Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 100 (2016) 19 – 28

Procedia Computer Science

Conference on ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2016, October 5-7, 2016

Technological, organizational and environmental security and privacy issues of big data: A literature review

Khairulliza Ahmad Salleh[a,b,*], Lech Janczewski[a]

[a]*The University of Auckland, Business School, 12 Grafton Road, Auckland 1142, New Zealand*
[b]*Universiti Teknologi Mara Perak, Tapah Campus, Tapah 35400, Malaysia*

Abstract

This paper provides a literature review on security and privacy issues of big data. These issues are classified into three contexts; technological, organizational and environmental that is meant to facilitate future research. The main objectives of the review are to identify security and privacy issues of big data and to categorize the issues into a classification framework. The outcome of this review reveals that security and privacy issues of big data not only originate from technological deficiencies, but it may also be the outcome of organizational culture and environmental influences. At the end of review for each of the contexts, main issues were extracted and presented as potential factors that may affect organizational intention to adopt big data.

Peer-review under responsibility of the organizing committee of CENTERIS 2016

Keywords: big data; TOE framework; security and privacy; big data adoption

1. Introduction

Big data is a term that frequently appears in current business and academic discussions on recent technology trends. In publications, this term is rarely discussed without the inclusion of its unique characteristics; the 3Vs. The first ‘V’ refers to ‘Volume’, which describes large amount of data, the second ‘V’ is for ‘Variety’- different types

[*] Corresponding author. Tel.: +64 2108270573
E-mail address: k.salleh@auckland.ac.nz

Peer-review under responsibility of the organizing committee of CENTERIS 2016
doi:10.1016/j.procs.2016.09.119

and sources of data and the final 'V' refers to 'Velocity' – the speed of data transfer and creation[1]. Else, other V's have also been described as forming the unique characteristics of big data, such as 'Value' and 'Veracity'[2]. These characteristics notably differentiate big data from the traditionally known methods used to capture, store, and analyze data. At present, big data is gaining greater attention due to increasing number of connected devices that generate very large amount of data. With proper use of big data technologies and applications, organizations will be able to exploit these data and transformed it into valuable information.

While the benefits of big data may reach diverse functions in organizations and individuals' life in digitized world, this extent of reach however, introduces far greater exposure to security and privacy risks. Although it is undeniable that big data sources may be utilized to derive better insights[3]; the underlying security and privacy concerns remain. These concerns may possibly be amplified by big data's volume, variety and veracity when deploying system infrastructure in supporting big data applications [4]. Organizations today are already confronted with overwhelming tasks of protecting their information assets, hence to some organizations; the idea of having big data applications deployed will invite further security issues and larger number of breaches. In fact, security and privacy issues have been cited in several big data survey done by technology providers and market research companies as one of the hindering factors in big data adoption[5 6 7].

Even though these issues have been reported multiple times as one of big data adoption's hindering factors, the specific security and privacy related issues that is of concern to organizations considering big data adoption are rarely discussed in publications. This study therefore intends to derive the possible security and privacy issues that may be influencing big data adoption by reviewing literatures in information systems domain. The following sections proceed as follows: section 2 briefly presents the motivation/objectives of the study and section 3 described the research methodology. The following sections present the findings of the literature review by classifying it into three contexts (section 4, 5, 6). The final sections draws a conclusion and provides future research direction.

2. Motivation, scope and objectives

Existing scholarly literature on big data were written from different perspectives to highlight the various applications of big data and its associated challenges in today's data driven era. Majority of literature on big data at present can be grouped into the following categories: big data overview, big data processing algorithm, big data applications, big data infrastructure and big data security, privacy and trust [8]. The largest number of publication can be found under the big data overview category, where scholars provide a general overview of big data, its challenges, the framework, techniques and technologies as well as other issues related to big data and its future direction in research. Examples of publications that fall under this category are those written by Chen and Zhang [9], an article that discusses on big data's impact on privacy, security and consumer welfare by Kshetri [10] and an article by Abbasi et.al.[11] that critically discuss the research agenda for big data research in information systems (IS).

This study chooses to add to the body of knowledge in the area of big data adoption/application and its associated security and privacy related concerns. While there are numerous publications that highlight the application of big data, the ones that specifically present the relation between security and privacy issues in big data adoption are still fragmented and scarce. Most discussion on security and privacy issues of big data exist as a sub-section in articles that surveyed big data challenges and opportunities in general.

Hence, this study aims to contribute to big data domain by conducting a literature review on big data's security and privacy related concerns and to present on how these security concerns may affect big data adoption by organizations. The main objectives of this study are: 1) To identify studies that discuss on security and privacy concerns of big data, and, 2) To categorize the security and privacy concerns/issues found in the articles into a classification framework (TOE – Technological, Organizational, Environmental).

3. Methodology

References to big data, analytics, big data technologies and certain combination of these terms can be found in most popular publication - in both online and physical form of publication. For the purpose of this study, the initial literature search were made on top IS academic journals. The IS journals selected were the eight leading journals under the Association for Information Systems (AIS) Senior Scholars' Basket of Journals; European Journals of

Information Systems, Information Systems Journal, Information Systems Research, Journal of Information Technology, Journal of MIS, Journal of Strategic Information System, Journal of The Association of Information Systems and MIS Quarterly. The keyword used was "big data" and the years of publication were restricted to those published in 2010 to February 2016. This initial search yielded only 9 relevant articles.

Second phase of literature search was then made on the Web of Science platform, specifically using two citation indices, the Science Citation Index (SCI) and Social Science Citation Index (SSCI). This search retained the same keyword (big data) and the timeframe of publication (2010 – 2016), while the Web of Science categories of articles were restricted to 'computer science and information systems'. The search returned a total of 516 articles and after refining the search to include only articles and reviews written in English, it went down to 439. Next, taking into account that new ideas and theories are commonly presented in academic conferences, a search was also made on leading information systems conference proceedings. Association for Information Systems (AIS)'s and its affiliated conferences were chosen and as a result 9 articles were found (including 4 from AIS journals). In total, 457 articles were considered for final assessment. The final assessments were then conducted based on the following criteria:

- The article falls under 'overview' or 'security and privacy' category. (Categories based on Chen et.al. 2016[8])
- Articles under 'overview' category must include contents on security and privacy.

Based on the selection criterias, 44 articles were found to fall under the 'overview' category and 25 articles under 'security and privacy'. The articles under 'overview' category were then checked for any inclusion of security and privacy content which resulted in 25 relevant articles. Security and privacy articles were also checked for its relevance in supporting the aims of this study, and 18 articles were found to have contents of high relevance. At the end of this process, 43 articles were identified for content extraction. Table 1 summarized the results of the literature search. For further review of the articles, an inductive categorization will be used in classifying the contents into three contexts; technological, organizational and environmental (TOE). These contexts are part of an organizational level technology adoption framework, known as TOE Framework [12]. The reason for this classification is to provide a basis for further research on how technological, organizational and environmental security issues of big data may influence its adoption process by organizations. As security and privacy issues may encompass various factors other than its technological aspects, TOE Framework is deemed suitable for this classification purpose.

Table 1. Summary of results of according to categories

Category of big data articles	Number of Studies	Publication & References
Big data overview	25	Journal of AIS (1, [11]), Business & Information Systems Engineering (2,[13] [14]), Journal of Information Technology (2,[15] [16]), Decision Support System (1,[17]), MIS Quarterly (2,[18] [19]), Mobile Networks and Applications (1,[20]), Journal of the Association for Information Science and Technology (2,[21] [22]), Foundations and Trends in Information Retrieval (1,[23]), KSII Transactions on Internet and Information Systems (1,[24]), Journal of Strategic Information Systems (1,[25]), IBM Journal of Research and Development (1,[26]), IT Professional (2,[27] [28]), Information Sciences (1,[9]), Communications of the Association for Information Systems (3,[29] [30] [31]), MIS Quarterly Executive (1,[2]), IEEE Network (2,[32] [33]), IEEE Transactions on Services Computing (1,[34]).
Big data security and privacy	18	Ad Hoc Networks (1, [35]), Security and Communication Networks (1,[36]), Tsinghua Science and Technology (1,[37]), IEEE Security and Privacy (1,[38]), Proceedings of Pacific-Asia Conference on Information Systems 2013 (1,[39]), Information Security (4,[40] [41] [42] [43]), Information Systems Frontiers (1,[44]), Network Security (1,[45]), IEEE Network (1,[46]), Thirty Fifth International Conference on Information Systems (1,[47]), IT Professional (1,[48]), Conf-IRM2015 Proceedings (1,[49]), IEEE Transactions on Multimedia (1,[50]), Information Sciences (1,[51]), Twenty-First Americas Conference on Information Systems (1,[4]).

4. Security and Privacy Issues in Technological Context

Technological context refers to both internal and external technologies relevant to organizations [12]. Hence, technology in this context may include current practices, equipment and processes [52]. Most of the reviewed articles include a discussion on how big data creates technological-related security and privacy issues, where some of the issues were associated to big data's unique characteristics [4]. Each of these characteristics will pose certain security concerns that require a strong security solution and mechanisms in ensuring the confidentiality, integrity and availability of data.

The sheer volume of data collected and created in a typical big data environment is one the factors inviting security issues. Accordingly, new and improved security tools and mechanisms are needed in order to provide effective protection towards data. However, in an article by Adrian Lane[41], the author suggests that "many security professionals who encounter big data environments for the first time don't understand why security is a big issue". This shows that at present, the degree of difficulty and impact of big data related security issues are yet to be realized by security professionals. The same tools and techniques used to provide security to a relational database for example, will no longer be sufficient in a big data environment [20,41]. A typical multi-node architecture of a big data environment, coupled with the volume of data will naturally outrun the capacities of any standard security products. In another article that proposes a framework for secure sensitive data sharing for big data platform, the inadequacy of existing security technology is also discussed. By looking at data sharing and privacy protection issues, the authors noted that existing technologies did not take into account the whole process of data security life cycle hence endangering a big data environment [37]. In addition, Chen and Chun-Yang [9] asserts that data security issues for big data application are somehow "awkward" for a number of reasons, among it is the protection approaches required are closely related to the size of big data – larger size of data means larger protection coverage needed. Due to the distributed nature of a big data environment, threats arising from networks may also magnify the problems in protection, resulting to a heavier workload for security functions[9]. In essence, the 'volume' characteristic of big data will pose challenges to existing security technologies and solution. As described above, one the key challenges is to provide security technologies and solution that are able to scale to the large size of data sets and distributed nature of big data [53].

The speed in which data are being created and the speed of how it should be analysed and acted upon may also pose some security threats. In a big data environment, data is being generated in an unprecedented rate, either in batch, real time/near time, or streams [53]. Many organizations are currently generating high frequency data and this may create difficulties in maintaining data protection. In presenting a new secure transmission method for big data, Chen et.al.[36] highlights that collection and transmission of data through any communication networks will essentially introduced critical requirements for security. The same concern is reiterated by Dong et.al[37] by providing some examples on how security issues may appear during rapid transmission of sensitive data. For instance, during the phase of data creation, a rapid transfer of data streams from owner's local server to a big data platform could create security issues which may lead to the loss of sensitive data. Else, during the rapid transmission, creation and processing of data, an organization must ensure that data are aggregated or anonymized to prevent any access to personal identifiable information. Strict control and measures must be readily available during these transmissions of data to alleviate risks and errors [17]. Rapid frequency of data creation and processing will also create issues when there is a lack of security capabilities in securing data storage particularly during peak data traffic [10]. Rapid data flows will also increase the need to have a security technology with the ability to screen and audit access while at the same time protecting data stored across repositories. It is now apparent that 'velocity' of data in a big data environment amplifies security complications commonly found in any traditional data environment, and at the same time produces new issues that requires special treatment [51].

Another unique characteristic of big data is the various sources and types of data that are collected and stored in a big data environment. The 'variety' of data often originates from structured, semi-structured and unstructured data. Thus far, most organizations are familiar with the security mechanisms that are applicable in protecting structured data, but with the inclusion of unstructured data, the experience may be lacking [10]. Samuel et.al.[50] states that variety of data posed security and privacy challenges for organizations and to "compose a unified, broad privacy policy" will be unsuitable. Secure access management will also be a problem when the data derived are stored in data repositories that reside in distributed location across a big data environment. Wang et.al.[51] emphasizes that the variety of data will involve cumbersome tasks of providing different restrictions for access and security policy that suits each sources of data. Consequently, it will be difficult to balance the appropriate security mechanisms needed with the tasks of extracting value from the data. The variety nature of big data may also create new challenges in data encryption. According to Chen et.al.[20], high diversity big data demands for newly developed efficient cryptography approaches which could not be met by previous encryption approaches. The authors then highlight on the requirement for an effective security schemes (safety management, access control and safety communications) for all types of data; from structured to unstructured. At present, it is understood that existing mechanisms for the protection of unstructured data is still in its growing phase and data governance issues are still not fully addressed. Without effective input validation, identifying malicious data sources may prove to be an overwhelming process. Hence, Malik[26] proposed for organizations planning to launch big data initiatives, to consider the requirements of producing liable mechanisms for security and privacy, including defence in depth for each type of data.

As illustrated above, organizations that are already a part of big data initiatives or are planning to jump into big data bandwagon, are faced with numerous security and privacy issues in relation to infrastructure, processes and protection mechanisms. To summarize, all the technological challenges posed by big data, reflects the complexity in providing effective protection to big data environment. Whereas, the level of preparedness of organizations in embracing all challenges that comes with big data, may be attributed to the organizations' perceived compatibility of their current security mechanisms with those required by big data. It is thus interesting to see whether these two factors, 1) Complexity and 2) Compatibility have any influence on organizations planning to adopt big data.

5. Security and Privacy Issues in Organizational Context

Organizational context can be described as characteristics that represent an organization, such as company strategies, culture, structure and policies [54]. From information security view, these characteristics may describe the organizational security practices and culture, security planning, security policy and risk mitigation strategies. After a thorough review of all the selected articles, several security and privacy issues discussed by the authors can be classified as organizational-related.

Organizational culture and awareness on the security and privacy issues brought upon by big data is an important factor to consider in safeguarding data from human-related breaches. Philips-Wren et.al.[29] in their article revealed that addressing organizational culture in the context of big data is highly important. This importance is highlighted by the fact that "attitudes on ethics, privacy, and security can vary significantly across organizations". In another article that presents a paradigm shift in computational social science in big data era, best practices in safe handling of big data are said to come from the way organization provided encouragement and work structure to all of their employees instead of relying on individual's way of working with data. Thus, in order for organizations to derive the intended benefit of big data and to protect data from security breaches, organizations are required to make alterations and enhancement in terms of its business processes and applications in addition to making an incremental change in its business model [13]. And, to avoid catastrophic consequences should there be a data breach, it is vital that organizations have the right protection mechanisms prepared – the consequences of wrongful treatment of customers or employees data must be made known throughout the whole organization [45]. To make the changes in culture and awareness a successful effort, top management role is also important in promoting security culture and providing necessary support and security technology resources. Lack of top management support may deter the efforts made by IS security professionals in protecting and securing organizational data and systems from functioning at optimum level [55].

Another organizational-related issue derived from the review is organizational learning capacity and employees competencies in the implementation of necessary big data protection mechanisms. As asserted by Chang et.al [17], implementation of protection required for a big data environment can be an expensive and challenging tasks. This process require several necessary steps, such as designing data handling process, as well as identifying suitable training and procedures for employees. Other steps include periodic auditing of the protection mechanisms put in place and problem identification of security issues that may arise. Again, the authors stress for all employees to be aware of their responsibilities in the protection chain, and this demands for organization-wide effort. Organizational competencies and learning abilities will provide needed support in developing employees' competencies and skills in safeguarding big data environment [17]. It is important for organizations to realize the need to relearn skills in managing the security and privacy of big data. Although some organizations may view the required skills as being similar to those needed for traditional business intelligence, there are some requirements which are unique to big data, e.g. strategies and policies required to identify and retain big data-ready workforce, managing security and privacy mechanisms that cater to the unique characteristics of big data, defining storage parameters and methods for secure disposal of big data [29].

Another issue is related to organizational development and use of big data - it is essential for organizations to ensure privacy principles are integrated into the development process. One author suggests that organizations with predefined privacy measures in development and use of big data, will garner the most desirable outcome and less number of consumer pushback [40]. Mennecke et.al.[47] supported this idea by stating that privacy principles should be built into business processes and information systems "as a default, rather than as an afterthought". System development that proactively address the need for security and privacy may potentially helped organizations should there be any privacy violation. In essence, getting big data security and privacy as an afterthought must be avoided at all cost. The importance for organizational recognition on the vital requirements in securing big data is undisputable, for it needs to be addressed and embedded in any development and use of big data components from the very beginning[51].

Several main issues can be derived from the review above, in relation to organizational-related security and privacy of big data. The first is organizational culture and awareness on the security and privacy requirements of big data. This may be translated to the need for organizational information security culture. With organization-wide and top management support, this culture may be cultivated and spread across the organization, hence minimising the risks associated to employee-linked security breaches. Another factor is organizational learning culture and competence. It is expected that organizational abilities to learn new protection procedures and new development processes that integrate security and privacy principles from the very start will lead to a more secure big data environment. These issues may be studied further in order to explore the correlation between the issues and organizational intention to adopt big data.

6. Security and Privacy Issues in Environmental Context

Big data's security and privacy issues in environmental context are recognized in a number of articles. This context refers to the domain "in which a firm conducts its business – its industry, competitors, access to resources supplied by others, and dealing with the government" [12]. Essentially, it suggests that there will be influences coming from the environment in which the organization operates whenever the organization is planning for new technology adoption. In a typical big data environment, the collections of data about individuals are often involved – achieved though organization's interaction with their consumers and through other business collaborations. Thus, whenever these sensitive data are collected and being used within and across organization, the issue of privacy and confidentiality will emerge [56]. As such, organizations need to consider its external environment that may affect the use of sensitive data in its big data initiatives.

One environmental-related factor that often appeared in the reviewed articles is the issue of privacy and its associated rules and regulations. In protecting consumers' privacy and private data, many countries have introduced data protection act that aims to regulate the use of individual's personal identifiable information (PII) by organizations. For example, in an article that explores the main factors that affect the intention of individuals to grant their network operators to use their PII, Saenz et.al.[39] indicated that governments "have attempted to protect individuals' privacy by enacting laws or directives, which must be followed by all sectors, including the highly regulated telecom industry". While these enacted regulations are meant to protect the privacy of end consumers, it is fast becoming one of the challenges faced by organizations working with big data. Buhl and Heidelman[13] in their editorial article agreed that numerous country-based privacy regulations and restrictions are "big data's most serious challenges". The authors also suggested that while present generation of consumers are no longer reserved when it comes to revealing their personal information while on the web, privacy regulations that are country-specific may seriously hinder big data initiatives and its corresponding business models. This impediment may also be attributed to a significant number of consumers who refuse to allow for a long-term storage of their private data[13].

As the regulations that administers the use of personal data differs across countries, this will pose some pressure towards organizations wanting to leverage the potential of big data but at the same time having to abide to the legal provisions concerning the use of data [10]. Privacy acts and regulations in the EU for instance, is generally considered as much stricter that the regulations in the US (foreign companies operating in the EU will have to abide to these regulations) [2].Consequently, an extensive big data governance program is needed in order for organizations to comply with society's ethical and governmental legal expectations [14,26,35]. Malik in his article asserts that security challenges of data sharing between applications as well as the compliance with "geographical trans-border data regulations" need to be addressed in any big data governance program. In addition, organizations are also expected to address the fundamentals of strong protection required for any personal, health and financial data[26]. Inevitably, organizations will therefore need to deliver on these expectations without compromising their business goals, which can be a daunting task.

Security issues of outsourcing and the use of third-party tools is another environmental-related factor that can be found in the reviewed articles. In a big data environment, there may be a need for organizations to outsource some part of the tools and applications that support data storage, sharing and access [57]. According to Wood [58], most organizations are still unable to build and maintain a full-fledged big data environment in-house. As a result of this incapacity, it creates dependence to, for example, service providers and other third-party tools vendors [10]. The need to outsource, although critical to creating and capturing value of big data, will create the need for a further consideration on security and privacy. In one article that provides comprehensive overview of big data, Chen et.al.[20] reiterates the need to rely on professionals and tools in order to analyse huge datasets, which in turn will create further safety risks for the data. The authors then stresses for a proper security measures to be put in place before the owner of big data delivers the datasets for processing and storage by a third-party service providers. These measures are required as preventive mechanisms in protecting sensitive data [20].

Cloud computing services have consistently been linked to the operation of big data environment. Goodendorf[40] in her article argued that the cloud is in fact needed for cost-effective implementation of big data. Even though this outsourcing practices are normally viewed as a way to transfer operational and adoption risks to the service provider, the truth is it does not eradicate the risks of data loss [35]. Cloud storage for instance, may invite data security problems (e.g. requirements of data integrity checking) and it may also lead to privacy issues when the datasets are hosted in a server that is publicly accessible [9]. For a mitigation approach in ensuring security and privacy in the use of cloud services; Phillips-Wren et.al.[29] suggested that organizations need to verify that a cloud service provider has an up-to-date security and privacy policies for data sharing and inter/intra organizational collaboration. This approach is also supported by Goodendorf[40], by stating that both cloud service provider and user organizations need to clearly define their responsibilities in regards to data privacy controls. The drawn contractual clauses must be more extensive than the standard general-security responsibilities [40].

From the review above, it can be deduced that there are two highly possible environmental-related security and privacy concerns for organizations looking to embark on big data initiatives. The first factor is privacy related regulations while the second factor is organizational concern on outsourcing and use of third-party services. These two factors may possibly be the hindering factors for big data adoption due to lack of competency of some organizations in ensuring the security and privacy of big data that are externally hosted, and the difficulties in complying to unsurmountable privacy related regulations.

7. Conclusion

There are numerous contributions and publications in the big data area. Issues on security and privacy of big data particularly, have gathered great interest of academics and practitioners. However, these issues are still in its infancy in the IS domain. Based on the literature review conducted, security and privacy issues of big data are found to be mostly described within big data overview articles. Specific security and privacy articles otherwise, tackles the problems by introducing new framework, methods or processes in providing protection to big data components. This study attempted to identify security and privacy issues from articles categorized under 'overview' and 'security and privacy' categories. Through the review, important security issues and privacy concerns were classified under three major contexts: technological, organizational and environmental (taken from TOE framework – an organizational level technology adoption framework). The reason these three contexts were chosen as the classification framework is to provide future research with a foundation on the possible security determinants that may influence big data adoption by organizations. Based on the findings of the review, the main security and privacy issues that could possibly have an effect towards organizational intention to adopt big data were identified (refer to Fig. 1below).

Security and Privacy Issues In Technological Context	Security and Privacy Issues In Organizational Context	Security and Privacy Issues In Environmental Context
- Security and Privacy Technological Complexity - Security and Privacy Technological Compatibility	- Organizational learning culture and competencies - Information security culture and top management support	- Privacy Regulatory Concerns - Risks in Outsourcing and use of third-party tools

Fig. 1. Identified Security and Privacy Issues for each Technological, Organizational and Environmental Context

From this literature review, it is evident that security and privacy issues of big data are not restricted to technological incapability, in fact, the problems and challenges may also arise from organizational culture as well as environmental facets. While these findings shows the relevancy of looking at security and privacy issues of big data from different perspectives, and especially how these issues may play a role in encouraging/discouraging organizations' big data adoption, it is yet to be addressed empirically in IS publications. This fact opens up future research opportunities.

8. Limitations and future research

There are several limitations identified in this study. The major limitation is the use of only one keyword for every phases of literature search. Therefore, the resulting search returns may have excluded some articles that discuss about big data in a different term such as 'datafication'. Additional literature review should include other databases as well as this study only focuses on two citation indices – the SSCI and SCI. Furthermore, future research that aims to link the factors identified in this study with big data adoption, must also consider the inclusion of articles from technology adoption area.

The aim of a future research activity is to find appropriate conceptual framework that will be able to predict the causal relationship between the identified issues with big data adoption. With this framework, empirical investigation may be conducted to provide support for any developed hypotheses. Security and privacy issues have been quoted by some organizations as one of the hindering factors in big data adoption, thus it will be beneficial to seek for the actual issues that deter the adoption process. Organizational case studies will be one of the efficient methods to achieve clarification on how security and privacy issues may affect organizational intention to adopt new technology such as big data. Findings from this future research may be beneficial to practitioners by providing information on the factors that may hinder big data adoption as well as factors that can be leveraged to encourage adoption.

Acknowledgement

The authors would like to thank the anonymous reviewers for their helpful comments. The first author would also like to thank Malaysia's Ministry of Higher Education and Universiti Teknologi Mara, Malaysia for financing her PhD research.

References

1. Bansal, A., Kaur, A. & Aggarwal, A. Big data explosion: insight for new age managers. *Int. J. Sci. Engineering Res.* **5,** 7–11 (2014).
2. Martin, K. E. Ethical Issues in the Big Data Industry. *MIS Q. Exec.* **14,** 67–85 (2015).
3. Dhar, S. & Mazumdar, S. Challenges and best practices for enterprise adoption of Big Data technologies. *2014 IEEE Int. Technol. Manag. Conf. ITMC 2014* (2014). doi:10.1109/ITMC.2014.6918592

4. Alshboul, Y. & Wang, YongNepali, R. K. Big Data LifeCycle : Threats and Security Model. in *Twenty-first Americas Conference on Information Systems* 1–7 (2015).
5. Gartner Inc. *Survey Analysis : Big Data Investment Grows but Deployments Remain Scarce in 2014*. (2014).
6. Sans Institute. *Enabling Big Data by Removing Security and Compliance Barriers*. (2015).
7. IDG Enterprise. *Big Data: A Survey*. **19,** (2014).
8. Chen, Y. *et al.* Big data analytics and big data science: a survey. *J. Manag. Anal.* **3,** 1–42 (2016).
9. Philip Chen, C. L. & Zhang, C.-Y. Data-intensive applications, challenges, techniques and technologies: A survey on Big Data. *Inf. Sci. (Ny).* **275,** 314–347 (2014).
10. Kshetri, N. Big data's impact on privacy, security and consumer welfare. *Telecomm. Policy* 1–12 (2014). doi:10.1016/j.telpol.2014.10.002
11. Abbasi, A., Sarker, S. & Chiang, R. Big Data Research in Information Systems: Toward an Inclusive Research Agenda. *J. Assoc. Inf. Syst.* **17,** i–xxxii (2016).
12. Tornatzky, L. G. & Fleischer, M. *The processes of technological innovation*. (Lexington Books, 1990).
13. Buhl, H. U. & Heidemann, J. Big Data A Fashionable Topic with (out) Sustainable Relevance for Research and Practice ? *Bus. Inf. Syst. Eng.* **5,** 66–69 (2013).
14. Jarke, M. Interview with Stefan Wrobel on ' Applied Big Data Research '. *Bus. Inf. Syst. Eng.* **6,** 303–304 (2013).
15. Bhimani, A. Exploring big data's strategic consequences. *J. Inf. Technol.* **30,** 66–69 (2015).
16. Markus, M. L. New games, new rules, new scoreboards: the potential consequences of big data. *J. Inf. Technol.* **30,** 58–59 (2015).
17. Chang, R. M., Kauffman, R. J. & Kwon, Y. Understanding the paradigm shift to computational social science in the presence of big data. *Decis. Support Syst.* **63,** 67–80 (2014).
18. Chen, H. & Storey, V. C. Business Intelligence and Analytics: From Big DAta to Big Impact. *MIS Q.* **36,** 1165–1188 (2012).
19. Goes, P. B. Editor's Comments: Big Data and IS Research. *MIS Q.* **38,** (2014).
20. Chen, M., Mao, S. & Liu, Y. Big data: A survey. *Mob. Networks Appl.* **19,** 171–209 (2014).
21. Ekbia, H., Bowman, T. & Weingart, S. Big Data , Bigger Dilemmas : A Critical Review. *J. Assoc. Inf. Sci. Technol.* **66,** 1523–1545 (2015).
22. Frické, M. Big Data and Its Epistemology. *J. Assoc. Inf. Sci. Technol.* **66,** 651–661 (2015).
23. Gurrin, C. & Smeaton, A. F. LifeLogging : Personal Big Data. *Found. Trends Inf. Retr.* **8,** 1–107 (2014).
24. Jeong, S. R. & Ghani, I. Semantic Computing for Big Data : Approaches , Tools , and Emerging Directions. *KSII Trans. Internet Inf. Syst.* **8,** 2022–2042 (2014).
25. Loebbecke, C. & Picot, A. Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda. *J. Strateg. Inf. Syst.* **24,** 149–157 (2015).
26. Malik, P. Governing Big Data: Principles and practices. *IBM J. Res. Dev.* **57,** 1:1–1:13 (2013).
27. Miller, H. G. & Mork, P. From Data to Decisions : A Value Chain for Big Data. *IT Prof.* **15,** 57–59 (2013).
28. Kemelor, P. Digital Data Grows into Big Data. *IT Prof.* **17,** 42–48 (2015).
29. Phillips-Wren, G., Iyer, L. S., Kulkarni, U. & Ariyachandra, T. Business analytics in the context of big data: A roadmap for research. *Commun. Assoc. Inf. Syst.* **37,** 448–472 (2015).
30. Shim, J. P., French, A. M. & Jablonski, J. Big Data and Analytics: Issues, Solutions, and ROI. *Commun. Assoc. Inf. Syst.* **37,** 797–810 (2015).
31. Watson, H. J. Tutorial: Big Data Analytics: Concepts, Technologies, and Applications. *Commun. Assoc. Inf. Syst.* **34,** 24 (2014).
32. Yin, H., Jiang, Y., Lin, C., Luo, Y. & Liu, Y. Big Data: Transforming the Design Philosophy of Future Internet. *IEEE Netw.* **28,** 14–19 (2014).
33. Fang, H., Zhang, Z., Wang, C. J. & Daneshmand, M. A survey of big data research. *IEEE Netw.* **29,** 6 (2015).
34. van der Aalst, W. & Damiani, E. Processes Meet Big Data: Connecting Data. *IEEE Trans. Serv. Comput.* **1,** 1–1 (2015).
35. Chang, V. Towards a Big Data system disaster recovery in a Private Cloud. *Ad Hoc Networks* **000,** 1–18 (2015).
36. Chen, J., Liang, Q. & Wang, J. Secure transmission for big data based on nested sampling and coprime sampling with spectrum efficiency. *Secur. Commun. Networks* **8,** 2448–2456 (2015).
37. Dong, X. *et al.* Secure sensitive data sharing on a big data platform. *Tsinghua Sci. Technol.* **20,** 72–80 (2015).
38. Eckhoff, D. & Sommer, C. Driving for Big Data? Privacy Concerns in Vehicular Networking. *IEEE Secur. Priv.* **12,** 77–79 (2014).
39. Saenz, C. F. L., Chang, Y., Kim, J. & Park, M. Exploring big data challenges : factors affecting individuals ' intention for authorizing their network operators the usage of their personal information. in *PACIS 2013* (2013).
40. Goodendorf, L. Managing Big Data. *Information Security,* Fourth Qua**,** 29–33 (2013).
41. Lane, A. In Defense of Big Data. *Information Security* 4–11 (2014).
42. Ranum, M. Free-Form Versus Off-the-Shelf: Big Data Security Still a Ways Off. *Information Security* 9–13 (2014).
43. Richardson, R. Big Data Creates Cloudy Security Forecast. *Information Security* 2–4 (2013).
44. Hota, C., Upadhyaya, S. & Al-Karaki, J. N. Advances in secure knowledge management in the big data era. *Inf. Syst. Front.* **17,** 983–986 (2015).
45. Lafuente, G. The big data security challenge. *Netw. Secur.* **2015,** 12–14 (2015).
46. Lu, R., Zhu, H., Liu, X., Liu, J. & Shao, J. Toward efficient and privacy-preserving computing in big data era. *IEEE Netw.* **28,** 46–50 (2014).
47. Mennecke, B. *et al.* Privacy in the Age of Big Data : The Challenges and Opportunities for Privacy Research. *Thirty Fifth Int. Conf. Inf. Syst.* 1–5 (2014).
48. Perera, C., Ranjan, R., Wang, L., Khan, S. U. & Zomaya, A. Y. Big Data Privacy in the Internet of Things Era. *IT Prof.* **17,** 32–39 (2015).
49. Perreault, L. Big Data and Privacy. in *Conf-IRM 2015 Proceedings* (2015).

50. Samuel, A., Sarfraz, M. I., Haseeb, H., Basalamah, S. & Ghafoor, A. A Framework for Composition and Enforcement of Privacy-Aware and Context-Driven Authorization Mechanism for Multimedia Big Data. *IEEE Trans. Multimed.* **17,** 1484–1494 (2015).
51. Wang, H., Jiang, X. & Kambourakis, G. Special issue on Security, Privacy and Trust in network-based Big Data. *Inf. Sci. (Ny).* **318,** 48–50 (2015).
52. Oliveira, T. & Martins, M. F. Literature Review of Information Technology Adoption Models at Firm Level. *Electron. J. Inf. Syst. Eval.* **14,** 110–121 (2011).
53. Demchenko, Y., Ngo, C., Laat, C. De & Membrey, P. in *Secure Data Management* (eds. Jonker, W. & Petković, M.) **8425,** 76–94 (Springer International Publishing, 2014).
54. Teo, T. S. H., Ranganathan, C. & Dhaliwal, J. Key Dimensions of Inhibitors for the Deployment Commerce. *IEEE Trans. Eng. Manag.* **53,** 395–411 (2006).
55. Mbowe, J. E., Zlotnikova, I., Msanjila, S. S. & Oreku, G. S. A Conceptual Framework for Threat Assessment Based on Organization ' s Information Security Policy. *J. Inf. Secur.* **5,** 166–177 (2014).
56. Hayashi, K. Social Issues of Big Data and Cloud: Privacy, Confidentiality, and Public Utility. in *2013 International Conference on Availability, Reliability and Security* 506–511 (Ieee, 2013). doi:10.1109/ARES.2013.66
57. Jagadish, H. V. *et al.* Big data and its technical challenges. *Commun. ACM* **57,** 86–94 (2014).
58. Wood, P. How to tackle big data from a security point of view. *Computer Weekly* (2013).