Computers in Industry 94 (2018) 52–61

Contents lists available at ScienceDirect

Computers in Industry

journal homepage: www.elsevier.com/locate/compind

An argumentation reasoning approach for data processing

Erisa Karafili[a,*], Konstantina Spanaki[b], Emil C. Lupu[a]

[a] Department of Computing, Imperial College London, 180 Queen's Gate, SW7 2AZ London, UK
[b] School of Business and Economics, Loughborough University, LE11 3TU Leicestershire, UK

ARTICLE INFO

Article history:
Received 31 May 2017
Accepted 8 September 2017
Available online xxx

Keywords:
Data processing
Data quality
Usage control
Argumentation reasoning
Data manufacturing
Case scenarios

ABSTRACT

Data-intensive environments enable us to capture information and knowledge about the physical surroundings, to optimise our resources, enjoy personalised services and gain unprecedented insights into our lives. However, to obtain these endeavours extracted from the data, this data should be generated, collected and the insight should be exploited. Following an argumentation reasoning approach for data processing and building on the theoretical background of data management, we highlight the importance of data sharing agreements (DSAs) and quality attributes for the proposed data processing mechanism. The proposed approach is taking into account the DSAs and usage policies as well as the quality attributes of the data, which were previously neglected compared to existing methods in the data processing and management field. Previous research provided techniques towards this direction; however, a more intensive research approach for processing techniques should be introduced for the future to enhance the value creation from the data and new strategies should be formed around this data generated daily from various devices and sources.

© 2017 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

1. Introduction

Big data paradigm as a shifting phenomenon [14,33,7,40] provides access to a large pool of data resources; coupled with new storage, management and analytical techniques. These unprecedented opportunities arising from 'Big Data' are stressing firms to position themselves within this highly competitive data-intensive scheme, altering the way they generate, collect and transform data to actionable knowledge [10]. Gaining a competitive posture requires more than analytical techniques [36]; making sense [68] of this data is the challenge of organisations, forming a new way of data-based decision-making, disrupting the business landscape while moving from the world of "making things" to a "world of outcomes" [44]. The industrial world was disruptively changed during the last century; while the manufacturing process has gone through multiple revolutions (agricultural, industrial, digital etc.) and respectively multiple alterations in the way products and services are formed. A critical view of the literature associated with the manufacturing context [41,62] of the last decades, reveals that this evolution around data has influenced radically also the production, distribution and supply chain world.

The data evolution (also often referred as "Big Data" evolution) has also accelerated the popularity of service industries around data (for storing, analysing, processing etc.). In the context of these data services; myriads of data are shared as well as stored, used and transformed, not only by users but also by companies, organisations, and governments. Security concerns regarding shared data, e.g., privacy, confidentiality, integrity, and the necessity of protecting them are becoming serious issues. Towards this direction, the regulatory and legislative environment is continuously updated for meeting citizens' rights, protecting their data privacy, anonymity, and security. The regulatory and legislative implications of security issues are becoming rather more severe when we extend the scope across the immediate organisational, governmental or even country borders; where multiple legislative domains are applied, and frequently they lead to conflicting behaviours and interests. Exchanging data implies that all parties agree on the associated rules to be enforced; this is often referred as a data sharing agreement [59] (DSA). The DSA can be seen as a contract, between two or more parties, and the different rules are the terms of the contract. The terms express how and who is permitted or denied to access, delete, use, and share the data, along with the different constraints that should be respected.

* Corresponding author.
E-mail addresses: e.karafili@imperial.ac.uk (E. Karafili), k.spanaki@lboro.ac.uk (K. Spanaki), e.c.lupu@imperial.ac.uk (E.C. Lupu).

http://dx.doi.org/10.1016/j.compind.2017.09.002
0166-3615/© 2017 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

The enforcement is done when the data are used, and it evaluates the requests and usage of the data against the set agreements.

Constructing and representing DSAs is not trivial, as they should incorporate data access and usage rules for the security and privacy of the data, as well as users preferences, business and legislative rules applicable to that case. All the above rules are applied to the same bunch of data; therefore there can be conflicting behaviours between rules, and differentiated legislative, regulatory rules and domain contexts that bring inconsistencies inside the DSAs rules. Different techniques [42,63,70] were introduced for data services towards various security solutions, with a major focus on data access permissions and an efficient usage control [17,69], suitable for stored or integrated data from multiple parties and sources. Access and usage control is a well-studied research area [39,53], however the existing solutions do not permit a fine grained representation of the different types of rules and their constraints, as well as the associated conflict detection and resolution.

The aim of this study is to propose a novel data processing technique using a policy analysis language for the representation of the sharing agreements and quality attributes of the data. We extend our research scope in an industrial context where the data quality control should also be studied as it is often a neglected aspect in the context of data sharing agreements. Initially, we provide the theoretical background where this study was based, coupling two streams of literature. Previous research in data management was examined in order to explain the data manufacturing analogy and the quality problem which was also highlighted in past decades, as well as the data access and usage control background for building the concepts associated with DSAs. The following sections develop the proposed methodological approach based on a policy language for argumentation and abductive reasoning used in the data processing context, and its explanation through a use case scenario and the relevant analysis and representation. Our study ends up with a research agenda for the future implications of this approach, as well as how this can be extended and applied in industrial data-intensive environments.

2. Theoretical background

The analogy of the data processing to the manufacturing processing of physical materials is prevalent in the literature of data management. There are many similarities between the mechanisms of data processing and the manufacturing processing; however, there are some significant differences. In a manufacturing process, physical materials are input into a process, the materials are transformed, and the resulting output is a manufacturing product. In the data processing, the data represent the input into the processing mechanism, and a transformed data product is the output of the process. Data of bad quality used through the data process will remain bad until the quality is improved (until the problem is actively cleaned up or removed). Data sharing controls were not well-studied in previous decades, as the data were mostly shared within the boundaries of a company or between single databases, where the trust and security issues were solved by the individual sharing entities and the associated agreements between interested parties.

The data manufacturing framing presented in data management literature of the previous decades should be extended in a context across boundaries between individuals, firms and countries and the target should be tailored data products, as these are mostly the results of the data evolution. Data manufacturing analogy was based on the data artefact as a unit of analysis; however, data era requires novel techniques focusing on the processing of data but not solely on their processing mechanism, but also the quality and sharing attributes associated with them. This section will explore the previous research of data management and data sharing literature, with the view to provide a background for the problem area and how this is expanded in a data-intensive industrial context.

2.1. Data management and quality attributes

Plenty of examples nowadays can provide evidence that companies from multiple industries invest in data management solutions, with the view to improve and expand the production of enterprises through the use of their analytical skills, or by viewing and optimising their supply chains of their core business [62,61]. Although data can be used along with the core business focus in different industries, the recent data evolution expanded the business scope and disrupted the operating models providing opportunities to process this data, create new data and information products/services and also to resell and exchange this data. Reviews of the literature in the context of data management in an industrial context mostly focus on “Supply Chain Analytics (SCA)” [64] as a way in “developing supply chain strategies and efficiently managing supply chain operations at tactical and operational levels” [64]. Supply Chain Management (SCM) focuses mostly on how the analytics can be applied to strategic decisions related to SCM [64,62], how efficiency and effectiveness of supply chains can be improved through the use of data [61] as well as the data strategies and servitization around supply chains [46]. This direction reflects that the research focuses mostly the use of data within an industrial context; nevertheless, our research focus will be on data processing techniques, setting data manufacturing analogy from data management literature as the main theoretical background, analogous to the product/service manufacturing processes. Literature reviews and frameworks referring to data/information processing are presented and summarised in Table 1, in Appendix A. This summary reveals that data analogous to physical materials are moved through a manufacturing process which reshapes/reconfigures them in information/data products.

Data processing was initially introduced by Brodie [6] through the analogy between product manufacturing and data manufacturing when data quality was a primary concern in transforming data to valid information and knowledge [1]. Some of the most indicative studies around these areas developed the concept of data manufacturing analogy in order to find out the path for better data quality [38,1,18] and they provided frameworks to describe and track data manufacturing process [65,2,66,56]. A simple framework of input-process-output describing the similarities between the two manufacturing processes was proposed in [66] and calls for continuously defining, measuring, analysing, and improving data quality. Mostly, the data manufacturing analogy was focusing on data quality and the ways to ensure that we can trust the data we use in manufacturing processes. Recent studies following the data manufacturing path can be considered those in [19,16] where they introduce the need for continuous improvement in the SCM data production process, suggesting a framework for establishing a data quality control mechanism. These two studies are investigating the data manufacturing process via a data quality lens and expand the research focus to new topics related to the processing of data, and how to improve the quality of this data with the use of various techniques and methods.

2.2. Data access and usage control

Research around data sharing has provided data-centric solutions for protecting the used and shared data, aside from focusing on protecting the databases where they are stored [15], the network used for their transfer [28], or constructing

coordination techniques for data re-use [25]. The focus in data-centric solution is due to the increase in the connectivity and the diversity of attacks. Protecting and ensuring the security of all the environments where the data are collected, processed, and shared is a major challenge for all the interested parties. Therefore, data-centric security solutions have an important position in the literature [4,31,42,63,70] with focus on protecting data transfers and transactions. Data-centric security solutions present two main challenges: the control of data access and the usage of data. Both of them, have been widely studied and various solutions are developed for solving these problems [34,12].

Previous approaches in role-based access control [12] are based on different user roles for data access controls. Motivated by this direction, we will expand these aspects with a data representation technique for different user roles with specific access and usage policies for the data. Usage control (UCON) [48] is a widely studied concept following different approaches, for controlling the access and usage of digital information emphasising the problem of rights delegation [47], or a two level policy language that represents the notions of prohibition and obligation, and a generic server-side architecture for UCON [52]. Applications of UCON are also presented in the context of distributed systems [29], when having a data flow in-between different connected systems, or in the context of multiple distributed systems as a fully decentralised infrastructure for enforcement of global usage control [30]. Our work is building on the previous research of UCON while expanding the scope regarding the policies that represent permissions, denials, obligations and delegations of rights.

Another interesting approach to sharing and accessing data is the use of sticky policies [42,43]. Sticky policies are machine readable policies that contain conditions and constraints attached to data that describe how the data should be treated while shared among multiple parties. The sticky policy paradigm [27] and technologies for enterprise privacy enforcement and exchange of customer data are represented through a privacy control language [26] for specified privacy rights and obligations. The privacy control language presents authorisation management and access control for user consents, obligations and distributed administration, with the extension of the sticky policy paradigm also for the cloud environment [49,60]. Our research will build on the policy language for policy representation and will expand the application of this technique in the industrial use of data.

Data usage concerns are usually expressed by the different entities using the data. These entities, before creating, sharing and using the data, should agree regarding the different rules that describe how the data should be treated, called data sharing agreements [59] (DSAs). The DSAs describe not only the agreements between the involved parties but also the compliance to the different business, legislative and regulatory rules for the various contexts of the data sharing. A language representation of different rules for data sharing agreements (DSAs) as presented by [39] fails to provide expressivity. This language cannot permit the representation of complex DSAs, as well as analysis for the DSAs and leaves unsolved the problem of deciding which rules to apply to the DSAs.

All the above-represented approaches, from the data access and usage control to the sticky policies and finally the DSAs representation, seem incomplete to provide a decision background for the rules that should apply to the shared data. Following this motivation, we propose a combinatory analysis of the rules with a conflict resolution technique. The proposed analysis is an enhancement of the one introduced in [24,23], as we enrich it with data quality analysis that can be easily extended for big data applications. Our solution is based on abductive [22] and argumentation based reasoning approach [5,11], as this technique can facilitate decision making mechanisms [21,3] under conflicting knowledge.

2.3. Introduction to the use case scenario

In this work, we show our data processing technique based on DSAs in a realistic use case. Let us introduce our scenario, taken from an e-health example of a European Project (Coco Cloud project[1]). In this use case, the data needs to be collected, processed and shared between different actors, e.g., data subject, data controller, recipients, and data processor. The actors need to stipulate agreements between each other that describe how the data should be treated, the data sharing agreements, composed of security, legislative and business rules. Deciding the rules to apply to particular cases is not trivial, as various conflicts might arise. The conflicts need to be captured and solved.

One of the main actors is the *data subject*, in our use case is the patient, some of his rights are to access/delete his medical data and to know who is processing his data. The *data controller* is an entity (public authority, agency, legal person), which determines the purpose and means of processing the data of the data subject. In our use case, the hospital is the data controller of the patient's data and determines the purpose for which the data are processed (e.g., administrative purpose or treatment purpose). The doctors of the hospital are the *data recipients* that need to comply with the data controller rules. The data recipients are considered as part of the data controller, the employees within the hospital do not stand as separate entities than the hospital itself. The hospital that is the data controller has various rules of how the doctors can access the patient's data, e.g., a doctor needs to be inside the hospital for accessing the patient's data (geographical constraint), he needs to be during his office hours (temporal constraint), and he needs to be the patient's treating doctor (role-based constraint).

The *data processor* is an entity (public authority, agency, legal person) that is processing the data on behalf of the controller. In our use case, the cloud provider is considered the data processor as far as it respects the instructions of the controller. The controller rules that should be respected by the processor can also have a legal nature, e.g., if the controller is in an EU country, the cloud provider should as well be in an EU country and cannot send the data to countries outside the EU and EEA.

A *third party* is an entity (public authority, agency, legal person) that is not the data subject, data controller or processor, and that under the direct authority of the controller or processor is authorised to process the data. In our use case, a doctor outside the controller hospital is considered a third party. Once access is obtained, the third party becomes a data controller and has to comply with the data protection principals. The patient can be in different situations, e.g., intensive treatment, unconscious, emergency, that affect how the data are shared and used.

3. Methodology

The study presents the proposed approach, where the bunches of data are processed from different entities. The latter establish different agreements between each other, called data sharing agreements. The DSAs are composed of various constraints and rules. We use an expressive policy analysis language for representing the DSAs. An important aspect of the data processing mechanism is data quality. We enrich the policy language to capture various data quality properties like accessibility, timeliness and accuracy. The used policy language permits the analysis of the various policies and the detection of the rising conflicts,

[1] http://www.coco-cloud.eu/.

redundancies or the missing cases. The proposed method implements an analysis and representation based on argumentation and abductive reasoning to capture and solve conflicts between context dependent rules. The introduced analysis permits the construction of correct and efficient DSAs that apply in different contexts during the processing of data.

3.1. Policy language for DSA and data quality representation

The proposed model is based on the policy analysis language [8] that is constructed using the Event Calculus [32]. This language represents the required rules and constraints during the access, usage and sharing of data. The policy regulation rules are composed of predicates and domain description ones, and represent authorisation and obligation rules, and have in their structure *subject*, *targets*, and *actions*.[2] Some of the predicates of the policy language are introduced below.

$req(Sub, Tar, Act, T)$ $\quad obl(Sub, Tar, Act, T_s, T_e, T)$
$permitted(Sub, Tar, Act, T)$ $\quad denied(Sub, Tar, Act, T)$

The above predicates represent correspondingly: a request made from the subject *Sub*, at the instant of time *T*, to perform a certain action *Act* at the target *Tar*; the obligation for a given subject to perform an action during the period of time from T_s to T_e; that a given subject is permitted/denied at time *T*, to perform a certain action to the target. A domain description predicate is *holdsAt*, which means that a given property/predicate is true at a given instant of time. The used policy language can represent the permission, denial and obligation concepts for the DSAs. In the following examples, we introduce the representation of some DSAs rules from our use case.

Example 1. Bob (*B*) is the family doctor (*fDoc*) of the patient Alice. The family doctor has the permission to access Alice's prescriptions,[3] (*A_presc*), at the instant of time *T*.

$$permitted(B, A_presc, access, T) \leftarrow holdsAt(fDoc(B, Alice), T), holdsAt(owner(Alice, A_presc), T).$$

Example 2. The hospital (*H*), where Alice was hospitalized (*hosp*), needs to delete her data at maximum 2 years (700 days) after she was discharged, (*disc*), from the hospital.

$$obl(H, A_presc, delete, T_2, T, T_1) \leftarrow holdsAt(hosp(Alice, H), T_1), holdsAt(disc(Alice, H), T_2), holdsAt(owner(Alice, A_presc), T_2), T_1 < T_2,\ T > T_2,\ T \leq T_2 + 700.$$

Example 3. Bob can access Alice's prescriptions when he is inside the hospital. For ensuring that Bob is inside the hospital we use *pos*(*Bob*, *Location*) that gives Bob's location, and *hospP* (*Hospital*, *Location*) that gives the hospital geographical location. Thus, we use the function *same*(L_1, L_2) that checks if the two given locations L_1, L_2, are the same or are geographically nearby each other, to be considered the same location.

$$permitted(B, A_presc, access, T) \leftarrow holdsAt(fDoc(B, Alice), T), holdsAt(owner(Alice, A_presc), T), holdsAt(work(B, H), T), holdsAt(hospP(H, L_1), T), holdsAt(pos(B, L_2), T), same(L_1, L_2).$$

3.1.1. Ensuring data quality

The used policy language permits the representation of different predicates, authorisation, and obligation policies, together with domain description policies. The sharing and usage of data bring the need of describing other properties related to the quality of the collected data. When working with data quality the entities that are using, sharing, storing the data are called *data consumers*. In our case, the data consumers are considered the data collectors and the data processors. The data quality is a major factor when we are working with data consumers, where *data quality* is defined as data that are fit to be used by data consumers [67]. Through our DSAs representation and the applied policies, we grant an important characteristic of data quality, which is the data *accessibility*. We ensure the data accessibility that complies with the constraints for accessing the data.

3.1.2. Timeliness/freshness

Another important data quality characteristic is data *timeliness*, or better the degree to which data represent reality from the required point in time when the event occurred. For the context we are working on, generally, the data have a specific subject and a data controller that together with the various legislations and business rules can decide the different policies to be used for accessing and using the data. For representing the data timeliness, we use the concept of data *freshness*. Data freshness is a predicate that expresses the last time when a given piece of data has been updated: *freshness*(*Tar*, *T*), where *Tar* is the targeted data, and *T* is the last instant of time when the data were updated. Through the use of the *freshness* predicate, we are able to represent the data timeliness depending on the different contexts. Let us see how we can apply the above predicate to our use case.

Example 4. Suppose that a patient is hospitalized for a particular illness or symptoms related to an illness that is still being studied. He is offered to be part of a pilot project, and give the consent of sharing his medical data (anonymized/ sanitised) with a team of researchers. Therefore, the patient will be monitored/ visited in specific instants/intervals of time, e.g., the doctor should visit, (*visit*), the patient every four hours. For granting the data timeliness,[4] every time the patient is visited/ monitored his medical data are updated, *upd*. In case, there are no changes to the patient's data (e.g., same vital functions) the old data are confirmed for that instant of time.

$$freshness(Tar, T) \leftarrow fulfilled(Sub_1, Tar, upd, T', T_e, T'), holdsAt(visit(Sub_1, P), T'), holdsAt(owner(P, Tar), T'), \mathbf{not}\ holdsAt(visit(Sub_2, P), T''), freshness(Tar, T'''), T_e > T > T', T' > T'' > T'''.$$

The above predicate states that the given data (*Tar*) at the instant of time *T* are fresh, as the data of the patient are updated, every time the patient is visited. A deontic obligation holds for the doctor to update the patient's medical data every time he visits the patient.

$$fulfilled(Sub, Tar, T, T_e, T) \leftarrow obl(Sub, Tar, upd, T, T_e, T), holdsAt(Sub, Tar, upd, T).$$

$$obl(Sub, Tar, update, T, T_e, T) \leftarrow holdsAt(Sub, P, visit, T), holdsAt(owner(P, Tar), T), T_e > T.$$

[2] For the sake of space, we give a brief introduction to the language. For a detailed representation of the language, we address the reader to [8].

[3] We use the *owner* property for relating the patient to his data.

[4] We use the predicate *fulfilled*(*Sub*, *Tar*, *Act*, T_s, T_e, *T*) that denotes that an obligation for a subject to perform an action to the target, from T_s to T_e, is fulfilled.

The above predicates ensure that every time a patient is visited, the doctor updates the patient's data. Thus, the data freshness is in line with the visiting time, and the data timeliness is respected.

The timeliness of the patient's data described above is linked to the actions of actors like doctors and nurses. The patient can also be monitored by medical IoT devices that measure, (*meas*), different vital functions. In this case, for ensuring the timeliness of the data, we expect that the patient's medical data are collected and saved simultaneously. The latter can be ensured by the below predicates.[5]

$$\begin{aligned} freshness(Tar,T) \leftarrow\ & fulfilled(Sub,Tar,upd,T,T,T),\\ & holdsAt(meas(Sub,P),T),\\ & holdsAt(owner(P,Tar),T),\\ & \textbf{not}\ holdsAt(meas(Sub,P),T''),\\ & freshness(Tar,T'''),\ T > T'' > T'''. \end{aligned}$$

$$\begin{aligned} fulfilled(Sub,Tar,T,T,T) \leftarrow\ & obl(Sub,Tar,upd,T,T,T),\\ & holdsAt(Sub,Tar,meas,T). \end{aligned}$$

$$\begin{aligned} obl(Sub,Tar,upd,T,T,T) \leftarrow\ & holdsAt(Sub,P,meas,T),\\ & holdsAt(owner(P,Tar),T). \end{aligned}$$

3.1.3. Linked data

An important problem related to the data sharing is the linked data problem. One of the main facets of this problem is deciding the policies that should be applied to the new data, that were produced by processing existing ones. The new data are linked to the existing ones, and deciding their policies is not trivial, as processed data can have different policies, also in the conflict with each other, and the nature of new data is not known. The solution we propose is the use of the *type of data*. While working on our use case, the data are divided into different types, e.g., personal information, prescriptions, private prescriptions, and every type has its corresponding sets of policies. When new data are created, after the processing of old ones, the data subject and recipients (e.g., patient, doctor) are the ones that decide the type of data and consequently their corresponding set of policies. In this particular case, the responsibility of deciding the policies for the new data is given to the data subject and recipient that often can suffer from human errors. Despite the human errors, we believe this would be a good solution, especially for the e-health scenario, where a division of access related to the security type of data cannot be applied, e.g., the doctor can process private prescriptions of the patient (e.g., depression treatment) for producing routine prescriptions of the patient (prescription with a low privacy level).

Another interesting future solution, for the linked data problem, would be the extension of an *audit process* [50] which verifies the use of data for the intended purpose. Different tags should be added to the audit system and the purposes. Thus, if the audit process confirms the purpose of the data, the policies associated with that purpose are applied to the data.

3.1.4. Data accuracy

Another important property of data quality is the *accuracy* of the collected data. When the data collection is made by a human actor, we can put in the act a deontic obligation for the actor to use a particular accuracy when getting and saving the data. This case can suffer from human errors. On the other hand, when a device is collecting the data, e.g., an IoT device, we can be more specific and ensure the data accuracy by checking the parameters of the various devices.

$$\begin{aligned} accuracy(Tar,T) \leftarrow\ & holdsAt(meas(Sub,P),T),\\ & holdsAt(acceptP(Sub),T),\\ & holdsAt(owner(P,Tar),T). \end{aligned}$$

In the above case, we state that the data collected for a particular subject are accurate, as the device that collected them is able to measure the data with acceptable parameters, (*acceptP*), for ensuring data accuracy. The same can be stated for a doctor visiting the patient and updating the data with an acceptable accuracy.

3.2. Data processing with argumentation reasoning

The data are collected, used and shared between different entities. The rules to be applied while processing the data are given through a decision process, which given the data, the various entities together with their preferences, and the applicable legal, security and business rules, decide the rules that apply to particular contexts. As introduced above these rules are called data sharing agreements, and are represented as policies. Due to the heterogeneity of the rules, and their context dependability the policies that represent them can be in conflicts, redundant, or not complete. We introduce a policy analysis for capturing the above, solving the various conflicts, and perform a decision process. The introduced analysis permits to implement and accomplish an efficient data processing.

The policy language enables an analysis based on an abductive constraint logic programming system, A-system[6] [45], which is performed to the rules and permits their efficiency and soundness. In particular, the *modality conflicts* analysis task finds conflicts between policies regulation rules, and permits to have sound DSAs. It can capture the case when an action is both permitted/obliged and denied on the same instant of time, as well as more complex conflicts. The *coverage of gaps* analysis finds the different gaps (cases) that are not covered by the DSAs rules, and permits the construction of a complete list of rules that should be part of the DSAs, e.g., when there is an explicit request from a subject to perform an action, and there is no authorization policy rule that neither permits nor denies this request. The *policies comparison* analysis checks whether a policy is included/equivalent/implied by another one. This analysis improves the efficiency of the DSAs, by identifying redundant rules, that can be easily removed from the DSAs.

The above analysis cannot capture the *conceptual conflicts*, as the latter are not direct conflicts between predicates (e.g., permitted/obliged and denied predicates) and are context dependent. The rules can be in conflict with each other, as they might hold for general domain description predicates but not for specific ones, or vice versa. The resolution of the conceptual conflicts is done by introducing priorities between rules [3], and is a decision-making problem. Techniques based on argumentation reasoning [21,5], (that is a non-monotonic reasoning [11]) together with abductive one, is introduced to find and solve the conceptual conflicts. Argumentation reasoning implements decision-making mechanisms for conflicting rules that have priorities/preferences between them and that is strongly context dependent. Argumentation reasoning permits to represent the various conflicting rules, the context where they are valid and the preferences between them. The priorities between rules permit us to work with

[5] In the previous case, when the doctor visits the patient, we give an interval of time $T - T_e$ to him, for updating the data. We expect IoT devices to make a live update of the data, without the need of extra time.

[6] A-system http://dtai.cs.kuleuven.be/krr/Asystem/.

conflicting policies and to analyse them. The above analysis is implemented using GorgiasB[7] [57], which is a tool for preference-based argumentation with a graphical user interface.

Our decision-making technique has as input the rules together with the domain description predicates that can be facts or defeasible knowledge, and finds the conflicts between rules, if there is any, and solves them. The resolution of the conflicts is made by introducing priorities between rules, called *priority rules*, and explicitly specifying when a rule has to be considered stronger than another one. A preference/priority relation, denoted by $>$, is used to indicate preferences between rules. Given two conflicting rules r_1 and r_2, where for the context and the information we have, r_1 should be applied instead of r_2, we denote it with $r_1 > r_2$. The introduced priority rules together with the existing rules are checked, and if any conflict is found, other priorities rules are introduced.

For every context and information given, the above analysis and conflict resolution provide the DSAs that apply to the data. The DSAs are used as regulatory rules between entities while processing the data and permit the compliance of all the various requirements and constraints: security, business, and legal.

4. Case representation and analysis

In this section, we continue with our use case that was already introduced in the previous sections. In our use case, we deal with an EU e-health scenario, where we want to model the data sharing agreements between different entities, for sharing and using the data. The different entities are the patients $\mathcal{P} = \{P_1, P_2, \ldots\}$, the service providers that are the hospitals $\mathcal{H} = \{H_1, H_2, \ldots\}$, and the doctors $\mathcal{D} = \{D_1, D_2, \ldots\}$, that work in hospitals. Every patient has his associated *data*. The data can be of three types:

- prescriptions: *Presc*(*data*), e.g., blood pressure, analyses, X-rays;
- private prescriptions: *PData*(*data*), e.g., anti-depressive treatments;
- personal information: *PInfo*(*data*), e.g., contact and emergency contacts.

Every patient (*P*) has a *family doctor*: *FDoc*(*D*, *P*). When the patient is treated/hospitalized in an hospital he has also the *treating doctors*: *TDoc*(*D*, *P*). In this case, for *D* to be the treating doctor of *P*, then *D* should work in the same hospital where *P* is treated/hospitalized, as follows:

$$TDoc(D,P) \text{ when } Hosp(P,H) \wedge Work(D,H).$$

The patient's data are used, accessed, and shared between different entities by respecting their DSAs. The first step is to agree on the terms of the DSAs, where some DSAs terms, usually legal ones, are irrefutable. Let us give some of the DSAs terms for our scenario.

1. The family doctor can access to all the data of the patient.
2. The patient can access to all his data.
3. The treating doctor can access to the prescription data of the patient.
4. The hospital regulation says that the treating doctor can access the patient's data during his working time, and while he is in the hospital.
5. The treating doctor cannot access the other types of the patient's data (private prescriptions and personal information), and cannot access to all types of data when he is not in the hospital, or not during his shift.
6. Nobody else can access the data.

The family doctor accesses to all the patient's data, described as follows[8]:

$$Access(data,P,permitted) \leftarrow FDoc(D,P) \wedge Owner(P,data). \quad (1)$$

Rule 2 states that the patient can access to all of his data:

$$Access(data,P,permitted) \leftarrow Owner(P,data). \quad (2)$$

Rule 3 states that the treating doctor is permitted to access the patient's prescriptions. Rule 4 states that the treating doctor can access the patient's data during his shift, *shift*(*Doctor*), and while he is in the hospital. For ensuring the latter, we use *hospP*(*Hospital*, *Location*) and *pos*(*D*, *Location*). The other accesses, e.g., when the doctor is not in the hospital, not during his working hours are not allowed, rule 5. Below, we represent rule 3 and 4 together, and rule 5.

$$\begin{aligned} Access(data,D,permitted) \leftarrow\ & TDoc(D,P) \wedge Owner(P,data) \wedge \\ & Presc(data) \wedge shift(D) \wedge pos(D,L_1) \wedge \\ & hospP(H,L_2) \wedge same(L_1,L_2) \end{aligned} \quad (3)$$

$$\begin{aligned} Access(data,D,denied) \leftarrow\ & TDoc(D,P) \wedge Owner(P,data) \wedge (PData(data) \\ & \vee PInfo(data) \vee \textbf{not } shift(D) \vee (pos(D,L_1) \wedge \\ & hospP(H,L_2) \wedge \textbf{not } same(L_1,L_2))) \end{aligned} \quad (5)$$

A patient might be in an emergency situation (means a high level of risk for his life): *Emerg*(*P*, *H*). When the patient is an emergency situation, the policies for the legislative and business rules are as below.

7. The treating doctor can access the prescriptions of the patient, when the patient is in an emergency situation, and the doctor is in the hospital and during his shift.
8. The treating doctor can access the personal information of the patient, e.g., for notifying the family members, when the patient is in an emergency situation, and the doctor is in the hospital and during his shift.
9. The treating doctor cannot access the patient's private prescription, when the patient is in an emergency situation.

$$\begin{aligned} Access(data,D,permitted) \leftarrow\ & Emerg(P,H) \wedge TDoc(D,P) \wedge \\ & Presc(data) \wedge Owner(P,data) \wedge \\ & pos(D,L_1) \wedge hospP(H,L_2) \\ & \wedge same(L_1,L_2) \wedge shift(D) \end{aligned} \quad (7)$$

$$\begin{aligned} Access(data,D,permitted) \leftarrow\ & Emerg(P,H) \wedge TDoc(D,P) \wedge PInfo(data) \\ & \wedge Owner(P,data) \wedge pos(D,L_1) \wedge hospP(H,L_2) \\ & \wedge same(L_1,L_2) \wedge shift(D) \end{aligned} \quad (8)$$

$$\begin{aligned} Access(data,D,denied) \leftarrow\ & Emerg(P,H) \wedge TDoc(D,P) \wedge \\ & PData(data) \wedge Owner(P,data) \end{aligned} \quad (9)$$

Our analysis finds that rule 7 is a sub-case of rule 3. Thus, we can remove rule 7. Rules 8 is in conflict with rule 5. This type of conflict is captured by the argumentation reasoning analysis. For solving this conflict, we put a preference relation stating that the emergency situation has higher priority. Thus, the doctor can

[7] GorgiasB http://gorgiasb.tuc.gr/.

[8] We represent the rules with the use of a semi-natural language.

access the personal information of the patient, represented as rule 8 > rule 5. The redundancy analysis finds that rule 9 represents the same policy as rule 5, where actually the latter is more generic. For improving the efficiency of our DSAs, rule 9 can be removed.

As described in the previous sections, the patient (P) may decide to be part of a research study for a particular disease, *Study*(P). In this case, his data are shared with third parties, e.g., research institutes, insurance company, government entities. Some of the uses that these entities can do with the data are for studies in particular diseases, creating adequate health campaign or stipulating new insurance plans. How and to whom the data are shared depends on their freshness, (*Fresh*), and accuracy, (*Accurate*), and the entity to whom they are shared. The entities are divided into *basic* (e.g., insurance company), *silver* (e.g., government entities), and *gold* (e.g., research institutes) members, depending on the type of agreements they have with the data subject and controller. The rules that apply in the patient data are as below[9]:

10. The gold members (*Gold*) can access to the patients normal and private prescriptions that are fresh and accurate.
11. The silver members (*Silver*) can access to the patients normal and private prescriptions that can be accurate or fresh.
12. The basic members (*Basic*) can access to the patients normal prescriptions that are not accurate, but can be fresh.

For the last case, if the data is accurate, an impoverishment process takes place, that takes part of the data accuracy out, (*Cast*).

$$Access(data, M, permitted) \leftarrow Gold(M) \wedge Owner(P, data) \wedge Study(P) \wedge (\text{Presc}(data) \vee PData(data)) \wedge Accurate(data) \wedge Fresh(data) \quad (10)$$

$$Access(data, M, permitted) \leftarrow Silver(M) \wedge Owner(P, data) \wedge Study(P) \wedge (\text{Presc}(data) \vee PData(data)) \quad (11)$$

$$Access(data, M, permitted) \leftarrow Basic(M) \wedge Owner(P, data) \wedge Study(P) \wedge (\textbf{not}\ Accurate(data) \vee Cast(data)) \wedge \text{Presc}(data) \quad (12)$$

The above rules are in conflict with rule 6, where nobody else except the doctors can access the data. As the patient is part of the study, the above rules are stronger then rule 6, represented as rule 10 > rule 6, rule 11 > rule 6, and rule 12 > rule 6.

The legislation says that the medical data of the patient can be shared just between entities inside the EU or EEA. Thus for the above case we have that[10]:

13. If a member that is part of the study is not part of the EU/EEA, than it cannot access the patient's data.

$$Access(data, M, denied) \leftarrow (Basic(M) \vee Silver(M) \vee Gold(M)) \wedge Owner(P, data) \wedge Study(P) \wedge \textbf{not}\ EU^*(M) \quad (13)$$

This rule is a sub-case of rule 6, but is stronger then the above rules, as is a legal requirement that should be respected. Thus, rule 13 > rule 10, rule 13 > rule 11, and rule 13 > rule 12.

5. Conclusion and future research directions

The purpose of this research was to extend the 'data manufacturing' concept of previous decades, to a data-intensive environment across organisational, individual and country boundaries, where 'data products' are accessible to different entities who have the approved rights on them. By using the data processing approach, we unfold the potentialities of data marketplaces, where tailored "data products" can be created, shared, sold, used or even accessed by various entities. We also identify the emerging areas of interest arising within the context of "Big Data". Within this context, we argue that data can be processed and can create value through tailoring techniques across organisational boundaries with the help of DSAs and usage control rules while developing data products/services as well as disrupting existing business models to facilitate such a change.

Future research should consider that data nowadays are multiform and multi-source; therefore new approaches are required for value extraction appropriate for any of these forms, creative enough for innovative industrial usage and extensive enough to process the masses of heterogeneous data. Data processing and manufacturing approaches should be investigated further for the path to better data quality, along with new frameworks to describe and track data processing in different industrial applications. Except for data quality, data privacy is an emerging concern, as often serious threats arise when the datasets are shared among third parties. Thus, the ways to prevent such issues provided a new research agenda around trust and shared responsibility among the actors and entities involved. Furthermore, data collection, processing and storage techniques and methods is a progressively expanding research area, as there is a wide interest in how data can be generated and exploited and therefore what are the right tools and methods for that. Data generation and exploitation strategies can also focus on the organisational aspects as well as the capabilities and skills the firms should acquire for building innovation in data-intensive contexts. Moreover, a strategic way of coupling multi-source data in different innovative ways while creating data product/services and new value streams for the companies should be proposed and explored further the necessary capabilities, skills and innovative ways of handling and processing the data.

Acknowledgments

Supported by FP7 EU-funded project Coco Cloud grant no.: 610853, and EPSRC Project CIPART grant no. EP/L022729/1.

[9] For sake of simplicity, we omit the data sanitisation process, but we assume that all the shared data during the study are sanitised.

[10] A predicate $EU^*(M)$ is used to check if the given entity is located in an EU/EAA country or not.

Table 1
Studies with focus on data manufacturing process.

Studies with focus on data manufacturing process		
Study	Description	Key points
[66]	Analysis of data quality literature following "data manufacturing" analogy as a framework for literature synthesis	– Data quality issues – Data aspects – Data manufacturing/ processing – Data products
[1]	Review of the information manufacturing stages through a discussion, raising issues of data quality	– Extracting information from databases – Information manufacturing/processing – Data quality
[2]	Introducing the problem of "information product" quality providing an assessment model of information quality (tracking information attributes-timelines, accuracy and cost)	– Information manufacturing/processing – Information products – Information manufacturing systems – Information quality – Data quality
[6]	Discussing the role of data quality for the effective use of information systems -examining the tools, concepts and techniques around data quality	– Data reliability – Data quality in programming and databases – Data quality assessment
[13]	Literature review on "data" definition (5 approaches) expanding the discussion to data quality issues, introducing 4 dimensions (accuracy, completeness, consistency, current-ness)	– Data definition – Data quality dimensions
[56]	Information as an inventory approach, involving a 3 stage process (raw materials-process-finished goods)	– Information processing/ manufacturing – Input-process-output for information manufacturing – Data as a key resource
[65]	Positioning the "data quality" problem in Total Data Quality Management (TDQM) perspective proposing a methodology around TDQM	– Information product – Information product characteristics – Information manufacturing – Information quality assessment – Information manufacturing systems
[66]	An attribute-based model for data quality assessment requirements analysis to serve quality indicator identification	– Data quality – Data manufacturing – Data management – Data quality requirements
[67]	A framework for data quality following a data consumer perspective – organizing data quality dimensions (intrinsic, contextual, representational, accessible). A survey approach is followed to test and refine the framework	– Data manufacturing systems – Data raw material – Data products – Data consumers
[58]	Conceptualizing data quality in a context of organizational processes, procedures, roles employed in collecting, processing, distributing and using data	– Data quality – Data from multiple sources – Databases – Information for decision making
[35]	Information quality assessment tool developed through surveys in 5 organizations	– Information quality – Information product – Information quality assessment
[51]	Data quality assessment metrics – highlighting the distinction between "data" and "information" (information is presented as processed data)	– Data and information – Processed data (information as an outcome) – Data quality dimensions
[20]	Information quality benchmarks for product and service performance introducing a measurement instrument for Information Quality dimensions	– Information quality benchmarks – Dimensions of Information Quality
[54]	Discussion about poor data quality and its impacts (operational, strategic, tactical) on the enterprises and their customers in the "Information Age"	– Information ecology – Data quality issues – Data accuracy
[9]	"Information Ecology" approach as a holistic view of the information environment (endogenous and exogenous), distinguishing "data", "information" and "knowledge" as distinct aspects	– Data storage – Databases mastering information complexity – Technology as enabler of information improvement – Data, information, knowledge
[55]	Methodologies for data quality programs in Information Age enterprises	– Aspects of data management – Management roles around data – Data quality design
[37]	Overview of data and information quality landscape providing a framework for categorization of topics and methods	– Data and information quality – Data quality methods – Data quality topics

Table 1 (*Continued*)

Studies with focus on data manufacturing process		
Study	Description	Key points
[18]	Data quality attached to the development and delivery of products/services as a crucial quality factor – suggestions of a 4-part quality program	– Dimensions of data quality – Data tracking and quality control
[19]	Proposing the use of control charting methods for data quality monitoring – stressing the data quality problem as crucial in Data Analytics within 2010ies	– Data production process – Data quality – Data analytics
[38]	Decision-making based on integrated, high quality information (systems theory in decision-making) – highlighting themes for data warehousing decision-making (integration, implementation, intelligence, innovation)	– Data warehousing challenges – Input-process-output – Data-based decision-making – Aspects of data-based decision-making (integration, implementation, intelligence, innovation)
[16]	Ways of producing, organizing and analysing data – presenting data quality problem in the notion of SCM problems	– Data quality – Monitoring and controlling data quality

Appendix A.

See Table 1.

References

[1] S.E. Arnold, Information manufacturing: the road to database quality, Database 15 (5) (1992) 32–39.
[2] D. Ballou, R. Wang, H. Pazer, G.K. Tayi, Modeling information manufacturing systems to determine information product quality, Manag. Sci. 44 (4) (1998) 462–484.
[3] A.K. Bandara, A.C. Kakas, E.C. Lupu, A. Russo, Using argumentation logic for firewall configuration management, 11th IFIP/IEEE International Symposium on Integrated Network Management, IM 2009, (2009) , pp. 180–187.
[4] J. Bayuk, Data-centric security, Comput. Fraud Secur. 2009 (3) (2009) 7–11.
[5] A. Bondarenko, P.M. Dung, R.A. Kowalski, F. Toni, An abstract, argumentation-theoretic approach to default reasoning, Artif. Intell. 93 (1997) 63–101.
[6] M.L. Brodie, Data quality in information systems, Inf. Manag. 3 (6) (1980) 245–258.
[7] H. Chen, R.H.L. Chiang, V.C. Storey, Business intelligence and analytics: from big data to big impact, MIS Q. 36 (4) (2012) 1165–1188.
[8] R. Craven, J. Lobo, J. Ma, A. Russo, E.C. Lupu, A.K. Bandara, Expressive policy analysis with enhanced system dynamicity, Proceedings of the 2009 ACM Symposium on Information, Computer and Communications Security ASIACCS, (2009) , pp. 239–250.
[9] T.H. Davenport, L. Prusak, Information Ecology: Mastering the Information and Knowledge Environment, Oxford University Press on Demand, 1997.
[10] D. Delen, H. Demirkan, Data, information and analytics as services, Decis. Support Syst. 55 (1) (2013) 359–363.
[11] P.M. Dung, On the acceptability of arguments and its fundamental role in nonmonotonic reasoning, logic programming and n-person games, Artif. Intell. 77 (2) (1995) 321–358.
[12] D.F. Ferraiolo, D.R. Kuhn, Role-based access controls, 15th National Computer Security Conference, (1992) .
[13] C. Fox, A. Levitin, T. Redman, The notion of data and its quality dimensions, Inf. Process. Manag. 30 (1) (1994) 9–19.
[14] G. George, M.R. Haas, A. Pentland, Big data and management, Acad. Manag. J. 57 (2) (2014) 321–326.
[15] M. Gertz, S. Jajodia, Handbook of Database Security: Applications and Trends, Springer Science & Business Media, 2007.
[16] B.T. Hazen, C.A. Boone, J.D. Ezell, L.A. Jones-Farmer, Data quality for data science, predictive analytics, and big data in supply chain management: an introduction to the problem and suggestions for research and applications, Int. J. Prod. Econ. 154 (2014) 72–80.
[17] M. Hilty, A. Pretschner, D.A. Basin, C. Schaefer, T. Walter, A policy language for distributed usage control, Computer Security – ESORICS, (2007) , pp. 531–546.
[18] Y. Huh, F. Keller, T. Redman, A. Watkins, Data quality, Inf. Softw. Technol. 32 (8) (1990) 559–565.
[19] L. Jones-Farmer, J.D. Ezell, B.T. Hazen, Applying control chart methods to enhance data quality, Technometrics 56 (1) (2014) 29–41, doi:http://dx.doi.org/10.1080/00401706.2013.804437.
[20] B.K. Kahn, D.M. Strong, R.Y. Wang, Information quality benchmarks: product and service performance, Commun. ACM 45 (4) (2002) 184–192.
[21] A. Kakas, P. Moraitis, Argumentation based decision making for autonomous agents, Proceedings of the Second International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS '03, (2003) , pp. 883–890.
[22] A.C. Kakas, R.A. Kowalski, F. Toni, Abductive logic programming, J. Log. Comput. 2 (6) (1992) 719–770.
[23] E. Karafili, A.C. Kakas, N.I. Spanoudakis, E.C. Lupu, Argumentation-based security for social good, CoRR (2017) abs/1705.00732.
[24] E. Karafili, E.C. Lupu, Enabling data sharing in contextual environments: policy representation and analysis, Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies, SACMAT 2017, Indianapolis, IN, USA, June 21–23, 2017, (2017) , pp. 231–238.
[25] E. Karafili, H.R. Nielson, F. Nielson, How to trust the re-use of data, Security and Trust Management – 11th International Workshop, STM, Springer, 2015, pp. 72–88.
[26] G. Karjoth, M. Schunter, A privacy policy model for enterprises, Proceedings 15th IEEE Computer Security Foundations Workshop (CSFW-15), (2002) , pp. 271–281.
[27] G. Karjoth, M. Schunter, M. Waidner, Platform for enterprise privacy practices: privacy-enabled management of customer data, in: R. Dingledine, P. Syverson (Eds.), Privacy Enhancing Technologies: Second International Workshop (PET), 2003, pp. 69–84.
[28] C. Kaufman, R. Perlman, M. Speciner, Network Security: Private Communication in a Public World, second ed., Prentice Hall Press, Upper Saddle River, NJ, USA, 2002.
[29] F. Kelbert, A. Pretschner, Data usage control enforcement in distributed systems, Third ACM Conference on Data and Application Security and Privacy, CODASPY'13, (2013) , pp. 71–82.
[30] F. Kelbert, A. Pretschner, A fully decentralized data usage control enforcement infrastructure, Applied Cryptography and Network Security – 13th International Conference, ACNS, 2015, pp. 409–430.
[31] Y.-J. Kim, M. Thottan, V. Kolesnikov, W. Lee, A secure decentralized data-centric information infrastructure for smart grid, IEEE Commun. Mag. 48 (11) (2010) 58–65.
[32] R.A. Kowalski, M.J. Sergot, A logic-based calculus of events, New Gener. Comput. 4 (1) (1986) 67–95.
[33] S. LaValle, E. Lesser, R. Shockley, M.S. Hopkins, N. Kruschwitz, Big data, analytics and the path from insights to value, MIT Sloan Manag. Rev. 62 (4) (2013).
[34] A. Lazouski, F. Martinelli, P. Mori, A prototype for enforcing usage control policies based on XACML, Trust, Privacy and Security in Digital Business – 9th International Conference, TrustBus, Proceedings, (2012) , pp. 79–92.
[35] Y.W. Lee, D.M. Strong, B.K. Kahn, R.Y. Wang, AIMQ: a methodology for information quality assessment, Inf. Manag. 40 (2) (2002) 133–146.
[36] M. Lycett, "Datafication": making sense of (big) data in a complex world, Eur. J. Inf. Syst. 22 (4) (2013) 381–386.
[37] S.E. Madnick, R.Y. Wang, Y.W. Lee, H. Zhu, Overview and framework for data and information quality research, J. Data Inf. Qual. (JDIQ) 1 (1) (2009) 2.
[38] S.T. March, A.R. Hevner, Integrated decision support systems: a data warehousing perspective, Decis. Support Syst. 43 (3) (2007) 1031–1043.
[39] I. Matteucci, M. Petrocchi, M.L. Sbodio, CNL4DSA: a controlled natural language for data sharing agreements, Proceedings of ACM Symposium on Applied Computing (SAC), (2010) , pp. 616–620.
[40] A. McAfee, E. Brynjolfsson, T.H. Davenport, D.J. Patil, D. Barton, Big data: the management revolution, Harv. Bus. Rev. 90 (10) (2012) 61–67.
[41] D. Mishra, A. Gunasekaran, T. Papadopoulos, S.J. Childe, Big data and supply chain management: a review and bibliometric analysis, Ann. Oper. Res. (2016) 1–24.
[42] M. Casassa Mont, S. Pearson, Sticky policies: an approach for managing privacy across multiple parties, Computer 44 (2011) 60–68.
[43] M.C. Mont, S. Pearson, P. Bramhall, Towards accountable management of identity and privacy: sticky policies and enforceable tracing services, 14th International Workshop on Database and Expert Systems Applications, 2003, Proceedings, (2003) , pp. 377–382.
[44] I.C.L. Ng, J. Williams, A. Neely, Outcome-based contracting: changing the boundaries of B2B customer relationships: an executive briefing, Adv. Inst. Manag. Res. (2009).

[45] B. Van Nuffelen, A.C. Kakas, A-system: declarative programming with abduction, Logic Programming and Nonmonotonic Reasoning, 6th International Conference, LPNMR, Proceedings, (2001) , pp. 393–396.
[46] D. Opresnik, M. Taisch, The value of big data in servitization, Int. J. Prod. Econ. 165 (C) (2015) 174–184.
[47] J. Park, R.S. Sandhu, Towards usage control models: beyond traditional access control, SACMAT, (2002) , pp. 57–64.
[48] J. Park, R.S. Sandhu, The UCONABC usage control model, ACM Trans. Inf. Syst. Secur. 7 (1) (2004) 128–174.
[49] S. Pearson, M.C. Mont, L. Chen, A. Reed, End-to-end policy-based encryption and management of data in the cloud, 2011 IEEE Third International Conference on Cloud Computing Technology and Science, (2011) , pp. 764–771.
[50] M. Petkovic, D. Prandi, N. Zannone, Purpose control: did you process the data for the intended purpose? Proceedings of Secure Data Management – 8th VLDB Workshop, SDM, (2011) , pp. 145–168.
[51] L.L. Pipino, Y.W. Lee, R.Y. Wang, Data quality assessment, Commun. ACM 45 (4) (2002) 211–218.
[52] A. Pretschner, M. Hilty, D.A. Basin, Distributed usage control, Commun. ACM 49 (9) (2006) 39–44.
[53] A. Pretschner, M. Hilty, D.A. Basin, C. Schaefer, T. Walter, Mechanisms for usage control, Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, ASIACCS, (2008) , pp. 240–244.
[54] T.C. Redman, The impact of poor data quality on the typical enterprise, Commun. ACM 41 (2) (1998) 79–82.
[55] T.C. Redman, A. Blanton, Data Quality for the Information Age, Artech House Inc., 1997.
[56] B. Ronen, I. Spiegler, Information as inventory: a new conceptual view, Inf. Manag. 21 (4) (1991) 239–247.
[57] N.I. Spanoudakis, A.C. Kakas, P. Moraitis, Gorgias-B: argumentation in practice, Computational Models of Argument – Proceedings of COMMA, (2016) , pp. 477–478.
[58] D.M. Strong, Y.W. Lee, R.Y. Wang, Data quality in context, Commun. ACM 40 (5) (1997) 103–110.
[59] V. Swarup, L. Seligman, A. Rosenthal, Specifying data sharing agreements, 7th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY), (2006) , pp. 157–162.
[60] S. Trabelsi, J. Sendor, Sticky policies for data control in the cloud, Proceedings of the 2012 Tenth Annual International Conference on Privacy, Security and Trust, PST '12, IEEE Computer Society, 2012, pp. 75–80.
[61] M.A. Waller, S.E. Fawcett, Data science, predictive analytics, and big data: a revolution that will transform supply chain design and management, J. Bus. Logist. 34 (2) (2013) 77–84.
[62] S.F. Wamba, S. Akter, A. Edwards, G. Chopin, D. Gnanzou, How 'big data' can make big impact: findings from a systematic review and a longitudinal case study, Int. J. Prod. Econ. 165 (2015) 234–246.
[63] C. Wang, Q. Wang, K. Ren, W. Lou, Privacy-preserving public auditing for data storage security in cloud computing, INFOCOM, 2010 Proceedings IEEE, (2010) , pp. 1–9.
[64] G. Wang, A. Gunasekaran, E.W.T. Ngai, T. Papadopoulos, Big data analytics in logistics and supply chain management: certain investigations for research and applications, Int. J. Prod. Econ. 176 (2016) 98–110.
[65] R.Y. Wang, A product perspective on total data quality management, Commun. ACM 41 (2) (1998) 58–65.
[66] R.Y. Wang, M.P. Reddy, H.B. Kon, Toward quality data: an attribute-based approach, Decis. Support Syst. 13 (3) (1995) 349–372.
[67] R.Y. Wang, D.M. Strong, Beyond accuracy: what data quality means to data consumers, J. Manag. Inf. Syst. 12 (4) (1996) 5–33.
[68] K.E. Weick, Sensemaking in Organizations, vol. 3, Sage, 1995.
[69] X. Zhang, F. Parisi-Presicce, R. Sandhu, J. Park, Formal model and policy specification of usage control, ACM Trans. Inf. Syst. Secur. 8 (2005) 351–387.
[70] W. Zhou, M. Sherr, W.R. Marczak, Z. Zhang, T. Tao, B.T. Loo, I. Lee, Towards a data-centric view of cloud security, Proceedings of the Second International Workshop on Cloud Data Management, CloudDB '10, (2010) , pp. 25–32.