

Modeling Legal and Regulatory Requirements for Ranking Alternatives of Cloud-based Services

Radhika Garg
Communications Systems
Group CSG
Department of Informatics
IfI
University of Zurich
Zurich, Switzerland
garg@ifi.uzh.ch

Bram Naudts
Internet Based Communication
Networks and Services
Department of Information
Technology
Ghent University / iMinds
Ghent, Belgium
bram.naudts@intec.ugent.be

Sofie Verbrugge
Internet Based Communication
Networks and Services
Department of Information
Technology
Ghent University / iMinds
Ghent, Belgium
sofie.verbrugge@intec.ugent.be

Burkhard Stiller
Communications Systems
Group CSG
Department of Informatics
IfI
University of Zurich
Zurich, Switzerland
stiller@ifi.uzh.ch

Abstract—The decision to adopt a new technology in an organization is a complex task because of several Non-Functional Requirements (NFR) *e.g.*, availability, interoperability, and presence of several alternatives, *e.g.*, service providers can offer multiple packages. To support such a decision and to select the best alternative a Trade-off based Adoption Methodology for Cloud-based Infrastructure and Services (TrAdeCIS), based on NFR for cloud-based services, was proposed. This methodology makes the decision based on multi-criteria decision algorithms, namely the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) and the Analytic Network Process (ANP). However, in addition, the decision for adopting cloud-based services is also influenced by the presence of various legal and regulative constraints. Therefore, it is crucial to understand, identify, and model the effect of such constraints on the evaluation of NFR and available alternatives. This paper, therefore, uses the Goal-oriented Requirement Language (GRL) to model the effect of legal and regulative constraints on ranking available alternatives with respect to NFR. The paper also discusses the extensibility and applicability of this methodology to other domains that require evaluating the effect of legal and regulative constraints on the adoption decision. To illustrate this, decisions within the domain providing better voice and data quality on-board train is also discussed in this paper.

Index Terms—Adoption of Technology, Legal and Regulatory Constraints, Business Goals, Goal Oriented Requirement Language, Non-Functional Requirements.

I. INTRODUCTION

The advent of new technologies, such as Cloud Computing (CC), Software-defined Networking (SDN), or Network Function Virtualization (NFV), has lead to organizations decide whether or not to adopt such technologies. This decision is complex owing to following reasons: (1) The decision maker can select from numerous available alternatives, in terms of implementations, or packages provided by various Cloud Service Providers (CSP); (2) The decision is influenced by various NFRs, including constraints, non-behavioral requirements, and quality of service. In case of CC, NFRs can be cost, interoperability, liability, or data storage. These NFRs can also have different priorities based on business objectives, for example cost can be more important to an organization than interoperability that a CSP provides.

To facilitate the selection of the best alternative, TrAdeCIS [9] was developed, which establishes a trade-off based decision in order to select the best available alternative based on NFRs. This methodology is based on Multi-Criteria Decision Algorithms (MCDA) - TOPSIS and ANP. In MCDA, multiple criteria (for example NFRs) are used to evaluate multiple alternatives in decision-making environments. TrAdeCIS includes multiple criteria from both the technical- and the business domain to evaluate available alternatives in the decision-making process. These criteria are allowed to have different weights based on preferences or business objectives. These algorithms also need a finite number of alternatives as an initial input. The final input is the ranking of these alternatives according to their performance in each of the criteria [6].

However, in addition to technical- and business-related criteria, organizations also need to comply and adhere to a large number of legal and regulative requirements. Therefore, in order to evaluate accurately the performance of an alternative with respect to a criteria or NFR, the influence of legal and regulative constraints must be considered. But these regulations are complex and vague, and can be interpreted in different ways based on the specific scenario [11]. For example, when an organization wants to retrieve data from the cloud in a reusable format, this implies that they also need the meta-data from the CSP. However, not every contract guarantees the portability of the data. Also the Service Level Agreement (SLA) may not clearly state if both data and metadata are included [1]. In such cases it is important to identify who bears losses and how liability is distributed, when the data stored in the cloud cannot be re-used by the organization. Clarification of this will help organizations to rank several alternatives differently (provided by different cloud service providers) on the criteria of portability.

Therefore, this paper extends the existing TrAdeCIS methodology to incorporate the effects of legal- and regulative constraints on the evaluation of an alternative per NFR. Modeling such constraints is done with the Goal-oriented Requirement Language (GRL), since GRL has been used to model regulations in recent years [11][12][23]. These modeling efforts assist requirement engineers and software developers in analyzing regulative compliance of systems. However, these efforts do not model evaluation of available alternatives under the influ-

ence of legal and regulative constraints while adopting a new technology. Such an evaluation of available alternatives is necessary to identify the best alternative, which fulfills the requirements (in terms of NFRs) of the organization, in the most optimum way. As these constraints and requirements are specific to the technology under consideration, this paper develops a model specific to the decision of adoption of cloud-based services. However, as shown at the end of the paper, this methodology is extensible and can be used in decision making of adopting any new technology in an organization.

The remainder of this paper is structured as follows. Section 2 discusses related work and identifies the existing gap of a methodology with which legal and regulative constraints can be encapsulated, while making the decision to adopt a new technology. In addition, a brief introduction to the semantics of GRL is also provided. Section 3 briefly describes the methodology of TrAdeCIS and the reason why an inclusion of legal considerations, while ranking cloud-based alternatives, is important. Section 4 identifies the effect of by the legal and regulative constraints that have to be evaluated while making the decision of adoption of cloud-based service. Section 5 uses GRL and applies this modeling to rank alternative solutions, when a cloud-based solution is to be adopted in an organization. Section 6 discusses the applicability and extensibility of the methodology developed in the domain of smart transportation. Finally, section 7 summarizes and concludes the paper.

II. TERMINOLOGY AND RELATED WORK

GRL is a modeling language used in system developments to support goal-oriented modeling and includes requirements, specifically non-functional requirements [13]. The syntax of GRL is introduced in Fig. 1.

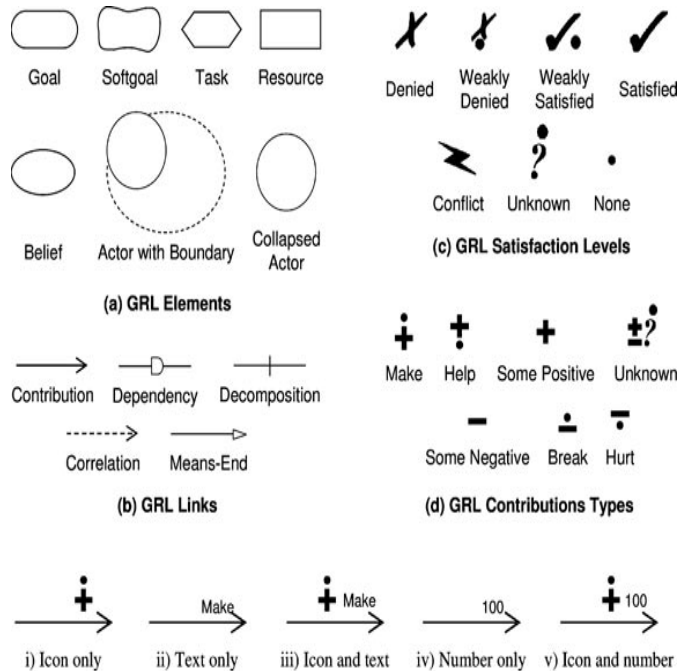


Figure 1: Basic Elements and Relationships of GRL [1]

Definitions of main elements and relationships that will be used in this paper are as follows:

- **Goal:** It represents the condition or state that is to be achieved.
- **Soft Goal:** It represents the NFR, which are quantifiable.
- **Task:** This represents various alternatives, in order to achieve a goal.
- **Actor:** He is an entity that performs all the tasks to achieve the goals.
- **GRL Links:** They are used to connect elements. For example, a decomposition link, allows an element to be subdivided into two or more elements.
- **GRL Satisfaction Levels:** These are used to describe the current or future values given to each alternative. These levels can be qualitative or quantitative.
- **Contribution link:** A contribution link shows impact of one element over the other, and can have different types as shown in Fig. 1 (d).

The work proposed and developed in this paper is multi-disciplinary. It includes modeling of legal and regulative requirements or constraints, which are crucial while making the decision of adopting new technology in an organization. The technology considered as an example is that of cloud-based services. Therefore, this section presents the related work from following perspectives:

1. Modeling of legal and regulative requirements.
2. Decision support systems for adopting new technology.

In the field of requirement engineering, research activities have been concentrating on developing models to evaluate legal compliance of a system, and to generate law-complaint requirements. These research activities cover following topics:

- Modeling legal requirements or compliance using Goal modeling notations, such as GRL [11][23]. These approaches extract legal requirements and map it to goal models in an organization.
- In case of multiple relevant legal documents, there exists a framework to prioritize legal requirements [16][18].
- Evaluating legal compliance of business processes in an organization [16].

These contributions extract relevant legal requirements from regulations and establish a certain degree of traceability between business process, goals, and regulations [10]. They concentrate only on compliance issues while developing a system, but do not include legal and regulative issues that need to be considered, while adopting a new technology in an organization. For example, when a cloud-based service is used to fulfill IT requirements of an organization, it also has to fulfill various legal and regulative constraints. In such cases it is important to incorporate not only technical and economical requirements of an organization, but also legal and regulative requirements or constraints into the evaluation of the various offerings (alternatives) from different service providers.

Previous work on decision support systems for adopting new technology is limited. Adopting a new technology such as CC is influenced by factors from various perspectives including technical, economical, and organizational ones [9]. In addition to those, legal and regulative constraints also influence such a decision making process. Various approaches [15][19][22] use MCDA to support the decision making process in finding the best alternative. However, these approaches fail to identify and include all relevant factors that influence the decision process. Also, besides technical, economical, and organizational factors it is crucial to include legal and regulative constraints in the decision making process. They also do not have a capability of making a trade-off based decision. However, this is needed as influencing factors are mutually dependent and can be conflicting in nature. For example, an organization would have a requirement to get high level of quality, and more resources but at the lowest cost possible. Therefore, a trade-off has to be made between the requirements.

As a solution to these challenges, TrAdeCIS was developed [9]. The first version of TrAdeCIS takes three inputs. First, various influencing criteria (from technical and business perspective), second the priorities of each criteria, and third ranking of alternatives per criteria. TrAdeCIS first ranks all the alternatives based on technical and business requirements separately and then the best technical alternative is selected at a trade-off of business criteria.

TABLE I. COMPARISON OF RELATED WORK WITH RESPECT TO MAIN TO CURRENT WORK

Features	GRL based Systems	MCDA based Decision Systems	TrAdeCIS V1	TrAdeCIS V2
Technical Analysis	Partially	×	✓	✓
Economical Analysis	Partially	×	✓	✓
Legal and Regulative Requirements	✓	×	×	✓
Ranking of Alternatives	×	✓	✓	✓

TABLE I. shows gaps in terms of modeling and applying legal and regulative constraints to the decision making process of adopting a new technology. Thus, TrAdeCIS V2 extends with a new layer the inclusion of the influence of legal and regulative constraints per NFR, while maintaining the capability of ranking the alternatives with respect to NFRs. For example in the case of CC this shows: (1) how the location of data storage is influenced by legal and regulative constraints and (2) how to rank different alternatives based on these constraints.

III. INCORPORATING LEGAL- AND REGULATIVE CONSTRAINTS INTO TRADECIS

The organizational decision to adopt cloud-based services to fulfill new IT requirements is influenced by multiple factors from the technical, economical, and organizational domain [8]. To facilitate the selection of the best alternative, TrAdeCIS was

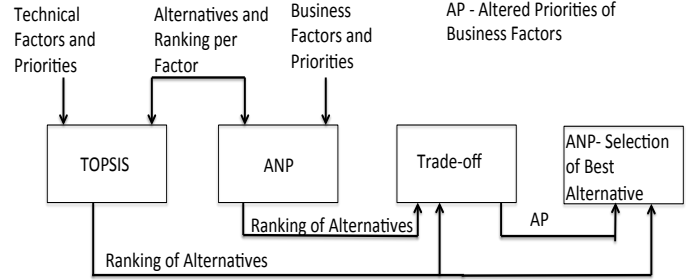


Figure 2: Steps of TrAdeCIS v1

developed [9]. It allows for the selection of the best available cloud-based service, as per requirements set. TrAdeCIS categorizes these requirements in terms of technical and business requirements (including economical and organizational factors).

To apply TrAdeCIS, the following inputs need to be identified (as shown in Fig 2):

- Alternative cloud-based solutions, for example Google App Engine, Microsoft Azure.
- Technical factors, as an input to MCDA of TOPSIS. For each factor, the relative priority has to be specified as an input. Examples of factors are availability, security, and reliability.
- Business factors, as an input to MCDA of ANP. For each factor, relative priority has to be specified as an input. Examples of business factors can be both from economical and organizational perspective, such as, cost, return of investment, change in organizational structure.
- Each of the alternatives is also ranked per factor and given as input to both TOPSIS and ANP.

Once the above-mentioned inputs are gathered, ranking of alternatives is obtained from TOPSIS and ANP. As the ranking of alternatives obtained is based on technical (using TOPSIS) and business requirements (using ANP), they can be different. TrAdeCIS allows the user to alter priorities of business factors and to select the best technical solution as a trade-off of business value.

The initial input of ranking each alternative per factor affects the results obtained from TrAdeCIS. In order to reach an optimized result, it is necessary to rank all alternatives while considering all relevant influences on each factor in the ranking process. Some of these factors are influenced by legal constraints. Therefore, the ranking of alternative solutions should incorporate how well it abides to legal requirements imposed by legal authorities and/or the organization adopting these cloud-based services.

In the context of CC, regardless of which cloud-based services will be used, an organization needs to consider legal issues, specifically those related to data collection, storage, and processing. There are also issues related to interoperability, privacy, liability of data loss, and control of data that are affected by legal constraints. Therefore, the following section identifies the interrelation between these factors and the rele-

vant laws (within the EU) that influence them and models those constraints using GRL.

IV. LEGAL AND REGULATIVE REQUIREMENTS AND CONSIDERATIONS

Moving and storing data in the cloud means that in certain cases data will be moved outside the direct control of the organization. Therefore, an organization needs to evaluate the service provider with respect to adherence to security and privacy laws. Key points to keep in mind while making a contract with service providers are the following:

- The level of security and encryption, the levels of access security protocols provided by the service provider should be identified as a contractual term.
- As per requirements, service providers must be able to guarantee an appropriate level of confidentiality.
- Based on the sensitivity of the data, the separation of data (logical or hardware level) must be provided by the service provider. This ensures that, legitimate access is provided by the service provider only.
- When an agreement between an organization and a service provider ends, the data needs to be destroyed completely from all locations.

Therefore, for each of the factors mentioned in Fig. 3 there are specific requirements that are to be considered while evaluating different alternatives. These requirements also vary as per country different laws may apply within the European Union (EU). In the following section such legal constraints and considerations are discussed.

A. Data Storage and Deletion

According to the European Data Protection Directive (DPD), a CSP has to abide with the local laws of the region where the server is located [4]. That implies that a CSP from any country, say the United States of America, who hosts the data on a server located in an EU member state, has to abide by the laws of the EU member state for transferring data. DPD introduces two responsibilities with the role of a data controller and a data processor. The EU Directive's rules on data protection states that the location of the data controller determines the national law applicable for data processing, as he is liable for data protection violations. Only in cases where the user modifies the data without the involvement of the CSP, he becomes the controller as well.

In case of multiple locations, the responsibility of data controller can be on the CSP and/or the Infrastructure Provider (InP). As the exact location for data storage is not known, it complicates data protection, specifically in terms of personal access and deletion rights. When the data is transferred to multiple jurisdictions, the applicable law is still that of the data controller. Only in case of federated clouds, when the CSP is not in a member state, but the InP is located in the member state, the applicable law is that of the InP, even when it is just processing the data [14].

During the negotiation of the contract with the CSP, customers also have to be aware of licensing terms, intellectual property rights, indemnities and protection, or content access

rights to the service provider. Data security also has to be taken into consideration from the CSP's side. It includes encrypting the data as well as applying correct policies for data sharing. In addition, resource management and allocation algorithms have to be secure. Organizations must have a right to audit security control within SLAs with the CSP, so that they can ensure security of a system that is not directly under their control. Also, cloud customers can review, if the application of encryption is mandatory by the jurisdiction of the CSP [25].

B. Interoperability

Interoperability stands for multiple things: (1) Ability of applications to move from one environment to next, (2) applications being able to share data, which is hosted on different cloud environment. In other words, interoperability means different cloud providers can exchange data without a data schema or format translation, and dependency across different Application Programming Interfaces (API). As a common standard does not exist, an organization has a risk of facing vendor-lock in. When the application or data is to be moved between clouds (within the same or different CSPs), following key challenges have to be considered:

- Setting up the network and security to match capabilities provided by the source cloud-based service.
- Handling data movement and encryption on the data in transit.
- Checking security policies and access rights of resources provided by the CSP

When the data or application is moved from one cloud provider to another, the data format (including the extent and semantics) has to remain the same, in case of the application app the code has to run also on the new service, and interface considerations have to be taken into account. It is important that a CSP includes the following points in its SLAs [3]:

- Use of standard APIs (Application Programming Interfaces), data formats, and well defined services
- For PaaS (Platform-as-a-Service) the application environment is based on open technologies
- For IaaS (Infrastructure-as-a-Service), broadly accepted application formats packaging formats such as Open Virtualization Format (OVF) for images.

V. MODELING LEGAL CONSTRAINTS TO RANK THE CLOUD ALTERNATIVES

In order to rank various alternatives under the influence of legal and regulative constraints this paper proposes to use GRL to model requirements. The aim of this modeling is to evaluate and rank all available alternative cloud-based solutions in a standardized way. This evaluation is done based on the degree of fulfillment of these requirements, by each of the available alternatives. Legal- and regulative requirements are qualitative in nature and can be categorized as NFRs. Therefore, the goals of data protection (in terms of data storage and deletion) and interoperability are modeled as soft goals as shown in Fig. 3 and Fig. 4. These GRL graphs are generated using jUCMNav v6.0.0, an open source Eclipse plug-in [7]. The list of these soft

goals and tasks to fulfill those goals can vary, based on the specific scenario and requirements of an organization. The GRL presented here illustrates a general scenario. The following subsections explain the two GRL graph generated and the logic behind the modeling:

A. Data Protection: Storage and Deletion

The first soft goal, as shown in Fig. 3, is that of compliance to data protection requirements. These requirements can be regulatory in nature or driven from the side of the organization. Towards the satisfaction of this soft goal following soft goals and tasks contribute:

- Accepted Level of Security: Three tasks contribute to this goal. Each of them having an AND contributions link toward the satisfaction of this soft goal. These tasks are:
 - Encryption of data: Again decomposed into resources of “Data in Transit” and “Stored Data”. This means both such data must be encrypted to satisfy the soft goal of encryption of data.
 - Policies of data sharing: This is decomposed in tasks of “Encryption of data”, “Logical separation of data”. These elements also share an AND link.
 - Counter-measures against attacks: As the data is in control of a third party and can be in transit, too, it can be susceptible to various attacks. Examples of these attacks are XML signature wrapping attacks on Web services [24].
- Location of Stored Data: This is an important task to be fulfilled by the service provider. The location of the data controller that is the service provider decides the applicable jurisdiction in case of any conflicts. Also, according to DPD, the data of member states shall remain in the member states. Therefore, the SP must also fulfill such constraints.
- Access of Data: This soft goal is decomposed into the following tasks toward the satisfaction of this soft goal:
 - Confidentiality: In order to implement confidentiality, the SP needs to implement access control rights. These rights can be based on roles, IP addresses, or domains. Confidentiality also includes encryption of data, for example, by symmetric or asymmetric methods.
 - Counter-measures against attacks: This task is similar to that as explained in the soft goal of “Accepted Level of Security”.
 - Access Rights: The SP shall provide different levels of access rights as per requirement of the organization. This ensures that only authorized users have access to the data.
- Deletion of Data: The contract shall specify how long it takes to delete the data from servers of the CSP, once the contract ends. Initially the data is only marked for deletion by the CSP. The actual deletion happens at a later stage, which might be after months. This is specifically important in case of sensitive data being stored in the cloud. It is decomposed into tasks of “Backup of Data” and “Access Rights”
 - Backup of data: As the data stored on the cloud is susceptible to data loss and leakage, an SP must provide

data backup. This can be done with the help of data archiving, online backup or on-premise back up, and disaster recovery.

- Safeguarding Intellectual Property:
 - Licensing: CSP must provide appropriate licenses, when

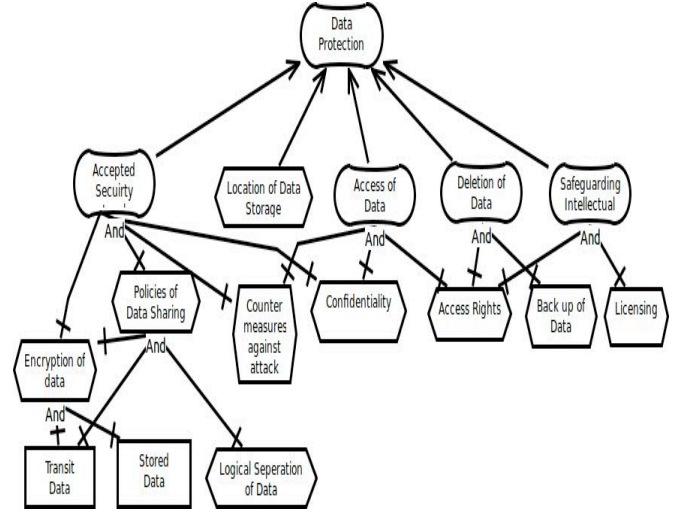


Figure 3: GRL Graph for Data Protection

a service is provisioned to an organization. This would enable an organization to legally use the provisioned service without committing copyright infringement.

- Access Rights: As CSP is liable for taking down any offensive or defamatory content, it will try to have content license from the cloud customers. Organizations must have a condition in SLAs pertaining to indemnity loss, caused due to loss, deletion of moving of data from CSP’s side.
- #### B. Interoperability
- The top-level soft goal, as shown in Fig. 4 is that of interoperability. This is contributed by an OR contribution link, from the following sub-goals:
- Move Data Between Different Applications: This is a sub-goal
 - Standards: a Hypervisor is a piece of computer software, firmware, or hardware that creates and runs virtual machines. Hypervisors can be different between different IaaS providers. However, if the user decides to change the hypervisor special tools are to be used to convert to another hypervisor. Another solution is that of the Open Virtualization Format (OVF). OVF is an open standard for packaging and distributing virtual appliances [21]. Therefore, an organization must take into account the data format used by a CSP, if an organization sees the need to share data between applications. Thus, the CSP can make applications interoperable by selecting platforms that support standardized tools and applications. However, a trade-off of standard APIs in case of PaaS is that it is more portable but it offers less control [2].

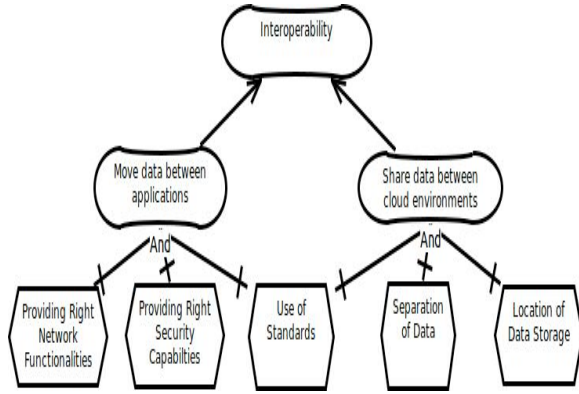


Figure 4: GRL Graph for Interoperability

- Security capabilities: The target CSP must be able to set up the security settings similar to that provided by the source cloud. Also, the source CSP must ensure that the data is encrypted during the transit.
- Network capabilities: The target CSP must be able to match the network capabilities provided by the source cloud.
- Share Data between Different Cloud Environment:
 - Separation of data: As data is stored alongside with data from other organizations, it is to be properly separated by the CSP to ensure secured storage of data. Data can be either logically or physically separated. This is important due to threat of loss, unauthentic access, and reliability issues.
 - Standards: This is same as mentioned in previous sub goal of “Move Data between Different Applications”.
 - Storage location: In case of a federated cloud, the question of location is very unclear as there are multiple locations at which data can be stored. As mentioned before, the applicable jurisdiction in case of any conflicts is decided based on the location of the data controller, which is the CSP.
 - Licensing: This is the same as discussed under safeguarding intellectual property.

These GRL graphs are used while applying TrAdeCIS, when alternatives are to be ranked (as shown in Fig. 5), with respect to factors that are influenced by legal and regulative constraints. The higher the fulfillment of GRL elements of a solution, the higher the ranking of that solution will be. So for each alternative solution it has to be identified how many soft goals are fulfilled. Also, each soft goal can have different priority, depending on the requirements of the organization. If a sub goal is (not) completed SG_i is equal to $1(0)$, where $i \in [1, n]$ n is the total number of sub-goals. And priority of each soft-goal is given P_i . Therefore the final ranking of each alternative per NFR (R_{NFR}) is given by:

$$R_{NFR} = SG_1 \cdot P_1 + SG_2 \cdot P_2 + SG_3 \cdot P_3 + \dots + S_n \cdot P_n$$

By using GRL modeling applicable legal- and regulative constraints are logically structured and the ranking of alternatives can be done in a standardized way.

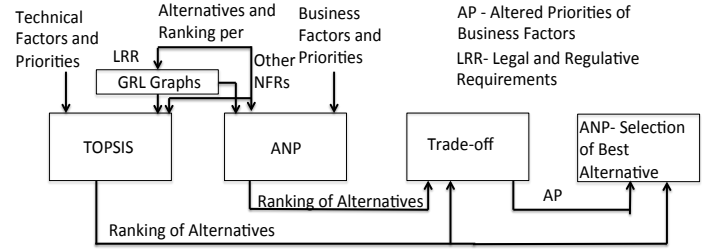


Figure 5: Steps of TrAdeCIS v2

VI. APPLICABILITY OF TRADECIS IN OTHER DOMAINS

TrAdeCIS was primarily developed to support organizations in the adoption of cloud services. However, organizations may also benefit from the usage of TrAdeCIS to improve their understanding of the value of technologies from other domains than cloud services. Also, this methodology can be extended to other domains that face similar decision making criteria. This is illustrated by applying TrAdeCIS to the adoption decision that Train Operating Companies (TOC) need to make when they research the possibility to improve both voice- and data coverage on-board in trains.

Even though a train journey can be a perfect time to answer a phone call, read an e-mail, or browse the Internet on a personal device, such as a smartphone, tablet, or laptop, coverage on trains is generally bad due to the attenuation by the train carriage and lack of coverage along the rail corridor. Three broad types of on-board systems exist to improve coverage on-board the train: IP-based data access points (e.g., Wi-Fi), wideband repeaters, and small cells (e.g., femto cells). These repeaters resolve the attenuation challenge, but they still require a connection to and from the wayside. Each of these solutions uses a mobile backhaul, thus, the provider of the on-board repeaters collaborates with an existing cellular network provider. This is, however, not the only option as other types of networks also can be used such as the network of a satellite network provider. In some cases even a dedicated network has been developed (e.g., a WiMAX network). Referring the interested reader to [20] provides for a more detailed discussion of different technological alternatives. For the application of TrAdeCIS, these different choices form the alternative offerings.

The TOC will have a set of functional- and non-functional requirements to be matched with each of these solutions. Requirements from business perspective cover both organizational and economic aspects. We mention two key requirements in this domain. First, there are different types of end-users. Not only employees of the company (internal customers) will use the technological solution, but also passengers on-board the train and even third parties, such as the train constructing company. As such the offering should be able to differentiate between different user groups (e.g. service prioritization, differentiated pricing, etc.). Second, suppliers of the technology may be a group of companies offering the technological solution to the TOC instead of a single vendor. As such, transaction costs should be taken into account. Other relevant requirements are the return on investment, the

reputation of the supplier and the deployment speed. Requirements from a technical perspective include the achievable improvements in voice quality and data bit rate as well as the interoperability with existing systems. Competing technology providers may also offer different possible technological solutions that are able to resolve the same problem each with their own benefits and drawbacks. As such the extent to which a technology is future proof should be taken into account. From a legal and regulative perspective, compliance with national legislation and contractual obligations has to be taken into account. As certain technologies (*e.g.*, femto cells and wideband repeaters) use licensed spectrum, the operator of the service should hold the required licenses. Also, on train strict regulation with regard to radio frequency exposure may apply (*e.g.*, for the train staff). To illustrate how these requirements will be converted into GRL graphs, let's consider modeling the requirement of privacy and data protection. Trains may also cross several countries; as such the rules with regard to user privacy and data protection of each of these countries should be taken into account. Therefore, two of the sub goals can be as that of following:

- Protecting data based on several data protection laws of the countries that are in the route of the train.
- Providing required level of security to the data transfer while being on-board in the train. This would include tasks such as ensuring required level of encryption or counter-measures any security-attack. Also confidentiality of user has to be ensured.

The combination of these requirements is the list of criteria on which each of the different solutions has to be ranked. Clearly, the requirements of cloud services and smart transportation solutions are different but TrAdeCIS has been developed with flexibility in mind and is as such able to cope with that diversity, and guide companies to the best solution while meeting their business-, and technical requirements as well as legal- and regulative constraints. As TrAdeCIS is able to incorporate each of these aspects in an integrated manner it defines a suitable method to find the best matching solution from available offerings. In a first step, the legal- and regulative requirements will be modeled using GRL. The ranking of these NFRs, which are influenced by legal and regulative constraints, depends on the number of sub-goals fulfilled by the available alternative. Similarly, all available alternatives will be ranked using business- and economical requirements. These rankings will be an input to both TOPSIS and ANP. In the second step, a relative priority will be given to each of these requirements as input to the MCDA of TOPSIS. Once these inputs are provided to TOPSIS and ANP, the user can obtain the ranking of the different alternatives. Finally TrAdeCIS allows the user to alter priorities of requirements in order to select the best available solution based on the trade-off between the business, technical, and legal, regulative perspective.

By applying TrAdeCIS, the TOC is able to reach a clear overview and to facilitate the decision making process as well as to understand how the choice of priorities affects the out-

come. This second applicability of TrAdeCIS to TOCs indicates that even besides the Cloud domain the same and new methodology can be applied to others, too.

VII. SUMMARY AND CONCLUSIONS

This paper recognized the need and relevance of including legal- and regulative requirements in the decision of adopting any new technology in an organization. These requirements are qualitative in nature. This paper fills that gap by modeling such requirements using GRL. This modeling comprises of NFRs including the relevant legal and regulative constraints. In addition, these GRL based graphs are used to rank different available alternative. To illustrate the application of GRL in this context, a use case from the domain of cloud computing was discussed in detail. This use-case illustrated how GRL graphs are used to evaluate and rank various cloud-based alternatives based on legal and regulatory constraints and requirements. This paper showed detailed GRL graphs to model the requirements of data storage, data deletion, and system interoperability and it lists their legal- and regulative implications. Finally, the use of GRL is linked back to TrAdeCIS as a method to rank alternatives based on the degree of fulfillment of tasks and sub-goals by an available alternative. Also, towards the end of the paper extensibility and adaptability of TrAdeCIS to other domains is illustrated.

It can be concluded that numerous available alternatives (for the decision of adopting any technology), can be ranked based on the degree with which they fulfill not only technical requirements but also legal and regulative requirements and constraints. As the ranking is based on generic approach of GRL graphs, it is an extensible to other domains with similar requirements as is illustrated in the paper with an example from the smart transportation domain. Therefore, the methodology illustrated and extended with respect to including legal and regulative constraints for ranking the alternatives in this paper can be used for the decision and a possible trade-off of any technology, when the three following conditions are met:

- An organization needs to adopt a new or changed technology,
- There are several, technologically available alternatives, which are quantifiable and qualified and which need to be ranked, and
- Numerous legal- and regulative constraints and requirements affect the decision.

ACKNOWLEDGMENT

This work was partly funded by FLAMINGO, the Network of Excellence Project ICT-318488, supported by the European Commission under its Seventh Framework Program.

REFERENCES

- [1] D. Amyot, G. Sepideh, J. Horkoff, G. Mussbacher, L. Peyton, E. Yu, "Evaluating Goal Models Within the Goal-oriented Requirement Language", *International Journal of Intelligent Systems* Vol. 25, No. 8, pp. 841-877, 2010.

- [2] L. Badger, T. Grance, R. Patt-Corner, J. Voas, "Cloud Computing Synopsis and Recommendations", Computer Security Division, Informational Technology Laboratory, National Institute of Standards and Technology, Maryland, USA, 2012.
- [3] Cloud Standards Customer Council, "Interoperability and Portability for Cloud Computing: A Guide", White Paper, pp. 1-31, November 2014.
- [4] European Commission, "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", Official Journal L 281, pp. 31-50, Nov. 1995.
- [5] Expert Group on Cloud Computing Contracts, "Working paper on "Switching - Transfer and Deletion of Data after the End of the Relationship", http://ec.europa.eu/justice/contract/files/expert_groups/switching_working_paper_en.pdf, Last Accessed on March 26, 2015.
- [6] C. Hwang, K. Yoon, "Multi Attribute Decision Making: Methods and Applications", Springer, Berlin, 1981.
- [7] jUCMNav v6.0.0, University of Ottawa, Version Released in August 2014, <http://jucmnav.softwareengineering.ca/ucm/bin/view/ProjetSEG/WebHome>.
- [8] R. Garg, B. Stiller, "Factors Affecting Cloud Adoption and their Interrelations", 5th International Conference on Cloud Computing and Services Science (CLOSER 2015), Lisbon, Portugal, pp. 1-8, May 2015.
- [9] R. Garg and B. Stiller, "Trade-off-based Adoption Methodology for Cloud-based Infrastructures and Services", 8th International Conference on Autonomous Infrastructure, Management and Security (AIMS 2014), Monitoring and Securing Virtualized Networks and Services, Brno, Czech Republic, pp. 1-13, June 2014.
- [10] S. Ghanavati, D. Amyot, and A. Rifaut, "A Systematic Review of Goal-oriented Requirements Management Frameworks for Business Process Compliance", Fourth International Workshop on Requirements Engineering and Law (RELAW), Trento, Italy, pp. 25-34. IEEE, 2011.
- [11] S. Ghanavati, D. Amyot, and A. Rifaut, "Legal Goal-oriented Requirement Language (Legal GRL) For Modeling Regulations", 6th ACM International Workshop on Modeling in Software Engineering, Hyderabad, India, pp. 1-6, June, 2014.
- [12] S. Ghanavati, "Legal-URN Framework for Legal Compliance of Business Process", <http://www.ruor.uottawa.ca/handle/10393/24028>, Ph.D. thesis, University of Ottawa, Canada, 2013.
- [13] ITU-T. Recommendation Z.151 (09/08), "User Requirements Notation (URN)-Language Definition", pp. 206, Geneva, Switzerland, 2008.
- [14] A. Kertesz, S. Varadi, "Legal Aspects of Data Protection in Cloud Federations", Security, Privacy and Trust in Cloud Systems, Springer Berlin Heidelberg, pp. 433-455, 2014.
- [15] A. Khajeh-Hosseni, D. Greenwood, J. W. Smith, I. Sommerville, "The Cloud Adoption Toolkit: Supporting Cloud Adoption Decisions in Enterprise", Software: Practice and Experience Vol. 42, No. 4, pp. 447-465, February, 2012.
- [16] R. Lu, S. Sadiq, and G. Governatori, "Compliance Aware Business Process Design", International Conference on Business Process Management, pp. 120, 2008.
- [17] A. K. Massey, P. N. Otto, and A. I. Anton, "Prioritizing legal requirements", 2nd Int. Workshop on Requirements Engineering and Law (RELAW'09), Atlanta, Georgia, USA, pp. 27-32, 2009.
- [18] A. Massey, P. Otto, L. Hayward, and A. I. Anton, "Evaluating Existing Security and Privacy Requirements for Legal Compliance", Special Issue on RE'09: Security Requirements Engineering, REJ, Vol. 15, pp. 119-137.
- [19] M. Menzel, S. Marten, T. Stefan. "(MC2) 2: Criteria, Requirements and a Software Prototype for Cloud Infrastructure Decisions", Software: Practice and Experience Vol. 43, No. 11, pp. 1283-1297, 2013.
- [20] B. Naudts, J. Spruytte, J. Van Ooteghem, S. Verbrugge, D. Colle, M. Pickavet, "Internet on Trains: A Multi-criteria Analysis of On-board Deployment Options for On-train Cellular Connectivity", 16th IEEE International Conference on Telecommunications Network Strategy and Planning Symposium (Networks), Funchal, Portugal, pp. 1-7, September, 2014.
- [21] B. Rashidi, M. Sharifi, T. Jafari, "A Survey on Interoperability in the Cloud Computing Environments", I. J. Modern Education and Computer Science, Vol. 6, pp. 17-23, July, 2013.
- [22] P. Saripalli, G. Pingali, "MADMAC: Multiple Attribute Decision Methodology for Adoption of Clouds", IEEE International Conference on Cloud Computing (CLOUD), pp. 316-323, 2012.
- [23] A. Siena, J. Mylopoulos, A. Perini, and A. Susi, "Designing Law-compliant Software Requirements", Conceptual Modeling-ER, Vol. 5829, pp. 472-486, 2009.
- [24] H. Singh, H. and S. Kalra, "A Survey on Security Threats in Cloud Computing Technology", International Journal of Research, Vol.1, No. 8, pp. 1071-1081, 2014.
- [25] J. Sen, "Security and Privacy Issues in Cloud Computing", Architectures and Protocols for Secure Information Technology Infrastructures, pp. 1-45, doi:10.4018/978-1-4666-4514-1.ch001, 2014.