Article:
Djemame, K, Barnitzke, B, Corrales, M et al. (5 more authors) (2013) Legal issues in clouds: towards a risk inventory. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 371 (1983). 20120075. ISSN 1364-503X

https://doi.org/10.1098/rsta.2012.0075

Legal Issues in Clouds: Towards a Risk Inventory

Karim Djemame*[1], Benno Barnitzke[2], Marcelo Corrales[2], Mariam Kiran[1], Ming Jiang[1], Django Armstrong[1], Nikolaus Forgó[2]

[1]School of Computing, University of Leeds, Leeds, LS2 9JT, UK
{K.Djemame, M. Jiang, M.Kiran, D.J.Armstrong04}@leeds.ac.uk

[2]Institute for Information Law (IRI), Leibniz Universität Hannover, Hannover 30167, Germany
{barnitzke, corrales, forgo} @iri.uni-hannover.de

Cloud computing technologies have reached a high level of development, yet a number of obstacles still exist that must be overcome before widespread commercial adoption can become a reality. In a cloud environment, end-users requesting services and cloud providers negotiate Service Level Agreements (SLAs) that provide explicit statements of all expectations and obligations of the participants. If cloud computing is to experience widespread commercial adoption, then incorporating risk assessment techniques is essential, during SLA negotiation and service operation. This paper focuses on the legal issues surrounding risk assessment in Cloud Computing. Specifically, it analyses risk regarding data protection and security, and presents the requirements of an inherent risk inventory. The usefulness of such risk inventory is described in the context of the OPTIMIS project.

Keywords: cloud computing; risk assessment; risk inventory; data protection; data security

---

1. Introduction

After decades in which companies used to host their entire IT infrastructures in-house, a major shift is occurring where these infrastructures are outsourced to external operators such as data centers and Clouds (Carr 2008). Clouds by definition are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms, storage and services). These resources can be dynamically re-configured to adjust to a variable load, allowing for optimum resource utilization. A pay-per-use model in which the Cloud providers offer guarantees, typically exploit this pool of resources.

A successful Cloud infrastructure is underpinned by delivering the required Quality of Service (QoS) levels to its users. Additionally, success relies on a user's ability to express QoS requirements of their applications prior to their deployment and operation on a Cloud infrastructure. The notion of QoS usually focuses on a number of factors, which consist of performance, trust, security, energy consumption and cost, all of which stand as challenging issues in Cloud infrastructures.

However, significant developments in the areas of risk assessment are necessary before widespread commercial adoption can become a reality. Specifically, risk assessment mechanisms need to be incorporated into cloud infrastructures, in order to move beyond the best-effort approach to service provision that current cloud infrastructures follow.

This paper focuses on a specific aspect of risk management as applied to cloud computing: legal issues, which are viewed as high-level concerns that underpin the non-functional properties of cloud infrastructures. Specifically, it analyses risk regarding data protection and security, for example risk of loss of data and ownership rights.

The importance of risk management in Cloud computing is a consequence of the need to support various parties involved in making informed decisions regarding contractual agreements (Djemame et al. 2011). Consider a cloud provider that wishes to offer use of its resources as a pay-per-use service. Interactions between a cloud provider and an end-user (a service consumer) can then be governed through a Service Level Agreement (SLA), contractually defining the cloud provider's obligations, the price the end-user must pay and the penalty the cloud provider needs to pay in the event that it fails to fulfil its obligations. The use of SLAs to govern such interactions in Cloud computing is gaining momentum (Ferrer 2011). However, such agreements may represent a legal risk to the parties involved. An SLA violation could be caused by various events such as disclosure and alteration of end-user data. Consequently a provider may be unwilling to implement such an approach without effective risk assessment. Similarly, end-users benefit from an evaluation of the legal implications of agreeing to particular SLA offer. Therefore, the main contributions of the paper are: 1) an analysis of risk from the legal perspective in clouds, focusing on data protection and security, and 2) the requirements of an inherent risk inventory.

The rest of the paper is structured as follows. Section 2 motivates the problem of assessing legal risk in Clouds and introduces the risk assessment methodology. Section 3 analyzes data protection policies and the minimum security standards, and provides legal guidance on the appropriate measures to be implemented. Furthermore, despite all the economic benefits Cloud Computing can offer, there are many other risks enterprises/end-users should be aware of before entering into a contractual agreement with a provider. We analyze these risks and scrutinize the ways of mitigating such risks. Section 4 describes how legal requirements can be taken into account when creating a risk inventory framework for the Cloud. Section 5 presents the implementation details of such risk inventory, showcasing the application of the methodology against two use cases (Ferrer et al. 2010): federated and multi-Clouds. Section 6 addresses related work, while conclusions and future work are summarised in Section 7.

2. Motivation and Background

By its distributed nature, Cloud Computing often blurs the location of and the security measures associated with data. This situation when it occurs can collide with legal data protection requirements. End-users must, however, be familiar with the regulations that govern their business in order to assess the risk levels of putting their data, network services and processing into the cloud. There are several risks, especially with regard to data protection and security (ENISA 2009). Examples include destruction of data, loss of data and ownership rights, disclosure and alteration of data, unauthorised access by third parties or authorities of countries outside EU/EEA and uncertain regulatory compliance. From the legal perspective, the realities cloud computing end-users must reconcile:

i. How their data, applications and infrastructures are stored and managed by others in remote locations.
ii. If their proprietary data can be stored with the data of other tenants (some of whom may even be competitors) on shared infrastructure (at least in the public cloud).
iii. Data provisioned dynamically can bring loss of control to personal data processed in Cloud.

iv. Cloud Computing providers often subcontract and outsource the provisioning of their services to unknown third parties in unknown locations.
v. Data and databases can be easily reproduced on Virtual Machines (VMs) running in Cloud.
vi. Cloud Computing has the technology which can potentially generate new information derived from the data made available from users (either individuals or companies).

Risk is defined as "Hazard, danger, exposure to mischance or peril" (RMS 2009). In the present context, risk corresponds to hazardous events that have a negative impact on SLA fulfilment. In a cloud environment providers aim to assess and manage the risk associated with offering an SLA to an end-user. Hence the hazardous events from this perspective are any events which potentially adversely affect the provider's ability to ensure that the SLA is fulfilled. The risk associated with such events can be characterised using two key parameters: the probability of occurrence and the impact of occurrence. Consider the example of unauthorised access to end-users personal data. In order to evaluate the risk of such event, the provider must take into account the possible causes of such an event and their likelihood of occurring. For example, unauthorised access to personal data could be caused by hacking, malware, malicious activities or even human error. Each of these causes must be accounted in order to enable an assessment of risk. All such events and their impact need to be considered in order to compute an overall probability of SLA violation. Regarding the impact of an SLA failure on an end-user, this is dependent on the application domain and requires a legal framework for a detailed analysis.

Figure 1 describes the risk assessment steps. Note that risk assessment takes place at: 1) the service deployment stage for initial placement of services on cloud providers, possibly taking the legal factor as a criterion for cloud providers' selection, and 2) the service operation, where cloud resources and data are managed by the cloud provider to fulfil the Service Level Objectives (SLO), including the legal ones. During deployment and operation stages, risk needs to be constantly monitored in order to prevent any additional costs to be incurred to the end-users and cloud providers.

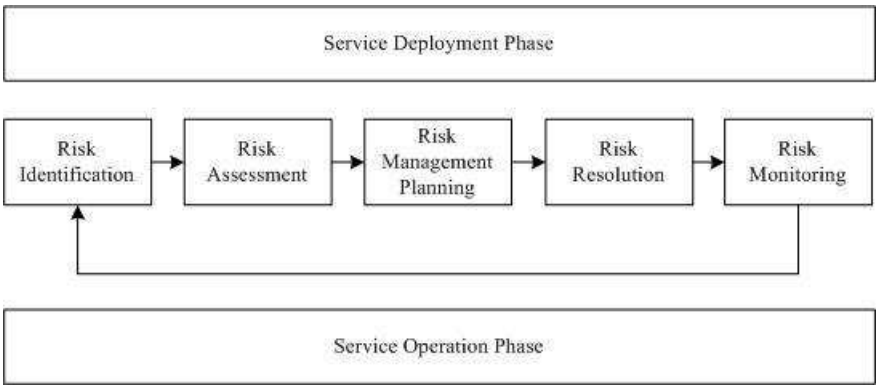

Figure 1. Risk assessment lifecycle during service deployment and operation.

In this paper, we firstly analyse data retention policies and the minimum security standards. Secondly, we describe the steps towards the design of a legal risk inventory and its implementation in Clouds.

3. Legal Risks

Legal risk in the IT industry continues to be an active area of research (Burnett, R. 2005, Rejas-Muslera et al. 2007) and covers many aspects of the law, including topics such as copy protection, privacy and censorship. However our core interest lies in the risks associated with managing data, specifically:

- **Data protection and data security.** A key inhibitor of the Cloud, where trust and control of the data is critical to building confidence.
- **Intellectual property rights.** Includes the question "Who owns the data in *the Cloud?"*. Cloud Computing creates new data using various tools (data mining etc.). The concept of ownership implies the owner can control how the data will be regulated and issues of jurisdiction apply.

In the following subsections, we discuss these legal aspects in the context of Cloud Computing. We group them according to two different perspectives, the end-user and the cloud provider.

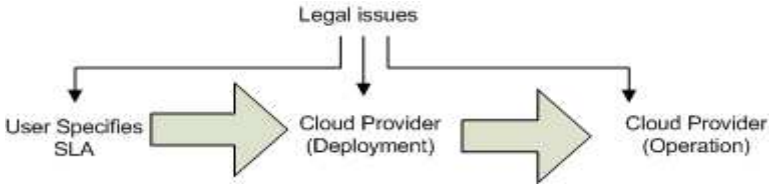

Figure 2. Legal issues and service lifecycle stages.

Legal issues are present during all stages of the service lifecycle (Figure 2). In the initial contractual agreement which the end-user makes with a Cloud Provider, the end-user can specify legal clauses, which will satisfy certain service requirements on how data is to be protected. This is a legally binding contract, which must be fulfilled by the Cloud Provider. The Cloud Provider must ensure all clauses will be adhered to before deploying the service. Therefore constant monitoring of legal risks will be required during the operation phase.

(a) End user Perspective

Art. 17 (1) of the Data Protection Directive (DPD 1995) stipulates that the controller, i.e. the end user, must implement appropriate technical and organizational measures to protect personal data against *"destr*uction, [...], loss, alteration, [...] disclosure or access, [...] and against all other unlawful forms *of processing"*.

Destruction of data. Personal data must be protected against accidental or unlawful destruction to ensure integrity and availability as well as business continuity. Destruction of personal data represents the complete removal or serious corruption of physical data (i.e. on the hard disk or in main memory) in the way that their recovery is impossible.

The provision aims to ensure the physical and logical **integrity** and **availability** (ensuring business **continuity**) of the data processed. Cloud providers in general such as Amazon make use of VMs which process the data on physical hardware in data centers. On the one hand, compared to physical servers, data inside VMs are more volatile than data in traditional IT environments. If VMs crash or are shut down, the data are usually lost. Furthermore, if VM images or instances are stored on a physical server directly attached to the server itself, all hosted VMs totally depend on the physical machine they are running on. In the worst case, all data processed in a VM running on the server could be destroyed when the physical machine crashes or is destroyed, regardless whether caused by disasters or malevolent acts by unauthorised persons. This is an important issue in cloud computing, as more business-critical workloads are deployed in VMs. A catastrophic failure of a single physical server might therefore result in an interruption of a large number of services (VMWare 2009).

Because cloud offerings are providing their services by using VMs, the data may be put at risk because of the fact that VMs containing personal data can easily be erased. Furthermore, there is the

danger of physical machines being a Single Point of Failure for hosted VMs. Where the physical machine is destroyed, all VMs running on this machine will be affected. On the other hand, the relatively simple and inexpensive replication of VMs in multiple locations increases redundancy and independence from failure.

Loss. The Data Protection Directive (DPD 1995) aims to protect the logical and physical availability of personal data by requiring the EU Member States to implement security measures against unplanned events (natural disasters, hardware failures). This element protects the physical and logical **availability** of the data. It emphasises the obligation to implement safeguards to prevent data from being unavailable due to unplanned events such as power interruption, natural disasters or spontaneous hardware failures. Keeping data in backup, the provision aims to keep data as available as possible since recovery measures might be costly and time consuming. However, as already mentioned, cloud computing benefits from increased redundancy and independence from failure as it stores data dynamically in different locations (ENISA 2009). Also, stored VMs will be available in much shorter time than physical servers. By taking measures against destruction of personal data, the requirement to prevent data loss should be fulfilled at the same time. One possible technical measure could be to implement Data Loss (Leak) Prevention (DLP) concepts in Clouds.

Alteration. Another security measure to be taken is to protect personal data against alteration. The implementation of such safeguards aim to guarantee **integrity** of the data processed. To protect data against alteration, an IT system has to ensure that data may not be modified undetectably or adapted by unauthorised persons. This requires functions for input control in order to retrace who accessed which data, the time and purpose of access (Schultze-Melling 2010). The input control aims mainly to identify and retrace errors in the data processing, but it is also a tool to monitor unauthorised access and the integrity of the data processed in the IT system.

Alteration means any modification applied to existing data which results in a difference compared to the time before the modification came into effect. Our analysis has shown that national data security obligations require controllers or processors to log whether data has been entered into the system, with date and time and by whom this has been done. This is of relevance for audits, i.e. for certification, but also with regard to possible security incidents or unlawful input or modification of personal data into the information processing system. The obligation to create logs will mainly affect the application (SaaS) layer. Only applications processing personal data will have to implement logging capabilities. The minimum content of a log file could look like:

> [date (dd-mm-yyyy)] [time (hh:min:sec)] [person accessing the data (user name)] [identification of cloud customer (i.e.by customer no.)] [application accessed (application name or module)] [nature of data (i.e. special categories of personal data)] [security level (basic, medium, high)] [action taken (input, adaption removal)]

The information given above should provide a sufficient overview to trace to what extent data have been altered.

Concerning the retention period of audit logs, a general assessment is out of question. Instead, it depends on the nature and quantity of data concerned. Where special categories of data (Art. 8 Data Protection Directive) and/or large sets of personal data are concerned, the log file should be stored for a longer period even after the final removal of the original data, while log file information about non-sensitive and/or small sets of personal data may be deleted earlier. Log files should be kept separately subject to the same security measures as the original data. Their content should be structured in a way that it is possible to segment it in order to make it available to customers.

Disclosure. A very important data security requirement is that data have to be protected against unauthorised disclosure. Disclosure is the act of making something known that was previously secret or private. This element is one of the cornerstones of the data security framework. In fact, the data subject is only in the position to preserve the right to the protection of personal data, in case both controller and processors (the end user and cloud provider respectively), do not disclose the data to third parties. Thus, this element of the provision strives to preserve the **confidentiality** of data in a technical way. Especially in cloud computing environments, the aspect of confidentiality is of utmost importance. There are several reasons to this: Firstly, cloud computing supports multi-tenancy (ENISA 2009). Different service consumers or customers might be working on the same physical machine, only separated by a software abstraction layer. Therefore, personal data processed in a VM must strictly be separated from the data inside another VM so that the data cannot be disclosed to another tenant working on the same physical machine. For that reason, Clouds can ensure that at all times, data inside a VM is kept separately from other VMs that are not assigned to the same client. Secondly, data can be frequently distributed within the Clouds using a VM management component. Such a component would be responsible for efficient management of VMs running in a cloud infrastructure. The task of the component is to optimise how the VMs are placed on the physical resources so that the provider's internal goals are maximised. Distributing the workload is inherent in all matured cloud architectures, such as the Amazon Web Services with Elastic Load Balancing[1]. Data are dynamically allocated according to a large number of different factors. This leads to continuous data streams between different locations (data centres) of different providers, in order to find the optimal location for maximum performance and to keep the agreed service levels. Consequently, the risk that unauthorised persons in clouds are intercepting data, is higher than in traditional infrastructure as more data is in transit (ENISA 2009). The legislator has explicitly addressed this risk in Art. 17 Data Protection Directive (DPD 1995), where he states that data need to be protected against unauthorised disclosure 'in particular where the processing involves the transmission of data over a network'. This provision is therefore of high relevance, as cloud computing involves the transmission of large amounts of data 'in the cloud', which is basically a network of data centres sharing and distributing resources and should strive to guarantee safe and uninterrupted data transfer.

Access. Another protective measure is to prevent unauthorised access to personal data. This element refers to the requirement of restricted permission to access data and process them. Its aim is therefore to implement measures for access control and guarantee the **confidentiality** of the data. Access control can be defined as a procedure used to determine if an entity should be granted access to resources, facilities, services, or information based on pre-established rules and specific rights or authority associated with the requesting party (ITUN 2010). Access control is very important, since only the data controller and/or the processors should be authorised to access the data. In addition, within the organisation of a cloud provider acting as a controller or processor, access rights should be carefully assigned to particular persons only. Finally, on the Software as a Service (SaaS) level, cloud services/applications should provide service consumers with the ability to assign access rights and restrictions for their own organisation, in order to avoid unauthorised access to personal data.

In view of cloud computing, Identity and Access Management (IdAM) are important keywords here. Identity management can be defined as a set of functions and capabilities used for the assurance of identity information, assurance of the identity of an entity and supporting business and security applications.

[1] http://aws.amazon.com/elasticloadbalancing/?preview=true

Transfer of data. There is a risk that personal data may be transferred and stored outside the EU or EEA countries. Respectively, the European Commission has decided that several countries ensure an adequate level of protection (e.g. Switzerland and the US, provided the importer is registered under "Safe Harbour") to which data may be transferred without specific additional. Any other transfer of personal data in the cloud to third countries is generally prohibited if there are no further legal safeguards. Data retention post termination of the SLA is another risk for customers. According to Data Protection Directive 95/46/EC (DPD 1995), the data may only be processed for adequate and relevant purposes. Upon termination of the SLA, the purpose ceases to exist; hence the data must be erased. There may also be cases where a Cloud provider terminates the SLA without notice to the end-user, resulting in a risk of the end-user losing access to all data.

(b) Cloud Provider Perspective

Ownership of data. Data ownership refers to both the possession of and responsibility for information which implies control over that information. Such control involves the capability to access, create, modify, package, derive from, sell or remove data as well as the right to assign these rights.

Data has an intrinsic as well as an added value. This is usually something produced in the process of making something else. 'At the core, the degree of ownership (and by corollary, the degree of responsibility) is driven by the value that each interested party derives from the use of that information' (Data Management 2004).

In an environment where there is shared control of data (such as cloud computing), there should be a complete understanding of the different matters related to data ownership in order to know who is entitled to claim such data. Accordingly, Gartner submitted a list of rights concerning rights and responsibilities with regard to cloud computing, expressly mentioning the right to retain ownership, the right for use and control of one's own data (Gartner Newsroom 2010).

Data ownership does not have any practical value if one is not able to access his own data. For instance, if an end-user wants to migrate data away from the cloud computing provider it is important to ensure the contract allows for access to "back-end data". As usually subscribing to a cloud service, allows you to get access to the functionality of the application that you use, it is important to ensure customers can still access the data, provided such access is removed. Agreements between end-users and providers should offer export data capabilities, either directly or via the provider, even after the termination of the contract (Longbottom 2010).

Therefore, loss of ownership rights will not only reduce or even compromise shareholders value, but may put at risk the organisation's ability to migrate to another provider. The opportunity and ability to switch cloud providers is relevant for the competition of enterprises in the market. Avoiding "lock in" and enabling switching between providers will encourage better service levels at lower costs thus fostering competition in the market (Kallenbach 2009).

We conclude that it is of utmost importance to make sure the end-users "own their data" that they make available to the Cloud provider and that these ownership rights are mentioned and clarified in any formal agreement such as a SLA.

Other unlawful forms of processing. Data must be protected against all other unlawful forms of processing. This vague legal term seems to be understood as a very broad concept. However, it is not easy to determine specific security measures in order to be compliant with this stipulation. In our view, the provision aims to ensure that data processing systems are designed in such a way that they

ensure that data processing operations meet the obligations under the law. In short, this element tries to **establish compliance** with the provisions of the Data Protection Directive (DPD 1995) as a data security obligation. This refers to so-called "privacy enhancing technologies" (PET) which are specifically designed for protecting privacy (Terstegge 2006). PET stands for a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system.. For instance, one measure could be the automatic anonymisation of data after a certain lapse of time or encryption tools.

"appropriate [...] measures". The data controller is only obliged to implement appropriate measures. The objective of this element is to eliminate or minimise the impact that different security related threats and vulnerabilities might have on an organisation's data processing (ENISA 2006). The Directive is not clear with regard to the level of security to be implemented by cloud providers. Security measures must be appropriate with regard to the anticipated risks inherent in the data processing, as well as with regard to the nature of data and the costs of their implementation (Terstegge 2006). Sensitive data as mentioned in Art. 8 (1) Data Protection Directive (DPD 1995) may require even more sophisticated security measures, while other data may require less strict measures. As the applications of security frameworks within cloud structures have a significant impact on performance, data management and costs, we recommended cloud providers to provide measures allowing service consumers to separate personal data from other data. This way, data not falling under the Data Protection Directive's scope can be processed more efficiently without the boundaries marked by data protection laws.

Assessing appropriate security measures for cloud computing is not an easy task. In general, we have already highlighted that one of the specific cloud computing risks involves massive transfer of data. ENISA rates the risk of data being intercepted in transit as “high” (ENISA 2009). The ongoing debate about data protection and data security in clouds shows that there are major concerns and objections to cloud computing. Out of these considerations, we conclude that the overall risk of using cloud computing is higher than compared to using traditional IT. Consequently, to cope with these increased risks, the appropriate measures with regard to cloud computing require higher security efforts. However, appropriate security measures always have to be adjusted to the isolated case. While some cloud services host customer information of very low sensitivity, others represent mission critical business functions (CSA 2010). Where cloud computing involves the use of special categories of data (particularly sensitive data) according to Art. 8 Data Protection Directive (i.e. health data), they must be even more strictly secured. However, even this does not mean that every theoretically conceivable risk requires technical and organisational measures. Security measures protecting data in the cloud against these particular risks or threats should in any case be considered thoroughly (CSA 2010).

4. Towards a Risk Inventory

(a) Design

When dealing with legal risks, one has to consider the actors involved when creating the risk inventory as introduced earlier: the end-users and the cloud providers. These actors can acquire different roles in the area of data protection law – either data controller or processor. Since only the controller is legally responsible for the processing, as a matter of course the risk is higher than that connected with being a processor and processing data only on behalf of the controller. This has to be taken into account when creating the risk inventory, which will be populated with the following:

- Assets: what to protect, e.g. data and their characteristics. Risk events will be assessed in terms of these.
- Incidents/Risk Scenarios: to describe any event, condition or their combination that has the potential to reduce the capacity or availability of an asset. These are composed of vulnerabilities and threats. Adaptive capacity on the other hand is the description of the mitigating strategies in place for the specific asset.
- Impact/Consequences: of a risk incident are defined using as degraded performance, loss, destruction, alteration, disclosure of data, service unavailability, etc.

Various research areas have developed risk inventories for determining how certain risks can be managed and evaluated to be brought up to an acceptable level (ENISA 2012). Most of the steps towards creating the risk inventory vary across the different disciplines and context they are going to be used in. In terms of Cloud Computing, a set of processes are identified to create and manage a risk inventory for the implementation of the framework:

1. Determine which use case scenario to focus on: private cloud, federated could, multi-Cloud.

2. Determine the areas of interaction in the Cloud. Interaction takes place at various levels such as end-user/cloud provider or within the cloud provider between the service deployment and operation phases. During each of these levels an SLA is agreed between parties and its fulfilment monitored.

3. Identify the assets involved, which have to be protected from external and internal dangers, as well as the vulnerabilities and threats these assets may have during operation.

4. Identify the risk triggering factors for these assets.

5. Identify the relationships between assets and various factors or events which may lead to risk mitigation. These relationships can be as follows:

(i) Relationship between assets and vulnerabilities: Vulnerabilities describe the inherent weakness of an asset and their impacts. Assets (A) and Vulnerabilities (V) have an interrelationship where each asset can have a number of vulnerabilities, and each vulnerability can pertain to more than one asset.

$$A = V_i, \qquad for\ i = 1, \ldots, m$$

$$V = A_j, \qquad for\ j = 1, \ldots, n$$

$$V \leftrightarrow A$$

(ii) Relationship between vulnerabilities, threat and risk: Threats (T) represent the other side of risk which depend on external factors which are independent of the asset. As vulnerabilities reflect the possibility of a risk, these can be related to the threatening factors being present. This leads to a risk (R).

$$R = V_i \times T_k, \qquad for\ i = 1, \ldots, n \ \ and \ \ k = 1, \ldots, o$$

(iii) Relationship between risk and events: Each risk can propagate a number of events (E) to take place which can in turn lead to further risks. Each risk consists of a risk category (RC) and risk level (RL). A risk level comprises of the impact of the risk and its likelihood. The impact is defined as the evaluation according to the indicators selected to describe the asset.

The impact and likelihood can be categorised as – very low, low, medium, high or very high. These determine the level of the risk by multiplying the risk impact and risk likelihood.

$$R = E_l, \qquad for\ l = 1, \dots, p$$

$$E = R_q, \qquad for\ q = 1, \dots, r$$

$$\forall R = RC \cap RL$$

$$RL = I \times L$$

(iv) Relationship between risks and their mitigations: Mitigation strategies depend on the asset, the event and any additional environmental factors (X).

$$M = A \times E \times X$$

Different Cloud scenarios can allow different assets to be at threat, depending on the service running on the providers. These threats can be of various kinds generated by the different interacting components such as the data, SLA or security management. Following is a list of legal threat scenarios associated with the different managers which cause them.

- Threat: Data transfer to other countries, Causing agent: Data manager

This threat can be monitored using all the current processing operations in the data manager, particularly with regard to the location of processing. It can be insured that there is no externalization of resources to data centers in countries without an adequate level of protection only when additional legal safeguards are in place (e.g. standard contractual clauses).

- Threat: SLA violations, Causing agent: SLA manager

This threat can be monitored by using all the current processing operations on the data. All processing should follow instructions from controllers and any further subcontracting with other processors must require consent with the cloud end-user.

- Threat: Data protection and security issues, Causing agent: Security framework manager

The data manager must ensure that personal data is protected against accidental or unlawful destruction. It can create logs concerning any alteration made to the data. Personal data must be protected against unauthorised disclosure in order to guarantee the safe and uninterrupted transfer of data by using encryption. This can be protected by implementing an Identity and Access Management. The Cloud security framework should be based on a recognized Information Security Related Standard such as ISO/IEC 27001:2005.

Table 1 describes the risk inventory design presenting the asset names and values they possess which highlights how important the asset is. These values can be set by the experts who are involved in managing the cloud. The risk inventory documents all the risks to the assets and their related vulnerabilities and threats. Starting with the assets, vulnerabilities and threats with their probabilities can be documented in advance. Vulnerability Exploitability (VE) represents to what degree the vulnerability can be exploited and its affect on the impact level of the risk, i.e. IL=Level(AV×VE). Vulnerability Severity (VS) represents the degree that the vulnerability exhibits and contributes to the final risk.

Later, Section 5 discusses the implementation details on how the risk inventory will work as part of the cloud infrastructure. The risk inventory works as an automated process that can be easily used by the providers to check the risk levels of the associated architectures and service and not applicable at the end-user level.

Table 1. Examples of Cloud Provider Risk Inventory Entries.

Attribute Name	Value Range	Value Calculation	Example1	Example2
Asset Name	N/A	By Expert Opinion	Application Generated Data	Personal Data
Asset Value(AV)	0.00-1.00	By Expert Opinion	0.9	0.9
Main Vulnerability	N/A	By Expert Opinion	Subcontracting in Federated Clouds	Hidden Dependency of Cross Multiple Cloud Applications
Vulnerability Exploitability(VE)	0.00-1.00	By Expert Opinion	0.8	0.6
Vulnerability Severity(VS)	0.00-1.00	By Expert Opinion	0.9	0.9
Main Threat Event to the Main Vulnerability	N/A	By Expert Opinion	Loss of Data Ownership	Loss of Governance
Impact Level of Risk(IL)	[1-5]	IL=Level(AV*VE)	0.9*0.8 (i.e., Level 5)	0.9*0.6 (i.e., Level 4)
Risk Category	[General, Technical, Policy, Legal]	By Expert Opinion	**Legal**	**Legal**

The risk inventory will work in conjunction with a rule-based risk model to assess some of the risks during processing. The rule-based risk model will allow certain threats to be detected and trigger which events in the risk inventory. For example, the threat of data moving to a not trusted zone can be detected by constantly monitoring the log files which document every time the data is processed or moved. While traversing the files, the rule-based model will repeatedly fire the following rule:

If (location == 'unknown_ip_address') then

Check risk inventory where "Asset==Data", Output "Impact Level of Risk"

This level of risk can be communicated to the controllers, which can then make a decision on which risk mitigation strategy should be employed, whether to accept the risk, if the impact level is down, or shut down certain processes, if the impact level is too high.

(b) Usage in Scenarios

Clouds can process services in different ways or scenarios such as the private cloud, cloud bursting or multi-Clouds and federation of Clouds. From the legal risk perspective, this becomes a particular issue in scenarios such as the multi-Cloud and the federation of Clouds. The main stakeholders in both scenarios are both the end-user and the cloud provider. Some legal threats in both scenarios are discussed next. The CORAS tool **(**Vraalsen et al. 2005**),** an open source risk modelling tool, is used to illustrate risk.

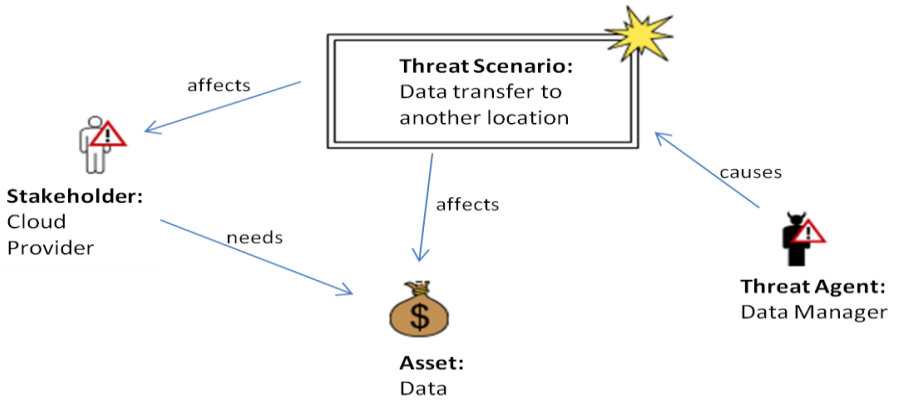

Figure 3. Modelling Legal Risk in a Multi-Cloud Scenario (Prevention: Check Monitoring Logs)

In a multi-Cloud scenario the service is deployed to run on multiple providers. Using multiple providers gives access to additional resources at the service operation, and allows the choice of the most appropriate providers depending on the functional and non-functional requirements of the SLA. The legal risk described in Figure 3 depicts the threat of data being transferred to a provider in an unknown location. The asset in thus the data to be protected and the stakeholder affected by such threat is the cloud provider which had deployed the service. Therefore, this threat needs to be monitored by traversing the logs which record where the data is moved during the cloud lifecycle.

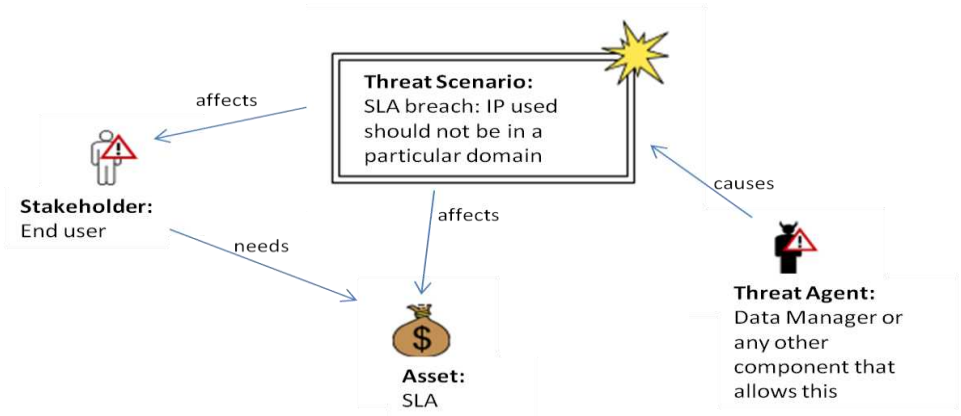

Figure 4. Modelling Legal Risk in a Federated Cloud Scenario (Prevention: Monitor SLA Violations during Processing)

In a federation of clouds, a service can be deployed into a set of providers working in collaboration to meet the service requirements. This use case differs from the multi-Cloud use case as the providers have previously entered into a mutual agreement between all members of the federation before coming into contact with the deployed service. The threat described in Figure 4, depicts what happens if one of the provider in the federation running the service is in an unknown location. This provider is called the 'IP' in the figure. In Clouds in most cases, the end-user can specify that the providers used should not be located in particular countries. In such a case, data deployed to that particular provider can lead to a violation in the SLA. Therefore, the asset here is the SLA and the stakeholder affected is the end-user.

5. Implementation and Evaluation

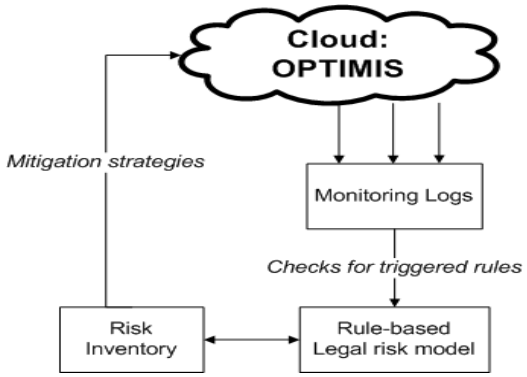

Figure 5. Risk inventory's role in the cloud architecture helping the identification of legal risks.

The OPTIMIS (Optimized Infrastructure Services) project (Ferrer 2011) is an EC funded R&D project that aims to enable an open and dependable Cloud Service Ecosystem (CSE) that delivers IT services that are adaptable, reliable, auditable and sustainable both ecologically and economically. The OPTIMIS project is delivering an open specification and a software toolkit that supports the construction of the multiple coexisting architectures that make up the next generation CSE. The OPTIMIS Base Toolkit provides functionalities common to components that are used during cloud service deployment and operation phases. These include TREC (Trust, Risk, Eco-efficiency, and Cost) factors assessment tools, cloud infrastructure monitoring infrastructure, and capabilities for secure interconnection of multiple clouds as well as end-to-end security. The TREC factors are harmonized to support the optimisation decision-making by high level components such as the Virtual Machine Manager and the Data Manager. In OPTIMIS, two stakeholders are considered: the Service Provider (SP) responsible for the deployment of the service on behalf of the end-user, and the Infrastructure Provider (IP) responsible for running the service.

As a knowledge base for risk assessment, the risk inventory designed in Section 4 is being integrated with a rule-based risk modelling component as part of the risk assessment software tool (Figure 5). The risk assessment tool is a self-contained independent functional module that is able to perform as a "plug-in" for other high level cloud management and control tools, specifically for service optimization at deployment and operation stages. In the context of OPTIMIS, the risk assessment tool is implemented as two independent components: the Service Provider Risk Assessment Tool (SPRAT) and the Infrastructure Provider Risk Assessment Tool (IPRAT) for the service deployment and operation phases respectively. Regarding the service construction phase, the end-user of a Cloud service can specify the legal aspect related requirements in the SLA via the Cloud Programming IDE provided by the OPTIMIS toolkit.

(a) Service Deployment

Figure 6 depicts the various factors that can additionally input into the risk inventory for assessing certain events. This would take place particularly on the deployment phase where the risk assessment is based on the data which is communicated across about the profile of the provider in use. This can either be historical data based on the past or the current monitored events. To assess the profile of a provider, the figure depicts the seven criteria extracted from (Jansen & Grance. 2011) which can be used in conjunction with the DS-AHP (Dempster-Shafer Analytical Hierarchy Process) algorithm (Djemame et al. 2011) to help build a sorted list of the best to worst providers from the risk point of view. This list then helps to choose the most reliable provider to deploy the service on.

Figure 6. Risk inventory takes inputs from basic standards to assess the providers.

For the SPRAT, its high level functions (e.g. evaluate the reliability of a specific IP offer) are mainly exposed by its external interfaces defined in its sub-components. The risk inventory is designed as a knowledge base to consist of facts, scenarios and reasoning rules for risk assessments related decision-making activities.

(b) Service Operation

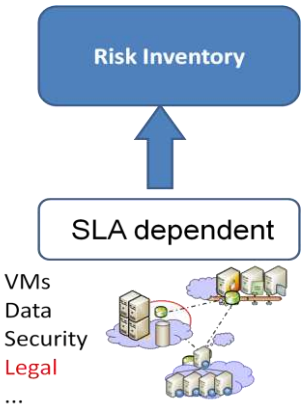

Figure 7. Risk inventory Use is SLA dependent during operation phase.

During the operation phase, the risk inventory would take inputs from the monitoring environment as depicted in Figure 7. At this stage, the service is tied to the SLA previously agreed between the SP and the IP. The SLA thus needs to be constantly monitored to ensure it does not get violated during the time the service is in operation.

For the IPRAT, its high level functions (e.g. evaluate the legal risk prior to data transfer) are mainly exposed by its external interfaces. The risk inventory is designed as a knowledge base to consist of facts, scenarios, and reasoning rules that are related to lower level hardware and software resources.

The risk assessment tools will be evaluated in the OPTIMIS test bed thanks to the interactions with other OPTIMIS toolkit components under different use case scenarios as presented in the Section 4. The accuracy of the risk assessment can then be judged by effectiveness of optimisation conducted by the high level components that depend on the assessments by the risk and other TREC factor tools collectively.

7. Related Work

In this section some related work on Cloud/Grid computing middleware and legal risk/security assessments is reviewed. Although the research work presented in this paper so far focuses on the legal aspects of data ownership and protection in clouds, it is worth noting other related aspects such as the assessment of cloud end-user privacy protection and confidentiality under different legal systems (Movius et al. 2009).

(Djemame et al. 2009) has considered specific aspects of SLAs and developed Grid architectural support for building risk aware brokering components. (Claessens J. 2008) aims to deliver a data-centric information protection framework based on data-sharing agreements in open computing environments. The framework enables dynamic management policies based on agreements that ensure end-to end secure protection of data-centric information incorporating models and implementation of risk and context-aware policy refinement mechanisms. A formal goal oriented risk framework is proposed for modelling, assessing, and treating risk on the basis of the likelihood and severity of failures in critical systems. (Balducelli et al. 2008) aims to increase dependability, survivability and resilience of information-based infrastructures such as communication technologies and pervasive systems. The work proposes a middleware which facilitates secure IT-based communication between different infrastructures providers. By supporting recovery actions and increasing service stability in case of critical situations through scenario and risk analysis, this middleware substantially enhances the security of large complex mission critical infrastructures.

Most of the above work focuses on either risks related to Grids or risks related to aspects of data security in general computing. They do not consider risk assessment in cloud computing or more specifically the legal risks associated with using cloud infrastructures. However, they do shed light on risk assessment from both end-user and server/provider perspectives and provide potential use cases for the work presented in this paper.

In many cases, the concerns of privacy and confidentiality are related to the ownership of data generated and stored on a Cloud Provider. For example, when an application is deployed into the Cloud, it generates indirect real time data that can be used to build statistics on an application's user access behaviour patterns. The ownership of this data effects privacy and confidentiality from the point of view of the end-user. As investigated by (Gellman 2009), "A user's privacy and confidentiality risks vary significantly with the terms of service and privacy policy established by the cloud provider. Those risks may be magnified when the cloud provider has reserved the right to change its terms and policies at will". This conclusion is in line with our vision of conducting risk assessment from the perspectives of both Cloud users and Cloud Providers. In addition, the report discusses outsourcing, which due to the elastic and ubiquitous nature of cloud service provision, is normal practice for a Cloud Provider to contract out part of its user data and usages onto another provider. Under this circumstance we identify the need for delegating related legal risk assessment. In the work by (Ruiter et al. 2011), uncertainties with respect to privacy regulations in Cloud Computing are investigated and discussed. It concludes that even when the Cloud Provider is compliant with the privacy regulations the end-user still needs to ensure they adhere to the legislation set in the regulations themselves. More awareness amongst cloud users may eventually lead to an increase in the number of compliant Cloud Providers; on the other hand, it also highlights the juridical impact on privacy within Cloud computing.

8. Conclusions

The use of SLAs to govern interactions in Cloud computing between end-users and cloud providers is gaining momentum. However, such agreements may represent a legal risk to the parties involved.

End-users who wish to procure critical cloud computing services may need to challenge the cloud provider positions present in the SLA. In turn, cloud providers will need to appreciate end-users' need to obtain both technical and legal assurances. In such a scenario, only a fully negotiated SLA can provide both parties with a satisfactory allocation of risk.

Cloud computing necessarily implies data transfer and, possibly, a trans-border data flow. From this perspective, the legal qualification of the subjects involved with the data flow and the definition of the consequent responsibilities and obligations is fundamental. Therefore, this paper has addressed an important issue in relation to risk assessment in cloud computing. It has presented an analysis of risk from the legal perspective, focusing on data protection and security, as well the requirements of an inherent risk inventory.

The implementation of such risk inventory is currently under way (Ferrer 2011) as part of the OPTIMIS project use cases: Multi- and federated clouds. These use cases have various implications for OPTIMIS as the differing goal of each contribute to what vulnerabilities an asset may have and thus its associated legal risk factors.

Acknowledgements

This work has been partially supported by the EU within the 7th Framework Programme under contract ICT-257115 - Optimized Infrastructure Services (OPTIMIS).

References

Balducelli, C. , Di Pietro, A., Lavalle, L. & Vicoli, G. 2008 A middleware improved technology (MIT) to mitigate interdependencies between critical infrastructures published in "Architecting Dependable Systems" (Fifth book, LNCS State-of-the-Art Survey), Springer Berlin / Heidelberg, August 2008.

Burnett, R.2005 Legal risk management for the IT industry, Computer Law and Security Report, 21, 61 – 67, Elsevier, 2005.

Carr., N. 2008 The big switch: rewiring the world, from edison to google. W. W. Norton & Company, 2008.

Claessens J. 2008 Consequence vision and research, 4th July 2008, EC TG6 Trust and Security meeting, 2008.

CSA. 2010 , Top Threats to Cloud Computing, p. 6, available at http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, Accessed Jan 2012.

Data Management 2004, http://ori.dhhs.gov/education/products/n_illinois_u/datamanagement/dotopic.html, Accessed Jan 2012.

Djemame, K., Gourlay, I. , Padgett, J., Voss K. & Kao, O. 2009 Risk management in grids. Book chapter in: "Market-Oriented Grid Computing", Buyya, R. & Bubendorfer K. (Editors), Wiley, 2009.

Djemame K., J. Padgett, I. Gourlay, and D. Armstrong, Brokering of Risk-Aware Service Level Agreements in Grids, Concurrency and Computation: Practice and Experience, 2011.

Djemame, K., Armstrong, D., Kiran, M. & Jiang, M. 2011 A risk assessment framework and software toolkit for cloud service ecosystems, CLOUD COMPUTING 2011, The Second International Conference on Cloud Computing, GRIDs, and Virtualization, pp. 119-126.

DPD 1995, Data Protection Directive 95/46/EC of the European Parliament and the Council (Amended 2003), available at http://www.dataprotection.ie/viewdoc.asp?docid=89. Accessed Jan 2012.

ENISA (European Network and Information Security Agency) 2006, Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools, p. 9, available at http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/files/deliverables/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools/at_download/fullReport, Accessed Jan 2012.

ENISA (European Network and Information Security Agency) 2009. Cloud Computing – Benefits, risks and recommendations for information security. Available at: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport.

Ferrer, A., Hernández, F., Tordsson, J., Elmroth, E., Ali-Eldin, A., Zsigri, C., Sirvent, R., Guitart, J., Badia, R., Djemame, K., Ziegler, W., Dimitrakos, T., Nair, S., Kousiouris, G., Konstanteli, K., Varvarigou, T., Hudzia, B., Kipp, A., Wesner, S., Corrales, M., Forgó, N., Sharif, T. & Sheridan, C. OPTIMIS: a Holistic Approach to Cloud Service Provisioning, Future Generation Computer Systems, 2011.

Gartner Newsroom 2010, Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010, available at: http://www.gartner.com/it/page.jsp?id=1398913, Accessed Jan 2012.

Gellman, R. 2009 World Privacy Forum's(WPF) report: Privacy in the clouds: risks to privacy and confidentiality from cloud computing, February 23rd 2009.

Helbing T., How the New EU Rules on Data Export Affect Companies in and outside the EU, Available at: http://www.thomashelbing.com/en/how-new-eu-rules-data-export-affect-companies-and-outside-eu ,Accessed 20 April 2011. For further information see Commission decisions on the adequacy of the protection of personal data in third countries [online]. Available at: http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm [Accessed 20 April 2011].

ITUN 2010, International Telecommunications Union: Recommendation X.1252 2010, Baseline identity management terms and definitions, p. 2, available at http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1252-201004-I!!PDF-E&type=items, Accessed Jan 2012.

Jansen, W., Grance, T. 2011 Guidelines on Security and Privacy in Public Cloud Computing, Draft NIST Special Publication, Computer Security, Jan 2011.

Kallenbach, P. 2009, Cloud computing – avoiding the Storm, available at: http://www.minterellison.com/public/connect/Internet/Home/Legal%2BInsights/Newsletters/Previous%2BNewsletters/A-B-Cloud%2Bcomputing,%2Bavoiding%2Bthe%2Bstorm/, Accessed Jan 2012.

Kiran, M., Jiang, M., Armstrong, D. & Djemame, K. 2011, Towards a Service Life Cycle-based Methodology for Risk Assessment in Cloud Computing, International conference on Cloud and Green Computing (CGC 2011), Australia, December 2011.

Longbottom, C. 2010, Six Things for CIOs to Consider Before Moving to Cloud Computing,Available at: http://www.executivebrief.com/saas-cloud/consider-moving-to-cloud-computing/, Accessed Jan 2012.

Movius, L. & Krup N. 2009 U.S. and EU Privacy Policy: comparison of regulatory approaches. International Journal of Communication, 2009 Vol 3 pp. 169–187.

OPTIMIS Deliverable D7.2.1.1 – Cloud Legal Guidelines [online] available at: http://www.optimis-project.eu/content/d7211cloud-legal-guidelines [Accessed 16 May 2011], and OPTIMIS Deliverable D7.2.1.2 submitted May 2011.

Rejas-Muslera, R. and Cuadrado-Gallego, J. and Rodriguez, D. 2007 Defining a legal risk management strategy: Process, legal risk and lifecycle, Proceedings of Software Process Improvement - 14th European Conference (EuroSPI), Germany, September 2007.

RMS, The Risk Management Standard. Institute of Risk Management. The Association of Insurance and Risk Managers,National Forum for Risk Management in the Public Sector. 2009, http://www.theirm.org/publications/PUstandard.html.

Robinson, N., Valeri, L., Cave, J., Starkey, T., Graux, H., Creese, S., & Hopkins P. 2011 The Cloud: understanding the security, privacy and trust challenges (Final Report), Sponsored by the European Commission Directorate General Information Society and Media, Published by the RAND Corporation, 2011.

Ruiter, J. & Warnier, M. 2011 Privacy regulations for cloud computing, compliance and implementation in theory and practice. In book "Computers, privacy and data protection: an element of choice", pp. 293-314 Springer.

Schultze-Melling. 2010, in: Taeger/Gabel, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, margin no. 64, Frankfurt/M. 2010.

Terstegge 2006, in: Büllesbach/Poullet/Prins, Concise European IT Law, Directive 95/46/EC, Art. 17 no. 3, Alphen aan den Rijn 2006.

VMWare. 2009, Protecting Mission-Critical Workloads with VMware Fault Tolerance, Whitepaper, p. 3, Available at http://www.vmware.com/files/pdf/resources/ft_virtualization_wp.pdf, Accessed Jan 2012.

Vraalsen, F., Lund, M. S., Mahler, T., Parent, X. & Stolen, K. 2005 Specifying legal risk scenarios using the CORAS threat modelling language, Springer-Verlag, Berlin 2005.