26th International Congress on Modelling and Simulation, Adelaide, SA, Australia, 30 Nov–4 Dec 2025
mssanz.org.au/modsim2025

Toward an Internet of Things data governance approach

S Seo [a], N Evans [a] and D Velasquez [a]

[a] *STEM, University of South Australia, Australia*
Email: Sam.Seo@unisa.edu.au

Abstract: The rapid advancement of technology in recent years has resulted in an exponential increase in the amount of data being generated, collected, and processed. While multi-technology integration has driven innovation, it exposes organisational managers to new data management challenges (Ma et al. 2013; Cooper and James 2009). These include responding to sudden threats or undesirable situations due to the difficulty of implementing data governance when there are many unknowns. This has led to the need for effective management and governance of data, particularly regarding its increasing significance in various domains, including business, science, and society. In this context, data governance emerges as a crucial field of study and practice.

The IoT has unique data challenges. For example, unlike many other technologies that primarily undertake dedicated tasks and still require human input, IoT increasingly self-governs (Misra et al. 2020). This presents a new set of challenges for data governance; the unique requirements of IoT are more complex than anything envisaged when traditional data governance models were designed (Sicari et al. 2018). It is important to question whether traditional data governance models can effectively handle the impact of IoT.

Traditional data governance frameworks - such as DAMA-DMBOK, DGPC, DGI, and MIKE2.0 - were designed for conventional IT systems and often fail to address the complexity, autonomy, and distributed nature of IoT environments. This paper presents a review of selected data governance frameworks and evaluates their applicability to IoT contexts. Drawing on an extensive literature review, IoT characteristics are categorised across technology, organisation, and people dimensions to highlight how they amplify governance challenges. The analysis reveals persistent gaps in areas such as data ownership, interoperability, security, lifecycle management, and regulatory alignment. Moreover, current frameworks place disproportionate emphasis on technological aspects while neglecting managerial and organisational considerations critical to IoT adoption. The findings underscore the urgent need for a dedicated IoT-focused data governance approach that integrates technical, organisational, and human factors. This review provides a foundation for developing such a framework and calls for further empirical research and interdisciplinary collaboration to bridge the gap between theory and practice in IoT data governance.

This paper shows that IoT scholarship emphasises technology and applications while under-addressing data governance; This paper identifies 5 recurrent governance gaps and contribute a TOP-based synthesis and actionable agenda for IoT data governance.

Keywords: *Data Governance, Internet of Things, Frameworks*

1. INTRODUCTION

The Internet of Things (IoT) is an integration of diverse technologies (Seo and Evans 2021), giving it distinctive characteristics and inherent issues. Over the years, research and resources invested in IoT previously focused on technical and implementation aspects. Less attention was given to IoT data management and data governance. Minor data governance issues can be easily neglected, but as time passes these issues can accumulate, eventually resulting in financial loss or even life-threatening incidents. For example, one notable case study is NASA's Mars Orbiter disaster, including the loss of a robot space probe because of a simple failure of data governance (NASA 1999). The inadvertent use of English units instead of metric units in computing the total impulse generated led to the disintegration of the Mars Orbiter due to atmospheric stresses. Luckily, no lives were lost in this instance (Sauser et al. 2009). Weak data governance creates the opportunity for security vulnerabilities to be criminally exploited (Lilly 2016). Poor IoT data governance poses threats not just to the IoT itself but to the public if IoT vulnerabilities are exploited and weaponised. In one report hackers were exploiting vulnerabilities in IoT to launch Distributed Denial of Service (DDoS) attacks against multiple United States websites and online services (Lilly 2016). It is therefore necessary to consider proper data governance implementation as an essential and urgent matter. If those responsible for data governance are unprepared, incidents such as those described above could be repeated at a much larger order of magnitude, especially given that IoT coverage is much wider than that of most individual computing devices or networks. Existing data-governance frameworks (e.g., DAMA /DGPC/ DGI/ MIKE2.0) assume centralised, stable IT and offer little specificity for IoT's distributed, high-velocity, heterogeneous, and increasingly autonomous environment. Unlike relational databases, the complexity of IoT systems – which often involve multiple devices and systems communicating with one another – demands a comprehensive approach to data governance. At the same time, the decentralised nature of IoT systems makes it challenging to establish a unified data governance framework. Thus, there is a need to investigate data governance from an IoT perspective.

This review addresses a persistent gap: data governance remains under-specified for distributed, heterogeneous, and increasingly autonomous IoT systems. It examines three research questions (RQs): RQ1 – What are the unique characteristics IoT relative to traditional IT, complicate data governance. RQ2 – Where do enterprise data governance framework fall short in IoT context? RQ3 – Is there a need for data governance framework for IoT? The contributions are threefold: (1) a synthesis of IoT characteristics gaps using a Technology–Organisation–People lens; (2) an explanation of structural reasons enterprise frameworks underperform in IoT; and (3) an emphasis on the need to have an IoT data governance framework that would address the IoT characteristics identified.

2. IOT CHARACTERISTICS AND THEIR IMPACT ON DATA

IoT data differs fundamentally from traditional IT data, creating distinct governance requirements. Traditional data is often static, human-generated, centrally stored, and accessed on request, whereas IoT data is dynamic, sensor-driven, continuously real-time collecting, and frequently consumed in real time to trigger automated actions (Ashton 2009). Unlike conventional datasets that support retrospective analysis, IoT data supports immediate, context-aware decisions, demanding governance mechanisms that address velocity, heterogeneity, and cross-functional integration (Pritika et al. 2023; Qin et al. 2016). IoT data exchange behavior (push, request and response, subscribe and notify), reliance on distributed cloud and edge storage, and dependence on device precision introduce new risks of bias, inconsistency, and interoperability challenges (Abu-Elkheir et al. 2013; Alvi et al. 2015; Jernigan et al. 2016). These IoT characteristics do not align with the assumptions of traditional data governance frameworks designed for centralised, well-defined data models, emphasising the need for IoT-specific governance approaches that can manage decentralisation, real-time intelligence, and diverse data lifecycles (Aggarwal et al. 2013; Tönjes et al. 2014).

Technology, Organisation and People (TOP) frames challenges from three dimensions (Khalid et al. 2006). Each dimension has major influence over changes in the business environment and vice versa (Evans et al. 2022). Technology is driven by business process; organisation set business goals, strategy, roles, and define relationship with both internal and external stakeholders while managing resources effectively; people are dynamic and with different behaviours but they are core integration of any organisation. Many scholars have adopted the Strategy, Technology, Organisation, People, and Environment (STOPE framework) (Bin-Abbas and Bakry 2014; Saleh and Alfantookh 2011; Bakry 2003). However, its context may not be fully applicable for the IoT. From the IoT perspective, the Strategy element can be considered as part of the organisation, which defines the strategy for its overall business operations. On the other hand, Environment is part of both Technology and Organisation, with Technology relating to environmental issues and Organisation dealing with external parties. Therefore, it is more relevant to adopt the 'TOP' as the three critical dimensions in the context of IoT. It is also crucial to recognise challenges based on the constitution of IoT – namely, the hardware, software, and processes of IoT technologies. Hardware is the sensors that detect and capture the events or changes of the surrounding environment; software processes and analyses the data captured based on the programmed instructions; and process is the IT Asset Lifecycle Management, which includes planning, acquiring, deploying, managing and retiring IT assets.

The following table presents a comprehensive list of IoT characteristics sourced from an extensive literature review. The table highlights the coverage of scholarly perspectives on IoT and maps how these characteristics are distributed across Technological, Organisational, and People factors. This categorisation serves two purposes: it demonstrates the wide-ranging and interdisciplinary of IoT research; and it lays the foundation for identifying where existing data governance frameworks fall short, since most focus on technical issues while underrepresenting organisational and people-related dimensions.

IoT Characteristics (Grouped with TOP)	References
(T) Enormous scale and wide range of adoption. e.g. more than ten thousand sensors in each Airbus wing.	(Covington and Carskadden 2013; Kitchin 2014; Ma et al. 2013; Barnaghi et al. 2015; Jurvansuu et al. 2013; Wang et al. 2015a; Tönjes et al. 2014; Lee 2018; Vermesan and Friess 2014; Lis and Otto 2020)
(T) Constant data collection and real-time data streaming. e.g. Traffic monitoring, radiation monitoring	(Kitchin 2014; Ma et al. 2013; Wang et al. 2015a; Tönjes et al. 2014; Yang et al. 2013)
(T) Dynamic Nature of status. e.g. due to mobility, sleeping & wakeup, connected & disconnected	(Ma et al. 2013; Tsai et al. 2014; Vermesan and Friess 2014)
(T) Semantic coherence. e.g. data need to be processed and integrated with other data so it can be interpreted to reflect the physical environment	(Barnaghi et al. 2015; Tönjes et al. 2014; Ishaq et al. 2013)
(T) Networked interconnection. e.g. to be able to communicate and share data across the Internet with other devices or interact with others.	(Silverio-Fernández et al. 2018; Manate et al. 2013; Kitchin 2014; Wang et al. 2015a; Burhanuddin et al. 2017; Borgia 2014)
(T) Automated Metadata Tagging. e.g. data collected are spontaneously tagged.	(Jian-Min et al. 2014)
(T) Mobility. e.g. portability has reduced the size of functioning devices.	(Covington and Carskadden 2013; Silverio-Fernández et al. 2018; Ma et al. 2013)
(T) Constant technology advancement and innovation. e.g. technological evolution causes more enhanced or additional features to be embedded.	(Karkouch et al. 2016; Swan 2012; Botta et al. 2014; Chen et al. 2014)
(O) Cross organisational accessibility. e.g. data on stock level is shared among Inventory Department, Logistic Department, Accounting Department.	(Jurvansuu et al. 2013; Sun et al. 2016)
(O) Data sharing with external party. e.g. connecting organisation with government, customer, supplier, and competitors.	(Jernigan et al. 2016; Wang et al. 2015a; Sun et al. 2016; Yang et al. 2013)
(O) Diverse in vendors and service developers. e.g. SQL & MongoDB & NoSQL.	(Jurvansuu et al. 2013; Wang et al. 2015a; Chen et al. 2014)
(O) Autonomy and self-recovery. e.g. performing task without direct human interaction.	(Silverio-Fernández et al. 2018; Kitchin 2014; Wang et al. 2015b; Wang et al. 2015a; Burhanuddin et al. 2017; Ishaq et al. 2013; Borgia 2014; Villamil et al. 2020)
(P) Multi discipline skill requirement. e.g. sensor data analysis, data centre management, predictive analysis, programming in Hadoop, and others.	(Jernigan et al. 2016)
(O) Customisation and personalisation. e.g. devices programmable to fit business requirements	(Lee 2018; Perera et al. 2014)
(O) Emerging IoT policies and regulation. e.g. guide to help organisation adopt IoT. Such as Amazon Web Service (AWS) IoT policies	(Lee 2018; Gubbi et al. 2013; Borgia 2014; Vermesan and Friess 2014)
(O) Industrial or area specific IoT guidelines. e.g. GSMA IoT Security Guidelines, EU AIOTI.	(Jorge Oliveira et al. 2017; Haller et al. 2008; Li et al. 2022)
(O) Ecosystem based. e.g. community or context dedicated, including medical, military, industrial, consumer	(Barnaghi et al. 2015; Yang et al. 2013; De Prieëlle et al. 2020)

IoT Characteristics (Grouped with TOP)	References
(T) Intelligence with embedded, action, reaction and responses. e.g. automation, action triggered functions, and etc.	(Silverio-Fernández et al. 2018; Villamil et al. 2020)
(T) Endpoint environment sensing capability. e.g. reflect physical environment in digital form.	(Silverio-Fernández et al. 2018; Manate et al. 2013; Chaudhary et al. 2019)

3. DATA GOVERNANCE FRAMEWORK EXEMPLARS

The literature on data governance presents a wide range of frameworks, each emphasising different priorities and contexts. Broadly, existing frameworks can be grouped into three streams of focus. First, enterprise-wide frameworks such as DAMA-DMBOK adopt a holistic perspective, integrating governance with multiple data management disciplines and emphasising alignment with organisational objectives. Second, compliance-oriented frameworks such as Microsoft's DGPC focus on privacy, confidentiality, and regulatory requirements, reflecting the strong influence of legal and compliance pressures in highly regulated industries. Third, practitioner-driven frameworks such as the DGI model and MIKE 2.0 address practical implementation challenges, with DGI highlighting stewardship, roles, and data quality, while MIKE 2.0 emphasises collaborative, open-source approaches to enterprise information management. Taken together, these frameworks illustrate the diversity of the literature's focus: some are comprehensive and high-level, others targeted to specific risks or industries, and still others designed for operational adoption. What unites them, however, is that they were all conceived primarily for traditional IT environments rather than for IoT ecosystems – a gap that motivates the need for IoT-specific adaptation. The following section briefly outlines four widely cited frameworks – DAMA-DMBOK, DGPC, DGI, and MIKE 2.0 - which together exemplify the main strands of existing governance literature.

DAMA-DMBOK (Data Management Association - Data Management Body of Knowledge)

In 2008, DAMA published a framework with ten distinctive components of data management (Mosley 2008). The author also outlines 102 activities in total for the ten components. These activities help to guide the designing and producing of a functional framework. It encompasses a more comprehensive range of areas and has been widely adopted in the industry. However, DMBok emphasis on data-at-rest rather than data-in-motion, whereas IoT context are characterised by real-time, dynamic workflows. While the framework is strong on *what* should be governed, it offer limited guidance on *how* to operationalise governance in IoT.

Data Governance for Privacy, Confidentiality and Compliance (DGPC)

Microsoft Data Governance for Privacy, Confidentiality and Compliance (DGPC) framework was introduced to address governance concerns centred on privacy, confidentiality, and regulatory compliance (Salido 2010). Salido argues that, beyond the well-known information lifecycle, an additional transfer stage creates a new governance dimension. DGPC is therefore best suited to compliance-driven contexts, particularly in highly regulated sectors such as healthcare and finance. Although Microsoft has not released a revised "DGPC" since 2010, the framework's emphasis on lifecycle-wide privacy, confidentiality, and compliance is reflected in Microsoft's current tooling – including Microsoft Purview (governance, classification, policy), Purview Compliance Manager (regulatory assessments and controls), and Microsoft Fabric governance (catalogue, lineage, and DLP).

Data Governance Institution (DGI) Framework

The DGI framework was developed by Thomas (2004) during a time when data was more centralised. It highlights that the DGI framework encompasses not only data quality, but also business intelligence and compliance. DGI emphasis on establishing a central Data Governance Office (DGO) and formalising roles like Data Owners and Data Stewards. However, DGI offers limited operational guidance for dynamic, decentralised IoT ecosystems. Its strengths in accountability and rule-setting are offset by limited focus on architecture, and metadata. Establishing and maintaining DGI data governance framework requires significant resources, including skilled personnel, tools and technology. It can be financially demanding, especially for organisations with limited resources.

Mike 2.0 (Information Governance Framework)

MIKE2.0 (Method for an Integrated Knowledge Environment) is an open-source, wiki-based framework for Enterprise Information Management (EIM) that was developed prior the "Big Data" era. Its key innovation was a collaborative, community-driven approach with publicly available resource for information professionals (Gregory 2011). However, in contrast to frameworks stewarded by major vendors or industry bodies, MIKE2.0 lacked a sustained central governing authority to drive updates, formal certification, and market adoption. As a result, it has been less visible as a de facto standard, which can make it harder to source practitioners with recognised credentials or to gain executive buy-in compared with more widely institutionalised frameworks.

4. IDENTIFIED GAPS IN THE LITERATURE

Overall, this literature review has illustrated that most IoT studies focus on the technological aspects and applications of IoT, with a lack of emphasis on the administrative aspects of the use of IoT. Synthesising the literature, the key gaps are:

- **Focus on Technology, Not Administration**: Most IoT studies focus on the technical and application-based aspects of IoT, leaving a significant gap in the administrative and data governance.
- **Organisational Blind Spots**: Organisations often prioritise the functional benefits of IoT technology and its resilience, but fail to integrate these considerations into a proper data management and governance framework.
- **Limited Guidance**: While some industry publications, like an IBM white paper, address IoT data governance, they often lack empirical evidence or a clear framework for implementation, and may not be relevant to the unique, process-level complexities of IoT.
- **Shift in Governance Needs**: Traditional data governance focused on internal controls, but IoT introduces new complexities, such as third-party control and external data maintenance, similar to cloud computing. This requires new roles and responsibilities to manage risks, privacy, and accountability.
- **Shared Decision-Making**: The increasing intelligence of IoT sensors means that decision-making is no longer solely human, necessitating a different governance approach to accommodate the shared roles of people and smart technology.

5. DISCUSSION

This review highlights the evolving needs brought about by the unique characteristics of the IoT. While existing frameworks - such as DAMA-DMBOK, DGPC, DGI, and Mike2.0 offer structured guidance for data governance in enterprise IT environments, they often fall short when applied to the complexities of IoT ecosystems, especially in addressing the unique characteristics of IoT discussed earlier.

A key finding is the lack of specificity in current frameworks regarding data generated by IoT devices. Unlike traditional IT systems, IoT environments are characterised by high data volume, velocity, variety, and volatility. The distributed, autonomous, and real-time nature of IoT data challenges data governance assumptions around ownership, managerial control, and data modelling. Traditional frameworks tend to emphasise centralised governance structures, whereas IoT systems demand more flexible, or edge-aware data governance mechanisms. Existing literature largely centres on technological concerns, with relatively limited attention to the managerial dimensions of IoT data governance. This imbalance raises concerns on the practicality and adoptability of data governance in IoT context. Another observation is that current research has yet to sufficiently integrate the success factors required for effective data governance in IoT environments. Factors such as stakeholder engagement, regulatory alignment, metadata design, and role clarity are mentioned sporadically but not cohesively embedded into a holistic governance strategy tailored for IoT.

These findings emphasise the urgent need for a dedicated data governance framework that is responsive to the distinct features of IoT. Such a framework must move beyond repurposing traditional models and instead accommodate ever changing and unique IoT characteristics. It should also consider how emerging technologies intersect with governance responsibilities, accountability mechanisms, and data modelling.

In summary, the literature review reveals the gap lies in the current practical limitations that hinder data governance in its real-world implementation. Addressing this gap will require interdisciplinary collaboration, sector-specific case studies, and empirical validation of governance models in IoT contexts.

REFERENCES

Abu-Elkheir M, Hayajneh M and Ali NA (2013) Data management for the internet of things: Design primitives and solution. Sensors 13(11), 15582-15612.

Aggarwal CC, Ashish N and Sheth A (2013) The Internet of Things: A Survey from the Data-Centric Perspective. Managing and Mining Sensor Data, 383-428. Doi: 10.1007/978-1-4614-6309-2_12.

Al-Ruithe M, Benkhelifa E and Hameed K (2016) A Conceptual Framework for Designing Data Governance for Cloud Computing. Procedia Computer Science 94, 160-167.

Alvi SA, Afzal B, Shah GA, Atzori L and Mahmood W (2015) Internet of multimedia things: Vision and challenges. Ad Hoc Networks 33, 87-111. Doi: http://dx.doi.org/10.1016/j.adhoc.2015.04.006.

Ashton K (2009) That 'internet of things' thing. RFiD Journal 22(7), 97-114.

Bakry SH (2003) Toward the development of a standard e-readiness assessment policy. International Journal of Network Management 13(2), 129-137. Doi: 10.1002/nem.466.

Barnaghi P, Bermudez-Edo M and Tonjes R (2015) Challenges for Quality of Data in Smart Cities. ACM Journal of Data and Information Quality 6(2-3), 1-4. Doi: 10.1145/2747881.

Bin-Abbas H and Bakry SH (2014) Assessment of IT governance in organizations: A simple integrated approach. Computers in Human Behavior 32, 261-267. Doi: https://doi.org/10.1016/j.chb.2013.12.019.
Borgia E (2014) The Internet of Things vision: Key features, applications and open issues. Computer Communications 54, 1-31. Doi: 10.1016/j.comcom.2014.09.008.
Botta A, de Donato W, Persico V and Pescape A (2014) On the Integration of Cloud Computing and Internet of Things. 2014 International Conference on Future Internet of Things and Cloud. IEEE - Computer Society.
Burhanuddin MA, Ismail R, Basiron H and Mohammed AA-J (2017) Internet of Things Architecture: Current Challenges and Future Direction of Research. Research India Publications.
Chaudhary S, Johari R, Bhatia R, Gupta K and Bhatnagar A (2019) CRAIoT: Concept, Review and Application(s) of IoT. IEEE.
Chen S, Hui X, Dake L, Bo H and Hucheng W (2014) A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective. IEEE Internet of Things Journal 1(4), 349-359. Doi: 10.1109/JIOT.2014.2337336.
Cooper J and James A (2009) Challenges for Database Management in the Internet of Things. IETE Technical Review 26(5), 320. Doi: 10.4103/0256-4602.55275.
Covington MJ and Carskadden R (2013) Threat implications of the Internet of Things. 2013 5th International Conference on Cyber Conflict (CYCON 2013).
De Prieëlle F, De Reuver M and Rezaei J (2020) The role of ecosystem data governance in adoption of data platforms by Internet-of-Things data providers: Case of Dutch horticulture industry. IEEE Transactions on Engineering Management 69(4), 940-950.
Evans N, Miklosik A, Bosua R and Qureshi A (2022) Digital business transformation: an experience-based holistic framework. IEEE Access 10, 121930-121939. Doi: 10.1109/ACCESS.2022.3221984.
Gregory A (2011) Data governance — Protecting and unleashing the value of your customer data assets. Journal of Direct, Data and Digital Marketing Practice 12(3), 230-248. Doi: 10.1057/dddmp.2010.41.
Gubbi J, Buyya R, Marusic S and Palaniswami M (2013) Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems 29(7), 1645-1660. Doi: 10.1016/j.future.2013.01.010.
Haller S, Karnouskos S and Schroth C (2008) The internet of things in an enterprise context. In: Future Internet Symposium. Springer, 14-28
Ishaq I, Carels D, Teklemariam G, Hoebeke J, Abeele F, Poorter E, Moerman I and Demeester P (2013) IETF Standardization in the Field of the Internet of Things (IoT): A Survey. Journal of Sensor and Actuator Networks 2(2), 235-287. Doi: 10.3390/jsan2020235.
Jernigan S, Kiron D and Ransbotham S (2016) Data Sharing and Analytics are Driving Success With IoT. MIT Sloan Management Review 58(1), 0.
Jian-Min B, Tian-Tian H, Lin P, He X and Hai-Feng H (2014) Heterogeneous Data Integration and Fusion System Based on Metadata Conflict Algorithms in USPIOT. 2014 International Conference on Wireless Communication and Sensor Network. IEEE, Wuhan, China.
Jorge Oliveira ES, João Cacho S, José Luís P, Francisco P and Manuel M (2017) Internet of Things: An Evolution of Development and Research area topics. Advances in Science, Technology and Engineering Systems 2(1), 240-247. Doi: 10.25046/aj020129.
Jurvansuu M, Belloni K, Ailisto H, Sihvonen S, Tukeva P, Aikio J, Virkkunen R, Kortelainen H, Heilala J and Rauma T (2013) Productivity leap with IoT: visions of the Internet of Things with a special focus on global asset management and smart lighting. VTT.
Karkouch A, Mousannif H, Al Moatassime H and Noel T (2016) Data quality in internet of things: A state-of-the-art survey. Journal of Network and Computer Applications 73, 57-81.
Khalid H, Kay HK and Robert H (2006) E-business capabilities model: Validation and comparison between adopter and non-adopter of e-business companies in UK. Journal of Manufacturing Technology Management 17(6), 806-828. Doi: doi:10.1108/17410380610678819.
Kitchin R (2014) The real-time city? Big data and smart urbanism. GeoJournal 79(1), 1-14. Doi: 10.1007/s10708-013-9516-8.
Lee G (2018) What roles should the government play in fostering the advancement of the internet of things? Telecommunications Policy.
Li S, Zhao S, Min G, Qi L and Liu G (2022) Lightweight Privacy-Preserving Scheme Using Homomorphic Encryption in Industrial Internet of Things. IEEE Internet of Things Journal 9(16), 14542-14550. Doi: 10.1109/JIOT.2021.3066427.
Lilly P (2016) Carelessly Unsecured IoT Devices Again Were Leveraged For Yesterday's Massive DDoS Attack. HotHardWare.
Lis D and Otto B (2020) Data governance in data ecosystems–Insights from organizations. AMCIS 2020 Proceedings.

Loh TY, Brito M, Bose N, Xu J and Tenekedjiev K (2019) Policy recommendations for autonomous underwater vehicle operations through hybrid Fuzzy System Dynamics Risk Analysis (FusDRA). In: International Association of Maritime Universities Conference (IAMUC) (30/10/19 - 01/11/19).

Ma M, Wang P and Chu C-H (2013) Data Management for Internet of Things: Challenges, Approaches and Opportunities. In: 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, 1144-1151

Manate B, Munteanu VI and Fortis T-F (2013) Towards a Scalable Multi-agent Architecture for Managing IoT Data. 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. IEEE Computer Society.

Misra N, Dixit Y, Al-Mallahi A, Bhullar MS, Upadhyay R and Martynenko A (2020) IoT, big data, and artificial intelligence in agriculture and food industry. IEEE Internet of Things Journal 9(9), 6305-6324.

Mosley M (2008) DAMA-DMBOK Functional Framework Version 3. DAMA International.

NASA (1999) Mars Climate Orbiter Mishap Investigation Board Phase I Report November 10, 1999.

Patra J, Gantait A and Mukherjee A (2018) Governing your IoT data. IoT solution governance Part 3.

Perera C, Zaslavsky A, Christen P and Georgakopoulos D (2014) Sensing as a service model for smart cities supported by Internet of Things. Transactions on Emerging Telecommunications Technologies 25(1), 81-93. Doi: 10.1002/ett.2704.

Pritika, Shanmugam B and Azam S (2023) Risk Assessment of Heterogeneous IoMT Devices: A Review. Technologies 2023 11(1), 31.

Qin Y, Sheng QZ, Falkner NJG, Dustdar S, Wang H and Vasilakos AV (2016) When things matter: A survey on data-centric internet of things. Journal of Network and Computer Applications 64, 137-153.

Saleh MS and Alfantookh A (2011) A new comprehensive framework for enterprise information security risk management. Applied Computing and Informatics 9(2), 107-118.

Salido J (2010) Data Governance for Privacy, Confidentiality and Compliance: A Holistic Approach. ISACA Journal 6, 17.

Sauser BJ, Reilly RR and Shenhar AJ (2009) Why projects fail? How contingency theory can provide new insights–A comparative analysis of NASA's Mars Climate Orbiter loss. International Journal of Project Management 27(7), 665-679.

Seo WJ and Evans N (2021) Internet of things adoption challenges in enterprise asset management organisations. In: th World Congress on Engineering Asset Management WSJ (ed). Switzerland Springer, Switzerland, 175-186. 10.1007/978-3-030-64228-0_16.

Sicari S, Rizzardi A, Cappiello C, Miorandi D and Coen-Porisini A (2018) Toward Data Governance in the Internet of Things. In: Yager RR and Pascual Espada J (eds), New Advances in the Internet of Things. Springer International Publishing, Cham, 59-74. 10.1007/978-3-319-58190-3_4.

Silverio-Fernández M, Renukappa S and Suresh SJViE (2018) What is a smart device? - a conceptualisation within the paradigm of the internet of things. Visualization in Engineering 6(1), 3.

Sun Y, Song H, Jara AJ and Bie R (2016) Internet of Things and Big Data Analytics for Smart and Connected Communities. IEEE Access 4, 766-773. Doi: 10.1109/ACCESS.2016.2529723.

Swan M (2012) Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0. Journal of Sensor and Actuator Networks 1(3), 217-253. Doi: 10.3390/jsan1030217.

Thomas G (2004) The DGI Data Governance Framework. The Data Governance Institute.

Tönjes R, Barnaghi P, Ali M, Mileo A, Hauswirth M, Ganz F, Ganea S, Kjærgaard B, Kuemper D and Nechifor S (2014) Real time iot stream processing and large-scale data analytics for smart city applications. In: poster session, European Conference on Networks and Communications. sn

Tsai C-W, Lai C-F, Chiang M-C and Yang LT (2014) Data Mining for Internet of Things: A Survey. IEEE Communications Surveys & Tutorials 16(1), 77-97. Doi: 10.1109/surv.2013.103013.00206.

Vermesan O and Friess P (2014) Internet of things-from research and innovation to market deployment. River Publishers Aalborg.

Villamil S, Hernández C and Tarazona G (2020) An overview of internet of things. Telkomnika 18(5), 2320-2327. Doi: 10.12928/TELKOMNIKA.v18i5.15911.

Wang H, Osen OL, Li G, Li W, Dai H-N and Zeng W (2015a) Big data and industrial Internet of Things for the maritime industry in Northwestern Norway.

Wang M, Tan J and Li Y (2015b) Design and implementation of enterprise asset management system based on IOT technology.

Yang L, Yang SH and Plotnick L (2013) How the internet of things technology enhances emergency response operations. Technological Forecasting and Social Change 80(9), 1854-1867.

