

HUOM! Tämä on alkuperäisen artikkelin rinnakkaistallenne. Rinnakkaistallenne saattaa erota alkuperäisestä sivutukseltaan ja painoasultaan.

Käytä viittauksessa alkuperäistä lähdettä:

Alamäki A., Mäki M. & Ratnayake, R. (2019). Privacy Concern, Data Quality and Trustworthiness of AI Analytics. Teoksessa Ketamo, H. & O'Rourke, P. (toim.): Proceedings of Fake Intelligence Online Summit 2019, May 7, Pori, Finland, ss. 37–42.

PLEASE NOTE! This is an electronic self-archived version of the original article. This reprint may differ from the original in pagination and typographic detail.

Please cite the original version:

Alamäki A., Mäki M. & Ratnayake, R. (2019). Privacy Concern, Data Quality and Trustworthiness of AI Analytics. In Ketamo, H. & O'Rourke, P. (eds.): Proceedings of Fake Intelligence Online Summit 2019, May 7, Pori, Finland, pp. 37–42.

The final version of the publication is available online: <http://urn.fi/URN:NBN:fi-fe2019051315372>

Copyright © Satakunta University of Applied Sciences, All rights reserved.

# Privacy Concern, Data Quality and Trustworthiness of AI-Analytics

ARI ALAMÄKI

*Haaga-Helia University of Applied Sciences, Ratapihantie 13, 00520 Helsinki, Finland, ari.alamaki@haaga-helia.fi*

MARKO MÄKI

*Haaga-Helia University of Applied Sciences, Helsinki, Finland*

R. M. CHANDIMA RATNAYAKE

*University of Stavanger, N-4036 Stavanger, Norway*

*The present study investigates the role of trustworthiness of data analytics from the data quality and privacy concern perspectives. In addition to the privacy concern of users, we investigated conceptually the requirements and impacts of data quality to the business processes. The goal of the conceptual analyze was to gain more knowledge about the factors affecting to the data quality, its accuracy and business impacts. The privacy concern is a part of data quality. The behavior of users is closely related to the data that they insert to the software systems. The research approach is the case study, that allowed to develop a new understanding of the relationship of privacy concern, data quality and trustworthiness of machine learning. The case study used the abductive qualitative research method, as the study aims to build a new conceptual understanding trustworthiness of AI-based data analytics. Using the iterative research process allowed for developing a deeper understanding while contributing to the conceptual models. The contribution of this paper is to show that data quality affects the trustworthiness of results. The privacy concern is a factor that influences indirectly to the trustworthiness. For the managerial implication, this paper suggests to put special emphasizes to the very first phases of data collection processes where human factors or sensor technological shortages might corrupt the data quality. To sum up, the present study underlines the importance of data quality, reliability and validity in different data categories. Data trustworthiness and data quality evaluation should be included to all marketing and business operations where data is utilized.*

## 1. Introduction

The trustworthiness of data analytics, privacy concern and data quality are interrelated concepts. Companies need the consent from users to use their personal information. This enables large, more accurate and detailed databases about the users' online behaviour. Furthermore, if users do not have privacy concern and they trust to the digital service provider, they probable do not fake their personal information in registering, filling and using the data collection menus of digital services. Privacy concern refers in this study to users' emotional uncertainty to provide consent or correct information to the digital service provider in using her or his personal information. The prior research points [1] (Fletcher, 2003) it out that there is a growing concern among users about having to reveal personal information. In addition, many users are not satisfied with the way in which service providers collect and use information [1] (Fletcher 2003). Furthermore, this research shows that privacy concern is very important for the users of digital services.

The quality of data is also essential for the trustworthiness of analytics generated by AI. Data quality refers the features of data that affects its consistency, integrity, accuracy and completeness. Thus, in developing artificial intelligence based solutions, it is important to identify the quality of data that the AI-systems processes. If users provide fake data as they do not trust the service provider or they do not allow to use their real data in a legal way, the data analyses concerning users' online behaviour might become trustworthiness. Similarly, the conclusions are inaccurate or even misleading if the quality of original data is poor.

The present study investigates the role of trustworthiness of data analytics from the data quality and privacy concern perspectives. In addition to the privacy concern of users, we investigated conceptually the requirements and impacts of data quality to the business processes. The goal of the conceptual analyze was to gain more knowledge about the factors affecting to the data quality, its accuracy and business impacts. The privacy concern is a part of data quality. The behavior of users is closely related to the data that they insert to the software systems.

The research approach is the case study, [2] that allowed to develop a new understanding of the relationship of privacy concern, data quality and trustworthiness of machine learning. The case study used the abductive qualitative research method, [3] as the study aims to build a new conceptual understanding trustworthiness of AI-based data analytics. Using the iterative research process allowed for developing a deeper understanding while contributing to the conceptual models. The abductive research method enabled us to build explanations about the phenomena by combining empirical findings of the

privacy concern survey to conceptual study and literature of data quality. In this research process, we simultaneously processed the prior literature and the analysis of the survey and conceptual study [2].

The aim of this paper is to focus on the relationship of privacy concern, data quality and trustworthiness of data analytics. There is little prior research on this relationship, and research on data privacy concern in connection with AI-based analytics is scant. The research questions of this study were as follows: To study empirically how users think about the privacy concern, to study conceptually data quality from the business perspective and how these findings contribute to the trustworthiness of machine learning capabilities.

## **2. Prior research on privacy concern**

The privacy concern is the natural part of users' online behavior. Privacy concern is related to the perceived risk that triggers the feeling of uncertainty. Thus, perceived risk estimation is a significant determinant of privacy concern [4]. The users may feel uncertainty while sending personal information to the digital services as the Internet-based information systems have ability to monitor, track and save their online behavior. The brand or reputation of service provider affect to the privacy concern. The research shows that users felt less concerned about privacy issues if they interacted with the service providers that they were able to trust [5,6]. Similarly, if users felt that service provider's data collection processes is fair, the users allowed easier to use their personal information [7].

The previous research [5,6,8] show that users differ from each other in terms of their privacy concern. Their individual factors affect to the level of privacy concern, but also the service provider based factors trigger privacy concern and uncertainty. According to the prior research, females have higher privacy concern than males, and healthy adults have also higher privacy concern than the ailing elderly [8]. The opportunity to control personal information on the digital sites decreased privacy concern [9]. Sjöberg [10] has found that users evaluate negative risks, such as online shopping risks, differently. The usage of digital services may generate several risks that can cause financial, functional physical or social consequences [11].

Any information is not similar from the users' perspective and trustworthiness. Users differ from each other in their privacy concern and information sensitivity. In addition to individual factors of users, the reputation, brand and other features of service providers affect to the degree of privacy concern. The recognizing the factors that influence to the privacy concern assist companies to design digital services and their customer support functions to meet the expectation of users. This impact directly to the users' willingness to provide consent to utilize their personal information in data analytics. Additionally, trust to the service provider improve the reliability of data analytics as users can trust that the service provider use their personal information anonymously and legal ways. Privacy concern may even create as a major obstacle for service providers the growth and develop their business [12]. It is also a significant source for incorrect analyse as machine learning cannot recognize false information that users who do not trust the service providers insert to the websites and social media applications.

Users differ from each other in terms of information sensitivity. Information type affects to the privacy concern as users evaluate sensitivity of information [4,9,12]. Information sensitivity is closely related to the information type, such as gender, age, politics, religion, contact information, social networks, purchase behavior, attitude or socio-economic information. Users allow easier to collect information that is public and general information, such as age and gender [13]. Additionally, they allow easier to collect information that does not include personal identification information [9]. Similarly, the information that they provide to the service provider also affects their privacy concern. All information is not similar, and users evaluate the sensitivity of information that they allow to use. Our study is align with the prior research that reveals that users differ from each other concerning their privacy concern.

## **3. Users' privacy concern in using digital services**

The companies collect user information from different digital touchpoints when they are using their digital services in searching, purchasing and using products and services [14]. Technologically digital service primarily use cookies in identifying the individual online behavior. There are also other means to identify individual users in the Internet, such as the IP-address and hardware MAC-address that help to identify the device. Additionally, users have logged in to many digital services that reveal their user profile and behavior from the personal data and users' own posts. For example, Google's and Facebook's services know more details about users than the most users can expect. Several mobile applications are constantly communicating to the external web-servers for writing various usage information to their databases, sometimes without formal permission [15]. The location features of mobile services send users' location information to the service providers. Despite to those invisible backend-roaming processes, users also share quite openly their personal information in the Internet. It is important to notice that although users have provided consent to use their information, but it does not guarantee that information that they insert is correct. Thus, it is important to research the users' privacy concern concerning the usage of digital services.

We investigated user's privacy concern related to the digital services. From the viewpoint of trustworthiness of analytics, service providers should receive consent from users to use their authentic data in analyzing user behavior. The reliable analytic requires trust samples of user behavior. The information that companies collect through digital channels relates, for example, to demographics, personal characteristics, contact information, purchase history, financial transactions or emotional issues. The companies collect data from various digital touchpoints when users are searching, reading, communicating, purchasing and using services digitally and physically.

Data for understanding privacy concern of users was collected among university students (N=299) in Finland, representing potential users of artificial intelligence-powered e-commerce, social media and functional systems. The sample is female-dominant: 67 percent (n=201) of the respondents are female and 33 percent (n=98) are male. The questionnaire was sent to participants in the email that included the web-link. We measured privacy concern using four questionnaire items adopted from Martin et al. (2017). The respondents were asked to rate value using a five-point Likert scale ranging from totally agree (5) to totally disagree (1).

We found that 60 % of the respondents were worried about data privacy threats, and similarly they state that privacy is very important to them. Thus, the survey shows that significant part of users are concerned about their privacy in the Internet, whereas only 2% disagree. Additionally, 84 % of respondents perceived important that their privacy will remain untouched by on-line companies. Over 80 % of users perceived important that they know why the websites collect data from them. The findings indicate that privacy is very important to the respondents.

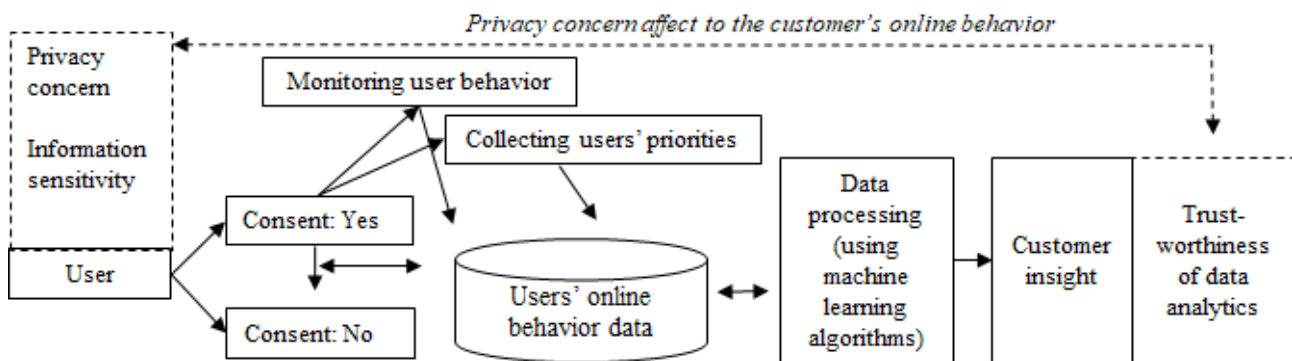


Fig. 1. The relationship of privacy concern and trustworthiness of AI-analytics.

The conceptual model (Fig. 1) illustrates how privacy concern of users and the sensitivity of information are related to the users' online behavior. The user may provide consent to use her or his personal information but it does not have causal connection to the trustworthiness of data analytics. The digital services are able to collect data in two ways; monitoring user behaviour by using e.g. cookies and collecting and saving users' direct comments, posts, writings or voice messages that they insert through the user interfaces of digital services.

#### 4. Data quality and machine learning from business process perspectives

Onshore and offshore industrial asset integrity assessment and control with the support of data analytics [i.e. together with machine learning (ML)] has been a significant challenge due to the data management difficulties arise by 'data quality'. For instance, Ratnayake and Kusumawardhani [16] have revealed that piping wall thickness reduction measurement data reliability is within the range of (82-90)% and (80-92)% for welds and bend respectively. Hence, operational/life cycle data requires thorough cleansing and preparation to be used as input to any analytics supported intelligent system. In this context, it is considered that data has a quality if they "fit for [its] intended uses in operations, decision making and planning and data is deemed of high quality if it correctly represents the real-world construct to which it refers" [17]. In an era of automated self-service analytics and intelligent systems, data quality has assumed even more significance as most of the users often have no prior knowledge or skills to differentiate between bad and good data. On the contrary, the piles of complex raw data are rapidly equipped with advanced analytics software tools supported by ML techniques (i.e. supervised or unsupervised) for extracting patterns to reflect competitive and actionable intelligence. However, modern IT systems are not yet fully capable of dealing with 'data quality', which directly has an impact on data extraction from multiple sources, data preparation, and data cleansing. This has been further exacerbated by heterogeneous data sources, high volumes of data, and a myriad of unstructured data types. The data quality has several dimensions: consistency, integrity, accuracy and completeness.

It is possible to assess data quality in relation to the level of compliance of a data set with a circumstantial normality in which the normality can be set by operational conditions' related and/or statistically (or empirically) derived rules. The data quality is contextual, in the sense that rules reflect the logic of particular industrial plant's design and fabrication resume, level of aging [i.e. "ageing is not about how old your equipment is; it is about its condition, and how that is changing over time" [18], geographical location (i.e. product and process conditions differs based on the production field [19], and regulatory concerns (i.e. Health, safety, environmental and societal conditions). For instance, a property (e.g. pumps, turbines, piping, structures, etc. in an offshore production and process facility) of the similar structural/ mechanical characteristics could have different validation rules depending on the operational environment or conditions [e.g. depending on the maturity of the production field [20] resulting different data quality requirements [i.e. reduced piping wall thickness as opposed to original design intent may not increase risk of a potential failure as the production well pressure goes down over the time; corrosion/erosion rates might be quite different at the end of the life, etc. [20] to make final assessments. Hence, the systems are in the need of exposing dirty, inaccurate or incomplete data when assessments, evaluations and recommendation about production components/clients have been made via data analytics.

In this context, an outlier is a critical operational discovery, or it can be an unknown/poorly-handled data. The worst case arises when the real-time decisions have been made by poor data with data analytics via ML. In this kind of situation, it may not be able to identify and handle poor data, which causes eventually, accidentally, or even intentionally to be fed them into the process. Hence, it is vital to integrate adaptive rule-based systems (i.e. to maintain circumstantial normality) to cater problematic situations resulting in poor-data quality entries in a way that the system will be able to recognize the level of quality and proactively notify the end users. This requires integrating risk-based assessments to evaluate the level of risk of serving data to the end users or to serve data whilst rising an alert/flagging about the level of risk of following the current recommendations. The aforementioned enables to mitigate data quality issues and improving the trust in data and data analytics, waste of resources and/or poor decisions. It is inherent fact that 'the things that do not measure, would not be able to manage' [21, 22], which does apply to the data quality. Hence, it is vital that the metadata underpinning an industrial data governance initiative to be assessed in relation to a set of metrics for data quality. Such assessment or measurement enables to benchmark current performance and to plan for future improvement. Figure 2 illustrates the metrics of data quality that has influence on assessment and control tasks, which deploy data analytics via ML.

The improved compliance is assessed in relation to the transparency of the risk potential fines, capital charges or reputational damage. The level of capability to satisfy regulatory requirements are assessed by knowledge of data sources, applicability and timeliness. The faster results are assessed in relation to the efficiency for accessing the data set to enable faster and better decision-making. Level of waste is assessed how the enhanced quality data can streamline operations across the overall target areas focusing on decreasing the risk of discrepancies and costly compromises, mitigating the occurrence of regulatory penalties, and minimizing the cost of unreliable data. It is possible to avoid using fake data having defined metrics and data quality assessment focus.

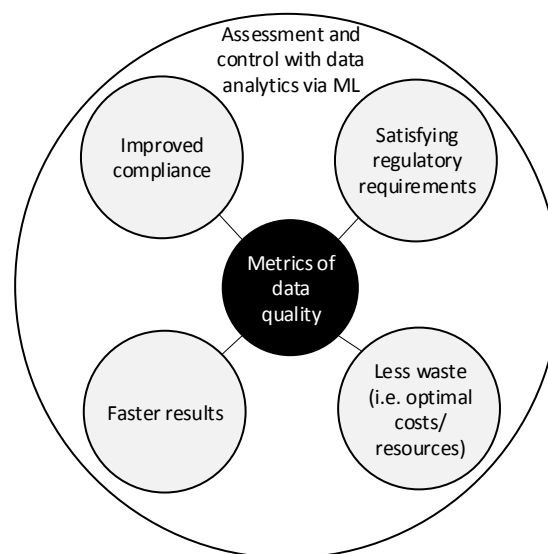


Fig. 2. Metrics of data quality assessment: data analytics via ML.

## 5. Discussion

This paper shows that data quality has several dimensions and factors that influence its trustworthiness. The trustworthiness is related to the accuracy, validity and business value of data. The privacy concern affects to the trustworthiness of data as users can manipulate information that they provide. The challenge for the most today's artificial intelligence system is that its machine learning is not able to recognize biased or corrupted data from the high quality data if data fulfills other requirements. In other words, the machine learning processes data but it is not able to evaluate the process how data is created. Data is often created, shared and managed in the business networks [23,24]. The trustworthiness of data is not the same thing than complete, integral and consistent data. Thus, data can fulfill "technically" the requirements although its content is biased or corrupted. Additionally, knowledge workers are often incapable to differentiate bad data from the high quality data if they do not know how data has been collected and pre-processed.

We summarized the findings to the Table 1. It presents different data how they are related to the user and business perspectives, reliability, validity, accuracy and machine learning. The fake data is an example of situation where users have provided wrong information or sensors' calibration have been broken and they are sending too low value. The knowledge workers or machine learning cannot recognize fake data from the high quality data. For example, the one in three users of a new digital service have told that they are younger and more educated than they are. The internet of things application measures temperature falsely as the exhaust of engine is heating its sensor. The incomplete data is easier to recognize as it has "technical" shortages, such as some values are missing. The compensatory data, such as testing or simulation data looks like the original high quality data but it is artificial. The outdated data have been collected from the real-life situation but its business value is out of date. Sometimes, data might become out of date within seconds like in the IoT-systems that control real-time processes of devices. The findings of this study is align with the research of data governance [25].

The contribution of this paper is to show that data quality affects the trustworthiness of results. The privacy concern is a factor that influences indirectly to the trustworthiness. For the managerial implication, this paper suggests to put special emphasizes to the very first phases of data collection processes where human factors or sensor technological shortages might corrupt the data quality. These human and technological factors merit further research.

TABLE I  
The relationship of privacy concern, data quality, trustworthiness of data and output of machine learning.

	High quality data	Fake data	Incomplete data	Compensatory data	Outdated data
<b>Definition</b>	Data represents sample, its sample size is sufficient for generalization and it does not have biases, etc.	Data looks like reliable and its sample size is sufficient but responders have given false information	Data represents the sample, but it has some faults or its sample size is too small for generalization	Data has not been collected from the real customers but it simulates the sample and it has been validated	Data represents sample and its sample size is sufficient but the actual situation that it measures is out of date.
<b>User perspective</b>	No privacy concern: users have trusted service provider or information is not sensitive	Privacy concern: users have not trusted service provider or information is sensitive	Privacy concern: users have not fully trusted service provider or information is sensitive	There is no users, information is highly sensitive or it cannot be used	No privacy concern: users have not updated information or they have rejected the service.
<b>Business perspective</b>	Data is consistent, integral and complete providing accurate results.	Data is consistent, integral and complete "technically" but its content is biased or corrupted.	Data is not consistent, integral or complete providing inaccurate results.	Data is consistent and integral providing accurate results with medium or high uncertainty	Data is consistent, integral and complete providing accurate results only from the history
<b>Reliability</b>	High	Low	Medium / Low	High / Medium	Low
<b>Validity</b>	Objective	Fake	Partly objective	Objective	Objective as history data
<b>Accuracy</b>	Reliable insight	False insight	Gives some hints or trends	Reliable insight	Trusted / Untrusted
<b>Ability to train machine learning</b>	ML is able to learn the patterns of real-life phenomena	ML is not able to learn the patterns of real-life phenomena, only fictional	ML has difficulties to create meaningful patterns and requires interaction of human experts	ML is able to learn the patterns of real phenomena, but results should be validated by the human expert	ML is partly able to learn the patterns of real-time phenomena if updated data is later available, and human expert validates results

## References

- [1] Fletcher, K. (2003). Consumer power and privacy: the changing nature of CRM. *International Journal of Advertising*, 22(2), 249-272.
- [2] Eisenhardt, K.M., Graebner, M.: Theory building from cases: opportunities and challenges. *Academy of Management Journal*, 50(1), 25-32 (2007)
- [3] Dubois, A., Gadde, L.E.: Systematic combining: An abductive approach to case research. *Journal of Business Research*, 55(7), 553-560 (2002)
- [4] Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22(3), 295-316.
- [5] Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information technology and management*, 6(2-3), 181-202.
- [6] Bleier, A., & Eisenbeiss, M. (2015). The importance of trust for personalized online advertising. *Journal of Retailing*, 91(3), 390-409.
- [7] Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, 10(1), 104-115.
- [8] Wilkowska, W., & Ziefle, M. (2012). Privacy and data security in E-health: Requirements from the user's perspective. *Health informatics journal*, 18(3), 191-201.
- [9] Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, 19(1), 27-41.
- [10] Sjöberg, L. (2000). Factors in Risk Perception. *Risk Analysis: An International Journal*, 20(1), 1-12.
- [11] Laroche, M., Bergeron, J. and Goutaland, C. (2003) "How intangibility affects perceived risk: the moderating role of knowledge and involvement", *Journal of Services Marketing*, Vol. 17 Iss: 2, pp.122 – 140
- [12] Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, 15(4), 336-355.
- [13] Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *International workshop on privacy enhancing technologies*(pp. 36-58). Springer, Berlin, Heidelberg.
- [14] Hallikainen, H., Alamäki, A., & Laukkanen, T. (2018). Individual preferences of digital touchpoints: A latent class analysis. *Journal of Retailing and Consumer Services*. Advanced online publication.
- [15] Yle, (2019) "Nokia 7 Plus handsets sent data to Chinese servers, broadcaster reports" YLE News [https://yle.fi/uutiset/osasto/news/nokia\\_7\\_plus\\_handsets\\_sent\\_data\\_to\\_chinese\\_servers\\_broadcaster\\_reports/10701132](https://yle.fi/uutiset/osasto/news/nokia_7_plus_handsets_sent_data_to_chinese_servers_broadcaster_reports/10701132)
- [16] Ratnayake, R.M.C., and Kusumawardhani, M., (2013), "Reliability analysis of condition monitoring data on aging plants: A case study from topside static mechanical systems", *Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, DOI: [10.1109/IEEM.2013.6962641](https://doi.org/10.1109/IEEM.2013.6962641)
- [17] Wikipedia (2019), "Data quality", [https://en.wikipedia.org/wiki/Data\\_quality](https://en.wikipedia.org/wiki/Data_quality) (accessed on 02.04.2019).
- [18] Horrocks P., Mansfield D., Parker K., Thomson J., Atkinson T., and Worsley J., (2010) "Managing Ageing Plant: A Summary Guide" <http://www.hse.gov.uk/research/rpdf/rr823-summary-guide.pdf> (accessed on 02.04.2019).
- [19] Ratnayake, R.M.C. (2012), " Challenges in Inspection Planning for Maintenance of Static Mechanical Equipment on Ageing Oil and Gas Production Plants: The State of the Art", *Proceedings of the ASME 31st International Conference on Ocean, Offshore and Arctic Engineering*, Paper No. OMAE2012-83248, pp. 91-103; doi:10.1115/OMAE2012-83248
- [20] Ratnayake, R.M.C., (2013), " Utilization of Piping Inspection Data for Continuous Improvement: A Methodology to Visualize Coverage and Finding Rates", *ASME 32nd International Conference on Ocean, Offshore and Arctic Engineering (OMAE2013)*, Paper No. OMAE2013-10025, pp. V003T03A001; doi:10.1115/OMAE2013-10025
- [21] Behn, B. (2005) 'On the philosophical and practical: resistance to measurement', *Public Management Report*, November, Vol. 3, No. 3, pp.1-2.
- [22] Ratnayake, R.M.C., and Markeset, T. (2010), "Implementing company policies in plant level asset operations: measuring organisational alignment ", *European Journal of Industrial Engineering* , Vol. 4, No. 3, pp. 355-371.
- [23] Alamäki, A, Rantala, T., Valkokari, K. and Palomäki, K. (2018). Business Roles in Creating Value from Data in Collaborative Networks". In Camarinha-Matos, L.M, Afsarmanesh, H. & Rezgui, Y. (Eds.) *Collaborative networks of cognitive systems. The proceedings of the 19th IFIP/SOCOLNET Working Conference on Virtual Enterprises, Pro-Ve 2018*, Cardiff, UK, September 17-19, 595-606.
- [24] Valkokari, K., Rantala, T., Alamäki, A. and Palomäki, K. (2018) Business Impacts of Technology Disruption – A Design Science Approach to Cognitive Systems' Adoption within Collaborative Networks". In Camarinha-Matos, L.M, Afsarmanesh, H. & Rezgui, Y. (Eds.) *Collaborative networks of cognitive systems. The proceedings of the 19th IFIP/SOCOLNET Working Conference on Virtual Enterprises, Pro-Ve 2018*, Cardiff, UK, September 17-19, 325-336
- [25] Aunimo, L., Alamäki, A. and Ketamo, H. (2019). Big Data Governance in Agile and Data-Driven Software Development: A Market Entry Case in the Educational Game Industry. In Strydom, S.K. & Strydom, M. (Eds.) *Big Data Governance and Perspectives in Knowledge Management*, 335 pages, IGI Global, pp. 179-199