Safeguarding Information in Service Science with Service Integration

Diego Padovan[1], *Javid* Taheri[2], *Fabrizio* d'Amore[3]

[1]Research & Digital Development, Civiltà Digitale – APS
[2]Department of Mathematics and Computer Science, Karlstad University Sweden
[3]Department of Computer, Control and Management Engineering Antonio Ruberti Sapienza Univiversity of Rome

Abstract. Service Science can be described through information, that underpins knowledge as enabler of service value chain. Therefore data, as a part of information, is a basic asset of the service market where undertakings constantly face high competition and try to protect such assets from malicious attackers. Information as to be preserved also for regulatory constraints, and traditional organizational models can have limits in doing so. In this paper it is discussed the possibility to manage both data protection and cyber security through an information security integrated management service (ISIMS). In fact, as per other cross-functional knowledge, information security and data privacy compliance can be managed via an integrated approach, as a possible evolution of the common organizational separation between their respective domains, namely Legal and IT. Moreover, this paper identifies major areas of benefits as well as current lack of integrated systems for information safeguard in Service Science.

1. Introduction

In today's interconnected business world, one of the main objectives is to manage efficiently and effectively information flows. This means to prevent data breaches, information alteration or unavailability, so as to avoid episodes where a single incident comprise millions of data loss, like credit cards leak back in January 2009 [1, 2]. Thus, most companies are constantly working on reduction of potential direct and indirect losses due to misuse, damage, destruction, or unavailability of information, using several approaches, including the implementation of an information security management system [3] and data protection tools. In order to avoid GDPR's fines and, at the same time, to save on the need to inform final users affected from data breaches, companies are using encryption to protect data, but this may be insufficient for such purposes, in spite lawyers often differently believe. The protection and security of company's data and systems became more and more important, representing a key factor even in terms of competitiveness, sustaining *de facto* the existence of enterprise [4] businesses.

This paper provides a literature review of relevant and recent papers from two research domains: information security and data protection, identifying the most common business approaches that are the most relevant in both cases and providing a new integrated and service-based approach.

As a matter of fact, Service Science combines human knowledge with technological understanding, employing service systems for value cocreation. At the same time, such combination of knowing can significantly improve the ability to design and scale service systems themselves [5], in which entities can cooperate for beneficial solutions. Likewise, considering people and technologies at the basis of Service Science, the latter is focused on knowledge elaboration through service systems with the objective to improve services provided to customers [6]. Therefore, innovation and research in Service Science is proceeding fast and it has been recognized that the emergence of Service Science [7] is fostering the need of a distinctive body of knowledge. The goal is to improve business models thanks to IT services as a commodity with cost benefits.

As a matter of fact, in the last decade new IT-based business models arose thanks to the dramatic Internet evolution and high-performance connectivity, which allowed service based on grid and cloud technologies. Consequently, vast amounts of data have been generated and distributed among data bases and networks around the globe. So, new ways of gathering, processing, and accessing information have supported innovation and competition, generating new service-based solutions in a smarter and more and more interconnected world [8, 9].

Thanks to this, today firms can benefit from access or temporary possession to other business services instead of paying for their ownership. Thus, new payment mechanisms for service market arose, like pay-per-use or access fees, stressing out an alternative view of Service Science implications. [10]

These new mechanisms lead to some adaptation by service-based businesses in terms of their organizational structure, and studies showed that developed countries are experiencing a migration of labour force to different service sectors. These sectors can be grouped into three basic system categories (i.e., Execute, Transform and Innovate) with two common specificities: basic knowledge and different supplementary professional competences [11]. For what concern knowledge, it is based on information composed by different kind of data, and its abundance poses challenging problem in the creation of efficient and secure service systems. So, the efficient integration, combination and reuse of data to customize services provided to users is fundamental to the economics of service activities [12].

2. Methods

This research identified studies and papers describing approaches for information security and data protection in Service Science and propose the use of an integrated service to manage such dual business requirement.

To do so, several sources has been taken into account: Google Scholar search engine, arXiv, SSRN, Elsevier, and GitHub.

It has been used articles published in the Service Science field of study using and combining the following keywords: Service Science, Data Management, Data Protection, Privacy, Cyber Security, Information Security, Integrated System, Organizational Model.

Analyzed studies are chosen by the criteria which follow, separating them in those that attempted to:

1. implement integrated systems on security and privacy activities for service-based firms
2. analyze new organizational models for information management in Service Science
3. analyze new business models or use case for information management and security in Service Science

Results has been sorted by number of citations, references and source relevance. A total of 51 publications was filtered among all of studies identified.

3. Information-based perspective

Service Science was launched by IBM in the early 2000s with the purpose of finding new, data-driven techniques for value generation thanks to knowledge integration from different domains. This implies changes in the organizations approach to service in the context of systems, and related relationship governance.

Considering that the value of data and analytics arose significantly in the past 5 years, today it is noticeable an exchange of data from many sources, including social media, boosting techniques of simulation and prediction for better value propositions, sustained also by customer digital transactions [13].

The business focus changed, from product-only perspective to a comprehensive approach, where processes are key elements for value creation. This entails a value increase of intangible assets, namely information, knowledge and human resources, where technologies are based on high capacity of data processing and described as knowledge technologies. In this light, ICT tools became basic elements of communication flows and stock of knowledge [14], namely a service management framework able to meet business goals and customer needs. Indeed, ITSM research field is de facto a subset of Service Science [15, 16].

The basic elements of Service Science can be described with a new model, namely through an information-based perspective.

To be more explicit if the core elements of Service Science are:

1. provider,
2. customer,
3. technology (enabler of customer-supplier relationship), and
4. multidisciplinary knowledge,

thanks to an information-centric perspective the Service Science basics can be reshaped and identified as follows:

1. Knowledge Holder (KH) - who detains information
2. Knowledge Provider (KP) - which interprets/provides resources of the KH
3. Knowledge user (KU) – who takes advantage from information
4. Knowledge – which is composed by information and data
5. Enabling Technology (ET) – which allows KUs to have access to KPs information and Knowledge

In this light, in Service Science there are rooms for a knowledge-based perspective [17], which in principle argues that the most important resource for the enterprise is the knowledge embedded in its employees and systems.

Therefore, in the Service Science sector, KHs need to protect such knowledge but KPs need to share it with KUs to cocreate value. Thus, the balance between the need to share information and its protection is a decisive exercise for service appreciation by KUs, that ultimately are customers.

In this paper, for the Service Science sector it is analysed the possibility to manage data protection and cyber security through an information security integrated management service (ISIMS), considering security and privacy cocreation is an important research topic. The ISIMS can foster value cocreation in service sector by virtue of the increasing weight that the risk analysis of data management has in strategic decisions and the ongoing regulatory changes on privacy field around the globe. This paper shows how the ISMS can manage efficiently the above-mentioned and contraposed balance of sharing and protection of knowledge, representing a turn-over from the traditional organizational separation between information security and data protection, an innovative approach, capable also to sustain enterprise architecture language to foster security and privacy cocreation.

4. Information security elements in Service Science

Information is the most important asset for computer-based industries as well as for other organizations, from governments, healthcare and education, to manufacturing, and retail sector.

Two authors [18, 19] describe security management on the basis of security policies, underpinned by security principles and regulations that define how to secure the organization and its information as a whole. Indeed, data and information are essential to meet business requirements and the most challenging and emerging issue became how to manage both privacy and security issues. Cloud Security Alliance (CSA) divides (Big) Data security and privacy into four main categories [20]: 1. Infrastructure security, 2. Data privacy, 3. Integrity and reactive security and 4. Data management. Considering the increase in big data heterogeneity, both data privacy and security challenges will increase in the future, stressing the need of future research on the field [21] of information privacy and security.

Information security is an ever-evolving complex issue for almost all businesses today. There are many recurrent problems in the cyber-space that can hit a company, from the proliferation and evolution of malware to phishing, thus companies seek for a reactive management on cyber security protection [22]. These threats occur on the basis of different likelihood and may have different negative outcomes, so technical and non-technical approaches are adopted in order to propose an information security framework capable to respond to such challenge [23]. A special role is played by cryptography, that can provide primitives for (symmetric or asymmetric) data encryption, data integrity and authenticity, and authentication. Even if modern solutions are well-performing, they often operate individually because they are designed for facing one only problem, and pretending they can simply overlap.

As a matter of fact, risk can be defined as effect of uncertainty on objectives [24, 25], and there are many other definitions by several international organizations and standards which can describe and manage the phenomena, for example ISO/IEC 27005 [26], ISO Guide 73:2009 [27], COSO [28] or NIST SP 800-30 [29].

Risk is the combination of likelihood and severity and can occur at different levels, thus has different effects and requires specific mitigation measures at any level [30]. In fact, all organizations are exposed to its underpinning security threats (e.g., malware, ransomware, phishing, denial of service, etc.), namely risks to their information systems, which in turns are risks to data control, often inadequately highlighting internal processes, people or systems [31]. To this extent, the risk management is recognized as a fundamental aspect of managing IT security risks [32].

At the basis of the most common risk management methodologies there is the risk assessment, which is a step-by-step process from the identification of risk sources and assets to risk estimation and prioritization. This means to analyse threats and vulnerabilities to determine how circumstances and events can adversely impact an organization and related likelihood [33]. An Information Security Management System (ISMS) planning phase is based on this process [34].

Moreover, the information security risk assessment (ISRA) starts with the definition and understanding of one of the two approaches to be used in the process itself: qualitative and quantitative [35]. In both cases, it should be considered that KHs can be found in relation of different assets, which often are placed also outside IT departments. This is also true for KPs, especially in consideration of data processed, which can be of personal nature or business sensitive, implying other department than legal involvement.

Furthermore, considering that risk management objective is to protect the organization itself, this implies the ability to protect people, IT and physical assets, as well as knowledge and know-how, which represent the core elements of value creation. This means to ensure confidentiality, integrity and availability (CIA) of information and related systems and securing the organization's resources [36].

According to several authors, achieving and maintaining CIA factors and IT services must be at an appropriate level, despite this is a complex activity because there is a need to manage risk with mitigating measures, taking into consideration business goals, insufficient amount of information, limited resources, and time constraints. In addition there are policies, that need to be established and at an appropriate level, because although the IT division knows risks and attacks very well, it is not prepared to make choices that are strategic for the company. In other words, somebody at the level of the board of directors should choose policies, and the IT department should only implement them.

More generally, this is a multicriteria decision-making (MCDM) problem, and a review of the literature highlights a significant application of MCDM in the context of risk assessment, as well as a need for a new hybrid model with the integration of information security elements [37]. There is a trend of research in hybrid models for risk analysis and assessment [38, 39], implying interdisciplinarity in conducting researches, and consequently integration with other business domains.

5. Data Protection key points in Service Science

Data protection, and more generally information protection, should be implemented in all information processes through logical, technical, physical and organizational measures that prevent data from loss of confidentiality, integrity and availability [40, 41, 42].

There are examples of inefficiency in a reactive, bottom-up, technology-centric approach to determining security and privacy requirements. [43]. Therefore, to reduce the risk of data breaches and other types of security incidents, the organization must be proactive and adopt preventive policies and related measures, including cryptography, that well fits and are proportionate to the organizational structure [44].

In a world changing at fast pace, where big data sources are ready to be integrated to enhance predictability analysis [45], data should be managed and shared in a secure way [46], taking into proper account people’s privacy. With the introduction of GDPR [47], companies are requested to implement rules and measures in performing data processing, as well as mechanism to foster security and privacy together, both from user and application oriented. The application of pseudonymisation or cryptography to personal data can reduce risks to data subjects concerned and help controllers and processors to meet their data-protection obligations, even if this may not be enough in the very next future. Indeed, new solutions to tackle security and privacy issues are necessary, otherwise the use of big data sources combined with new methodologies of data analysis will overcome current encryption and anonymization schemes, bringing computing techniques to reidentified unidentified data [48].

Thanks to the introduction of the new Regulation in EU (the GDPR), risk management concept is requested to be introduced in organizations processes in order to meet the principle of accountability, one of classic information security. Therefore, likelihood and severity of the risk is applicable even in the context of the rights and freedoms of the data subject and should be evaluated on the basis of an objective assessment. The aim at managing risks in data protection is to find measures to mitigate the risk of data loss of confidentiality, integrity, and availability, likewise for information security.

Today there are many companies that bring service in the field of data protection, from simple tools to support privacy compliance to software as a service (SaaS) product. This is a trend that has been boosted by the introduction of the GDPR, which is a regulation more focused than its predecessor [49] on processes and data flow mapping. Companies that offer data protection as a service (DPaaS) usually provide tools and services that can deliver compliance activities through a service model and help in securing data. DPaaS tools are provided on a cloud-basis, with possibilities of data backup solutions, integration with access controls tools, network virtualization tools, or firewalls. Moreover, the introduction of the Data Protection Officer (DPO) to ensure the compliance of organizational data processes with the GDPR, may directly influence the ability of organization to leverage data. This implies direct responsibilities on the way past data are processed, but even how predictive analysis are performed. Thus, the increase of the use of cloud-based services can bring to a DPaaS trend for companies.

6. Results

Data Protection and Information Security are sustaining the consistent evolution of business models. Failing in privacy and security measures implementation can lead to negative outcomes that can significantly prevent the value cocreation.

Today, more than in the past the capabilities and organizational structure of an organization, and its relations with customers are vital for business [50], but in the digital context these are not possible without implementation of data protection and information security mechanisms. The more synergies among these domains are developed the more efficiently value is created.

With regard of papers identified in this study, it emerges clearly that information is the most valuable asset in the digital world and personal data are a subset of information which have a great influence on how risk should be considered and mitigated within a company.

Moreover, there are several techniques and methodologies applied in the security sector, but data protection seems not yet fully integrated in such techniques and methodologies, rather privacy law and related measures are considered like external inputs.

It seems that there is a lack of literature and research which explore the possibility to integrate data privacy and security with information security, on the contrary all papers identified start from the assumption that IT departments continue to be the focal point for information security only.

It seems also that there is an upcoming trend in data protection as a service (DPaaS), thanks to the increase in cloud-based service adoption, but there have not founded evidence on synergies or interdependencies with information security domain, techniques, or tools.

There is a common view in papers identified that Service Science is more and more dependent from data processing and communication flows and emerge the need of companies to balance information sharing and its protection, due to the final goal of value creation for KUs, that ultimately are customers.

7. Conclusions

Thanks to results identified there are good basis to sustain that Service Science sector have rooms to manage data protection and cyber security through an information security integrated management service (ISIMS). Considering that security and privacy cocreation is an important research topic, the development of an ISIMS can foster value cocreation in service sector by virtue of the increasing weight that the risk analysis of data management has strategic decisions and the ongoing regulatory changes on privacy field around the globe.

It is true that the general principles are still coming from the requirements of information security but their integration, also with the requirements of sensitive data protection, is still far to be satisfactory. Confidentiality is obtained easily by cryptography but at which level should it operate? [50] In addition, there is access control (already used in DBMSs and operating systems) that can lead to confidentiality, but they are still used independently and are not integrated. Also, users want data integrity (not only for sensitive data), cryptography offers methods for ensuring it (e.g., keyed cryptographic hashing functions, digital signature) but the most correct and promising method is authenticated encryption, interesting and powerful, but not yet proved to be attack-resistant, although suspected. Access control is not integrated with authenticated encryption and poses several challenges that require ad-hoc design.

An ISMS can manage efficiently the above-mentioned and contraposed balance of sharing and protection of knowledge, starting from a turn-over from the traditional organizational separation between information security and data protection, an innovative approach, capable also to sustain enterprise architecture language [51] to foster security and privacy cocreation.

References

1. IBM Global CIO Study http://www-05.ibm.com/innovation/it/ciostudy/
2. Jaggi, S. ; Langberg, M. ; Katti, S. ; Ho, T., Resilient network coding in the presence of Byzantine adversaries , Browse Conference Publications > INFOCOM 2007, 26th IEEE
3. Leach, J. (2008): Do new information and communications technologies have a role to play in the achievement of education for all?. British Educational Research Journal, Vol. 34, No. 6, pp. 783-805. ISSN 1469-3518. DOI 10.1080/01411920802041392.
4. Marcela Hallová, Peter Polakovič, Edita Šilerová, Ivana Slováková: Data Protection and Security in SMEs under Enterprise Infrastructure. Agris on-line Papers in Economics and Informatics, Volume XI, Number 1, 2019
5. Paul P. Maglio & Jim Spohrer: Fundamentals of Service Science. Academy of Marketing Science, DOI 10.1007/s11747-007-0058-9 (2007)
6. Salvendy, G., Karwowski, W., Spohrer, J., Maglio, P.P.: Service Science: Toward a Smarter Planet. In: Introduction to Service Engineering. John Wiley (2010)
7. Chesbrough, Henry & Spohrer, Jim. (2006). A Research Manifesto for Services Science. Communication of the ACM. 49. 35-40. 10.1145/1139945.
8. Jim Spohrer, Paul P. Maglio, John Bailey, Dan Gruhl: Steps Toward a Science of Service Systems. IBM Research, DOI: 10.1109/MC.2007.33 (2007)
9. Spohrer, J., Maglio, P.P.: The Emergence of Service Science: Toward Systematic Service Innovations to Accelerate Co-Creation of Value. Production and Operations Management 17, 238–246 (2008)
10. Salvendy, G., Karwowski, W., Spohrer, J., Maglio, P.P.: Service Science: Toward a Smarter Planet. In: Introduction to Service Engineering. John Wiley (2010)
11. Monica Dragoicea, Theodor Borangiu: A Service Science Knowledge Environment in the Cloud. IFAC Proceedings Volumes, Volume 45, Issue 6, 2012, DOI: 10.3182/20120523-3-RO-2023.00438 (2012)

12. Lovelock C, Gummesson E.: Whither Services Marketing? In Search of a New Paradigm and Fresh Perspectives. Journal of Service Research. 2004;7(1):20-41. doi:10.1177/1094670504266131 (2004)
13. Borangiu T., Drăgoicea M., Oltean E., Iacob I. (2013) A Model for Open, On-Demand, Collaborative Education for Service Science. In: Falcão e Cunha J., Snene M., Nóvoa H. (eds) Exploring Services Science. IESS 2013. Lecture Notes in Business Information Processing, vol 143. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-36356-6_24

14 Theodor Borangiu, Francesco Polese (2017) Introduction to the Special Issue on Exploring Service Science for Data-Driven Service Design and Innovation. Service Science 9(4):v-x. https://doi.org/10.1287/serv.2017.0195

15. Resta B, Gaiardelli P, Cavalieri S, Dotti S (2016) Designing and configuring the value creation network for servitization. Borangiu T, Dragoicea M, Nóvoa H, eds. Exploring Services Science. Lecture Notes in Business Information Processing, Vol. 247 (Springer, Cham, Switzerland), 457–470.
16. Galup SD, Dattero R, Quan JJ, Conger S (2009) An overview of IT service management. Comm. ACM 52(5):124–127.
17. I. Nonaka e H. Takeuchi, The Knowledge Creating Company,NY; Oxford University Press, 1995
18. Wielky, J. (2017) "The impact of the internet of things concept development on changes in the operations of modern enterprises”, Polish Journal of Management Studies, Vol. 15, No. 1, pp. 262-275. ISSN 2081-7452. DOI 10.17512/pjms.2017.15.1.25.
19. Jones, P., Beynon-Davies, P. and Muir, E. (2003) "E-business barriers to growth within the SME sector”, Journal of Systems and Information Technology, Vol. 7, No. 2, pp. 1-25. ISSN 1328-7265. DOI 10.1108/13287260380000771.
20. V.N. Inukollu, S. Arsi, and S.R. Ravuri, Security issue Associated with Big data in Cloud Computing, Int. J. of Network Security and its Application, vol. 6, Issue 3, 2014
21. Christophe Feltus: Deriving Information System Security and Privacy From Value Cocreation Theory: Case Study in the Financial Sector. Luxembourg Institute of Science and Technology, Esch-sur-Alzette, LU
22. Dharminder Yadav, Himani Maheshwari, Umesh Chandra: Big Data Hadoop: Security and Privacy. 2nd International Conference on Advanced Computing and Software Engineering (ICACSE-2019)
23. Fielden, K. (2010): Information Security Framework, 2010 International Conference on Information Society, 25-30.
24. Muneeb-ul-Hasan, Siti Hajar Othman, Marina Md Arshad: A Conceptual Framework of Information Security Database Audit and Assessment. International Journal of Innovative Computing 9(1) 7-13
25. ISO 31000:2009. Risk management — Principles and guidelines

26 ISO/IEC 27005:2018. Information technology – Security Techniques – Information Security Risk Management, Switzerland

27 ISO Guide 73:2009. Risk Management – Vocabulary.

28. Enterprise Risk Management – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission (COSO), September 2004
29. Guide for Conducting Risk Assessments. Information Security, NIST Special Publication 800-30, Revision 1, September 2012. https://csrc.nist.gov/publications/detail/sp/800-30/rev-NIST Special Publication 800-30,

Revision 1, September 2012. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final, accessed on Jun. 21, 2018.

30. Mohyeddin, M.A., Gharaee, H. (2014). FAHP-TOPSIS risks ranking models in ISMS. Proceedings of the 7th International Symposium on Telecommunications (IST), Tehran, Iran, pp. 879-881. https://doi.org/10.1109/ISTEL.2014.7000827

31.Principles for the Sound Management of Operational Risk. Bank for International Settlements, June 2011.

32. Von Roessing, R. (2010). An Introduction to the Business Model for Information Security. ISACA

33. Guide for Conducting Risk Assessments. Information Security, NIST Special Publication 800-30, Revision 1, September 2012. https://csrc.nist.gov/publications/detail/sp/800-30/rev-NIST Special Publication 800-30, Revision 1, September 2012. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final, accessed on Jun. 21, 2018.

34. ISO/IEC 27001:2013. Information Technology – Security Techniques – Information Security Management Systems – Requirements, Switzerland, 2013.

35. Landoll, D.J. (2006). The Security Risk Assessment Handbook, A Complete Guide for Performing Security Risk Assessments. Auerbach Publications, Boca Raton, FL, US

36. Wheeler, E. (2011). Security Risk Management: Building an Information Security Risk Management Program from the Ground Up. Elsevier Inc., Waltham, MA, US.

37. Davor Maček, Ivan Magdalenić, Nina Begičević Ređep: A systematic literature review on the application of multicriteria decision making methods for information security risk assessment. International Journal of Safety and Security Engineering, Vol. 10, No. 2, April, 2020, pp. 161-174. https://doi.org/10.18280/ijsse.100202

38. Lo, C.C, Chen, W.J. (2012). A hybrid information security risk assessment procedure considering interdependences between controls. Expert Systems with Applications, 39(1): 247-257. https://doi.org/10.1016/j.eswa.2011.07.015

39. Lee, M.C. (2014). Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method. International Journal of Computer Science & Information Technology (IJCSIT), 1(1): 29-45. https://doi.org/10.5121/ijcsit.2014.6103

40. Bresnahan, T., Brynjolfsson, E. and Hitt, L. M. (2002) "Information technology workplace organisation and demand for skilled labour: firm level evidence", Quarterly Journal of Economics, Vol. 117, No. 1, pp. 339-76. ISSN 0033-5533. DOI 10.3386/w7136.

41. Zairi, M. and Sinclair, D. (1995) "Business process re-engineering and process management", Business Process Management Journal, Vol. 1, No. 1, pp. 161-173. ISSN 1463-7154.

42. Maglio, P. P., Vargo, S. L., Caswell, N. and Spohrer, J. (2009) "The service systemis the basic abstraction of the Service Science", Information Systems and eBusiness Management, Vol. 7, No. 4, pp. 395-406. ISSN 1617-9846.

43. David Houlding, MSc, CISSP: « Health Information at Risk: Successful Strategies for Healthcare Security and Privacy » Healthcare IT Program Office Intel Corporation, white paper 2011

44. Fabrizio d'Amore, Paolo Fantozzi, Luigi Laura, Diego Padovan: On Enterprise Data Encryption: Good, Bad and Ugly, in press 2021, accepted paper MENACIS 2020

45. Diego Padovan: Contact Tracing Tools and Social Media Platforms Analysis of Crossing Big Data Sources. In press 2021, accepted paper ICTO 2020.

46. A. Kiran: Privacy and Security in Big Data Management. International Journal in recent trends in engineering research, ISSN (online) 2455 – 1457
47. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
48. C.L.P. Chen, C.Y. Zhang, "Data Intensive applications, challenges, techniques and technologies: A survey on Big Data", Information Sciences, vol. 275, pp.314-347, 2014.
49. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
50. Baines T, Lightfoot H (2013) Servitization of the manufacturing firm: Exploring the operations practices and technologies that deliver advanced services. Internat. J. Oper. Production Management 34(1):2–35
51. Christophe Feltus: Deriving Information System Security and Privacy From Value Cocreation Theory: Case Study in the Financial Sector. International Journal of Service Science, Management, Engineering, and Technology, Volume 10 • Issue 4 • October-December 2019