리뷰논문 정보화정책 제23권 제1호, 2016년 봄호, pp.3~19

빅데이터 보안 분야의 연구동향 분석

박 서 기*, 황 경 태**

요 약 본 연구의 목적은 빅데이터 보안 분야의 기존 연구를 분석하고, 향후 연구 방향을 모색하는 것이다. 이를 위해 국내외의 총62편의 논문을 식별하여, 발간년도, 게재 매체, 전반적인 연구접근 방법, 세부적 연구 방법, 연구 주제 등을 분석하였다. 분석 결과, 빅데이터 보안 연구는 매우 초기 단계로서, 비실증 연구가 압도적인 비중을 차지하고 있고, 관련 개념/기법에 대한 이해를 해나가는 과정으로서 기술-관리-통합의 단계로 진화한 정보보안 분야의 연구 동향에 동조하여 기술적인 연구가 주로 진행되고 있다. 연구 주제 측면에서도 빅데이터 보안에 대한 전반적인 이슈를 다룬 총론적인 연구들이 보안 구현 방법론, 분야별 이슈 등의 각론적 연구에 비해 높은 비중을 나타내는 등 초기 단계의 모습을 나타내고 있다. 향후 유망한 연구 분야로는 빅데이터 보안에 대한 전반적인 프레임워크 수립, 업종별 빅데이터 보안에 대한 연구, 빅데이터 보안 관련 정부 정책 분석 등을 들 수 있다. 빅데이터 보안 분야의 연구는 본격적으로 시작된 지 얼마 되지 않아, 연구 결과가 상대적으로 매우 부족한 편이다. 앞으로 다양한 관점에서 빅데이터 보안과 관련해 풍부한 주제를 다루는 연구가 진행되기를 기대한다.

주제어: 빅데이터, 정보보안, 빅데이터 보안, 빅데이터 프라이버시

A Review of Research on Big Data Security

Seokyee Park, K.T. Hwang

Abstract The purpose of the study is to analyze the existing literature and to suggest future research directions in the big data security area. This study identifies 62 research articles and analyses their publication year, publication media, general research approach, specific research method, and research topic. According to the results of the analyses, big data security research is at its intial stage in which non-empirical studies and research dealing with technical issues are dominant. From the research topic perspective, the area demonstrates the signs of initial research stage in which proportion of the macro studies dealing with overall issues is far higher than the micro ones covering specific implementation methods and sectoral issues. A few promising topics for future research include overarching framework on big data security, big data security methods for different industries, and government policies on big data security. Currently, the big data security area does not have sufficient research results. In the future, studies covering various topics in big data security from multiple perspectives are anticipated.

Keywords: big data, information security, big data security, big data privacy

2016년 3월 16일 접수, 2016년 3월 17일 심사, 2016년 3월 24일 게재확정

* 동국대학교 서울캠퍼스 경영대학 경영정보학과 박사과정(innovationok@gmail.com)
** 교신저자, 동국대학교 서울캠퍼스 경영대학 경영정보학과 교수(kthwang@dongguk.edu)

Ⅰ. 서론

빅데이터 분석이 기업 경영과 학술 연구 분야의 핫 토픽으로 부상하고 있고, 실제로 많은 산업 분야에서 활발하게 활용됨에 따라, 빅데이터의 보안과 프라이버시에 대한 관심 또한 높아지고 있는 추세이다. 그러나 빅데이터의 광범위한 활용과 빅데이터의 보안 및 프라이버시 간에는 모순이 존재할 수밖에 없다(Bardi, 2014).

빅데이터 보안이 중요하다는 점은 여러 학자와 전문가들이 공통적으로 일관성 있게 지적하고 있다. 이들이 빅데이터 보안의 중요성에 대해 강조하는 공통된 입장 중의 하나는 빅데이터의 보안 솔루션은 빅데이터의 고유한 특성에 맞는 내용을 지원해야 한다는 것이다. 즉, 기존의 보안 솔루션으로는 빅데이터 보안을 준수하기 어렵다는 것이다(Murthy, 2014; Paryasto, 2014; Lafuente, 2015). 우리가 빅데이터가 아닌 환경에서 사용하고 있는 대부분의 기존 보안 솔루션들은 빅데이터 환경에서는 제대로 작동하지 않을 수 있다(Van Ginkel, 2013). 빅데이터가 가진 속성, 즉, 대용량, 빠른 속도, 데이터의 다양성이라는 특성을 기존의 보안 솔루션이 제대로 지원하지 못한다는 것이다.

빅데이터 분석에는 다양한 데이터가 동원되는 만큼, 개인정보의 유출 가능성을 막을 수 있는 프라이버시 솔루션에 대한 중요성도 시급하게 대두되고 있다. 또한 다양한 데이터 소스를 분석하는 것이 빅데이터 분석인 만큼 새로운 보안 및 거버넌스 정책도 필요하다(Paryasto, 2014). 특히 상이한 데이터에 대해 암호화를 해야 하는 만큼, 다른 형식의 보안 기술이 필요하다. 동일한 암호화 기술을 적용할 경우, 높은 비용이 초래되는 것은 물론 복잡한 구현 절차 때문에 어려움을 겪을 수도 있다.

빅데이터 보안과 프라이버시를 위해서는 다음과 같은 네 가지 관점을 고려해야 한다(Thuraisingham, 2015). 빅데이터 보안 및 프라이버스 보호를 위해 해결해야 할 가장 중요한 문제 중의 하나는 규제 사항을 준수하고 분석 효과를 향상시킬 수 있도록 균형있는 접근방식을 취하는 것이다. 두 번째 관건은 빅데이터 분석 처리를 위한 인프라를 안전하게 유지하는 일이다. 하둡, 맵리듀스, 하이브, 카산드라 등 다양한 빅데이터 기술을 안전하게 처리하면서 높은 성능을 구현하는 것이 관건인 것이다. 세 번째 이슈는 접근 방법, 인덱싱 및 질의(Query) 프로세스의 안정성을 확보하는 것이다. 마지막으로 빅데이터 보안이라는 관점에서 보안, 프라이버시, 정합성, 데이터 품질, 신뢰 정책 등을 검토해야 한다. 즉, 빅데이터 분석에 걸 맞는 정책을 마련해야 한다는 것이다.

빅데이터 보안과 관련해 주목해서 봐야 할 측면은 이외에도 여러 가지가 있다. 보안 측면에서 빅데이터 분석의 가장 중요한 도전 사항으로는 사용자의 프라이버시 보호를 들 수 있다(Lafuente, 2015). 빅데이터에는 거대한 양의 개인 식별 정보가 담기는 만큼, 사용자 프라이버시의 보호가 관건이 될 수밖에 없기 때문이다. 또 많은 사용자가 빅데이터를 접근할 수 있도록 해야하는 만큼, 암호화 솔루션과 접근 통제 솔루션에 대한 관심도 필요하다.

최근 들어 빅데이터 분석에 대한 기업의 관심과 활용은 급증하고 있지만, 아직까지 빅데이터 보안에 대한 학술적인 연구는 매우 미흡하게 수행되고 있다. 이 분야의 최근 한 연구(Thuraisingham, 2015)에서 빅데이터 보안과 관련해 연구해야 할 주제가 매우 광범위하고 복잡하므로 빅데이터 보안에 대한 연구의 도전 과제들을 논의하기 위한 커뮤니티를 만들자고 제안하고 있는 데서도 이를 확인할 수 있다.

따라서 이러한 상황 인식 하에서 본 연구에서는 점차 관심을 받고 있는 빅데이터 보안에 대한 기존 연구 동향을 파악하고, 향후 빅데이터 보안에 대한 연구가 지향해야 할 방향과 시사점을 제안하고자 한다. 이를 위해서 본 연구에서는 지금까지 출간된 관련 문헌을 식별하고, 선정된 문헌을 대상으로 발간 년도, 게재 매체, 연구의 전반적인 접근방법 및 세부

방법, 연구 주제 등의 측면에서 분석하고, 이러한 분석을 바탕으로 향후 연구 방향과 시사점을 제시하고자 한다.

본 논문은 다음과 같이 구성되어 있다. 다음의 제2장에서는 최근까지 발간된 빅데이터 보안 관련 문헌을 분석하고, 그 결과로부터 시사점을 도출하기 위한 방법을 설명한다. 여기에는 관련 문헌의 수집 및 선정 절차, 분석 기준 및 방법 등이 포함된다. 제3장에서는 분석 기준에 따라 분석한 결과를 정리한다. 마지막으로 제4장에서는 분석으로부터 도출한 시사점과 결론을 제시한다.

Ⅱ. 문헌 분석 방법

본 연구에서는 '구글 학술검색' 검색엔진을 활용하여 본 연구의 주제인 빅데이터 보안 분야에서 수행된 연구 문헌을 식별하였다. 구글 학술검색을 이용한 이유는 영어권의 방대한 학술정보를 검색하는데 유리하고, 논문 출간연도별 검색 등 특화된 기능이 있어 검색 결과를 분류하기 용이하기 때문이었다. 일관성을 위해 국내 논문의 검색도 구글 학술검색을 이용하였다. 구글 학술검색에서 해외 문헌의 경우에는 논문 제목에 'big data security' 라는 키워드를, 국내 문헌의 경우에는 ' 빅데이터 보안 '이라는 문구를 정확하게 포함하고 있는 문헌을 검색한 결과, 해외 문헌 129편, 국내 문헌 15편이 식별되었다. 본 연구의 분석 대상은 학술 논문이므로, 식별된 문헌의 출처를 확인하여 학술 논문에 해당하지 않는 단행본, 보고서, 백서 등을 제외하였다. 이러한 과정을 거쳐 최종적으로 해외 논문 51편과 국내 논문 11편 등 총 62건의 논문이 분석 대상으로 선정되었다. 선정된 논문이 게재된 학술지와 학술대회의 이름은 〈부록〉에 정리되어 있다. 최종 선정된 62편의 문헌을 대상으로 다음의 〈표 1〉에 정리되어 있는 기준을

〈표 1〉 분석 기준

분석 기준	설명	분석 항목
발간년도	해당 문헌이 발간된 연도	발간년도
게재 매체	해당 문헌이 공식적인 학술지에 게재된 논문인지, 학술대회에 발표된 논문인지의 여부	• 학술지 논문 • 학술대회 발표 논문
전반적인 연구 접근방법	해당 문헌이 실제 현상의 체계적인 관찰에 의존하는 실증 연구인지, 데이터나 관찰보다는 아이디어, 프레임워크, 고찰 등을 기반으로 한 비실증 연구인지의 여부	• 실증 연구 • 비실증 연구
비실증 연구의 세부 연구 방법	비실증 연구의 세부적인 연구방법을 식별[1]	• 개념적(프레임워크/모델) • 개념적(수리적/공학적 모델) • 튜토리얼/리뷰
실증 연구의 세부 연구 방법	실증 연구의 세부적인 연구방법을 식별[2]	• 서베이(survey) • 사례연구 • 현상 기술
연구 주제	해당 문헌에서 다루고 있는 연구 주제를 식별	• 빅데이터 보안의 전반적 내용 • 분야별 빅데이터 보안 이슈 • 빅데이터 보안 구현 방법론

1) 비실증 연구 세부 방법은 Alavi & Carlson(1992)의 분류를 기반으로 하였는데, 빅데이터 보안 분야의 기존 연구에서 사용한 방법만을 분석 기준으로 채택하였음.

2) 실증 연구의 세부 방법에는 오른편의 방법 이외에도 실험실 실험, 현장 실험, 도구 개발, 이차 데이터 분석 등 여러 가지 방법이 있으나, 빅데이터 보안 분야의 기존 연구에서 사용한 방법만을 분석 기준으로 채택하였음.

적용하여 분석을 실시하였다. 분석 기준에는 논문의 발간년도, 학술지 논문인지 학술대회 발표논문인지로 구분한 논문이 게재된 매체, 실증 연구와 비실증 연구로 분류한 전반적인 연구접근 방법, 실증 또는 비실증 연구의 세부적인 연구 방법, 연구 주제 등이 포함된다.

위의 분석 기준 중에서 연구 주제를 제외한 기준들은 본 연구와 같은 성격의 리뷰 논문에서 일반적으로 채택하고 있는 분류 방법에 속한다(Alavi & Carlson, 1992; Vessey, et al., 2002; 이종옥 외, 2012). 연구 주제의 경우에는 현재 빅데이터 보안 분야의 연구가 매우 초기 단계에 있기 때문에, 널리 인정받고 있는 하나의 일반적이고 공통적인 연구 프레임워크는 수립되어 있지 않은 상태이다. 이에 따라 본 연구에서는 분석 대상으로 선정한 62편의 논문의 내용을 검토한 이후, 빅데이터 보안의 전반적 내용, 분야별 빅데이터 보안 이슈, 빅데이터 보안 구현 방법론 등 세 가지 주제를 귀납적으로 도출하였다.

위의 기준을 적용한 분석은 국내외 문헌을 모두 포괄하여 수행되었고, 이에 추가하여 국내와 해외의 연구 동향을 비교해 볼 수 있는 분석도 수행하였다. 문헌을 분석하여 기준에 따라 분류하는 작업은 먼저 2인의 공동 저자들이 상호 독립적으로 수행한 후, 분석 결과를 비교해 보고 차이가 나는 부분이 있으면 2인의 저자가 분석 결과를 협의하여 최종 결정하는 상호교차 분석 방식을 채택하여 진행하였다.

분류 결과를 구체적으로 살펴보면, 비실증 연구의 세부 연구방법 분류에 2건, 실증 연구의 세부 연구방법 분류에 1건의 차이 이외에는 2인의 분류 내용이 모두 일치하는 결과를 얻었다. 차이가 난 부분에 대해서는 두 연구자가 분류한 이유 등을 토의한 후, 최종적으로 결정하였다.

Ⅲ. 분석 결과

1. 발간년도

문헌의 발간년도를 살펴보면, 〈표 2〉에서 볼 수 있는 바와 같이, 국내 및 해외 공히 2012년에 최초로 연구 결과들이 발표되었는데, 이것을 통해 빅데이터 보안이라는 분야는 매우 새로운 연구 분야라는 것을 확인할 수 있다.

전체적으로 봤을 때, 2012년에 연구가 시작된 이후 이 분야에서의 연구 노력이 지속적으로 증가하고 있다는 것을 알 수 있다. 해외와 국내 현황을 비교해 보면, 해외의 경우에는 2012년 이후 연구가 비교적 활발하게 추진되고 있는 반면, 국내의 경우에는 전체적으로 연구의 건수도 적고, 2013년을 정점으로 오히려 감소하는 추세를 나타내고 있다. 국내의 경우 빅데이터에 대한 업계의 관심은 높은 편이지만, 아직까지 눈에 띌 만한 대형 프로젝트가 드물고, 빅데이터의 활용 수준도 높지 않은 편이다. 국내 빅데이터 시장 자체가 워낙 초기 단계이다 보니, 관련 연구가 활성화되는데 근본적인 한계가 있는 것으로 판단된

〈표 2〉 발간년도 별 분석 결과

발간년도	전체	해외	국내
2012	3 (5%)	2 (4%)	1 (9%)
2013	13 (21%)	8 (16%)	5 (45%)
2014	25 (40%)	22 (43%)	3 (27%)
2015	20 (32%)	18 (35%)	2 (18%)
2016	1 (2%)	1 (2%)	0 (0%)
합 계	62 (100%)	51 (100%)	11 (100%)

〈표 3〉 게재 매체별 분석 결과

게재 매체	전체	해외	국내
학술지 논문	34 (55%)	27 (53%)	7 (64%)
학술대회 발표논문	28 (45%)	24 (47%)	4 (36%)
합 계	62 (100%)	51 (100%)	11 (100%)

다. 그러나 빅데이터 보안이라는 새로운 분야에 대해 국내의 연구자들이 보다 적극적인 관심을 가지고, 실무를 선도하기 위한 연구가 지속적으로 이루어지도록 하는 것이 필요한 것으로 보인다.

2. 게재 매체

논문들이 게재된 매체를 학술지와 학술대회 발표집(Proceedings)으로 구분하여 분석해 본 결과는 다음의 〈표 3〉에 정리되어 있다.

〈표 3〉에서 볼 수 있는 바와 같이, 전체적으로 봤을 때 학술대회 발표논문이 거의 절반(45%)을 차지하고 있다. 이것은 이 분야가 불과 몇 년 전부터 연구되기 시작한 신생 연구 분야라는 것을 반증해 주는 결과이다. 초기 연구 단계이기 때문에, 개념적이고 실험적인 연구들이 많이 수행되고, 이에 따라 공식적이고 비교적 확정적인 연구 결과를 제시해야 하는 학술지보다는 먼저 학술대회에서의 발표를 통해서 연구 결과를 연구자들과 공유하고, 이들의 의견을 수렴하여 정교화해 나가는 과정이라고 판단된다. 빅데이터 보안 분야의 연구가 초기 단계라는 점을 감안한다면, 이러한 추세는 당분간 장려되어야 하고, 향후 몇 년간에도 지속될 것으로 예상된다.

3. 전반적인 연구 접근방법

전반적인 연구 접근방법 측면에서 실증 연구와 비 실증 연구의 비중을 살펴보면, 전체적으로 봤을 때, 비 실증 연구가 94%로 압도적인 비중을 차지하고 있다(〈표 4〉 참조).

이처럼 비실증 연구의 비중이 높은 것은 비교적 성숙한 연구 분야에서는 찾아보기 힘든 현상이다. 예를 들면, 비교적 성숙한 연구 분야로 볼 수 있는 경영정보학 분야의 경우, 2002년~2007년의 기간 동안에 주요 해외저널에 게재된 논문들 중 실증 연구의 비중은 70%를 차지했고(Shao, et al., 2010), 국내의 경우 1991년~2003년까지 경영정보학 분야의 대표 학술지인 '경영정보학연구'에 실린 논문 중 실증 연구가 차지하는 비중은 89%에 달했다(김기문 외, 2005).

국내의 경우에도 비실증 연구의 비중이 매우 높은 편이지만(73%), 해외의 비중(98%)과 비교해보면 실증 연구의 비중이 상대적으로 높은 것을 알 수 있다. 이것은 국내 학자 및 학술지들이 실증주의에 입각한 연구를 보다 선호하는 국내의 경향(이종옥 외, 2012)을 반영하고 있는 결과로 보인다.

해외 및 국내를 망라해서 이처럼 비실증 연구의 비

〈표 4〉 전반적인 연구 접근방법별 분석 결과

전반적 연구방법	전체	해외	국내
실증	4 (6%)	1 (2%)	3 (27%)
비 실증	58 (94%)	50 (98%)	8 (73%)
합 계	62 (100%)	51 (100%)	11 (100%)

중이 높은 것은 빅데이터 보안의 기본 개념을 정립하고, 실증적으로 검정할 연구 가설들을 수립하기 위해서는 선행적으로 비실증 연구가 수행되어야 하는 이론 정립의 자연스러운 발전 단계로 보인다. 그러나 향후 연구에서는 단순히 현상을 설명하거나 개념적 또는 수리적인 모델을 제시하는 연구만을 추구할 것이 아니라, 빅데이터 보안에 관련된 일반적인 이론을 정립하는 것을 목표로 하여 관련 개념과 요인들 간의 인과 관계를 확인할 수 있는 설명적 연구의 기반을 구축하기 위한 실증적인 연구를 추진하는 것이 필요하다고 판단된다.

4. 비실증 연구의 세부적 연구방법

비실증 연구의 세부 연구방법별 비중은 다음의 〈표 5〉에서 볼 수 있는 바와 같이, 빅데이터 보안의 개념이나 기법을 설명하는 투토리얼 및 리뷰가 가장 큰 비중(48%)을 차지하고 있고, 그 다음으로 빅데이터 보안을 위한 수리/공학적 모델을 제시하는 연구(38%)로 나타났다. 그리고 빅데이터 보안에 대한 개념적 모델을 제시하는 연구는 가장 낮은 비중(14%)을 차지하고 있다. 이러한 추세는 국내외 공히 비슷한 양상을 나타내고 있다.

이러한 결과를 통해서 다음과 같은 몇 가지 사항을 유추해 볼 수 있다. 첫째, 빅데이터 보안 분야의 연구에서 개념이나 기법을 설명하는 투토리얼 및 리뷰 연구가 높은 비중을 차지하고 있다는 것은 아직도 이 분야가 연구의 초기 단계로서, 관련 개념이나 기법에 대한 이해를 해나가는 과정이라는 것을 반증하는 결과이다. 둘째, 두 번째로 높은 비중의 연구들이 빅데이터 보안을 위한 수리/공학적 모델을 제시하는 기술적인 연구가 차지하고 있는데, 이것은 일반적인 정보보안 분야의 진화 단계와 유사한 행태를 보여주는 결과이다. 정보보안 분야의 발전사를 살펴보면, 보안에 대한 접근방법은 기술-관리-통합의 단계로 진화했다(황경태, 2011). 빅데이터 보안 분야에서도 초기의 연구들은 진화 단계의 첫 번째에 속하는 기술적인 분야에 집중되고 있다고 볼 수 있다. 셋째, 개념적 모델을 제시하는 사회과학적이고 관리적인 연구가 미흡한데, 이것은 위에서 설명한 바와 같이, 기술적 연구 이후에 관리적인 연구가 추진된 정보보안 분야의 연구 동향에 동조하는 현상으로 볼 수 있다.

빅데이터 보안 분야의 향후 연구에서는 정보보안 분야의 진화 과정과 같이 기술적 연구들이 성숙된 이

〈표 5〉 비실증 연구의 세부 연구방법별 분석 결과

비실증 연구의 세부 연구방법	전체	해외	국내
수리/공학적모델	22 (38%)	20 (40%)	2 (25%)
개념 모델	8 (14%)	6 (12%)	2 (25%)
튜토리얼/리뷰	28 (48%)	24 (48%)	4 (50%)
합 계	58 (100%)	50 (100%)	8 (100%)

〈표 6〉 실증 연구의 세부 연구방법별 분석 결과

실증 연구의 세부 연구방법	전체	해외	국내
서베이	1 (25%)	0 (0%)	1 (33%)
사례연구	0 (0%)	0 (0%)	0 (0%)
현상기술	3 (75%)	1 (100%)	2 (67%)
합 계	4 (100%)	1 (100%)	3 (100%)

후에 관리적인 연구에 착수할 필요 없이, 기술적인 연구를 추진해 가면서, 이와 동시에 관리적인 연구와 기술과 관리를 통합하는 연구를 동시에 추진하는 것이 이 분야의 발전을 위해 바람직한 연구 방향으로 판단된다.

5. 실증 연구의 세부적 연구방법

분석 대상 문헌 중에서 실증 연구의 비중이 너무 낮기 때문에 세부적인 분석이 큰 의미는 없을 수 있지만, 현황을 정리해 보면 다음의 〈표 6〉과 같다.

표에서 볼 수 있는 바와 같이, 몇 건 안 되는 실증 연구의 대부분(75%)은 현상 기술 기법을 활용한 연구이고, 1건의 서베이(Survey) 연구가 집계되었다. 이러한 결과 또한 빅데이터 보안이라는 연구의 대상을 파악하고 설명하고자 하는 시도들로서, 이 분야가 연구의 초기 단계라는 것을 재확인시켜주는 결과이다. 그러나 향후 연구에서는 서술적 연구를 추진하는 경우에라도, 현상 기술적 접근방법뿐만 아니라 연구 방법론적인 측면에서 정교함의 수준이 상대적으로 높은 사례연구 방법론을 도입할 것을 권고한다. 또한 향후의 설명적 연구의 기반을 구축하는 것을 염두에 두고 실증 연구를 추진하는 것이 필요하다고 판단된다.

6. 연구 주제

전체적으로 분석 대상 논문을 세부 주제 영역별로 살펴본 결과, 빅데이터 보안 전반에 걸친 주제를 다룬 논문은 28건(45%), 클라우드 컴퓨팅, 하둡, 헬스케어 등 분야별 빅데이터 보안 이슈를 다룬 논문은 16건(26%), 분야별 빅데이터 보안 구현 방법론을 다룬 논문은 18건(29%)으로 나타났다 (〈표 7〉 참조).

빅데이터 보안 전반에 걸친 논문이 가장 많은 비중을 차지한 이유는 빅데이터 보안에 대한 관심이 높아지면서 빅데이터 보안 프레임워크를 정립하기 위한 시도가 활발해졌기 때문으로 풀이된다. 총론이라고 할 수 있는 빅데이터 보안에 대한 전반적인 이슈를 다룬 논문에 비해 각론격인 빅데이터 보안 구현 방법론과 분야별 빅데이터 보안 이슈에 대한 논문이 상대적으로 적은 비중을 차지하는 이유는 빅데이터 보안에 대한 연구가 최근 2~3년 사이에 본격화되었기 때문인 것으로 판단된다. 분석 대상 논문의 대부분이 2014년과 2015년에 저술된 만큼 관련 연구가 이제 막 본격화되기 시작한 것으로 생각된다. 총론에 대한 연구가 활발하게 추진되면서, 각론에 대한 연구도 서서히 활발해질 것으로 전망된다.

빅데이터 보안 관련 논문의 세부 주제별 분포는 해외 논문과 국내 논문 간에 큰 차이가 있는 것으로 나타났다. 해외 논문의 경우, 빅데이터 보안 전반에 걸친 주제를 소화한 논문은 26건으로 전체 해외논문 중 51%를 차지했다. 빅데이터 보안 구현 방법론을 다룬 논문은 15건(29%)로 두 번째로 많았고, 분야별 빅데이터 보안 이슈를 다른 논문은 10건으로 20%에 그쳤다. 이에 비해서 국내 논문의 경우에는 분야별 빅데이터 보안 이슈를 다룬 논문이 6건(55%)으로 가

〈표 7〉 연구 주제별 분석 결과

연구 주제	전체	해외	국내
빅데이터 보안의 전반적 내용	28 (45%)	26 (51%)	2 (18%)
분야별 빅데이터 보안 이슈	16 (26%)	10 (20%)	6 (55%)
빅데이터 보안 구현 방법론	18 (29%)	15 (29%)	3 (27%)
합 계	62 (100%)	51 (100%)	11 (100%)

장 많은 비중을 차지했다. 분야별 빅데이터 보안 구현 방법론을 다룬 논문은 3건(27%)으로 두 번째로 많은 비중을 나타냈고, 빅데이터 보안 전반에 걸친 주제를 다룬 논문은 2건에 그쳐 전체 국내 논문 중 18%에 불과했다. 즉, 보안 구현 방법론의 비중은 국내외 간에 차이가 별로 없었으나, 국내의 경우, 해외에 비해 전반적인 주제를 다룬 연구의 비중은 매우 낮고, 분야별 보안 구현 방법론의 비중은 상대적으로 높은 정반대의 현상을 나타내고 있다. 이러한 차이가 나는 이유로는 우리 나라의 학술지나 학술발표대회에서 전반적인 문제를 다루는 추상적인 연구보다는 구체적인 실천방안을 담고 있는 논문을 선호하는 현상을 반영하고 있는 결과라고 판단된다.

다음에서는 세 가지 연구 주제별로 추진된 연구의 주요한 내용 및 특성을 살펴보고, 향후 연구에서 참조할 수 있는 시사점을 도출하도록 한다.

1) 빅데이터 보안의 전반적인 내용에 관한 연구

빅데이터 보안에 대한 전반적인 이슈를 다룬 논문들은 대부분 빅데이터 보안과 프라이버시 보호 문제를 통합적으로 취급하고 있다. 이는 분석 대상 논문의 상당수가 제목에 '보안'과 '프라이버시'를 포함하고 있는데서 이러한 사실을 확인할 수 있다.

빅데이터 보안 전반에 걸친 주제를 다루는 논문들이 가장 큰 비중으로 차지하고 있지만, 분석 프레임워크가 아직 통일되지 않고 제각각이라는 점에서 향후 보다 활발한 연구가 필요한 것으로 보인다. 빅데이터 보안의 전반적인 이슈를 다룬 논문들이 채택하고 있는 분석 프레임워크는 독자적인 프레임워크를 제시한 논문과 기존 보안 프레임워크를 활용해 빅데이터 보안에 적용하려는 시도로 크게 나누어 볼 수 있다.

대부분의 논문들은 독자적인 분석 프레임워크를 채택하고 있는데, 이러한 접근방법을 채택한 대표적인 논문으로는 익명성, 암호화, 접근 통제 및 모니터링, 정책, 거버넌스 등 5가지를 기반으로 빅데이터 보안을 분석한 연구(Lafuente, 2015), 빅데이터의 데이터 비밀, 프라이버시, 신뢰성 측면에서 연구 과제와 방향을 제시한 연구(Singh, 2014), 빅데이터의 다양한 내재적 속성들이 프라이버시, 보안, 소비자 후생과 어떻게 연관돼 있는지를 분석한 연구(Kshetri, 2014) 등을 들 수 있다.

기존 보안 프레임워크를 활용해 빅데이터 보안에 적용 가능성을 검토한 연구도 눈에 띈다. 분석 대상 논문 중에는 두 가지 논문이 이에 해당하는데, 먼저 Paryasto, et al.(2014)에서는 미국 NIST SP800-30(위험 평가) 프레임워크를 빅데이터 보안에 적용할 수 있는지를 검토하였다. 이 연구에서는 NIST 위험 평가 프레임워크의 시스템 특징, 위협 인지, 취약점 인지, 통제 분석, 가능성 측정, 영향도 분석, 위험 측정, 통제 조언 등의 평가 항목과 빅데이터의 주요 특징인 분산 아키텍처, 실시간·스트리밍·지속 컴퓨팅, 비정형적 질의(ad hoc query), 병렬 프로그래밍 언어, 코드 이전, 비SQL 데이터, 오토 티어링, 다양성 등 8가지 항목과 비교한 결과, NIST 프레임워크가 빅데이터 보안에도 유효하게 적용할 수 있다고 평가하고 있다. 또 다른 연구(Lu, et al., 2013)에서는 ICT 산업의 공급망 분석 프레임워크를 이용해 빅데이터 보안을 분석했다. 역시 ICT 산업 공급망 분석 프레임워크를 빅데이터 보안에 적용할 수 있다는 결론을 내리고 있다.

이 연구 주제에 관련된 논문들은 종합적인 프레임워크를 다루고 있는 만큼 향후 연구 과제에 대한 아이디어도 다양하게 제시하고 있다. 다음에서는 이 분야의 연구에서 제시하고 있는 향후 연구 가능한 주제들을 정리해 본다. 앞서 언급한 NIST 위험 평가 프레임워크의 경우, 빅데이터 보안에 적용해도 좋은 만큼 이를 실제로 구현한 사례 연구를 통해 프레임워크를 실증적으로 검증함으로써, 해당 프레임워크의 효과성을 입증하고, 향후 연구의 기반을 제공할 수 있을 것으로 기대된다(Paryasto, et al., 2014). 또 다른 주제로는 빅데이터 환경에서 프라이버시와 보안

에 관한 압력이 나라마다 왜, 어떻게 다른지를 분석해 볼 필요가 있고, 개발도상국에서 빅데이터의 프라이버시와 보안에 관한 기업과 소비자의 인식에 대한 분석이 필요하다는 지적이 있다. 또 빅데이터 관련 행위 및 프로세스(수집, 저장, 분석, 처리, 재사용, 공유) 중 어떤 프로세스가 핵심 문제인지에 대해서도 탐구해볼 필요가 있다. 결론적으로, 빅데이터의 보안과 프라이버시를 종합적으로 분석하기 위해서는 컴퓨터공학, 정보시스템, 통계학, 위험 모델, 경제학, 사회과학, 정치학, 인간요인, 심리학 등 다양한 학문 영역에서 통합적으로 접근하는 학제적 접근 방식의 연구가 필요한 것으로 판단된다(Bertino, 2015).

2) 분야별 빅데이터 보안에 관한 연구

분야별 빅데이터 보안 주제를 다룬 논문들의 세부적인 내용을 보다 자세히 분석해 보면, 특정 기술 이슈, 업종별 이슈, 정책·사회적 이슈 등 크게 세 가지 종류로 구분해 볼 수 있다. 분석 대상 논문 중 총 16건의 논문이 분야별 빅데이터 보안을 주제로 하고 있는데, 이중 특정 기술 이슈와 관련된 주제를 다룬 논문은 10건, 업종별 이슈를 다룬 논문은 4건, 정책·사회적 주제를 다룬 논문은 2건으로 대다수는 특정 기술에 관련된 이슈를 다루고 있는 것으로 나타났다.

특정 기술을 다룬 논문 중에는 클라우드 컴퓨팅을 소재로 한 논문이 5건으로 가장 많았다(Ahmed, et al., 2014; Chen, 2015; Gangawane, et al., 2015; Grant, et al., 2014; Inukollu, et al., 2014). 하둡 보안에 대한 논문이 2건이었으며(Adluru, et al., 2015; Sharma, et al., 2014), 커버로스 인증 적용 정책(Lu, et al., 2013), 빅데이터 처리 프로세스(Abawajy, et al., 2014), 스마트그리드(Marchal, et al., 2014) 등의 주제가 각 1건씩으로 나타났다.

이 분야에서 가장 큰 관심을 받고 있는 빅데이터 클라우드 컴퓨팅 보안의 경우, 클라우드 컴퓨팅, 빅데이터, 맵리듀스, 하둡 등 다양한 환경에서 보안을 구현해야 하는 만큼, 향후 연구에서는 네트워크 레벨, 인증 레벨, 데이터 레벨, 포괄적인 유형 등 4가지 측면에서 체계적인 분석이 필요한 것으로 판단된다(Inukollu, et al., 2014). 또한 눈에 띄는 사실은 분야별 빅데이터 보안 주제와 관련된 국내 논문의 경우 클라우드 컴퓨팅 보안, 하둡 보안 등 최신 기술 이슈를 다룬 논문이 하나도 없다는 점이다. 미국 커버로스 인증 적용 정책에 대해 소개하거나(홍진근, 2013), 빅데이터 처리 프로세스에 따른 빅데이터의 위험요소를 설명(이지은 외, 2014)하는 식의 개념적이고 개론적인 연구이다, 그마나 스마트 그리드에 관한 논문(Kang, et al., 2015)이 있기는 하지만 빅데이터 플랫폼을 활용한 스마트 그리드 보안 모니터링 동향에 대한 연구로서, 빅데이터 보안의 신기술에 대한 것은 아니다. 따라서 향후 국내 연구에서는 최근 실무적으로나 학술적으로 관심을 많이 받고 있는 빅데이터 보안 기술에 대한 연구를 추진할 필요가 있다고 판단된다.

그리고 해외 연구에서는 찾아볼 수 없는 정책·사

〈표 8〉 분야별 빅데이터 보안을 다룬 연구의 세부 주제

	전체	해외	국내
특정 기술 이슈	10 (45%)	7 (70%)	3 (50%)
업종별 이슈	4 (24%)	3 (30%)	1 (17%)
정책·사회적 이슈	2 (31%)	-	2 (33%)
합 계	16 (100%)	10 (100%)	6 (100%)

회적 이슈에 대한 연구가 국내에서만 2편이 발표된 것으로 집계되었다. 이것은 고무적인 현상이고, 향후 빅데이터 보안을 둘러싼 정책 사회적 이슈에 대한 관심이 높아질 것으로 예상되기 때문에 활발한 후속 연구들이 진행되기를 기대한다.

업종별 이슈를 다루는 논문은 헬스케어 분야가 3건(Blobel, et al., 2016; Feng, et al., 2015; Kupwade, et al., 2014), 호텔 1건(공효순 외, 2013) 등으로 나타났다. 헬스케어 산업이 유독 많이 눈에 띄는 이유는 빅데이터 처리 과정에서 환자의 개인 정보 등 민감한 정보를 많이 다룰 수밖에 없는 만큼 보안과 프라이버시의 처리가 다른 산업보다 중요하게 대두되기 때문으로 풀이된다. 헬스케어 빅데이터 보안의 경우, 향후 연구에서 중요하게 분석해야 할 분야로는 데이터 거버넌스, 실시간 보안 분석, 프라이버시 보존형 분석 등 3가지 측면을 들 수 있다(Kupwade Patil, et al., 2014). 또한 헬스케어와 호텔업 외에는 업종별 빅데이터 보안 이슈를 탐구한 논문이 아직 없다는 점에서 향후 다양한 업종별 빅데이터 보안에 대한 연구 활동이 필요해 보인다.

정책·사회 분야 논문의 경우, 미국 정부의 보안 정책을 분석한 논문과 빅데이터와 사회 안전에 대해 분석한 논문이 있다(유영성 외, 2014; 홍진근, 2013). 미국 정부의 보안 정책을 분석한 논문(홍진근, 2013)은 미 정부의 빅데이터를 위한 주요 정책과 전략, 보안을 중심으로 추진되고 있는 연구 프로그램, 운영 보안의 가이드라인을 중심으로 고찰하고 있다. 유영성 외(2014)는 빅데이터 보안의 중요성을 서술적 기법으로 설명하면서, 빅데이터 활용이 사회적 공익에 기여하는 것은 물론 빅데이터로 무장된 새 보안체계를 도입함으로써 사이버보안 위협에 효율적으로 대응할 수 있다고 설명하고 있다. 빅데이터 보안의 특성상 정부 차원에서 각종 규제가 앞으로 본격화될 것인 만큼, 각국의 빅데이터 정책을 비교해 보고, 빅데이터 정책을 고도화하는 방안 등에 관한 후속 연구가 유망해 보인다.

3) 빅데이터 보안 구현 방법론에 관한 논문

빅데이터 보안 구현 방법론을 다룬 논문은 분야별 빅데이터 보안 이슈를 다룬 논문에 비해 좀 더 많은 18건으로 집계되었는데, 이 중에서 해외 논문은 15건이며, 국내 논문은 3건으로 나타났다.

빅데이터 보안 구현 방법론을 다룬 연구에서 가장 대표적으로 다룬 세부 주제로는 암호화, 속성 관계(Attribute Relationship) 구현 및 처리를 들 수 있다. 암호화에 관한 논문이 3편(해외 2편, 국내 1편)으로 가장 많았고, 속성 관계에 관한 논문이 2편이었고, 나머지 논문들을 모두 상이한 주제를 다루고 있었다.

암호화에 관한 연구에는 양자 암호화와 인증 기술을 이용한 프라이버시(Thayananthan, et al., 2015), 빅데이터를 위한 암호화 기술을 활용해서 네트워크 보안을 구현하는 방법(Yadav, et al., 2015), 기존의 속성 기반 암호화나 브로드캐스트 암호화 기법에 비해 추가 기능, 공유 거리, 저장소 수 측면에서 훨씬 유리한 ID기반 암호화 기법에 관한 연구(조영복 외, 2012) 등이 있다. 빅데이터 보안의 암호화 분야는 빅데이터의 취합, 정제, 분석, 활용 등의 전 프로세스에 적용되는 기술인만큼, 향후 세부적인 영역의 기술 발전과 적용 방안 등에 대한 후속 연구가 기대된다. 속성 관계에 관한 연구(Kim, et al., 2013a; Kim, et al., 2013b)에서는 데이터 자체보다 빅데이터의 가치에 초점을 맞춰 속성 관계 그래프를 이용할 경우, 빅데이터 보안을 좀 더 효과적으로 구현할 수 있다는 것을 설명하고 있다. 향후 빅데이터 유형에 맞춰 보호화 된 속성 선택 알고리듬에 대한 연구와 속성 간 관계 확장 방법론에 대한 추가적인 연구가 필요한 것으로 판단된다.

흥미로운 점은 빅데이터 보안 구현 방법론에 관한 해외 논문의 경우, 소프트웨어정의네트워크(Software Defined Network: SDN) 환경의 빅데이터 보안 분석 기술이나 머신러닝 기술을 이용한 실시간 빅데이터 분석 기술, 원격측정(Telemetry) 데

〈표 9〉 다양한 융합 환경에서 적용할 수 있는 빅데이터 보안 기술에 대한 연구

문헌	주요 내용
Choi, et al.(2015)	SDN 환경에서 빅데이터 보안 분석의 오버헤드를 줄이는 방법과 멀티 SDN 환경을 지원하는 방안 제시
Singh(2014)	머신러닝 기술을 활용한 보안 문제 해결 가능성 제안. 많은 보안 전문가들이 머신러닝 기술에 주목하는 이유는 해당 기법을 활용할 경우 보다 강력한 시스템을 설계하거나 더 나은 결과를 얻을 수 있기 때문
Kalibjian(2013)	하둡 기술을 활용한 원격측정 데이터 분석 기술 소개. 원격측정 제품과 원격측정 후처리 제품의 도입이 증가함에 따라 원격측정 영역의 빅데이터 관리 기술과 보안 기술 애플리케이션이 점차 증가.

〈표 10〉 빅데이터에 특화된 다양한 신기술 적용 방안에 관한 연구

문헌	주요 내용
Abawajy, et al.(2014)	빅데이터에 맞게 수정된 LIME(large iterative multitier ensemble) 분류자(classifier) 소개. LIME 분류자의 빅데이터 보안 문제에 적용한 결과 다양한 기반 분류자 및 표준 앙상블 메타 분류자(ensemble meta classifier)에 비해 분류사의 정확성이 크게 높아졌다는 실험 결과 제시
Marchal, et al.(2014)	네트워크 침해 시도를 탐지하고, 탐지 시도로부터 보호하기 위한 확장성 있는 아키텍처 소개
Tan, et al.(2014)	빅데이터 보안에 보다 효율적인 협업 침입탐지 기술 제시. 전통적인 침입탐지시스템(IDS)은 독립형(stand alone) 시스템으로 컴퓨터 네트워크나 호스트 머신에 존재하지만, 협업침입탐지시스템(Collaborative Intrusion Detection System: CIDS)은 로컬 네트워크의 진입지점(entry point)에 있는 IDS와 트래픽 정보를 공유하기 때문에 침입탐지에 더 효과적이라는 것을 증명
Hsu, et al.(2014)	빅데이터 기반의 안전한 그룹 커뮤니케이션을 보장할 수 있도록 온라인 키생성센터(Key Generation Center: KGC)가 없는 상태의 그룹 키 트랜스퍼(group key transfer) 프로토콜을 제안. 이 프로토콜을 이용할 경우 잠재적인 공격 방지 및 시스템 구현시 오버헤드 감소

이터 제품을 위한 빅데이터 보안 애플리케이션 등 다양한 융합 환경에서 적용할 수 있는 빅데이터 보안 기술에 대한 연구 등이 제시되고 있다. 다음의 〈표 9〉에는 이러한 보안 기술에 대한 연구의 주요한 내용들이 정리되어 있다.

또한 대규모 보안 모니터링 기술이나 협업 침입 탐지 기술, 그룹 키 트랜스퍼 프로토콜 기술, LIME(Large Iterative Multitier Ensemble) Classifier 등 빅데이터에 특화된 다양한 신기술을 적용하는 방안에 대한 논문들도 눈에 띈다. 다음의 〈표 10〉에는 이러한 보안 기술에 대한 연구의 내용을 정리한다.

빅데이터 보안 구현 방법론 분야의 해외 논문들이 이처럼 다양한 기술에 대해 소개하고 있는 반면, 국내 논문들은 보안품질평가모델(최주영 외, 2015), 빅데이터 ETL(Extract/ Transform/Load) 모델(이승하 외, 2014), ID 기반 암호화(조영복 외, 2012) 등 기존 기술 혹은 평가 모델의 연장선에 머문 연구들만 추진된 것으로 나타났다. 빅데이터 보안 구현 방법론 분야는 기존 보안 분야의 핵심 기술을 토대로 후속 연구가 활성화될 수밖에 없다. 따라서 향후 국내에서 빅데이터 보안 구현 방법론 분야에서 다양한 연구 성과를 내기 위해서는 보안 전문가들의 활발한

관심과 빅데이터 연구자들과의 협업 연구 등이 활발하게 이루어질 필요가 있다고 판단된다.

Ⅳ. 결론 및 시사점

본 연구에서는 빅데이터 보안과 관련된 국내외 연구 동향을 파악하고, 향후 연구를 위한 방향과 시사점을 도출하기 위해, 현재까지 학술지와 학술대회 발표집에 게재된 총 62편의 국내외 논문을 분석하였다. 선정된 논문을 대상으로 논문의 발간년도, 게재 매체, 연구의 전반적인 접근방법 및 세부 방법, 연구 주제 등의 측면에서 분석을 실시하였다.

분석 결과를 바탕으로, 빅데이터 보안 분야의 연구의 일반적인 경향을 다음과 같이 정리해 볼 수 있다. 첫째, 빅데이터 보안 관련 연구는 매우 초기 단계로서, 국내외 모두 2012년에 빅데이터 보안에 관한 논문이 처음으로 발표된 이후 매년 소폭으로 성장하고 있는 수준이다. 국내의 경우에는 해외에 비해 연구의 건수도 적고, 2013년을 정점으로 오히려 감소하는 추세를 나타내고 있다. 둘째, 연구의 게재 매체 측면에서 봤을 때, 학술대회 발표논문이 거의 절반(45%)을 차지하고 있는데, 이것 역시 이 분야가 신생 연구 분야라는 것을 나타내는 결과이다. 셋째, 이 분야의 전반적인 연구 접근방법은 비실증 연구가 압도적인 비중을 차지하고 있는데, 이것 역시 이론 정립의 자연스러운 발전 단계로 보인다. 넷째, 비실증 연구의 세부 연구방법별 비중을 살펴보면, 투토리얼/리뷰(48%), 수리/공학적 모델(38%), 개념적 모델(14%)의 순으로 나타났다. 이것은 이 분야가 연구의 초기 단계로서, 관련 개념이나 기법에 대한 이해를 해나가는 과정이고, 기술-관리-통합의 단계로 진화한 정보보안 분야의 연구 동향에 동조하는 현상으로 볼 수 있다. 다섯째, 연구 주제 측면에서도 빅데이터 보안 분야는 초기 단계의 모습을 나타내고 있다. 빅데이터 보안에 대한 전반적인 이슈를 다룬 총론적인 연구들이 보안 구현 방법론이나 분야별 이슈를 다룬 각론적인 연구에 비해 높은 비중을 나타내고 있고, 분야별 이슈에 대한 논의도 헬스케어와 호텔업 등에 한정돼 있기 때문이다.

위와 같은 분석 결과를 바탕으로, 빅데이터 보안 분야의 향후 연구에서 참고할 수 있는 몇 가지 시사점과 방향을 제시하면 다음과 같다. 첫째, 국내 연구자들은 빅데이터 보안이라는 새로운 분야에 대해 보다 적극적인 관심을 가지고, 실무를 선도할 수 있는 연구를 수행하는 것이 매우 필요해 보인다. 이러한 과정에서 학술지에 확정적인 연구 결과를 게재하는 것뿐만 아니라, 이 분야가 초기 단계라는 것을 감안하여 학술대회를 통해서 잠정적인 연구 결과를 발표하여 연구자들 간에 의견을 교환하는 활동도 추진할 필요가 있다. 둘째, 향후 연구에서는 단순 현상의 설명이나 개념적/수리 모델을 제시하는 비실증적인 연구뿐만 아니라, 장기적으로 빅데이터 보안 분야의 이론을 정립하기 위한 실증 연구 및 사회과학적인 연구를 추진하는 것도 필요한 것으로 판단된다. 셋째, 국내 빅데이터 산업의 활성화에 기여할 수 있는 다양한 실증적인 연구가 활성화될 필요가 있다. 빅데이터 클라우드 컴퓨팅이나 업종별 빅데이터 보안 이슈 등이 대표적인 예가 될 수 있다. 넷째, 빅데이터의 보안과 프라이버시를 종합적으로 분석하기 위해서는 컴퓨터공학, 정보시스템, 통계학, 사회과학, 정치학, 심리학 등 다양한 학문 영역에서 통합적으로 접근하는 학제적 접근 방식의 연구가 필요한 것으로 판단된다. 다섯째, 해외 연구에서는 찾아볼 수 없는 빅데이터 보안에 관련된 정책·사회적 이슈에 대한 연구가 국내에서 몇 번 발표되었는데, 이것은 고무적인 현상이고, 향후 활발한 후속 연구들이 진행되기를 기대한다.

이와 관련해서 국내에서 향후 연구해 볼만한 빅데이터 보안 이슈를 몇 가지 제안하면 다음과 같다. 첫째, 빅데이터 보안에 대한 전체적인 프레임워크를 정교화하는 후속 연구 작업이 필요하다. 해외에서 미국 NIST SP800-30(위험 평가) 프레임워크를 빅데이터

보안에 적용할 수 있는지를 검토한 연구(Paryasto, et al., 2014) 외에는 모두 다양한 독자적인 프레임워크를 제시하고 있다는 점에서 이들 프레임워크를 통합한 새로운 빅데이터 보안 프레임워크를 수립하는 연구가 필요해 보인다. 둘째, 업종별 빅데이터 보안에 대한 연구가 필요하다. 해외에서도 헬스케어 분야를 제외하고는 업종별 빅데이터 연구가 전무하다시피 한 만큼, 사례연구를 기반으로 업종별 빅데이터 보안에 대한 다양한 연구에 대한 관심이 점차 높아질 것으로 보인다. 셋째, 빅데이터 보안의 특성상 향후 정부 차원의 규제가 도입될 가능성이 높으므로, 정책적인 측면에서 각국의 빅데이터 정책 비교, 빅데이터 정책 고도화 등에 대한 연구가 유망해 보인다. 마지막으로 정보보호, 클라우드 컴퓨팅, 소프트웨어 등 다양한 IT 분야 연구자들의 활발한 참여가 필요하다. 빅데이터 보안을 구현하기 위해서는 기존 빅데이터 관련 기술은 물론 보안 기술, 클라우드 컴퓨팅 기술 등 다양한 기술 영역이 융합적으로 작용하는 만큼 학문적 성과를 내기 위해서는 협업 방식의 공동연구가 필수적이다.

빅데이터 보안 분야의 연구는 본격적으로 시작된 지 얼마 되지 않아, 연구 결과가 상대적으로 매우 부족한 편이다. 앞으로 다양한 관점에서 빅데이터 보안과 관련해 풍부한 주제를 다루는 연구가 진행되기를 기대한다.

■ 참고문헌

공효순·송은지 (2013). "빅 데이터를 이용한 호텔기업 CRM 및 보안에 관한 연구". 「융합보안논문지」, 13(4): 69-75.

김기문·박충신·김준석·이호근·임건신 (2005). "경영정보학연구의 연구 다양성 평가". 「경영정보학연구」. 15(2): 149-170.

김병철 (2013). "빅 데이터 보안 기술 및 대응방안 연구". 「The Journal of Digital Policy & Management」, 11(10): 445-451.

수브르더 비스워스·유진호·정철용 (2013). "AHP 기법을 활용한 Big Data 보안관리 요소들의 우선순위 분석에 관한 연구". 「한국전자거래학회지」, 18(4): 301-314.

유영성·이명수 (2014). "빅데이터와 사회안전". 「이슈 & 진단」, 135: 1-25.

이승하·강승원·김기홍·방세중 (2014). "보안 로그/이벤트 수집을 위한 Big Data ETL 모델 설계". 한국통신학회 종합학술 발표회 논문집(하계) 2014: 886-887.

이종옥·신성희·김홍근·황경태 (2012). "IT 서비스 관리(ITSM) 분야의 연구 프레임워크 및 연구 동향 분석". 「정보화정책」, 19(1): 3-24.

이지은·김창재·이남용 (2014). "빅데이터 처리 프로세스에 따른 빅데이터 위험요인 분석". 「한국IT서비스학회지」, 13(2): 185-194.

조영복·양일권·이상호 (2012). "ID 기반의 빅 데이터 정보보호 방안". 2012 중소기업정보기술융합학회 추계학술대회 논문집, 2(1): 18-21.

최주영·김명주 (2015). "빅데이터 서비스의 보안품질평가 모델에 관한 연구". 2015년도 한국인터넷정보학회 춘계학술발표대회 논문집, 145-146.

홍진근 (2013). "미정부의 빅데이터를 위한 보안정책". 「The Journal of Digital Policy & Management」, 11(10): 403-409.

홍진근 (2013). "빅데이터 환경에서 미국 커버로스 인증 적용 정책". 「The Journal of Digital Policy & Management」, 11(11): 435-441.

황경태 (2011), 「정보시스템 감사: IT 거버넌스의 핵심수단」, 탑북스.

Kang, B. S., Cho, J., Yun, S. & Lee, K. H. (2015). A Study on SmartGrid Security Monitoring Based on Big Data Platform. 중소기업융합학회 국제학술대회 논문집, 2(1): 49-50.

Abawajy, J. H., Kelarev, A. & Chowdhury, M. (2014). "Large Iterative Multitier Ensemble Classifiers for Security of Big Data". *IEEE Transactions on Emerging Topics in Computing*, 2(3): 352-363.

Adluru, P., Datla, S. S. & Zhang, X. (2015). "Hadoop Eco System for Big Data Security and Privacy". 2015 IEEE Long Island Systems, Applications and Technology

Conference, 1-6.
Ahmed, E. S. A. & Saeed, R. A. (2014). "A Survey of Big Data Cloud Computing Security". *International Journal of Computer Science and Software Engineering*, 3(1): 78-85.
Ahmed, W. & Hashmi, M. U. (2013). "Security Visualization on Big Data". *Journal of Independent Studies and Research*, 11(2): 18-22.
Alavi, M., & Carlson, P. (1992). "A Review of MIS Research and Disciplinary Development". *Journal of Management Information Systems*, 8(4), 45-62.
Aradau, C. & Blanke, T. (2015). "The (Big) Data-security Assemblage: Knowledge and Critique". *Big Data & Society*, 2(2), 1-12.
Bardi, A., Manghi, P. & Zoppi, F. (2014). "Coping with Interoperability and Sustainability in Cultural Heritage Aggregative Data *Infrastructures. International Journal of Metadata, Semantics and Ontologies*, 9(2), 138-154.
Bertino, E. (2015). "Big Data-Security and Privacy". 2015 IEEE International Congress on Big Data, 757-761.
Blobel, B., Lopez, D. M. & Gonzalez, C. (2016). "Patient Privacy and Security Concerns on Big Data for Personalized Medicine". *Health and Technology*, 1-7.
Bowers, K. D., Hart, C., Juels, A. & Triandopoulos, N. (2013). "Securing the Data in Big Data Security Analytics". *IACR Cryptology ePrint Archive*, 1-14.
Chen, Y. (2015). "When the Cloud Meets Big Data: Security Challenges and Solutions", Doctoral Dissertation, Indiana University.
Choi, S. H., Kim, J. S. & Kwak, J. (2015). "A Study of Basic Architecture for Big-Data Security Analysis in SDN Environment". Proceedings of the International Conference on Security and Management, 137-139.
Cuzzocrea, A. (2014). "Privacy and Security of Big Data: Current Challenges and Future Research Perspectives". *Proceedings of the First International Workshop on Privacy and Security of Big Data*, 45-47.
Cuzzocrea, A. (2014). "PSBD 2014: Overview of the 1st International Workshop on Privacy and Security of Big Data". Proceedings of the 23rd ACM International Conference on Information and Knowledge Management, 2100-2101.
Feng, X., Onafeso, B. & Liu, E. (2015). "Investigating Big Data Healthcare Security Issues with Raspberry Pi". 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, 2329-2334.
Gangawane, A.A. & Dvei, A. (2015) "Big Data Security Issues and Challenges in Cloud Computing", *Asian Journal of Convergence in Technology*, 1(6): 1-5.
Grant, E. S. & Mohammad, A. F. (2014). "Use of SOA 3.0 in Private Cloud Security Gateway Service Design: In the Era of Big Data". International Conference on Computer Games, Multimedia & Allied Technology, 94-97.
Gupta, A., Verma, A., Kalra, P. & Kumar, L. (2014). "Big Data: A Security Compliance Model". 2014 Conference on IT in Business, Industry and Government, 1-5.
Hsu, C., Zeng, B. & Zhang, M. (2014). "A Novel Group Key Transfer for Big Data Security". *Applied Mathematics and Computation*, 249: 436-443.
Inukollu, V. N., Arsi, S. & Ravuri, S. R. (2014). "Security Issues Associated with Big Data in Cloud Computing". *International Journal of Network Security & Its Applications*, 6(3): 45-56.
Islam, M. R. & Islam, M. E. (2014). "An Approach to Provide Security to Unstructured Big Data". 2014 8th International Conference on Software, Knowledge, Information

Management and Applications, 1-5.
Kalibjian, J. (2013). "Big Data Management and Security Application to Telemetry Data Products". Proceedings of International Telemetering Conference, 1-8.
Kaushik, M. & Jain, A. (2014). "Challenges to Big Data Security and Privacy". *International Journal of Computer Science and Information Technologies*, 5(3): 3042-3043.
Kim, S. H., Eom, J. H. & Chung, T. M. (2013a). "Big Data Security Hardening Methodology Using Attributes Relationship". 2013 International Conference on Information Science and Applications (ICISA), 1-2.
Kim, S. H., Kim, N. U. & Chung, T. M. (2013b). "Attribute Relationship Evaluation Methodology for Big Data Security", 2013 International Conference on IT Convergence and Security, 1-4
Koushikaa, M., Habipriya, S., Aravinth, S. S., Karthikeyan, T. & Kumar, V. (2014). "A Public Key Cryptography Security System For Big Data". *International Journal for Innovative Research in Science and Technology*, 1(6): 311-313.
Kupwade Patil, H. & Seshadri, R. (2014). "Big Data Security and Privacy Issues in Healthcare". 2014 IEEE International Congress on Big Data, 762-765.
Kshetri, N. (2014). "Big Data's Impact on Privacy, Security and Consumer Welfare". *Telecommunications Policy*, 38(11): 1134-1145.
Lafuente, G. (2015). "The Big Data Security Challenge". *Network Security*, 2015(1): 12-14.
Lan, L. & Jun, L. (2013). "Some Special Issues of Network Security Monitoring on Big Data Environments". 2013 IEEE 11th International Conference on Dependable, Autonomic and Secure Computing, 10-15.
Li, S., Zhang, T., Gao, J. & Park, Y. (2015). "A Sticky Policy Framework for Big Data Security". 2015 IEEE First International Conference on Big Data Computing Service and Applications, 130-137.
Liang, Q., Ren, J., Liang, J., Zhang, B., Pi, Y. & Zhao, C. (2015). "Security in Big Data". *Security and Communication Networks*, 8(14): 2383-2385.
Lu, T., Guo, X., Xu, B., Zhao, L., Peng, Y. & Yang, H. (2013). "Next Big Thing in Big Data: The Security of the ICT Supply Chain". 2013 International Conference on Social Computing, 1066-1073.
Marchal, S., Jiang, X., State, R. & Engel, T. (2014). "A Big Data Architecture for Large Scale Security Monitoring". 2014 IEEE International Congress on Big Data, 56-63.
Matturdi, B., Xianwei, Z., Shuai, L. & Fuhong, L. (2014). "Big Data Security and Privacy: a Review". *China Communications*, 11(14): 135-145.
Mell, P. (2012). "Big Data Technology and Implications for Security Research". Proceedings of the 2012 ACM Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, 15-16.
Mittal, S. & Varshney, S. (2015). "Big Data: Information Security and Privacy". *International Journal of Software and Web Sciences*, 1(1): 29-32.
Murthy, P. K. (2014). "Top Ten Challenges in Big Data Security and Privacy". 2014 IEEE International Test Conference, 1.
Paryasto, M., Alamsyah, A. & Rahardjo, B. (2014). "Big-data Security Management Issues". 2014 2nd International Conference on Information and Communication Technology. 59-63.
Shao, P. & Y. Wang & X. Tao (2010). "A Comparative Study on MIS Research at Mainland China and Abroad(2002-2007)." *International Journal of Management Science*, 16(2): 39-51.
Sharma, P. P. & Navdeti, C. P. (2014). "Securing

Big Data Hadoop: a Review of Security Issues, Threats and Solution". *International Journal of Computer Science and Information Technologies*, 5 (2): 2126-2131

Shen, Y. & Thonnard, O. (2014). "Mr-TRIAGE: Scalable Multi-criteria Clustering for Big Data Security Intelligence Applications". 2014 IEEE International Conference on Big Data, 627-635.

Singh, J. (2014). "Real Time Big Data Analytic: Security Concern and Challenges with Machine Learning Algorithm". 2014 Conference on IT in Business, Industry and Government, 1-4.

Tan, Z., Nagar, U. T., He, X., Nanda, P., Liu, R. P., Wang, S. & Hu, J. (2014). "Enhancing Big Data Security with Collaborative Intrusion Detection". *IEEE Cloud Computing*, 1(3): 27-33.

Tankard, C. (2012). "Big Data Security". *Network Security*, 2012(7): 5-8.

Telang, R. (2014). "Privacy and Security Policy Infrastructure for Big Data", *A Journal of Law and Policy for the Information Society*, 10(3): 783-798.

Thayananthan, V. & Albeshri, A. (2015). "Big Data Security Issues Based on Quantum Cryptography and Privacy with Authentication for Mobile Data Center". *Procedia Computer Science*, 50: 149-156.

Thuraisingham, B. (2015). "Big Data Security and Privacy". *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, 279-280.

Toshniwal, R., Dastidar, K. G. & Nath, A. (2015). "Big Data Security Issues and Challenges". *International Journal of Innovative Research in Advanced Engineering*, 2(2): 15-20.

Van Ginkel, W. (2013). "Holistic Approach Needed for Big Data Security", *Internal Auditor*, 70(1): 17.

Vessey, Iris, Ramesh, V. & Glass, R.L. (2002). "Research in Information Systems: An Empirical Study of Diversity in the Discipline and Its Journals." *Journal of Management Information Systems*, 19(2): 129-174.

Vidyavathi, B. M. (2015). "Security Challenges in Big Data: Review". *International Journal of Advanced Research in Computer Science*, 6(6): 199-201.

Vivekanand, M. & Vidyavathi, B. M. (2015). "Security Challenges in Big Data: Review". *International Journal of Advanced Research in Computer Science*, 6(6): 199-202.

Wang, H., Jiang, X. & Kambourakis, G. (2015). "Special Issue on Security, Privacy and Trust in Network-based Big Data". *Information Sciences*, 318: 48-50.

Yadav, G. & Dalal, S. (2015). "Improvisation of Network Security using Encryption Technique for Big Data Technology". *International Journal of Computer Applications*, 124(11): 27-30.

〈부록: 분석에 포함된 논문들이 게재된 학술지 및 학술대회 이름〉

해외 학술지

A Journal of Law and Policy for the Information Society
Applied Mathematics and Computation
Asian Journal of Convergence in Technology
Big Data & Society
China Communications
Health and Technology
IACR Cryptology ePrint Archive
IEEE Cloud Computing
IEEE Transactions on Emerging Topics in Computing
Information Sciences
Internal Auditor
International Journal for Innovative Research in Science and Technology
International Journal of Advanced Research in

Computer Science – 2건
International Journal of Computer Applications
International Journal of Computer Science and Information Technologies – 2건
International Journal of Innovative Research in Advanced Engineering
International Journal of Network Security & Its Applications
International Journal of Software and Web Sciences
Journal of Computer Science and Software Engineering
Journal of Independent Studies and Research
Network Security – 2건
Procedia Computer Science
Security and Communication Networks
Telecommunications Policy

해외 학술대회

ACM Conference on Data and Application Security and Privacy
ACM International Conference on Information and Knowledge Management
ACM Workshop on Building Analysis Datasets and Gathering Experience Returns for Security
Conference on IT in Business, Industry and Government – 2건
IEEE International Conference on Big Data
IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing
IEEE International Congress on Big Data – 3건
IEEE International Test Conference
IEEE Long Island Systems, Applications and Technology Conference
International Conference on Big Data Computing Service and Applications
International Conference on Computer Games, Multimedia & Allied Technology
International Conference on Dependable, Autonomic and Secure Computing
International Conference on Information and Communication Technology
International Conference on Information Science and Applications
International Conference on IT Convergence and Security
International Conference on oftware, Knowledge, Information Management and Applications
International Conference on Security and Management
International Conference on Social Computing
International Telemetering Conference
International Workshop on Privacy and Security of Big Data

국내 학술지

The Journal of Digital Policy & Management – 3건
융합보안논문지
이슈&진단
한국IT서비스학회지
한국전자거래학회지

국내 학술대회

중소기업융합학회 국제학술대회
중소기업정보기술융합학회 추계학술대회
한국인터넷정보학회 춘계학술발표대회
한국통신학회 종합학술 발표회