Towards a Conceptual Framework on the Importance of Privacy and Security Concerns in Audit Data Analytics

Manal M. Yunis
myunis@lau.edu.lb
Raed El-Khalil
raed.elkhalil@lau.edu.lb
Miray Ghanem
miray.ghanem@lau.edu
Adnan Kassar School of Business
Lebanese American University
Beirut, Lebanon

Abstract

Privacy and security concerns with Big Data have gained momentum in both research and business fields. Organizations in general have long recognized the need of data analytics to increase quality and provide better value for financial statements users. Audit firms, in particular, have made significant investments in the field of data analytics, as traditional auditing techniques have not kept pace with the evolving economy and large investments of organizations in data and technology. Audit data analytics have become an increasingly important tool for auditors to increase the quality and performance of their audit. However, such implementation have raised the concerns for privacy and security of client data. The main objective of this paper is to provide a context to organizations by highlighting on the security and privacy concerns triggered by big data analytics and the importance of this matter in the audit sector. To this end, using an in-depth literature review, and drawing on a sound theoretical framework comprising utility maximization theory and procedural fairness theory, the paper proposes a conceptual model that depicts the relationships between privacy and security concerns, data analytics and audit quality. The model implications are discussed, and recommendations for future research are presented.

Keywords
Privacy and security, Data analytics, Audit quality, Audit confidentiality, Audit Data Analytics

1. Introduction

"With great power of data comes great responsibility", (Singh, 2014). The field of big data analytics has witnessed increasing interest in both scientific and business fields for the tremendous value it has offered. In the business world, the real power of data resides in the value of insights organizations are able to gather for future opportunities and prosper. The term "Big data" refers to massive and complicated datasets, which are difficult to store, visualize and analyze with typical software (Terzi et al., 2015). According to the Mckinsey Global Institute, data volume was expected to grow 40% annually between 2009 and 2020 (Singh, 2014). With the emerging data analytics technologies, companies are capable of coping with such difficulties.

Audit firms in particular, have long recognized the need of data analytics to increase quality and provide better value for financial statements users. Traditional auditing has not kept pace with the changing economy and the large investments of organizations in data and technology. In 1989, Groomer and Murthy first discussed the concept of "Continuous Auditing" that aims to automate the auditing process to provide maximum assurance (Jans & Hosseinpour, 2018). With the help of data analytics, many auditors are finding ways to gain a deeper understanding of their clients' businesses than ever. They are able to establish better insights that help in assessing risks, detecting fraud, and performing substantive audit procedures.

Despite the appealing elements of big data analytics, being regarded as the engine of the economic growth, new privacy and security concerns are developed. Besides the vast benefits of data analytics in different sectors such as Marketing, Finance and Accounting, its widespread usage has pointed various questions regarding the integrity, confidentiality and monitoring of big data analyzed (Joshi & Kadhiwala, 2017). Numerous academic research is being conducted on the opportunities and challenges within the application of data analytics in businesses stating that privacy

and security is one of the key challenges limiting its use. According to Balaban (2019), the complexity in the data collected and analyzed in terms of processing, storage and volume may result in data breaches, leakage of confidential information, and spillage.

The Audit profession has long embraced the new data analytics technology. With the support of ACCA (Association of Chartered Certified Accountants), ICAEW (Institute of Chartered Accountants of England and Wales), and IMA (Institute of Management Accountants), audit firms have realized the significance of the utilization of data analytics as well as the associated risks and challenges perceived by the professionals (Rîndașu, 2017). Although many researchers discussed opportunities and successful stories of data analytics application in professional financial services firms, little research has been conducted on the challenges the auditing sector encounters while using data analytics. The audit field, coupled with increasing compliance standards regarding the importance of working with the information produced by the clients with confidentiality and integrity, has posed serious talks on whether utilizing data analytics tools is contradictory to the main characteristics of external audit.

This paper intends to: (1) provide a context to the work by highlighting on the security and privacy concerns triggered by big data analytics and the importance of this matter on the audit quality; (2) develop a conceptual model that depicts the relationship between privacy and security concerns, audit data analytics and audit quality; and (3) gain insights on the aspects of confidentiality and security of big data produced by the entities under audit when applying data analytics technologies.

2. Literature Review

2.1. Security and Privacy Challenges

With the emerging technologies and digitalization, massive research have been conducted on the privacy and security threats the use of communication technology has uttered in different domains such as home, health, utilities, business operations and information, and supply chain (Obaidat et al., 2020). While people continue to rely heavily on digital devices in their daily activities and businesses, the topic of cybersecurity maintains to attract considerable attention over the society. Since the focus of this research is on the security and privacy concerns in the business field, in particular financial statements auditing, non-business related research on this topic will not be reviewed in detail and will only be referred to as appropriate. By security and privacy concerns, we refer to the fear of the leakage of sensitive data that could severely damage the stakeholders (Skarmeta et al., 2014). According to Obaidat et al. (2020), the three basic security components are confidentiality, integrity and availability.

Al-Mhiqani et al. (2018) discussed and classified major cyber-attacks that targeted nations and economies, as societies are becoming more dependent on interconnected network communications. Examples on such incidents are the cyber-attacks on the Egypt Maritime Transport Sector targeting Egyptian governmental websites, attack on Istanbul Airport passport control system causing delay in service, and the cyber-attack of the Saudi Arabian Defense Ministry aiming to extract sensitive data from their systems. Moreover, Davis et al. (2009) analyzed a series of cybersecurity incidents as at 2007 reported by online businesses to determine their impacts on the customers' intentions to adopt online channels. In this article, the authors point out fraud incidents in financial institutions such as HSBC, Bank of America and TransUnion.

Nonetheless, out of the recent utilizations of technologies in organizations, cloud-computing techniques can be at odds with traditional security controls. Although cloud computing seems promising for enterprises and personal users due to its high performance and cheaper services, issues of compliance, trust, privacy and legislations are still among the main concerns and barriers that limit the adoption of cloud services (Sun et al., 2014). The risks of security breaches the cloud-computing systems present are fierce, whereby firms are reluctant to outsource information technology services to an outside public party when placing sensitive information and functions into the cloud environment (Jansen & Grance, 2011).

2.2. Data Analytics

Gandomi and Haider (2015) define data analytics as "the technique used to analyze and acquire intelligence from big data". The researchers emphasize that data can be extracted from any source whether structured or not. The term "Big Data" is different from other technologies based on the data's volume, variety, velocity and value (Mishra & Singh, 2016). Terzi et al. (2015) describe an additional feature of Big Data: veracity (*Figure 1*). According to Gantz and Reinsel, the amount of data was expected to increase 300 times between 2005 and 2020 (Matturdi et al.,2014).

Nowadays, the main data analytics methodologies such as data mining, machine learning, artificial intelligence and simulation are utilized for descriptive and predictive analytics (LaValle et al, 2011). Lepenioti et al. (2020) explain that the value of descriptive analytics resides within its ability to obtain the reasons behind something that happened in the past and understand how it can be eliminated in the future. LaValle et al. (2011) revealed that as the organization uses more data analytics, it is able to be qualified as a top performer among its competitors twice more than other organizations with less application of data analytics for their big data.

In this same article, the authors differentiate between three stages of adoption of data analytics. The aspirational organizations are the ones with the least analytics tools implemented. On another level are the experienced and transformed organizations with developing effective skills in data analytics.

2.3. Privacy and Security Challenges in Data Analytics

With the increase in the benefits of the application of data analytics across various industries, researchers and practitioners are raising concerns on the security and privacy issues related to data analytics. Mishra and Singh (2016) indicate that the characteristics of Big Data in terms of velocity, variety and volume explained in Figure 1 amplify the security issues challenges. Indeed, traditional security solutions are hardly capable of protecting Big Data because of these characteristics (Joshi & Kadhiwala, 2017). Mishra and Singh (2016) concluded that the additional benefits of Big Data analytics on businesses have created privacy concerns since anonymization in Big Data could be difficult to achieve. Srivastava and Jaiswal (2019) reconfirmed the latter stated privacy concerns with the additional emphasis on irrelevant patents and copyrights and concerns for "e-discovery".

According to Terzi et al. (2015), extra requirements in security and privacy methods should be implemented in all stages of data analytics including data collection, storage, analysis and transferring. Wieringa et al. (2019) expanded the explanation on the responsibilities for personal data and analytics and defined five main types of responsibilities data analytics practitioners should be aware of: data collection, verification, storage and control, analyzing and disseminating insights.

Similarly, Joshi and Kadhiwala (2017) expanded in their study the literature on the main security and privacy issues with Big Data as summarized in *Table 1*. On the other hand, Matturdi et al. (2014) emphasize on the concerns of security and privacy issues in Big Data context from the user's perspective. Users fear that their secretive data, when combined with large data sets for analysis and creating insights, are being exposed to interference.

Although there are still no concrete solutions for the security and privacy challenges in Big Data analytics, previous contributions proposed several techniques to limit the privacy and security concerns when dealing with large data sets for analysis. According to Borodo et al. (2016), a defined set of legal, policy and technical strategies would diminish privacy concerns when dealing with personal information of users. In fact, governments across the countries are willing to enforce privacy preservation laws similar to the EU Legal Framework on Data Protection (D'Acquisto et al., 2015) that aimed to limit the problems of privacy and security in large data analysis (Rao et al., 2018).

2.4. Audit Quality and security concerns

The ongoing sequence of business scandals such as Enron and WorldCom has sabotaged the credibility and quality of auditors and auditing (Alles et al., 2004). In response, the auditing profession has worked effectively to enhance the quality of audit engagements and enable the use of advanced data technologies to generate better insights on the client's business. Various audit professional standards and qualifications including The Generally Accepted Auditing Standards (GAAS), Public Company Accounting Oversight Board (PCAOB), and American Institute of Certified Public Accountants (AICPA) have emphasized the significant role of Audit Ethics. In other words, audit professionals are adhered to a set of standards and qualifications through verbal and written agreements with audit firms, which regulate responsibilities, independence, information security, and quality (Samonas & Coss, 2014). In this respect, audit confidentiality and integrity are key principles mandated by audit standards in order to protect sensitive client information that are under audit testing. In fact, data leakage from audit practices poses serious litigations against auditors and firmly disrupts the audit firms' reputation. According to Waldron and Hallstrom (2013), auditing firms are subject to numerous risks in the case of data breaches (Figure 2). However, accounting and auditing firms have experienced significant amount of data breaches incidents. Between 2014 and 2018, the office of Maryland Attorney General identified 132 accounting firms' incidents of data breaches, mainly due to unauthorized access of data and hacking systems (Cheng et al., 2019).

2.5. Audit Data Analytics

Audit firms have been slowly shifting from the traditional auditing procedures, adapting the big data future, and applying data analytics on larger and unstructured datasets (Richins et al., 2017). Yet, as stated by Waldrom and

Hallstrom (2013), these technologies expose professional services firms to "Network Damages". Moreover, Rîndaşu (2017) points out that the auditing standards bodies are emphasizing on the need to adopt appropriate skills to ensure data confidentiality when transferring and analyzing Big Data from clients.

To our knowledge, most of the existing literature on the concept of Audit Data Analytics tackled the opportunities and potential benefits in audit firms. On the bright side, Chan and Vasarhelyi (2011) discuss how innovative technology helps transform traditional auditing to a more efficient and effective model through seven perspectives, including the change in the frequency, approach, procedures and nature of auditing. Moreover, Earley (2015) explains how data analytics tools are helping auditors gain bigger insights into the clients' operations while providing faster and sufficient assurance on the fairly presented financial statements.

Notably, researchers stated different concerns when dealing with data analytics in the audit field, yet did not deeply elaborate on the challenges separately. For example, Earley (2015) points out the limitations of data analytics and categorizes them into three aspects: training, accessibility of data and expectations from financial statement users. In another study, Appelbaum and Vasarhelyi (2018) concluded that the lack of comprehensive auditing standards on analytical procedures does not motivate audit professionals to adapt powerful data analytics tools compared to other industries. Furthermore, Cao et al. (2015) raise concerns over the privacy of clients' non-public information when applying big data analytics using outer sources such as IBM, Teradata and Wipro.

Overall, although many studies emphasized the importance of big data analytics in audit, few researchers discussed the contingent factors needed to apply data analytics in auditing firms such as the regulatory environment, company size, and accessible technologies (Dagiliene & Kloviene, 2018). While the Financial Reporting Council (2017) stressed on the importance of the integrity of data analytics regarding the traditional auditing standards, tackling the impact of data analytics application on the data confidentiality and security with respect to laws and regulations is crucial and needs to be addressed. To the best of the authors' knowledge, substantial research on this matter remains lacking, favoring the contribution of this study.

3. Conceptual Model and Hypotheses

This research draws on two theoretical models, utility maximization theory and procedural fairness theory in order to conceptualize the relationship between privacy and security, data analytics, external auditing, and audit quality. To begin with, Akerlof and Dickens (1982) have long introduced the utility maximization theory and economists were continuously using this framework to optimize the quality and performance of businesses (Gilad et al., 1987). According to Li (2012), the principle of the utility maximization theory is to maximize the total satisfaction level by a firm or individual from economic decisions. However, Li (2012) distinguishes between the concept of finding the equilibrium between the benefits and costs of the decision and determining the association between the set of variables at hand. For example, the author discussed how the theory could be applied on the relationship between the concern for privacy and the users' perceived importance of information transparency. Similarly, Hann et al. (2007) constructed the utility theory to demonstrate that the stimulus of providing personal data is a function of anticipated benefits and privacy concerns. In terms of data analytics, the theory of utility maximization depicts the function of perceived potential benefits when implementing data analytics to gain valuable insights for decision-making and exposed privacy and security challenges.

Coming to the procedural fairness theory (Li, 2012), this theory refers to the perceived fairness by firms or individuals regarding a particular activity in which they participate. According to Brockner (2002), organizations do not simply ascribe responsibilities for their outcomes; rather, they utilize procedural fairness to identify the essence of the relationships with their exchange partners. According to Li (2012), procedural fairness includes the organizations' activities that assure that the potential outcomes are favorable. In case of privacy and security matters as an example, procedural fairness is enforced through organizational privacy statements and policies, government laws, and other measures (Li, 2012). With respect to the audit profession regarding the confidentiality and privacy of client data, the procedural fairness theory can be depicted in different ways. First, CPA firms are subject to international regulatory bodies and federal laws that govern privacy and security matters when accessing and analyzing client data (Waldron & Hallstrom, 2013). Second, as external auditing relies on the trust and effective relationship between the audit party and business client, audit firms strictly apply professional and ethical codes of conduct that prohibit any deviation from the privacy and confidentiality procedures. Accordingly, clients believe that there are fair procedures set by the auditing party that will protect their data. Finally, in terms of the application of audit data analytics, the privacy interventions set by the regulators and audit firms are important to evaluate the level of exposure to privacy and security breaches.

one can determine the main associations between the above-mentioned topics:

First, privacy and security concerns are increasingly arising with the emerging technologies. Notably, there has been enormous research that discussed the limitation of the usage of big data analytics and the concerns over the preservation of sensitive data when accessing, storing and analyzing the data for insights. Mostly, the literature covered the relationship between the characteristics of Big Data (the 5Vs described in *Figure 1*) and the challenges of privacy and security (Gahi et al., 2016; Mishra & Singh (2016); Terzi et al., 2015; Joshi & Kadhiwala (2017)). With this in mind, the first hypothesis can be derived:

- **H1:** The application of data analytics is positively related to the increasing privacy and security concerns.

Second, as organizations are employing huge investments in data and technology due to the increasing use of structured and unstructured data, several research have proposed to incorporate data analytics in the audit environment. This is because with the traditional auditing procedures, audit firms cannot keep pace with the evolving economy. Thus, the second hypothesis could be set:

- **H2:** There is a positive relationship between the application of data analytics in the financial statement audit and the continuity of the auditing profession.

Third, the above literature reviewed numerous articles that discussed the opportunities and potential benefits on audit firms when applying audit data analytics. Cao et al. (2015), Early (2015), Dagiliene & Kloviene (2018), Richins et al., (2017) and Jans & Hosseinpour (2019) have all presented the two-side perspectives of applying data analytics in external auditing. Although research have also contributed to the challenges of audit data analytics, yet as mentioned earlier in section II, there are limited elaborations on the privacy and security concerns with respect to client data. Based on this, the following two hypotheses could be stated:

- **H3:** Audit data analytics can potentially enhance audit quality.
- **H4:** Audit data analytics is positively related to increasing risks of perceived privacy and security concerns.

Finally, drawing on the importance of privacy and confidentiality in auditing derived from the procedural fairness theoretical model, the conceptual model hypothesizes the impact of privacy and security concerns imposed by the implementation of audit data analytics on the overall audit quality and auditor credibility. Therefore, the final hypothesis can be derived:

- **H5:** The quality of financial statements audit is negatively affected by the privacy and security concerns imposed by audit data analytics.

The above discussion and stated hypotheses could be portrayed in the following conceptual model. Based on the previous literature and the theoretical frameworks described above, as well as the derived hypotheses, a conceptual model is proposed to depict the relationships between the four main domains of study: privacy and security concerns, Data Analytics, Audit Data Analytics and Audit quality (*Figure 3*).

Analyzing the portrayed conceptual model, the model starts with the adoption and use of data analytics tools and technologies. In a world where "data is the new oil" (Clive Humby, 2006 as adopted from Mavuduru, 2020) and where organizations are competing on making data-driven decisions and strategies, data analytics use and implementation become mission critical. These tools and technologies will be used in auditing practices, aiming at enhancing audit quality. However, data analytics implementation is not risk-free as the previous discussion has shown. In fact, it raises privacy and security concerns, which if not properly handled, may probably lead to lower audit quality as the confidentiality and integrity of audit data may be violated. This indicates the importance of taking this challenge into consideration to ensure quality in the audit process outcomes.

Three important attributes characterize the audit-data analytics model portrayed above. First, it is an integrated model that assimilates theoretically-based and commonly known factors in the data and information security literature. This is anticipated to lead to a clearer picture pertinent to the strategies and policies needed to mitigate the threats of security and privacy violations that the use of data analytics in the audit field may raise. Second, the model shows a proactive approach regarding anticipating the security and privacy threats that may take place in audit data analytics, thus endangering the quality of audit outcomes. Such anticipation will most probably drive organizations to enforce security and privacy measures to ensure a cost-effective auditing process and audit quality. Finally, the model is dynamic. It takes into consideration the importance of sensing security and privacy possible violations posed by implementing data analytics for auditing and responding to them reactively or, more favorably, proactively.

4. Conclusion and Recommendations for Future Work

In an effort to determine the importance of the privacy and security concerns in the auditing profession imposed by the application of data analytics, this study identifies the previous literature on the existing privacy and security concerns including reasons and classifications of cyber incidents and their impact on the national and individual level. Considering data analytics as one of the major evolutionary technologies fueling businesses, this study also reviews the existing work on data analytics and the related concerns in privacy and security as a result of the main characteristics of Big Data. Finally, the literature review examines the application of data analytics in the particular field of audit, while also discusses the impact of such practices on the audit quality.

Although audit firms have long recognized the need of data analytics to increase quality and provide better value for financial statements users, the implementation of audit data analytics is still relatively new in due to the different concerns practitioners have to overcome. For this reason, this study is an attempt to conceptualize the importance of the privacy and security challenges of audit data analytics on audit quality. The conceptual model (*Figure 3*) can be of vital importance to researchers and audit practitioners, where the study encourages future detailed analyses on the impact of privacy and security concerns on audit quality. This means that this study, when empirically tested, can be a great tool to identify and classify privacy challenges according to different audit phases and procedures. Besides, this study allows future researchers to enhance previously recommended models or propose new privacy preservation techniques that are applicable to audit data analytics and that align with the auditing standards.

In conclusion, the transformation from traditional auditing to continuous auditing by applying audit data analytics is not easy, as the privacy and security concerns along with other challenges are yet to be addressed. If not properly tackled, the issue of privacy and security concerns in audit data analytics might cause drastic consequences in the audit quality, reputation of the firm, and compliance with the existing regulatory frameworks concerned in this matter.

References

Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2004). Restoring auditor credibility: tertiary monitoring and logging of continuous assurance systems. *International Journal of Accounting Information Systems*, *5*(2), 183-202.

Al-Mhiqani, M. N., Ahmad, R., Yassin, W., Hassan, A., Abidin, Z. Z., Ali, N. S., & Abdulkareem, K. H. (2018). Cyber-security incidents: a review cases in cyber-physical systems. *International Journal of Advanced Computer Science and Applications*, *9*(1), 499-508.

Appelbaum, D. A., Kogan, A., & Vasarhelyi, M. A. (2018). Analytical procedures in external auditing: A comprehensive literature survey and framework for external audit analytics. *Journal of Accounting Literature*, *40*, 83-101.

Balaban, M. A. Privacy Concerns with Big Data Analytics: US DoD/Army Landscape.

Borodo, S. M., Shamsuddin, S. M., & Hasan, S. (2016). Big data platforms and techniques. *Indonesian Journal of Electrical Engineering and Computer Science*, *1*(1), 191-200.

Brockner, J. (2002). Making sense of procedural fairness: How high procedural fairness can reduce or heighten the influence of outcome favorability. *Academy of management review*, *27*(1), 58-76.

Cao, M., Chychyla, R., & Stewart, T. (01/06/2015). *Big data analytics in financial statement audits* American Accounting Association.

Chan, D. Y., & Vasarhelyi, M. A. (2011). Innovation and practice of continuous auditing. *International Journal of Accounting Information Systems*, *12*(2), 152-160.

Cheng, C., Flasher, R., & Higgins, J. P. (2019). Accounting Firm Data Breaches: One State's Records; Find out the Most Common Types of Breaches and How to Guard against Them All. *Journal of Accountancy*, *227*(5), 40.

D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., de Montjoye, Y. A., & Bourka, A. (2015). Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics. arXiv preprint arXiv:1512.06000.

Davis, G., Garcia, A., & Zhang, W. (2009). Empirical analysis of the effects of cyber security incidents. *Risk Analysis: An International Journal*, *29*(9), 1304-1316.

Early, C. E. (2015). Data Analytics in Auditing: Opportunities and Challenges Business Horizons, 58, 493-500. doi:0.1016/j.bushor.2015.05.002

Gahi, Y., Guennoun, M., & Mouftah, H. T. (2016, June). Big data analytics: Security and privacy challenges. In 2016 IEEE Symposium on Computers and Communication (ISCC) (pp. 952-957). IEEE.

Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International journal of information management*, *35*(2), 137-144.

Gilad, B., Kaish, S., & Loeb, P. D. (1987). Cognitive dissonance and utility maximization: A general framework. *Journal of Economic Behavior & Organization*, *8*(1), 61-73.

Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems*, *24*(2), 13-42.

Hosseinpour, M., & Jans, M. J. (2016). Categorizing Identified Deviations for Financial Statements Auditing.

Jans, M., & Hosseinpour, M. (2019). How active learning and process mining can act as Continuous Auditing catalyst. *International Journal of Accounting Information Systems*, *32*, 44-58.

Jansen, W. A., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing.

Joshi, N., & Kadhiwala, B. (2017, April). Big data security and privacy issues—A survey. In 2017 Innovations in Power and Advanced Computing Technologies (i-PACT) (pp. 1-5). IEEE.

LaValle, S., Lesser, E., Shockley, R., Hopkins, M. S., & Kruschwitz, N. (2011). Big data, analytics and the path from insights to value. *MIT sloan management review*, *52*(2), 21-32.

Lepenioti, K., Bousdekis, A., Apostolou, D., & Mentzas, G. (2020). Prescriptive analytics: literature review and research challenges. *International Journal of Information Management*, *50*, 57-70.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision support systems*, *54*(1), 471-481.

Matturdi, B., Zhou, X., Li, S., & Lin, F. (2014). Big Data security and privacy: A review. China Communications, 11(14), 135-145.

Mavuduru, A. (2020). Is Data Really the New Oil in the 21st Century? (Dec. 12). Retrieved from: https://towardsdatascience.com/is-data-really-the-new-oil-in-the-21st-century-17d014811b88

Mishra, A. D., & Singh, Y. B. (2016, April). Big data analytics for security and privacy challenges. In 2016 International Conference on Computing, Communication and Automation (ICCCA) (pp. 50-53). IEEE.

Obaidat, M. A., Obeidat, S., Holst, J., Al Hayajneh, A., & Brown, J. (2020). A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. Computers, 9(2), 44.

Rao, P. R. M., Krishna, S. M., & Kumar, A. S. (2018). Privacy preservation techniques in big data analytics: a survey. *Journal of Big Data*, *5*(1), 33.

Richins, G., Stapleton, A., Stratopoulos, T. C., & Wong, C. (2017). Big data analytics: opportunity or threat for the accounting profession?. *Journal of Information Systems*, *31*(3), 63-79.

Rîndașu, S. M. (2017). Emerging information technologies in accounting and related security risks–what is the impact on the Romanian accounting profession. Journal of Accounting and Management Information Systems, 16(4), 581-609.

Samonas, S., & Coss, D. (2014). THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY. *Journal of Information System Security*, *10*(3).

Singh, J. (2014, March). Real time BIG data analytic: Security concern and challenges with Machine Learning algorithm. In 2014 Conference on IT in Business, Industry and Government (CSIBIG) (pp. 1-4). IEEE.

Skarmeta, A. F., Hernandez-Ramos, J. L., & Moreno, M. V. (2014, March). A decentralized approach for security and privacy challenges in the internet of things. In *2014 IEEE world forum on Internet of Things (WF-IoT)* (pp. 67-72). IEEE.

Srivastava, N., & Jaiswal, U. C. (2019, March). Big Data Analytics Technique in Cyber Security: A Review. In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC) (pp. 579-585). IEEE.

Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. *International Journal of Distributed Sensor Networks*, *10*(7), 190903.

Terzi, D. S., Terzi, R., & Sagiroglu, S. (2015, December). A survey on security and privacy issues in big data. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 202-207). IEEE.

Waldron, A., & Hallstrom, D. (2013). A Breach of Client Data: Risks to CPA Firms. *Journal of Accountancy*, *216*(2), 18.

Wieringa, J., Kannan, P. K., Ma, X., Reutterer, T., Risselada, H., & Skiera, B. (2019). Data analytics in a privacy-concerned world. Journal of Business Research.

Biographies

Manal M. Yunis is an Associate Professor of Information Technology Management in the Department of Information Technology and Operations Management at the Lebanese American University in Beirut, Lebanon. She holds a PhD in Business Administration with a concentration in Computer Information Systems from the University of Texas-Pan American. Her research interests include information and cybersecurity, data analytics, global information technology management, cloud computing, e-government, and adoption and diffusion of emerging technologies. She has several peer-refereed journal and conference publications, and is the recipient of many best paper awards from conferences and publishing groups. She is a member of the Association of Information Systems (AIS), Decision Sciences Institute, and AIS Special Interest Groups.

Raed El-Khalil is an associate professor and the chair of the Information Technology and Operations Management department at the Adnan Kassar School of Business. He holds a Doctorate in Industrial and Manufacturing Engineering from Lawrence Technological University and has a rich background in numerous areas, including an MS in Engineering Management and Industrial and Manufacturing Engineering, as well as a BSc in Industrial Engineering, Manufacturing Engineering and Computer Science, all from the University of Michigan. In addition, he works as a consultant for several companies in North America including Chrysler, General Motors, Boeing, and others in the areas of Operations management. His research focuses on subjects within the manufacturing industry.

Miray Ghanem graduated with high distinction with a BS in business with concentration in banking and finance and accounting. She pursued her graduate studies and earned a Masters degree in Business Administration at LAU while working in the professional services industry. After graduation, she joined Deloitte Lebanon for 3 years, and is currently working at KPMG Jeddah Saudi Arabia as an audit Supervisor.

Figures

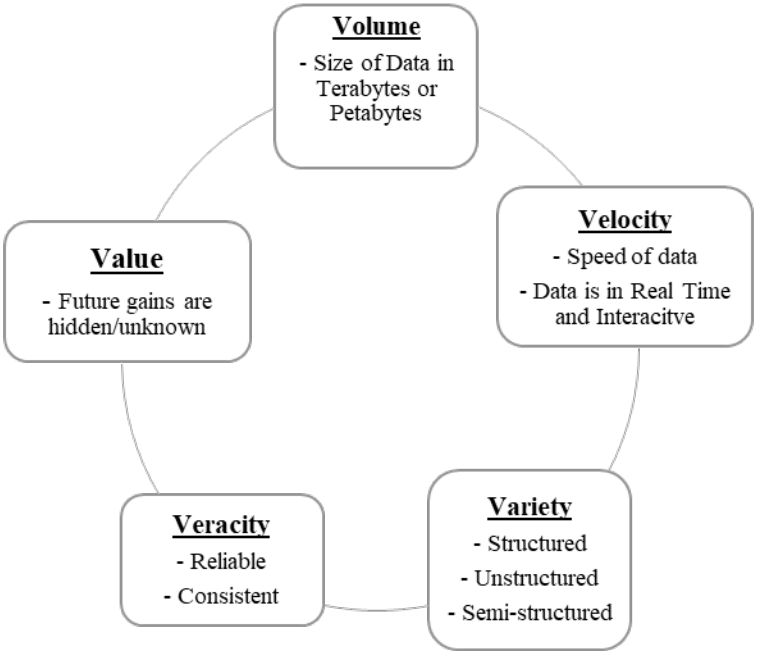

Fig. 1. Characteristics of Big Data (5Vs)

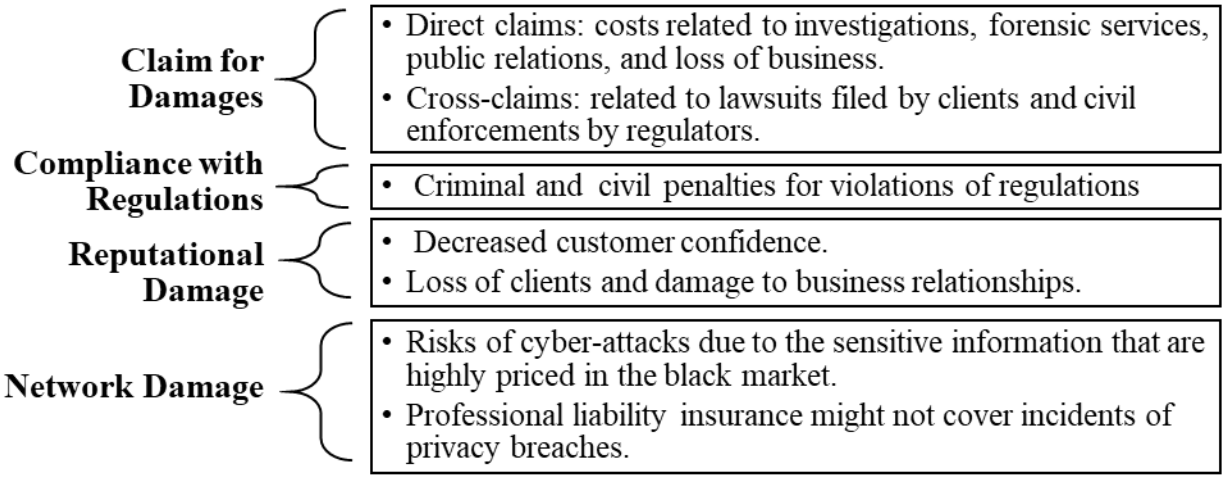

Fig. 2. Risk Exposures of CPA Firms with Data Breaches (Waldrom & Hallstrom, 2013)

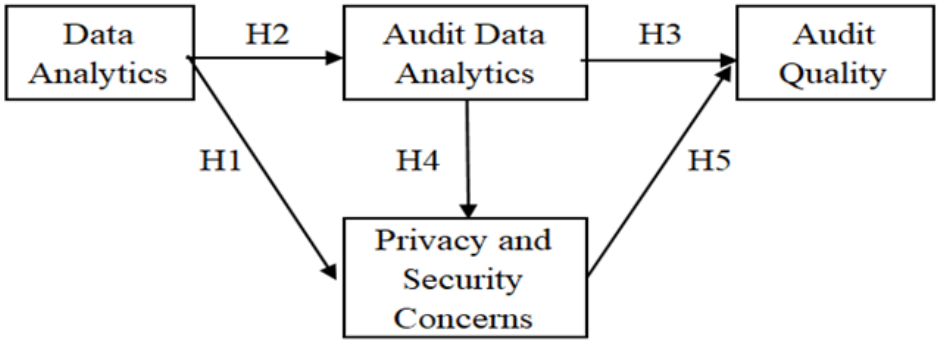

Figure 3. Conceptual Model

Tables

Table 1. Summary of Security and Privacy Challenges (Joshi & Kadhiwala, 2017)

Area of Concern	Issues with Big Data Analytics
Confidentiality	- Fear of illegal disclosures. - Authentication and authorization concerns.
Availability	- Ensuring data is available to authorized users only.
Integrity	- Concerns of data alteration in an unauthorized manner. - Data theft or leakage. - Data duplication
Monitoring and Auditing	- Concerns on whether conventional approaches to detect suspicious data activity are feasible for Big Data.
Key Management	- Concerns of sharing data between servers and users of Big Data.
Privacy of Data	- Sharing Personally Identifiable Information (PII) might not be restricted for specific reasons and without the consent of users.