	854.5M$
HCSS	165M$	179.6M$
HEC I&A	11.7B$	10.541B$
LSN	389.8M$	353.4M$

이에 반해 국내 빅데이터 R&D 예산은 차세대 메모리 기반의 빅데이터 분석관리 소프트웨어 원천기술 개발(5년, 29억(2012), 145억(전체)), 초소형 고신뢰 OS와 고성능 멀티코어 OS를 동시 실행하는 듀얼 운영체제 원천기술 개발(5년, 28억(2012), 140억(전체)), 빌딩 내 기기를 웹을 통해 연동하여 사용자 맞춤형 최적 제어 모니터링 서비스를 제공하는 소프트웨어 개발(4년, 16억(2012), 64억(전체)) 예산을 투입해오고 있다.†

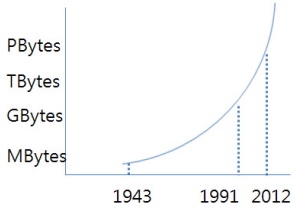
본 논문은 미국 정부가 추진하는 빅데이터 정책과 보안 이슈의 문제에 대해 접근하였는데, 이는 최근의 미 정부 정책을 고찰함으로써 국내 정책 방향과 관련 이슈를 검토하는데 일조할 것으로 판단되기 때문이다.

본 논문에서는 2장에서 미정부의 빅데이터 전략, 3장에서 빅데이터 환경에서 정보보호 이슈에 대해 살펴보고 4장에서 결론을 맺고자 한다.

2 미 정부의 빅데이터 전략[1-10]

미군이 군사작전에서 사용하는 빅데이터 량의 년도별 분석을 다음 그림에서 제시하였다.

1943년 허스키 작전의 경우 메가바이트 단위 정보처리 작전을 수행한 바 있고, 1991년 사막의 폭풍 작전에서는 기가에서 테라 바이트, 2012년 이후 항구 자유 작전의 경우 페타 바이트 이상의 정보처리를 수행하고 있다. 2015년이 되며 요타 바이트 수준의 센서정보를 활용할 것으로 내다보고 있다.



[Fig. 2] Big data capacity in US military environment

† 지식경제부(2012.1.9.) 자료. 국내 빅데이터는 스마트 전자정부 구현과 연결시켜 행정 공공기관 업무처리에 주민정보, 종합소득정보 등에 대한 활용방안을 검토중이다. 한국의 경우 국가정보화전략위원회(의사결정기구), 빅데이터 활용추진협의회(관련부처 과제검토, 이견조정, 실적확인, 성과점검-행안부, 국과위, 방통위, 지경부, 교과부 등), 방송통신위원회(빅데이터 서비스 활성화 방안 발표 '12.6), 안행부를 포함한 주요부처가 참여한다. 행안부는 정보화진흥원에 빅데이터 전략연구센터 개설('12.4) 추진하고, 교과부를 중심으로 핵심요소개발 및 활용 인프라 구축을 추진해 왔다('12.107억원).

또한 미군은 Joint2020 연합작전 수립을 위해 지휘관과 참모들이 휴대 가능하고 클라우드 서비스가 가능한 지휘통제 기술 개발, 빅 데이터 수집-분석-가공을 통한 능력 개선에 집중하고 있다. 정보 공유 환경에 민감한 빅 데이터와 클라우드 서비스로 활용하여 C2 어플리케이션을 수행할 수 있도록 추진하고 있다.

공유 정보 환경에 대한 이해와 관련하여, 공유된 정보 환경의 필요성이 수백 개의 보다 덜 최적화된 데이터 센터와 네트워크로부터 발생되는 불필요한 비용문제나, 한계가 있는 상호운용성이 위협이 있는 임무에 대한 정보 공유와 협업을 제한시킨다는 점, 새로운 기술로 무장된 급격하게 진화되어 가는 디바이스를 위한 요구가 증가한다는 점, IT 프로그램이 전장 요구를 만족시키기 위해 신속하고 효과적으로 새로운 기술을 현장에 배치할 수 없다는 점, 사이버 보안의 취약성이 비밀정보와 위험성이 가미된 임무를 성공시키는데 활용하는데 있어서 위협성이 존재한다는 점, 현재 IT 디바이스 보급 프로세스가 새로운 상용 기술의 장점을 갖도록 하는데 방해가 된다는 점 등과 관련하여 제기되고 있다.

미 국가 안보 주요 조직에는 DoD, NORTHCOM, DIA (Defense Intelligence Agency), DNI (Director of National Intelligence), FBI (Federal Bureau of Investigation), DHS (Department of Homeland Security)가 있으며, 국방을 지원하는 위원회 가운데 J-2(intelligence)는 주요 빅데이터에 대한 요구사항, 계획-수집-처리-이용-분배-정보저장 및 검색 등을 기능을 담당한다. J-5의 경우 임무 분석, COA (Course of Action, 행동 지침) 개발, COA 분석과 워게임, COA 비교, COA 승인을 수행한다. 미 정부는 정책을 수립하는 정제되지 않은 데이터를 세련된 필요한 정보로 만드는 프로세스로 정보 사이클 6단계로 제시하며, 사이클 구성은 요구사항, 계획 수립과 방향, 정보수집, 정보처리와 활용, 정보 분석과 생산, 정보 분배로 구분된다.

첩보 정보에 활용되는 빅데이터는 정보처리와 활용, 분석과 생산 측면에서 정제 처리되는데, 정보유형에는 SIGINT, IMINT, MASINT, OSINT, HUMINT, GEOINT 등으로 구분된다. 2012년이후 정보수집 단계에서는 적외선 센서, 컬러/흑백 TV 카메라, 영상 강도가 강화된 TV 카메라, 지시 레이저나 조명 레이더를 사용한다. 정보 처리와 활용, 분석과 생산 단계에서는 각 이미지 센서로부터 풀 움직임 비디오를 분리/합성된 비디오 스트림으로 볼 수 있다. 정보 분산단계에서는 항공 감시정찰팀이 지원부대와 통신을 통해 이루어지며, 2013년~2015년 시점에 항공 감시정찰 영역에서는 무인항공기(MQ-9 Reaper, Predator)와 같은 센서를 활용하여 동시 4Km 반경의 영역을 12개의 카메라를 활용하여 이미지를 수집하는 프로그램이 추진되고 있다.

미 정부는 빅데이터 연구개발과 관련하여, 거대한 데이터 량의 공유-분석-관리-유지-저장-수집에 소요되는 요소 핵심 기술, 국가 안보력 강화, 교육과 학습에 있어서 변혁, 과학과 공학에서 발전 가속화를 위한 기술 협력, 빅 데이터 기술 개발 및 적용에 요구되는 인력 확장이라는 측면에 초점을 맞추고 전략을 수립해 가고 있다.

그러나 문제는 어떤 데이터를 결정할 것인가 하는 것인데, 어떻게 빅데이터의 거대한 데이터양을 효과적으로 처리하고 저장할 것인지하는 것이다. 현실적으로 분석 검색에 적합한 도구가 부족한데, 실제 많은 양의 데이터와 센서의 확장은 분석가를 능가하고 있다. 이러한 측면에서 데이터 결정 문제는 데이터의 분석과 관리에 있어 새로운 패러다임을 도출하기 위해 현재 존재하거나 미래에 데이터 활용 도구를 위해서, 신속한 통합이 가능한 오픈 소스 구조의 시스템 개발이 무엇보다 선결되어야 한다.

빅데이터 기술적 목표와 관련하여 고찰할 때, 최소 3-5년 내에 선결되어야 할 빅데이터 문제가 지적되고 있다. 우선 빅데이터 분류를 강화시키는 것이 필요하다. 환경이나 환경설정이 어렵더라도, 목표를 정확하게 탐지하는 것, 그리고 위치 등록과, 정보 분류 및 식별이 가능하도록 하는 것이다. 또한 지상에서 대상 목표물의 활동성, 활동 패턴, 관련성 식별을 위한 수준 있는 자동화 도구가 요구된다. 공격자에 대응하여 지원 식별 및 영향을 조정할 수 있는 HUMINT 기반의 정보를 캡쳐・저장・검색할 수 있는 도구가 필요하다.

7-10년이 흐르면 빅데이터 분석계층에서는 마운트되지 않은 활동성과 활동 패턴, 관계성을 식별하기 위한 자동화도구가 요구된다. 공격자 네트워크의 전방위 측면에서 식별 가능한 오픈 소스 데이터를 검색, 마이닝, 이용하기 위한 강화된 도구가 필요하다.

현재 미 정부는 지나치게 많은 정보, 불완전하고 흩어져 있는 정보, 다양한 임무로 인해 수집된 정보에 대한 최적화가 어느 때 보다 절실히 요구되고 있다. 분석에서

부터 작전 수행까지 전 단계에서 빅데이터를 어떻게 처리할 것인지, 다양한 데이터 유형 즉 비구조적(텍스트 문서나 메시지 트래픽) 또는 반 구조적인(테이블식, 관계식, 카테고리식, 메타 데이터식)인 거대한 양의 데이터를 어떻게 효율적으로 분석할 것인지, 분석 기법이나 소프트웨어 도구 개발이 요구된다.

이외 최적의 알고리즘 개발, 커스터마이징된 시각화와 논리 추론이 포함된, 호환성이 있는 HCI 기반의 도구 개발이 중요하다.

미 정부는 빅데이터 연구에 영상 지능이 접목된 즉 비주얼한 이벤트 학습, 새로운 시공간 재표현, 비주얼 검사와 개념의 정착이라는 측면에서 더 한층 진일보하기 위해 투자하고 있다. 스마트 그리드 분야에서는 개선된 정보기술와 사이버 인프라 구조가 접목되고 있다. 수백만 개의 스마트 미터로부터 15분마다 샘플링된 정보들이 수집되며 프로파일이 작성된다. 빅데이터 소프트웨어 플랫폼은 정보 통합이라는 파이프 라인을 통해 센서와 동적 데이터 소스에서 실시간 정보 수집, 데이터의 안전한 저장 관리 및 협업이 가능하도록 하며, 확장성과 비쥬얼화를 기반으로 효율화를 높이고 있다. 미 정부의 빅데이터 정책은 보건 당국 중심의 헬쓰케어나, 국세청을 중심으로 세금 추적, 연구기관의 효율화 등을 중심으로 목표를 설정하여 추진하고 있다.

이에 반해 국내 빅데이터 정책은 국가전략 포럼에 참여하고 있는 기관으로 공공연구기관(28개)†, 빅데이터 전문기관(12개)†† 이 참여하고 있다. 국내 빅데이터 추진은 '12-'14년(초기 단계로 타당성 확인 및 우선추진 과제 수립), '15-'16년(기반조성단계, 대상과제 추진을 활용확산), '17년 이후 국가 전반의 활용 및 고도화를 추진 계획을 가지고 있다. 국내 빅데이터 대상과제로는 사회안전, 국민복지, 국가경제, 인프라, 산업지원, 과학기술로 분류되어 추진된다.

3. 빅데이터 환경에서 정보보호[11-17]

빅데이터 환경에서 실시간으로 의심스러운 이벤트를 탐지하는데 거대한 보안 이벤트를 수집하여 저장하고 분석하는 것이 무엇보다 중요하다. 이를 위해 자동화된 감사 기능, 위협 관리, 지속적인 모니터링, 포렌식 조사가 필요하다. 또한 필요한 보안 이벤트 저장 공간의 양을 감소하기 위해 DB에는 효율적인 데이터 압축 방법이 적용되어야 한다. 사용자와 시스템 그리고 네트워크 활동에 대한 통계적인 분석과 실시간 이벤트 데이터 상관성이 고려된 양방향 상호운용성이나 역할 기반의 접근통제, 자동화된 경보 기능, 히스토리컬한 질의 등이 제공되어야 한다.

3.1 미 정부기관의 주요 연구 주제

빅데이터 관련 정보보호 연구를 수행위한 미 정부 기관의 주요 연구 테마를 고찰하면 다음과 같다.

1) 트러스트 기반의 공간에 대한 연구

〈Table 2〉 Research based on Trust

Item	Organization
Trust for defend cyber space	AFRL, ARL, ARO, CERDEC, ONR, OSD
High assurance security architecture	AFRL, DARPA, NIST, NSA, ONR, OSD
Tactical assurance information project	OSD
IT security automation/ monitoring/ security content automation protocol program	DHS, NIST, NSA
System security based on Cloud	AFOSR, AFRL, DARPA, DHS, NIST
Secure wireless networking	ARL, ARO, CERDEC, DARPA, NSA, ONR, OSD
Secure trust cyber space(SaTC)	NSF
Digital provenance and HW trust program	DHS
Content and context awareness trust routing(C2R)	AFRL
Bio based technology for enhanced energy sector cyber security	DOE/OE
cross layer's recovering adaptable networking	OSD/NRL
critical cyber program	AFRL

† 건강보험심사평가원 외27개
†† 그루터 외11개 기관

2) 시간 변화에 따른 이동 목표물에 대한 연구

〈Table 3〉 Moving target research

Item	Organization
Secure trust cyber space (SaTC) program	NSF
Security strength cyber integration and operation framework security (CRUSHPROOF)	ARL, ARO, CERDEC, OSD
Network asset Morphing (Morphinator) for restricting attacker reconnaissance	ARL, ARO, CERDEC
Defend ability enhancement for Information Assurance (DEFIANT)	ARL, ARO, CERDEC
Moving target defend program	DHS
Proactive 및 Reactive adaption system	NSA
Security automation and vulnerability management	NIST
Trust management in service oriented structure	ONR
robustness automated computing system	ONR
Information security automation program (ISAP)	DHS, NIST, NSA
Recovery adaptable trust host's Clean-slate design (CRASH), mission oriented recovery cloud (MRC) program	DARPA
Network Randomization for energy	DOE/OE

3) 사이버 시장 경제 활성화를 위한 연구

〈Table 4〉 Effect Enhancement Research(Law etc)

Item	Organization
Secure trust cyber space (SaTC) program	NSF
Cyber economy motivation program	DHS
Electric subsector cyber security power capacity maturity model (ES-C2M2)	DOE/OE

4) 보안 설계

고보증성을 도출하고 설계 능력을 개발하며, 위험 비용의 품질 일정, 복잡성 등을 효과적으로 하기 위한 소프트웨어 집약적인 시스템 연구로 취약성, 결함 및 저항성 증명에 대한 주제이다.

〈Table 5〉 SW system research(vulnerability, fault)

Item	Organization
Survival system engineering	OSD
Trust computing	AFRL, NSA, OSD
SW development environment for secure system SW and application	ONR
Root trust	AFRL, NIST, NSA
SW assurance metric and tool evaluation (SAMATE)	DHS, NIST
Automated program analysis for cyber security (APAC)	DARPA
High assurance cyber military system (HACMS)	DARPA
Secure trust cyber space (SaTC) program	NSF
Cyber security program for energy transfer system(CEDS)	DoE/OE

5) 보안 과학

〈Table 6〉 security research of future cyber system

주제	기관
Science for cyber security(S4C)	ARL, ARO
Security science MURI	AFOSR
Trust and distrust basic research	AFOSR
Cyber Measurement Campaign (CMC)	OSD
Cyber Physical Assurance Metric	DOE/OE

6) 크로스 커팅 기초

〈Table 7〉 Cross cutting Research

Item	Organization
Cryptology	DARPA, NIST, NSA, NSF, ONR
Model, Standard, Test, Metric	ARL, ARO, DHS, DOE/OE, NIST, NSF, OSD
Trust Basics	AFRL, ARL, ARO, CERDEC, DARPA, DOE/OE, NIST, NSA, NSF, ONR, OSD
Security management and Assurance Standard	NIST
Quantum Information Science and Technology	AFRL, DOE/OE, IARPA, NIST, ONR

7) 국가 우선순위 결정지원

〈Table 8〉 Decision of Priority of Government

Item	Organization
Trust Cyber Infrastructure for Power Grid(TCIPG)	DHS, DOE/OE
Government strategy for Trust ID in cyber space	NIST
Health IT security program	NIST
Smart Grid interoperability Pannel-Cyber security working group(SGIP-CSWG)	NIST
Cyber application research and enhancement development	OSD
Critical cyber security research and engineering Journal(JSCoRE)	ODNI

8) 기술발견, 평가, 전이, 채택, 상용화

〈Table 9〉 Technical Process considering Long Term Effects

Item	Organization
Test bed and Infra structure for research development	DARPA, DHS, DOE/OE, NSF, OSD
Cyber Test environment, Cyber Measurement Campaign	OSD
Cyber transition for execution program	DHS
Information technology security enterprise forum(ITSEF)	DHS
Secure trust cyber space(SaTC) program	NSF
Small business innovation research (SBIR) conference	DHS, DoD
Government cyber excellence security center(NCCoE)	NIST

3.2 빅데이터 환경의 운영 보안 가이드라인[15]

빅데이터 운영보안 환경에 권고되고 있는 가이드라인은 다음과 같다.

〈Table 10〉 Guideline of Operation Security

Item	Organization
API security	Code/Command injection, overflow attack/Web attack security, node policy management
Application/ node authentication	Kerberos Applicaiton, kerberos ticket's theft and copy in Virtual Cloud, Robust authentication
Data security	User Access control/data protection copied from cluster
Configuration/ patch management	Effect consideration using difference OS platform in cluster
Monitoring, filtering, blocking	Security bottleneck at data/user request inspection in API layer
Management data access	unauthorized access in data file/ node process
Audit logging	Log management of detection action

3.3 빅데이터 환경에서 보안 가이드라인[17]

미 정부 기관에서 적용할 수 있는 빅데이터 보안 가이드라인은 다음과 같은 상용 빅데이터 보안 가이드라인의 권고안에 준하여 제시되고 있다.

1) 빅데이터 환경을 고려한 커버로스 보안 가이드라인을 수립해야 한다.
2) 빅데이터 환경에 적합한 키 인증서 관리 가이드라인을 수립해야 한다.
3) 빅데이터 환경에 적용되는 파일 OS 계층에서 암호 가이드라인을 수립해야 한다.
4) 빅데이터 환경에서 노드 검증 가이드라인을 수립해야 한다.
5) 빅데이터 환경에서 트랜잭션, 관리 활동 등 로그 가이드라인을 수립해야 한다.
6) 빅데이터가 적용되는 망 환경에서 SSL/TLS 적용을 위한 가이드라인이 제시되어야 한다.

4. 결 론

본 논문에서는 미 정부의 빅데이터를 위한 주요 정책과 전략, 보안을 중심으로 추진되고 있는 연구 프로그램, 운영 보안의 가이드라인을 중심으로 고찰하였다. 본 연구를 통해 미 정부의 빅데이터 추진방향과 그 규모를 예측할 수 있으며, 정부기관이 추진하는 빅데이터 보안 정책 또한 상용에서 권고되고 있는 각종 가이드라인을 기반하여 수립되고 있음을 알 수 있다. 이 추진정책을 검토함으로써 국내 정책 수립 방향 점검에 일조할 것으로 사료된다.

REFERENCES

[1] Martin Westphal, Big data the DoD Perspective.

[2] IT R&D Policy Trend, US NITRD Program's Background and funding support. IT R&D Policy Trend. 2012.

[3] Obama Administration Unveils, Big Data Initiative DOI:http://www.whitehouse.gov/administration/eop/ostp.

[4] J. H. Pollack and J. D. Wood, Enhancing Public Resilience to Mass-Casualty WMD Terrorism in the United States, DTRA ASCO Report. 2010.

[5] Big Data Solicitation: http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504767

[6] DOI:http://www.nsf.gov/publications/pub_summ.jsp? ods_key=nsf12058

[7] DOI:http://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf12059

[8] DOI:http://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf12060

[9] Sam Curry, et al., Bit Data Fuels intelligence-driven security, EMC. 2013.

[10] DOI:http://www.nitrd.gov/About/about_nitrd.aspx

[11] Supplement to the President's Budget, The Networking and Information Technology Research and Development Program FY 2014, May 2013.

[12] IT & Future Strategy, Big data : Echo system's market competition and strategy analysis, 2012.

[13] Report to the President and congress, Designing a digital future : Federally funded research and development in networking and information technology, 2010.

[14] Verizon Business, Data security violation report, 2012.

[15] Zettaset. The Big Data Security Gap: Protecting the Hadoop Cluster, white paper, 2013.

[16] Securosis, Securing Big Data: Security Recommendations for Hadoop & NoSQL Envrironment, 2010.

[17] RSA Security Brief, BIG DATA fuels intelligence-driven security, 2013.

홍 진 근(HONG, JINKEUN)

- 1991년 2월 : 경북대학교 전자공학과(공학사)
- 2000년 2월 : 경북대학교 전자공학과(공학박사)
- 2004년 3월 ~ 현재 : 백석대학교 정보통신학부 교수

- 관심분야 : 정보보호정책, 통신네트워크보안
- E-Mail : jkhong@bu.ac.kr