A Conceptual Framework for Data Governance in IoT-enabled Digital IS Ecosystems

Avirup Dasgupta[a], Asif Gill[b] and Farookh Hussain[c]
School of Software, University of Technology Sydney, Australia

Keywords: IoT, Data Governance, Framework, Data Management.

Abstract: There is a growing interest in the use of Internet of Things (IoT) in information systems (IS). Data or information governance is a critical component of IoT enabled digital IS ecosystem. There is insufficient guidance available on how to effectively establish data governance for IoT enabled digital IS ecosystem. The introduction of new regulations related to privacy such as General Data Protection Regulation (GDPR) as well as existing regulations such as Health Insurance Portability and Accountability Act (HIPPA) has added complexity to this issue of data governance. This could possibly hinder the effective IoT adoption in healthcare digital IS ecosystem. This paper enhances the 4I framework, which is iteratively developed and updated using the design science research (DSR) method to address this pressing need for organizations to have a robust governance model to provide the coverage across the entire data lifecycle in IoT-enabled digital IS ecosystem. The 4I framework has four major phases: Identify, Insulate, Inspect and Improve. The application of this framework is demonstrated with the help of a Healthcare case study. It is anticipated that the proposed framework can help the practitioners to identify, insulate, inspect and improve governance of data in IoT enabled digital IS ecosystem.

1 INTRODUCTION

IoT is an emerging concept in the Healthcare industry with new applications and devices being manufactured using the Internet of Things (IoT). Sensor fitted wearable devices or implantable devices are increasingly being used to monitor the well-being of a patient. These devices automatically monitor health conditions, notify abnormal situations and propose protective actions such as informing doctors, family and friends (Karahoca et al., 2018, Gill et al., 2016).

The complexity of gathering, storing and processing data, has given rise to many data related problems in particular the governance of data. The General Data Protection Regulation (GDPR) law (Cha et al., 2018) has introduced additional aspects to this issue. Hence, it is vital that we understand the dynamics of data governance and related regulations in the IoT enabled digital IS ecosystem. This includes comprehending data ownership, the process of gathering consent before processing the data as well as understanding data lineage in the IoT enabled IS ecosystem. Thus, data governance issues pertaining to data security, data confidentiality, and data ownership stand as obstacles to the exchange of data among distributed IoT network and applications. Therefore, it is important that organizations address these challenges from a data governance (DG) perspective (Gartner, 2016a).

Data governance is not a new concept and is in use in the financial sector for more than two decades (Kontzer, 2006). However, in an IoT-enabled IS context, it is still at a nascent stage. The evolution of decentralized IoT architectures like Fog, Cloudlets and Edge implies that centralized approaches to governance are not viable (Gartner, 2016a). Several authors have highlighted the unethical use of data (Dastjerdi and Buyya, 2016), reprogramming device to function beyond its intended purpose and lack of network-intrusion-detection mechanism (security) as a major challenge associated with deploying IoT

[a] https://orcid.org/0000-0002-0645-5984
[b] https://orcid.org/0000-0001-6239-6280
[c] https://orcid.org/0000-0003-1513-8072

Dasgupta, A., Gill, A. and Hussain, F.
A Conceptual Framework for Data Governance in IoT-enabled Digital IS Ecosystems.
DOI: 10.5220/0007924302090216
In *Proceedings of the 8th International Conference on Data Science, Technology and Applications (DATA 2019)*, pages 209-216
ISBN: 978-989-758-377-3

based applications (Dhillon et al., 2016, Dasgupta and Gill, 2017). This paper focuses on the following research question (RQ): How to establish the data governance in digital IS ecosystem? In order to address the above question, this paper presents the application of the 4I framework in the Healthcare domain.

This paper is organized as follows. Section 2 discusses the data and IoT governance concepts. Section 3 discusses the research method. Section 4 presents the existing frameworks related to data management and governance in the context of IoT. Section 5 summaries the 4I framework. Section 6 demonstrates the applicability of the 4I framework with the help of a Healthcare case study before concluding the paper in section 7.

2 RESEARCH BACKGROUND

This section describes the key concepts of data in the context of IoT enabled digital IS ecosystem in order to provide the research background and context

2.1 Data Management

Data Management is concerned with the use of data to make good business decisions. It focusses on defining data, its storage, structure and data flow. The Data Management Association (DAMA), an association of technical and business data management professionals, defines data management as the development and execution of architectures ,policies, procedures and practices to manage entire data lifecycle as well as planning, executing and managing the activities which acquire, control, protect, deliver and enrich data assets (Mosley et al., 2010, Stryk, 2015). Data Management Body of Knowledge (DAMA-DMBOK) identified 10 functions, which constitute Data management (Mosley et al., 2010) as shown in the figure below.

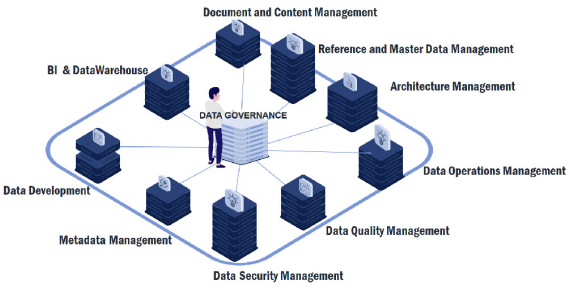

Figure 1: Data Management Functions (adapted from (Mosley et al., 2010)).

2.2 Data Governance

As corporations recognize the importance of data and the challenges they face in integrating the data from various disparate source systems, an increasing number of companies have started exploring data governance. Data governance enables corporate-wide accountabilities and decision rights for data quality management (Weber et al., 2009) and is essential for the existence of an organization (Stryk, 2015). It is defined as an organizational approach to data and information management (Janne J. Korhonen et al., 2013) that formalizes a set of policies and procedures to include the full life cycle of data, from acquisition to use and to disposal. Gartner defines it as the procedure of setting decision rights and answerability for an asset, establishing policies aligned to business objectives, investing in assets that aid business objectives, establishing measures to ensure compliance to corporate policies, and ensuring adequate corporate risk management (Gartner, 2016b).

While governance refers to the decisions that are taken to ensure effective use and management of resources, management is focused on executing the decisions. Thus, management is influenced by governance (Ibrahim Alhassan, 2016). Data governance defines standards and procedures to ensure the proactive and effective handling and guidance of data management practices such as data replication, data archival, security, data backup ,meta data management (MDM), data traceability and lineage, business glossary mapping, governance council, release and change management, master data and business (Infotech, 2016). Effective data governance results in profitable data use in an organization (Panian, 2010). With appropriate data governance, businesses can make insightful decisions by putting context to the data and transforming the information into knowledge and intelligence. This includes ensuring data has the necessary quality, availability, integrity and security throughout its lifecycle (Al-Ruithe et al., 2018).

2.3 IT Governance

IT governance is different from data governance and is concerned with the overseeing of IT resources such as computer networks, servers and applications through risk monitoring and control (Peterson, 2004) in alignment with the aims and strategies (Tallon et al., 2013) of an organization. Traditionally, financial assets and services (Gill et al., 2015) were administered using Governance, however, in last few

decades it has been extended to data and IT assets(Robert C. Rickards, 2012). There are several IT governance frameworks such as ISO 27001, Information Technology Infrastructure Library (ITIL) and Control Objectives for Information and Related Technology (COBIT) (Gehrmann, 2012). While ITIL was established to provide best practices for the IT services to its customers, COBIT framework supports governance of IT assets with a distinctive focus on ensuring IT procedures and activities align with the strategic goals of an enterprise (Egelstaff and Wells, 2013); (Juiz and Toomey, 2015).

2.4 IoT Governance

IoT governance is an extension to IT governance, where IoT governance is specifically focused on the lifecycle of IoT devices, data managed by the IoT solutions, and IoT applications in an organization's IT landscape (Gantait et al., 2018). IoT governance is can be considered a part of the existing IT governance landscape. It comprises of organizations such as Internet Engineering Task Force (IETF),Regional Internet Registry (RIRs), Information Security Operations Centre (ISOC), IEEE, The Internet Corporation for Assigned Names and Numbers (ICANN),Internet Governance Forum (IGF), and W3C and should leverage or tailor IT governance frameworks available to govern IoT(Virgilio A.F. Almeida 2015).

There is a need to have a clear distinction between the IT governance and data governance. While data governance deals with the data assets to improve business outcomes for business stakeholders, where IT governance is primarily focused on the IT assets. Further, these two concepts can be linked to strategy and enterprise architecture (Korhonen et al., 2016)) in modern adaptive enterprises. These are two different but related concepts and thus there are some overlapping areas between IT and Data Governance as shown in table below. Thus, the scope of this paper is limited to data governance in IoT (a kind of IT) enabled IS.

Table 1: Difference between IT and Data Governance (adapted from (Dimick, 2013)).

IT GOVERNANCE	DATA GOVERNANCE
IT driven led by (Chief Information Officer)	Business Driven
Oversee implementation of IT policy process and extract business benefits	Operational Focus
Policy and process ensuring effective evaluation, selection, prioritization, funding of competing IT assets and investment	Policy, process and practice that address accuracy, validity, completeness, timeliness, data integrity

3 RESEARCH METHOD

This research aims to address the data governance challenges in IoT and proposes the development and evaluation of the 4I framework using the Design Science Research (DSR) (Prat et al., 2014). DSR is problem focused (Kuechler and Vaishnavi, 2008) and seeks to design and evaluate an innovative product, or artefact, that provides a potential solution to a real-life problem within an organization as shown in figure 2 below. In DSR, the artefacts usually can be technical elements such as concepts, models, methods, frameworks or instantiations (March and Smith, 1995) as well as social elements such as humans, roles, work processes, teams, groups of organizations (Drechsler, 2015).

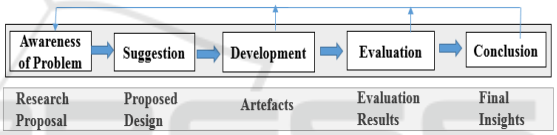

Figure 2: Design Science Research.

We applied the guidelines of DSR (Hevner and Chatterjee, 2010) to conduct this research. This paper focuses on the evaluation aspect of the proposed 4I framework.

4 RELATED IOT DATA MANAGEMENT AND GOVERNANCE FRAMEWORKS

The traditional data governance practices comprising of people, process and technology(Merkus, 2015) are going through a fundamental shift or transformation phase. This can be attributed to the changes in regulations (Wachter, 2018) as well as advancement in technologies such as Big Data, Blockchain, Cloud, IoT and Mobile (Copie et al., 2013). Thus, there is a need to tailor the data governance practices in an IoT context (Al-Ruithe et al., 2016), (Porambage et al., 2016), (IERC, 2015), (Banerjee and Sheth, 2017))., (*IOTAlliance*, 2017) in order to address IoT specific issues as indicated in figure 3 above. Few studies on

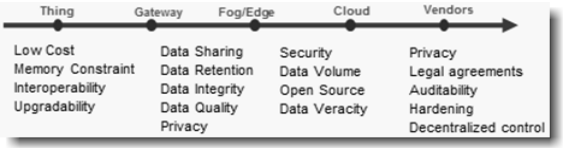

Figure 3: IoT introduced Data Governance challenges.

governance of data have been conducted in thedomain of healthcare such as HeathFog in (Verma and Sood, 2018) and attribute based smart health in (Fuentes et al., 2018). In (Sajid and Abbas, 2016), authors discussed encryption based data privacy in cloud based healthcare systems. In another study (Banerjee and Sheth, 2017), the authors put forward an evaluation model to contextually evaluate the data quality based on two use cases.

To the best of our knowledge, currently there is no concrete IoT framework, which is available and can provide a blueprint to establish a gata governance environment, particularly from a regulatory perspective. However, it is evident from the recent commercial works and analyst reports such as Gartner (Gartner, 2016a) and Frost and Sullivan(Sullivan, 2018), that there is an urgent need for more research and development in this area of governance.

5 THE 4I FRAMEWORK

This research developed a 4I framework (Dasgupta et al., 2019) (**I**dentify, **I**nsulate, **I**nspect and **I**mprove) for managing and governing the data assets in the IoT-enabled Digital IS ecosystem. The 4I framework (Version 2) depicted in figure 4 is an updated version of the framework introduced in (Dasgupta et al., 2019).

It is based on the extensive review of existing data governance literature from academia and industry such as DAMA-DMBOK2 Framework (Mosley et al., 2010), The Data Governance Institute Data Governance Framework (Proença and Borbinha, 2016), The IBM Data Governance Council Maturity Model (A. Wróbel, 2017), The Gartner Enterprise Information Management Framework, EDM Council

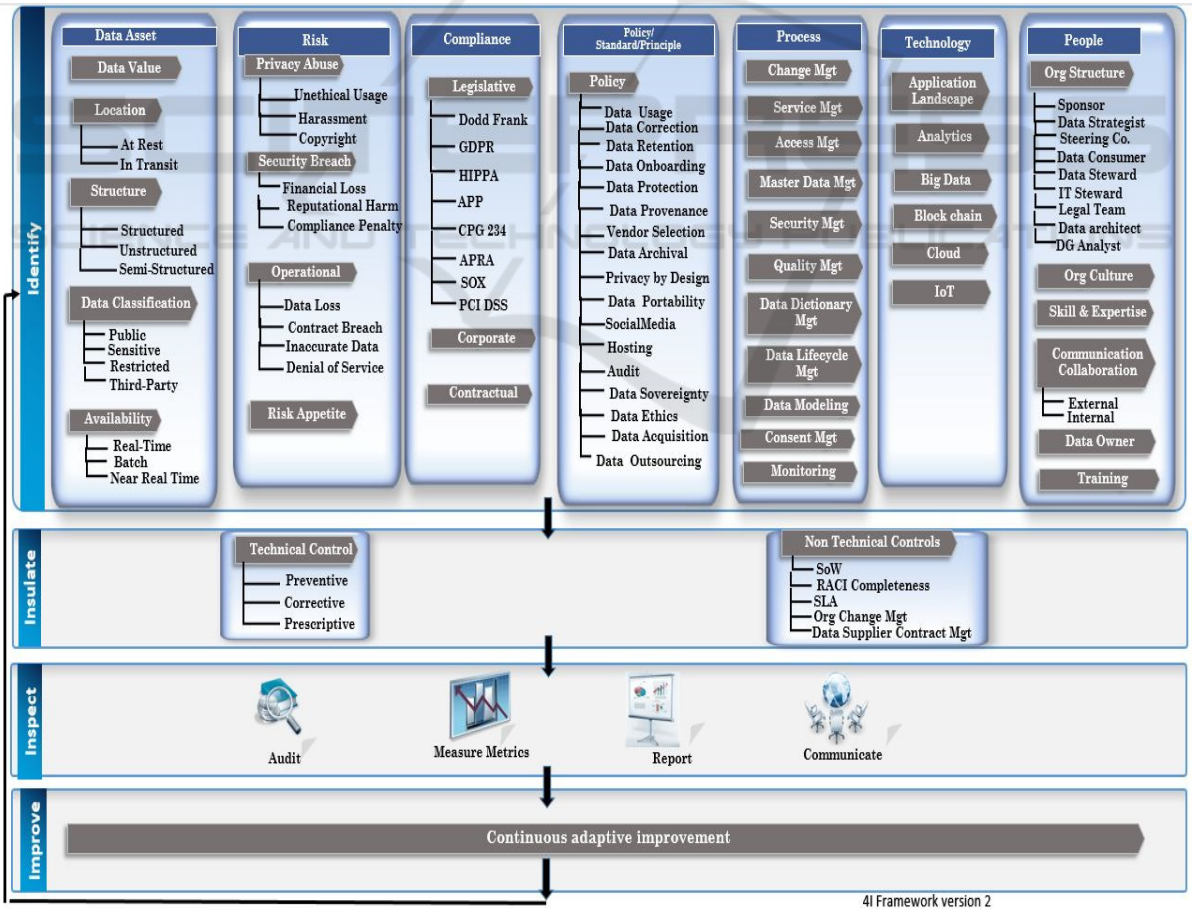

Figure 4: The 4I framework.

Data management Capability Maturity Model (Council, 2015), Generic Framework (Al-Ruithe et al., 2016), and DGMM Framework (Merkus, 2015).

It is intended for use by data governance personnel as a guide to ensure appropriate data collection ("what to use"), processing ("how to use"), and retention ("until when to use") mechanisms as well as significance ("why to use") of data. It is composed of four stages or phases and explained in detail with the Fitbit case study in Section 6.

6 APPLICATION OF THE 4I FRAMEWORK: HEALTHCARE CASE STUDY

Wearables are the main fitness trend for 2019(Thompson, 2018) according to American College of Sports Medicine (ACSM). Wearables rely on the collection of the consumer's private and personal data. Personal Identifiable Information (PII) can include First name, Last Name, Data of Birth, Address, Phone number, Financial and health of an IoT Fitbit user. This also constitutes sensitive personal information (SPI).

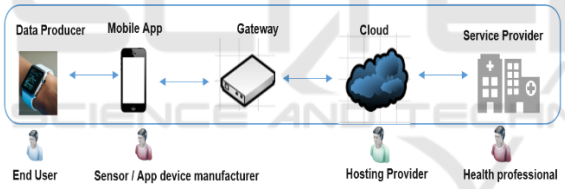

Figure 5: Wearable smart IoT-enabled ecosystem.

The "Fitbit" data is transmitted using Bluetooth technology to the consumer's mobile or desktop application before it is transferred to the cloud.
As shown in figure 5, the data exchange involves stakeholders such as App manufacturer, Cloud Providers, Health Service Provider and several systems to provide the end user with health service. From the Fitbit providers perspective, ensuring data is secured and compliant is of highest priority. Regrettably, the consumer has a lack of understanding of the risks (Skierka, 2018, Banerjee et al., 2018) linked with some of the wearable devices or products. For example, some wearable devices have default passwords that can be found on public websites and cannot be altered (Government, 2019).

In this section, we evaluate the applicability of the 4I and demonstrate how the 4I framework can be applied by the Fitbit service providers to avoid unethical usage of data.

1st I in the 4I Framework:
The **Identify** phase of the 4I Framework ascertains the key actions that the Fitbit service provider needs to perform to ensure that the users data is not compromised. It includes
1)Reviewing the laws such as Health Insurance Portability and Accountability Act (HIPPA) and GDPR to understand rights of smart health device user (Sharma et al., 2018) with regards to the data protection.

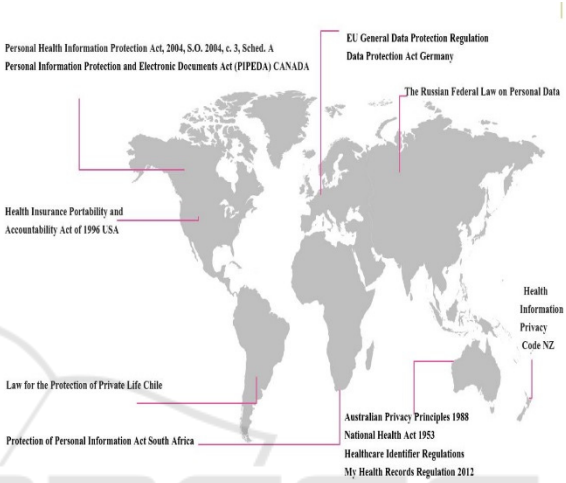

Figure 6: Healthcare data related Laws.

2) Identifying potential threats or risks around data management. For example, exploitation of security vulnerabilities to obtain user data is a common phenomenon. This is particularly important in Fitbit app context where apps running on Android are impacted by vulnerabilities from time to time(Linares-Vásquez et al., 2017), As a part of "identify" stage, Security advisories on vulnerability published periodically by Android can be documented and included in the patch management policy.
3) Classifying the sensitivity of data collected and determining the impacts of

- Sharing of health data publicly
- Sharing of data (health, PII, PCI and location) to a 3rd party such as medical providers(hospital, doctors), healthcare service provider, cloud or fog hosting service provider, network carrier
- Tracking of movement of individuals (including elderly patients) using motion sensors, camera, GPS tracker.
- Retention of data after customer stops using the device and its services
- Inferring customer's traits based on data.

4) Establishing policies related to data retention, data protection, patch management, Fitbit device procurement, data sharing and management techniques such as data anonymization, obfuscation are identified in this phase of the framework.

2nd I in the 4I Framework:
The second phase **Insulate** includes the preventive actions taken to mitigate the risks identified in the previous stage

Technology can be used to implement the data protection policies related to healthcare devices. This can include preventive measures such as ensuring software is patched to the current version in accordance with the patch management policy. It can also include implementing the data management processes formulated in "Insulate" phase. For example, an agent can be installed at wearable user's gateway or mobile application to ensure that data is passed to Cloud only if

- Latest firmware version is present in the IoT devices.
- Intended address to push data matches the hardware endpoint requirements such as Host IP address or Mac address
- Explicit Consent is recorded from customer
- Encrypted data is sent
- 3rd party software used is patched is upgraded.

3rd I in the 4I Framework:
The **inspect**ion phase is a combination of sophisticated real-time monitoring, auditing and reporting as performed by the software agent.

- A robust asset management software can map each Fitbit device all the way to the database where each record of data is stored in database or application server.
- For each Fitbit, security information and event management (SIEM) agent can scan the data records stored in the files or databases. The agent can flag a risk through automated alerts to the data governance team in case it finds non-encrypted records or inappropriate data access.
- With respect to data stored beyond the data retention requirement, the agent can check if any PII data is stored in fileservers or database in unencrypted form and may take remedial actions.

4th I in the 4I Framework:
In the **Improve** phase, continuous enrichment of the process is done to ensure that the operational process is continuously monitored and enhanced. For example, conducting a Third Party Vendor assessment to check cloud storage vulnerability and updating the Vendor Selection or SLA policy can be an improvement and outcome of this final phase of the 4I framework. Additionally, non-technical changes such as reworking the contracts to pass liability of data breach to the third party can be another consequence of the improvement phase. In nutshell, this case of Fitbit demonstrates the applicability of the 4I framework for data governance in IoT-enabled Digital IS ecosystem.

7 CONCLUSIONS

The effective and informed governance of data in IoT-enabled applications is a complex undertaking. Currently, there is no holistic framework exists to address the important research question: how to ensure data governance in IoT-enabled Digital IS ecosystems? This paper discusses the newly developed 4I framework that can provide the Governance coverage across the data lifecycle in IoT-enabled Digital IS ecosystem. The 4I framework is developed through analysis and review of existing scientific and practice-oriented literature related to IT, Data and Enterprise Governance within the context of IoT and Digital IS ecosystem. Data stewards can use the proposed framework to manage and define enterprise-wide guidelines, company rules, and data assets to deliver the essential data governance and quality. The initial applicability of the proposed framework is demonstrated with the help of a healthcare case study. We intend to conduct further detailed studies to enhance the 4I framework.

ACKNOWLEDGEMENTS

This research is supported by the Australian Government Research Training Program Scholarship scheme.

REFERENCES

A. Wróbel, K. K., K. Rudek. 2017. IBM data governance solutions. *2017 International Conference on Behavioral, Economic, Socio-cultural Computing (BESC), 16-18 Oct. 2017 2017. IEEE, 1-3*.

Al-Ruithe, M., Benkhelifa, E. Hameed, K. 2018. Data Governance Taxonomy: Cloud versus Non-Cloud. *Sustainability,* 10**,** 95.

Al-Ruithe, M., Mthunzi, S. Benkhelifa, E. Data governance for security in IoT & cloud converged environments. *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Nov. 29 2016-Dec. 2 2016 2016. 1-8*.

Banerjee, S., Hemphill, T. Longstreet, P. 2018. Wearable devices and healthcare: Data sharing and privacy. *The Information Society,* 34**,** 49-57.

Banerjee, T. Sheth, A. 2017. IoT Quality Control for Data and Application Needs. *IEEE Intelligent Systems,* 32**,** 68-73.

Cha, S., Hsu, T., Xiang, Y. Yeh, K. 2018. Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal***,** 1-1.

Copie, A., Fortis, T., Munteanu, V. I. Negru, V. From Cloud Governance to IoT Governance. *2013 27th International Conference on Advanced Information Networking and Applications Workshops, 25-28 March 2013 2013. 1229-1234*.

Council, E. 2015. EDMC DCAM version 1.0. Sl: sn.

Dasgupta, A. Gill, A. Q. 2017. Fog Computing Challenges: A Systematic Review. *Australasian Conference on Information Systems,*. Hobart.

Dasgupta, A., Gill, A. Q. Hussain, F. 2019. Privacy of IoT-Enabled Smart Home Systems. *IoT and Smart Home Automation.* IntechOpen.

Dastjerdi, A. V. Buyya, R. 2016. Fog Computing: Helping the Internet of Things Realize Its Potential. *Computer,* 49**,** 112-116.

Dhillon, G., Carter, L. Abed, J. 2016. Defining Objectives For Securing The Internet Of Things: A Value-Focused Thinking Approach.

Dimick, C. 2013. Governance Apples and Oranges. *Journal of AHIMA,* 84**,** 60-62.

Drechsler, A. 2015. Designing to inform: toward conceptualizing practitioner audiences for socio-technical artifacts in design science research in the information systems discipline. *Informing Science: the International Journal of an Emerging Transdiscipline,* 18**,** 31-45.

Egelstaff, R. Wells, M. 2013. Data governance frameworks and change management. *Studies In Health Technology And Informatics,* 193**,** 108-119.

Fuentes, J. M. d., Gonzalez-Manzano, L., Solanas, A. Veseli, F. 2018. Attribute-Based Credentials for Privacy-Aware Smart Health Services in IoT-Based Smart Cities. *Computer,* 51**,** 44-53.

Gantait, A., Patra, J. Mukherjee, A. 2018. *Defining your IoT governance practices* [Online]. IBM. Available: https://www.ibm.com/developerworks/library/iot-governance-01 [Accessed 2018].

Gartner 2016a. Data Risks in the Internet of Things Demand Extensive Information Governance.

Gartner 2016b. Organizing for Big Data Through Better Process and Governance.

Gehrmann, M. 2012. Combining ITIL, COBIT and ISO/IEC27002 for structuring comprehensive information technology for management in organizations. *Navus: Revista de Gestão e Tecnologia,* 2**,** 66-77.

Gill, A., Bunker, D. Seltsikas, P. 2015. Moving Forward: Emerging Themes in Financial Services Technologies' Adoption. *CAIS,* 36**,** 12.

Gill, A. Q., Phennel, N., Lane, D. Phung, V. L. 2016. IoT-enabled emergency information supply chain architecture for elderly people: The Australian context. *Information Systems,* 58**,** 75-86.

Government, A. 2019. Seven Steps to Securing Your Smart Health Devices. *In:* AGENCY, D. H. (ed.).

Hevner, A. Chatterjee, S. 2010. Design science research in information systems. *Design research in information systems.* Springer.

Ibrahim Alhassan, D. S. M. D. 2016. Data governance activities: an analysis of the literature. *Journal of Decision Systems*.

IERC, E. R. C. 2015. IoT Governance, Privacy and Security Issues.

Infotech, I. 2016. *Assessing and implementing a Data Governance program* [Online]. Available: http://docplayer.net/11775196-Assessing-and-implementing-a-data-governance-program-in-an-organization.html? [Accessed August 2018].

IOTAlliance 2017. Internet of Things Security Guideline.

Janne J. Korhonen, Ilkka Melleri, Kari Hiekkanen Helenius, M. 2013. Designing Data Governance Structure: An Organizational Perspective. *GSTF Journal on Computing (JoC),* 2.

Juiz, C. Toomey, M. 2015. To govern IT, or not to govern IT? *Commun. ACM,* 58**,** 58-64.

Karahoca, A., Karahoca, D. Aksöz, M. 2018. Examining intention to adopt to internet of things in healthcare technology products. *Kybernetes,* 47**,** 742-770.

Kontzer, T. 2006. An End To Data Anarchy. *InformationWeek***,** 73-75.

Korhonen, J. J., Lapalme, J., McDavid, D. Gill, A. Q. Adaptive enterprise architecture for the future: Towards a reconceptualization of EA. *2016 IEEE 18th Conference on Business Informatics (CBI), 2016. IEEE, 272-281*.

Kuechler, B. Vaishnavi, V. 2008. On theory development in design science research: anatomy of a research project. *European Journal of Information Systems,* 17**,** 489-504.

Linares-Vásquez, M., Bavota, G. Escobar-Velásquez, C. An empirical study on android-related vulnerabilities. *2017 IEEE/ACM 14th International Conference on Mining Software Repositories (MSR), 2017. IEEE, 2-13*.

March, S. Smith, G. 1995. *Design and Natural Science Research on Information Technology*.

Merkus, J. R. 2015. *Data Governance Maturity Model.* Open Universiteit Nederland.

Mosley, M., Brackett, M. H., Earley, S. Henderson, D. 2010. *DAMA guide to the data management body of knowledge*, Technics Publications.

Panian, Z. 2010. Some Practical Experiences in Data Governance. *World Academy of Science, Engineering and Technology*

Peterson, R. 2004. Crafting information technology governance. *Information systems management,* 21**,** 7-22.

Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A. Vasilakos, A. V. 2016. The Quest for Privacy in the Internet of Things. *IEEE Cloud Computing,* 3**,** 36-45.

Prat, N., Comyn-Wattiau, I. Akoka, J. Artifact Evaluation In Information Systems Design-Science Research – A Holistic View. *PACIS Proceedings. 23, 2014*.

Proença, D. Borbinha, J. 2016. Maturity Models for Information Systems-A State of the Art. *Procedia Computer Science,* 100**,** 1042-1049.

Robert C. Rickards 2012. Data Governance Challenges Facing Controllers. *International Journal Of Business, Accounting, & Finance***,** 25-42.

Sajid, A. Abbas, H. 2016. Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and Future Challenges. *Journal of Medical Systems,* 40**,** 155.

Sharma, S., Chen, K. Sheth, A. 2018. Toward Practical Privacy-Preserving Analytics for IoT and Cloud-Based Healthcare Systems. *IEEE Internet Computing,* 22**,** 42-51.

Skierka, I. The governance of safety and security risks in connected healthcare. Living in the Internet of Things: Cybersecurity of the IoT - 2018, 28-29 March 2018 2018. Institution of Engineering and Technology (IET), 1-12.

Stryk, B. 2015. *How do organizations prepare and clean Big Data to achieve better data governance? A Delphi Study*.

Sullivan, F. 2018. *Be Prepared! A Lively Discussion on Data Preparation* [Online]. Available: http://frost.com/prod/servlet/segment-brochure.pag?id=9A37-00-3C-00-00 [Accessed April 1 2018].

Tallon, P. P., Ramirez, R. V. Short, J. E. 2013. The information artifact in IT governance: toward a theory of information governance. *Journal of Management Information Systems,* 30**,** 141-178.

Thompson, W. R. 2018. Worldwide survey of fitness trends for 2019. *ACSM's Health & Fitness Journal,* 22**,** 10-17.

Verma, P. Sood, S. K. 2018. Fog Assisted-IoT Enabled Patient Health Monitoring in Smart Homes. *IEEE Internet of Things Journal,* 5**,** 1789-1796.

Virgilio A.F. Almeida, D. D., Monteiro 2015. Governance Challenges for the Internet of Things.

Wachter, S. 2018. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review*.

Weber, K., Otto, B. Österle, H. 2009. One size does not fit all---a contingency approach to data governance. *Journal of Data and Information Quality (JDIQ),* 1**,** 4.