Privacy risks, security and accountability in the Cloud

Marianthi Theoharidou, Nick Papanikolaou, Siani Pearson and Dimitris Gritzalis

Privacy Risk, Security, Accountability in Cloud Platforms

Marianthi Theoharidou[1], Nick Papanikolaou[2], Siani Pearson[2] and Dimitris Gritzalis[1]

[1]Information Security & Critical Infrastructure Protection Research Laboratory
Department of Informatics,
Athens University of Economics and Business,
Email: {mtheohar, dgrit}@aueb.gr

[2]Security and Cloud Lab, HP Labs
Email: {nick.papanikolaou, siani.pearson}@hp.com

***Abstract*—Migrating data, applications or services to the cloud exposes a business to a number of new threats and vulnerabilities, which need to be properly assessed. Assessing privacy risk in cloud environments remains a complex challenge; mitigation of this risk requires trusting a cloud service provider to implement suitable privacy controls. Furthermore, auditors and authorities need to be able to hold service providers accountable for their actions, enforcing rules and regulations through penalties and other mechanisms, and ensuring that any problems are remedied promptly and adequately. This paper examines privacy risk assessment for cloud, and identifies threats, vulnerabilities and countermeasures that clients and providers should implement in order to achieve privacy compliance and accountability.**

Keywords*—*Cloud Computing; Privacy; Risk; Accountability

I. Introduction

Privacy essentially refers to the protection of personal data or *Personally Identifiable Information* (PII) and is regarded as a human right in Europe, whereas in America it has been traditionally viewed more in terms of avoiding harm to people in specific contexts [1]. Privacy is a complex notion, and its regulatory protection varies across the world. Privacy has a variety of interpretations in different, non-IT contexts, as it can refer to bodily privacy, privacy of personal behaviour or privacy of personal communications [2].

Personal data is frequently processed in the cloud by service providers, without much information being made available about where and how data is being processed. Since data tends to get stored and transferred between data centers in different countries having different regulatory requirements, it makes privacy compliance during day-to-day operations a challenging task both for cloud service providers [3] and their customers [4].

One might argue that, when migrating data and operations to the cloud, a business has the same security requirements as before, but the risk can be partially transferred to the Cloud Service Provider (CSP) for a certain fee, via an appropriate Service Level Agreement (SLA). This does not apply for regulatory obligations in respect to personal data, which remain mandatory for the controller and cannot be transferred to the processor [5]. Moreover, the change of organizational context (including location, personnel, policies, legal and regulatory framework), coupled with new, technical vulnerabilities that may arise by the new configuration, has actually introduced new threats and affects risk assessment. Even if the organizational impact of personal information disclosure is not affected, the likelihood of an incident and of vulnerabilities in the infrastructure vary. Similarly, the lack of physical or administrative control makes the assessment of countermeasures on the CSP both an issue of trust, as well as an issue of accountability.

In this paper, we examine the privacy risk that is introduced when data, applications or services are migrated to the cloud. First, we discuss current approaches, and the concept of *privacy risk assessment*. Then we analyze privacy risks in the cloud (section III), detailing privacy impact and privacy threats separately. For each threat, we lay out the vulnerabilities that enable it and suggest mitigation controls, that need to be implemented by the client or the CSP. In section IV, we turn to accountability, and the challenges for risk assessment that enter into play when adopting an accountable approach to cloud service provision. Finally, we discuss lessons learned and future work.

II. Risks to Data Stored in the Cloud

There are a number of challenges specific to cloud environments which need to be taken into consideration during risk assessment; these challenges are due to the very nature of the cloud, such as multi-tenancy, dynamicity, data duplication and proliferation, and accesses from multiple locations. We discuss these in more detail next.

First, multi-tenancy, the sharing of the same infrastructure by different clients of a cloud service provider, makes it difficult to isolate the data and concerns of each client. When investigations need to be carried out involving one particular client, other client's data could be revealed in the process unintentionally. Furthermore, improper data deletion can enable one client to uncover data that was supposed to have been removed, causing further concern.

The dynamicity of cloud is its property of being complex and ever-changing, so that data flows are always happening and hence difficult to control and monitor. Ensuring appropriate data protection and identifying the responsibilities of particular actors on an ongoing basis are among the challenges

to consider here. Unauthorized secondary usage of data is always a possibility, particularly as contractual agreements evolve rapidly and cloud service providers share data with third parties. Cloud vendors can appear and disappear rapidly, causing data to be lost or orphaned; transparency can be lost when one provider's operations are taken over by another.

Data stored in the cloud is copied across data centres in multiple locations, making it difficult to pin-point the exact device(s) on which they are stored; this makes it difficult to allocate responsibility and hold the right entity to account when privacy breaches occur. According to the UK ICO's guidelines (2012) [5], transfers of data between different locations need to be encrypted so that they are protected from interception.

In addition, the ease with which data stored in the cloud can be accessed from multiple locations, with varying legal and regulatory regimes, exacerbates the complexity of transborder data flow compliance, enforcement of subpoenas, and can expose data to the hands of foreign governments. There is abundant opportunity for cloud surveillance, and developments such as the US Patriot Act and the recent Snowden affair, exposing the so-called PRISM programme of the US government, have increased awareness of the risks associated with such surveillance.

Further issues are explored in the ENISA study [6]. Among them there are issues such as vendor lock-in, loss of governance by a cloud service provider, compliance challenges and loss of business reputation, failure of a service provider's infrastructure and acquisition of one provider by another. Technical risks include threats by a malicious insider (abuse of their privileged roles), denial of service, loss of secret keys, the carrying out of malicious probes or scans, and more. Legal risks include service providers receiving subpoenas, changing jurisdictions, and more. All of these issues are important and cloud-focused.

It is important to note that privacy legislation places various obligations on cloud service providers depending on their exact role (*data processor* or *data controller*) in a cloud service provision chain. For instance, it is the duty of the data controller to ensure that the data processor has adequate *security measures* in place for the protection of data; data processors need to comply with obligations regarding location, purpose and usage of data, as directed by data controllers.

A. Existing risk assessment approaches

Prior to migrating an application, service or infrastructure to a CSP, the client needs to assess the risk of this business decision [7]. Existing algorithms treat the project as an outsourcing one, where various services are offered by different CSPs [8]. From a business perspective, the decision can rely solely on economic terms. e.g. use of pricing theory in order to identify an optimal rule of cloud migration [9]. One can also quantify cost, security, and business parameters for different CSPs [10]. While economic input is important, it needs to be balanced against privacy rights, customer expectations and mandatory legal requirements, which should also be taken into account when making decisions. Major challenges include the realistic representation of the decision in a quantitative and qualitative way, the collection of accurate CSP information, the need to identify the varying contextual requirements and assess the privacy impact of the decision to migrate to one or more CSPs.

Following the decision to migrate, an organization needs to perform regular risk assessment for its systems, as required by legislation, standards, and best practices. Cloud's on-demand, dynamic nature in terms of services, resources, infrastructures and providers, combined with the vagueness and complexity of configuration challenge the existing static risk assessments, as approaches such as CRAMM or OCTAVE can hardly address the dynamic parameters of the cloud environment [11], [12]. A novel approach for dynamic (or even real-time) cloud risk management is needed, accompanied by new modeling languages and tools [12], [13].

Risk may be partially transferred to the CSP (via SLAs), but the residual risk still needs to be assessed. This poses a modified risk profile, as additional cloud-specific threat scenarios need to be taken into account [6], [12], [14], e.g. insider threats posed by the CSP personnel [15] or threats posed by the CSP and co-tenants [16]. The protection of customer personal information becomes a shared task between different stakeholders, posing challenges both in privacy and accountability. These properties highlight the need for designing new methods for risk assessment, which will not only assess new threat scenarios applicable to the cloud, but will also model and capture its dynamic nature and lack of well-defined boundaries [11], [13].

Cloud-oriented risk assessment approaches include one proposed by ENISA [6], which assesses various cloud risks based on expert opinions and provides guidance to CSPs and customers. Another framework [17] uses the OCTAVE and COBRA models for analyzing and assessing threats of the cloud infrastructure. This framework clearly outlines the majority of the security elements of the cloud, while applying traditional tools and methods are used. A model for quantitative risk assessment in the cloud [18] defines the cloud deployment and assesses value of assets, threat likelihood, vulnerability, impact, and risk. In [19] a semi-quantitative risk assessment framework is presented; risk is assessed in terms of impact and probability of an event. The framework relies on statistical data for the assessment of likelihood and on expert opinion for impact assessment. Attack-Defense trees are used by [20] as a means of cloud threat analysis. These depict attack steps and vulnerabilities, as well as defense mechanisms, i.e. countermeasures. The method assesses the required defense cost, based on cost of the attack, probability of success and impact. The applicability of most of the above models relies on the presence of accurate statistical data (for probability), especially when multiple CSPs are involved.

We observe that existing approaches justify the need of integrating risk assessment methods into the cloud computing model [7]. Cloud, as every other deployment infrastructure, needs to be assessed by examining applicable, as well as novel threat and vulnerability scenarios, e.g. the threats posed due to multi-tenancy. Furthermore, we observe that any risk assessment approach in the cloud faces challenges such as, (a) the lack of trust in the CSP and to data provided for risk assessment, (b) the absence of a well-defined data flow or system topology, (c) the dynamic nature of both the infrastructure and the services provided, and (d) the lack of physical control [12].

B. Privacy Impact Assessments (PIAs)

The systematic process for identifying and addressing privacy issues in an information system that considers the future consequences for privacy of a current or proposed action is considered a *Privacy Impact Assessment (PIA)* [21]. It is a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use or disclosure of personal information [22]. The purpose of a PIA is to demonstrate that program managers and system owners have consciously incorporated privacy protections throughout the development life cycle of a system or program [23]. It can be used as a management, decision tool in order to assess the privacy risks of migrating to the cloud. It is essentially a special purpose risk assessment, i.e. a privacy-oriented one.

PIAs are currently used in the UK, Canada, USA and Australia, mainly for projects of the public sector, e.g. system, technology, pilot, rule, program, or other collection. These best practises will be reflected in the new ISO29134 standard, currently under development. PIAs are a proactive tool, not an audit one, and should be performed before a product is implemented. For example, the EU RFID industry is working on a PIA framework [24] that would require RFID operator to conduct an assessment prior to deployment of an RFID application. While differences occur between approaches, the underlying principles remain the same. According to the Canadian Office of Privacy Commissioner, a PIA should be conducted under ten fundamental principles [22], which are usually referred to as *Fair Information Practices*:

1) Accountability
2) Clear collection purpose
3) Consent
4) Limited collection
5) Limited use, disclosure and retention
6) Data accuracy
7) Data Security (safeguards)
8) Openness (of privacy policies)
9) Ability to access data
10) Ability to challenge privacy practises (compliance)

A PIA typically describes (a) the project, its owner/manager and other stakeholders, (b) the types of PIIs and their collection and use conditions, (c) the privacy risks which were identified and (d) the countermeasures used in order to mitigate the identified risks. In the section that follows we will describe a similar approach for cloud projects.

III. Assessing Privacy Risks in the Cloud

Risk assessment in the cloud entails a more complex decision mechanism and is usually performed proactively, even if the process is not documented or structured. The emphasis is placed mainly on these four questions:

a) what data/services can be migrated to the cloud?
b) what type of cloud to select for the specific data/service?
c) which deployment model is more suitable?
d) which CSP(s) is/are more secure?

Each combination of answers forms a different information system, with a different context, and therefore a varied risk profile, i.e. *(combination of data/services, type of cloud, deployment model, CSP)*. The assessment of each risk profile can be broken into two assessments, one that assesses the impact of disclosure for the particular data/service – a process that resembles typical PIAs – and one that assesses specific threat scenarios and identifies vulnerabilities that may increase the likelihood of an privacy breach – a process closer to risk assessment. Privacy needs to be considered from the initial planning stage [25] and throughout the system lifecycle, in order to reflect changes such as moving data to another CSP, adding services, etc. The recommended assessment processes are closely-related; their steps are described in the following sections.

A. Privacy Impact

Initially, the scope of the cloud project needs to be defined. The business that wishes to migrate one of its services or a system to cloud, needs to identify all relevant information, their nature and conditions of processing (where processing may refer to collection, use, storage, manual process etc.). Indicative steps are the following:

1) Identify the service, application or system to be deployed.
2) Specify the data types used in the deployment.
3) Identify personal data and document the profile of the data category:
   - type and nature of information, i.e. 'personal' or 'sensitive personal data', information about persons considered 'at risk', location of individual etc.
   - persons affected
   - purpose of data collection or combination with other data or metadata used
   - current location, networks or transmissions
   - current controls and policies
   - current users (operators, administrators, security or privacy officers)
   - current use(s), including surveillance or location tracking
4) Define current context:
   - conditions/procedures for acquiring consent
   - conditions/procedures for retention, deletion and destruction
   - notifications/permissions (if any) to/from regulatory bodies
   - notifications to individuals

The above process reflects the current conditions regarding privacy and it is the first step in order to define the current risk profile. The same exercise needs to be performed for all the applicable cloud decisions, i.e. for each *deployment profile*, which consists of four elements: i. the service, application or system, ii. the cloud type, iii. the deployment model and iv. the CSP. Before migrating to the cloud and for each alternative deployment profile, the client needs to identify and document the new conditions of processing, meaning the type of information, persons affected, purpose of data collection, location.

From a business perspective, personal data disclosure in the case of the cloud may affect multiple organizations, i.e.

clients, cloud service providers or other providers involved, such as the network provider, infrastructure provider or another cloud provider. Achieving accountability when multiple stakeholders are involved is very difficult, but privacy impact assessments can help prevent problems. Therefore, the next step is to assess the organizational impact of an incident for each deployment profile. For impact assessment, best practices can be used, or a full ISO or NIST compliant risk method. Threat likelihood will require a modified method, as cloud-specific threats, vulnerabilities and controls are not covered by traditional methods. The consumer or client needs to assess or revisit existing impact assessment results in terms of how confidential the data are, and determine the consequences of disclosure of particular data categories. It is important to take into account the legal context, as it defines responsibilities and consequences (legal, financial, etc.) in case of disclosure. This assessment can be extended to handle issues with corporate data, such as intellectual property, but this falls outside of the scope of privacy.

Possible organizational impacts in case of a privacy breach include:

- loss of reputation/goodwill
- loss of strategic advantage to a competitor
- breach of contractual obligation
- violation of regulatory statures or laws (enforcement action from the regulator)
- economic losses due to compensation claims from individuals
- economic losses due to project/system redesign
- economic losses due to project/system failure
- economic losses due to security measures, retrofitted after project launch

Impact assessment for a particular data type may vary depending on the deployment model (IaaS, PaaS, SaaS), the cloud type or the CSP. As we move from IaaS to SaaS and from private to public clouds, the level of control decreases [16]. This may (a) increase the overall impact of a privacy breach if worse conditions and time of recovery apply, or (b) decrease the accuracy of the assessment, due to lack of information. This means that impact should be assessed for every affect data category and for each cloud deployment profile. It is imperative that such differences are documented in detail, as these affect the decision and the conditions of the project to migrate to the cloud.

B. Privacy Threats and Vulnerabilities

The parameters mentioned above, i.e. the type of cloud or deployment and the particular CSP(s), also modify the risk profile of a cloud migration project in terms of threat likelihood and due to the presence of varied vulnerabilities and controls. Also, security risks and responsibilities vary across cloud service or deployment models. Among the top security threats identified by the CSA for 2013 [14], several refer to information disclosure, placing privacy as a top priority:

- Data Breaches/Leakage: unintentional or deliberate compromise or revealing of information, to an unauthorized party.
- Account or Service Traffic Hijacking: access or control of an account/service by an unauthorized party.
- Insecure Interfaces and APIs: attacks enabled by vulnerabilities on the (architectural) low level of cloud (API/ interface).
- Shared Technology Vulnerabilities: attacks enabled by sharing infrastructure, platforms and applications to multiple tenants.
- Malicious Insiders: violation of security policy by authorised personnel.
- Insufficient Due Diligence: lack of proactive actions prior to migration.

While these security threats are common in other environments too, they pose new mitigation challenges when applied to the cloud, due to multi-tenancy, loss of physical control, dynamic allocation of resources, or due to the complexity that arises when security responsibilities are shared between the client and the CSP(s). This dynamic context, with multiple players, makes compliance and accountability particularly complex. The ENISA threat landscape report [26] identifies several emerging threats, unique to the cloud environment. The report estimates that low level attacks (to insecure APIs of the virtual machines) will be common, targeting in particular, security services offered by the CSP to multiple tenants or used by various CSPs. The vulnerability of co-hosting enables both data breaches by insiders and by outsiders, giving the first ones access to multiple targets and increased attack capabilities. The use of cloud services can become the means for other attacks towards multiple victims, which reflects the increased impact of an attack to a cloud infrastructure.

In the tables that follow (Tables I-V), we present an analysis of the top privacy threats [14] in terms of vulnerabilities, security controls and their applicability. This is based on previous work of the authors [12] and recommendations by [6], [14], examined under the scope of privacy. Each threat is paired to the vulnerabilities that may enable it, and to mitigation controls as defined in CSA's Cloud Controls Matrix (CCM) [27]. The vulnerabilities which are cloud-specific are discussed below, in order to demonstrate how the attack pattern of each threat is modified when we consider it within the cloud context. We also attempt to identify the responsible party for implementing countermeasures, i.e. the CSP or the client. Here we considered the case of a hybrid or public cloud, as the private ones have clearer separation of duties in terms of security. Additional information is also provided in terms of applicability of controls to data, physical infrastructure, software (which mainly refers to applications, APIs or the Operating system) or network infrastructure. This allows for different assessments to be performed for varied risk profiles and also provides an initial roadmap towards accountability.

The threat of data breaches or leakage (see Table I) is key when we consider data privacy. Data leakage can occur when data are transferred between customer and CSP, or when they are transferred to other VMs, to different CSPs

or different locations. Undocumented data flows can provide channels for undetected data leakage of sensitive information. Breaches can also occur when existing controls fail, due to weak security practises on the client or on the CSP side (e.g. loss of encryption keys, ineffective deletion of data). The case where data are leaked by an insider are examined in the 'malicious insiders' category (see Table IV).

While the vulnerabilities, mentioned in Table I, are commonly found in information systems, multi-tenancy and reuse of resources introduce new requirements. For example, encryption, isolation of environments and data leakage prevention mechanisms need to be designed to suit multi-tenant environment or interfaces. We observe that many of the respective controls require implementation from the CSP. Risk assessment and the mitigation that ensues, entails the cooperation of CSPs in providing the information needed for the assessment of the above vulnerabilities. This can be partially done by applying questionnaires, like the ones provided by the Cloud Security Alliance Consensus Assessments Initiative (CAI) [28], which provides templates in order to document what security controls exist in IaaS, PaaS, and SaaS offerings by various CSPs. However, this process needs to be performed proactively (before the migration) and the effectiveness of such controls is still not evaluated. Such a process requires the design of appropriate tools.

Table II presents vulnerabilities and controls (with applicability parameters) for the 'Account or Service Hijacking' threat. Stealing credentials from users is not a new threat; yet it remains a common way to compromise the confidentiality of cloud computing services. Here privacy is affected both by the disclosure of credentials and by the disclosure of client data caused by the unauthorised access to services and platforms. Here, the cloud environment introduces vulnerabilities, such as the difficulty for the client to perform audit, detect intrusions and handle incidents, due to the lack of control. Potentially poor access control can affect multiple tenants, or customers that use similar applications or platforms, or give the attacker a means to launch other attacks.

The threats of 'Insecure Interfaces and APIs' and 'Shared Technology Vulnerabilities' (Table III) are closely-related and unique to the cloud environment. They are enabled by hypervisor vulnerabilities, weak security mechanisms on the CSP side or lack of isolation of the co-tenants, both on a technical and physical level. The first threat refers mostly to poorly designed, in terms of security, services by a CSP. The distinctive factor here is that these services are used by multiple clients/organizations and their respective clients. Similarly, one undetected vulnerability may affect multiple customers. This increases the potential effect of the particular threat scenario, due to the fact that multiple customers co-exist within a cloud or use similar platforms or applications. Even in the case where a customer is not truly affected, he may still suffer by loss of reputation, due to a co-tenant privacy-related incident.

Table IV examines the threat of malicious insiders. Insiders are more empowered in cloud environments [15], especially when a user holds the role of system administrator in a CSP or managed security service provider. A malicious insider in the cloud has increased access to data, and when security mechanisms are handled purely by the CSP, then the insider has increased capability to launch an attack, to multiple customers. Here, the inherent vulnerability is the increased potential impact of an insider attack, due to higher availability of targets and the use of similar mitigation controls by co-tenants. Risk mitigation requires implementation of multiple organizational or procedural controls on both the client and the CSP side.

The last threat (see Table V) refers to vulnerabilities that derive from the fact that the cloud is a new environment for many customers. As a result, customers often do not base cloud migration on an informed decision. This means that they may adopt services and applications that do not comply with current best practises and legal requirements, they may fail to assess the new risks that are introduced by such a decision and, therefore, fail to implement all the required contingency actions required to ensure data protection. As we have seen in Section II-A, defining a new 'cloud' risk profile for each deployment decision and assessing this new environment, requires novel techniques and is still an open issue. This fact coupled with a client's decision to migrate without the appropriate planning augments the problem. A failure to assess privacy impact of a deployment profile accurately (via a cloud-based PIA) may result to poor mitigation controls. This means that the client unknowingly accepts the privacy risk that is introduced instead of mitigating it. These remains one of the most difficult threats to deal as the industry is currently defining best practises, which constantly evolve, e.g. ENISA and CSA initiatives.

While this analysis focused mainly on the threats that refer to PII disclosure and therefore, affect privacy, there are additional mitigation controls that both the client and the CSP need to consider in order to ensure that all privacy principles are met [29]. These include mechanisms to ensure that (a). the data subject still has control over his/her data, (b). data access requests are enabled and served, (c). purpose specification is properly reflected, (d). data is accurate, (e). transborder data flow is respected, etc. These risk mitigation challenges set additional requirements to customers and CSP in terms of accountability. In the section that follows we will discuss how the two concepts are related, under the scope of privacy.

IV. Risk Assessment for Accountability

The privacy-oriented definition of accountability given in ISO standard 29100 [30] expresses accountability in terms of the practices associated with it in organizations:

> Accountability: document policies, procedures and practices, assign the duty to implement privacy policies to specified individuals in the organization, provide suitable training, inform about privacy breaches, give access to effective sanctions and procedures for compensations in case of privacy breaches.

The concept of accountability is enshrined in regulatory frameworks for data protection across the globe. It is present in the Asia Pacific Economic Cooperation's privacy framework [31], as well as in Canada's Personal Information Protection and Electronic Documents Act [32]. One expression of accountability that is common in all aforementioned documents are the obligations posed to the data controller for complying with that particular data protection legislation and, in most cases, the establishment of systems and processes

TABLE I. TOP THREAT: DATA BREACHES OR LEAKAGE

Vulnerability	CCM Code	Client	CSP	Infrastructure	Data	Software	Network
Undocumented data flows	-	x	x		x	x	x
Insecure or ineffective data disposal	DG-05		x		x	x	
Lack of or weak data leakage controls	DG-07		x		x	x	
Undefined or outdated data governance requirements	DG-08	x	x		x	x	
Weak per tenant encryption	IS-18		x		x	x	x
Weak key management procedures	IS-19	x	x		x	x	x
Weak user authentication and access policy	SA-02/-07	x	x			x	x
Ad hoc data security architecture	SA-03		x		x	x	x
Weak separation of production/non-production environments	SA-06		x	x	x	x	
Use of production data for non-production environments	DG-06		x		x	x	

TABLE II. TOP THREAT: ACCOUNT OR SERVICE TRAFFIC HIJACKING

Vulnerability	CCM Code	Client	CSP	Infrastructure	Data	Platform/Software	Network
Unclear roles and responsibilities	IS-07		x	x	x	x	x
Weak tenant authentication and access policy	IS-07	x	x			x	x
Weak user access management (authorization/revocation/review)	IS-08/09/10	x	x	x	x	x	x
Poor incident management mechanisms	IS-22	x	x	x	x	x	x
Undefined or outdated data governance requirements	DG-08	x	x		x	x	
Lack of physical protection (accidental or deliberate attacks)	SA-05		x	x			
Weak separation of production/non-production environments	SA-06		x	x	x	x	
Weak user authentication and access policy	SA-02/07	x	x			x	x
Lack of audit and intrusion detection mechanisms	SA-14		x	x	x	x	x

TABLE III. TOP THREAT: INSECURE INTERFACES AND APIS/SHARED TECHNOLOGY VULNERABILITIES

Vulnerability	CCM Code	Client	CSP	Infrastructure	Data	Platform/Software	Network
Ad hoc data security architecture	SA-03		x		x	x	x
Unclear roles and responsibilities	IS-07		x	x	x	x	x
Weak user access management (authorization/revocation/review)	IS-08/09/10	x	x	x	x	x	x
Weak policy for labeling, handling and security of data	DG-03	x	x		x	x	x
Lack of baseline security requirements/Non-compliance to standards	SA-04/IS-04		x	x	x	x	x
Non-compliance with legal, statutory or regulatory compliance obligations	SA-04		x		x	x	x
Weak tenant authentication and access policy	IS-07	x	x			x	x
Weak segregation of duties	IS-15		x	x	x	x	x
Weak per-tenant encryption	IS-18		x		x	x	x
Lack of vulnerability assessment mechanisms	IS-20		x			x	x
Delayed vulnerability and patch management	IS-20		x			x	x
Poor tenant segmentation	SA-09/SA-11	x	x	x	x	x	
Lack of audit and intrusion detection mechanisms	SA-14		x	x	x	x	x

TABLE IV. TOP THREAT: MALICIOUS INSIDERS

Vulnerability	CCM Code	Client	CSP	Infrastructure	Data	Platform/Software	Network
Failure to audit third-party providers	CO-03		x	x	x	x	x
Undocumented responsibilities for data stewardship	DG-01	x	x		x	x	x
Weak data labeling, handling and security policy	DG-03	x	x		x	x	x
Lack of or weak data leakage protection mechanisms	DG-07		x		x	x	x
Unrestricted physical access to data or facilities	FS-02/05		x	x			
Lack of policies for off-site authorization	FS-06		x	x	x		
Inadequate background screening	HR-01	x	x				
Weak user authentication and access policy	SA-02/07	x	x			x	x
Lack of disciplinary or sanction policy against violations	IS-06	x	x				
Weak user access management (authorization/revocation/review)	IS-08/09/10	x	x	x	x	x	x
Unclear roles & responsibilities: employees/contractors/temps	IS-13	x	x	x	x	x	x
Weak segregation of duties	IS-15	x	x	x	x	x	x
Need-to-know principle not applied		x	x	x	x	x	x
Weak per-tenant encryption	IS-18		x		x	x	x
Weak key management procedures	IS-19	x	x		x	x	x
Unrestricted access to audit tools	IS-29		x	x	x	x	x
Irregular or outdated risk assessment	RI-02	x	x	x	x	x	x
Poor tenant segmentation	SA-09/11	x	x	x	x	x	

TABLE V. TOP THREAT: INSUFFICIENT DUE DILIGENCE

Vulnerability	CCM Code	Client	CSP	Infrastructure	Data	Platform/Software	Network
Lack of baseline security requirements	IS-04		x	x	x	x	x
Non-compliance to industry best practises	IS-12	x	x	x	x	x	x
Irregular or outdated risk assessment	RI-01/02	x	x	x	x	x	x
Undefined or outdated data governance requirements	DG-08	x	x		x	x	
Undefined or outdated business continuity plan	RS-01/02/03	x	x	x	x	x	x
Lack of protection against disclosure during data exchanges	SA-03	x	x		x	x	x
Non-compliance of apps and APIs to legal or regulatory obligations	SA-04		x		x	x	x
Inadequate protection against network attacks	SA-08		x		x	x	x
Poor tenant segmentation	SA-09/SA-11	x	x	x	x	x	

which aim at ensuring such compliance. Accountability concepts are evolving as the current legal framework responds to globalization and new technologies, and indeed the current drafts of the proposed EU Data Protection Regulation [33] and US Consumer Bill of Rights [34] include this concept, at least at a conceptual level. Region block compliance tools such as the EU's binding corporate rules (BCRs) [5] and APEC's cross border privacy rules (CBPRs) [35] are being developed to provide a cohesive and more practical approach to data protection across disparate regulatory systems [36]. The Galway/Paris project started by privacy regulators and privacy professionals has been defining the concept of accountability for the last four years [37] and refining its implementation, measurement and scalability.

Risk assessment is particularly important for accountability because it is a central part of the process used to determine and demonstrate that the policies (whether reflected in corporate privacy and security policies or in contractual obligations) that are signed up to and implemented by the organisation (that is taking an accountability-based approach) are appropriate to the context. The type of procedures and mechanisms vary according to the risks represented by the processing and the nature of the data [38], [6], [39]. Automation can enhance this process [40], [41].

These elements of risk assessment, transparency and redress are captured within the core elements of implementing an accountability project within an organisation specified within the Galway and Paris projects, which were [37], [42]:

1) Policies that reflect current laws and relevant standards
2) Executive oversight and responsibility for privacy
3) Delegation of responsibility to trained resources; education of staff and suppliers
4) On-going risk assessment and mitigation relating to new products or processes
5) Regular risk assessment and validation of the accountability program
6) Policies to manage major privacy events or complaints
7) Processes to enforce policies internally
8) A method of redress if privacy rights are breached

Risk assessments are mentioned explicitly as being integral to an accountability-based approach. When organisations are moving part of their systems and services to cloud, it is imperative that they implement a method to proactively assess the risk of this change, and this involves assessment of the risk throughout the whole service provision ecosystem. The presented approach discussed in this paper contributes towards such a direction. These aspects are being examined further as part of the European Framework Programme 7 Project A4Cloud (The Cloud Accountability Project) [43].

V. CONCLUSIONS

We examined in detail how privacy risk is introduced when data, applications or services are migrated to the cloud. The decision of selecting an appropriate —security and privacy wise— deployment profile is a complex decision. Initially, we provided insight on how impact should be assessed prior to the migration, adjusting the PIA process to fit to the cloud environment. We then discussed the top five privacy threats [27] and identified vulnerabilities which enable them. These can be used for risk mitigation as they were matched to appropriate controls and their applicability, in terms of stakeholder (client or CSP) and part of the system (infrastructure, data, software or network). This enables the decision maker to identify factors that increase the likelihood of a threat and at the same time understand proactively the controls that need to be implemented by both the CSP and the client itself. We then discussed accountability, and the challenges for risk assessment that enter into play when adopting an accountable approach to cloud service provision. Our future work includes a risk assessment method for cloud, which will extend the analysis beyond the scope of privacy and will offer tools for more accurate assessment, both prior and after the migration. Challenges include assessing risk when multiple CSPs participate in one cloud deployment profile and designing methods or tools for more accurate and reliable audit data from CSPs.

ACKNOWLEDGMENT

M. Theoharidou has been supported by the Excellence and Extroversion Programme (Action 2) of Athens University of Economics and Business (AUEB).

REFERENCES

[1] S. Pearson, "Privacy, security and trust in cloud computing," in *Privacy and Security for Cloud Computing*, ser. Computer Communications and Networks, S. Pearson and G. Yee, Eds. Springer London, 2013, pp. 3–42.

[2] ICO. (2013, Jul.) "Privacy impact assessment handbook," v2.0, Information Commissioner's Office, UK. [Online]. Available: http://www.ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf

[3] H.W. Kuan, H. Julia, and M. Christopher, "Data protection jurisdiction and cloud computing when are cloud users and providers subject to eu data protection law? the cloud of unknowing, Part 3," *International Review of Law, Computers & Technology*, vol. 26, pp. 2–3, 2012.

[4] N. Virvilis, S. Dritsas, D. Gritzalis D., "A cloud provider-agnostic secure storage protocol", in *Critical Information Infrastructure Security, 2010 5th International Conference on*, 2010, pp. 104–115.

[5] ICO. (2013, Jul.) "Guidance on the use of cloud computing," Information Commissioner's Office, UK. [Online]. Available: http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_computing

[6] ENISA. (2009, Nov.) "Cloud computing: Benefits, risks and recommendations for information security." [Online]. Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[7] CSA. (2011, Nov.) "Security guidance for critical areas of focus in cloud computing," v3.0, Cloud Security Alliance. [Online]. Available: http://www.cloudsecurityalliance.org/guidance/

[8] B. Martens and F. Teuteberg, "Decision-making in cloud computing environments: A cost and risk based approach," *Information Systems Frontiers*, vol. 14, no. 4, pp. 871–893, 2012.

[9] M. Kantarcioglu, A. Bensoussan, and S. Hoe, "Impact of security risks on cloud computing adoption," in *Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on*, 2011, pp. 670–674.

[10] B. Johnson and Y. Qu, "A holistic model for making cloud migration decision: A consideration of security, architecture and business economics," in *Parallel and Distributed Processing with Applications (ISPA), 2012 IEEE 10th International Symposium on*, 2012, pp. 435–441.

[11] B. S. Kaliski, Jr. and W. Pauley, "Toward risk assessment as a service in cloud environments," in *Proceedings of the 2nd USENIX conference on Hot topics in cloud computing*, ser. HotCloud'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 13–13.

[12] M. Theoharidou, N. Tsalis, and D. Gritzalis, "In cloud we trust: Risk-assessment-as-a-service," in *Trust Management VII*, ser. IFIP Advances in Information and Communication Technology, C. Fernandez-Gago, F. Martinelli, S. Pearson, and I. Agudo, Eds. Springer Berlin Heidelberg, 2013, vol. 401, pp. 100–110.

[13] J. Morin, J. Aubert, and B. Gateau, "Towards cloud computing sla risk management: Issues and challenges," in *System Science (HICSS), 2012 45th Hawaii International Conference on*, 2012, pp. 5509–5514.

[14] CSA. (2013, Feb.) "The notorious nine: Cloud computing top threats in 2013," v.1.0, Cloud Security Alliance. [Online]. Available: http://cloudsecurityalliance.org/research/top-threats/

[15] M. Kandias, N. Virvilis, and D. Gritzalis, "The insider threat in cloud computing," in *Critical Infrastructure Security (CRITIS-2011), 2011 6th International Conference on*, S. Wolthusen *et al.*, Eds. Springer, 2011, pp. 95–106.

[16] C. Horwath. (2012, Jun.) "Enterprise Risk Management for Cloud Computing," COSO. [Online]. Available: http://www.coso.org/documents/Cloud\%20Computing\%20Thought\%20Paper.pdf

[17] X. Zhang, N. Wuwong, H. Li, and X. Zhang, "Information security risk management framework for the cloud computing environments," in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, 2010, pp. 1328–1334.

[18] H. Wang, F. Liu, and H. Liu, "A method of the cloud computing security management risk assessment," in *Advances in Computer Science and Engineering*, ser. Advances in Intelligent and Soft Computing, D. Zeng, Ed. Springer Berlin Heidelberg, 2012, vol. 141, pp. 609–618.

[19] P. Saripalli and B. Walters, "Quirc: A quantitative impact and risk assessment framework for cloud security," in *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, 2010, pp. 280–288.

[20] P. Wang, W.-H. Lin, P.-T. Kuo, H.-T. Lin, and T. C. Wang, "Threat risk analysis for cloud security based on attack-defense trees," in *Computing Technology and Information Management (ICCM), 2012 8th International Conference on*, vol. 1, 2012, pp. 106–111.

[21] A. Warren, R. Bayley, C. Bennett, A. Charlesworth, R. Clarke, and C. Oppenheim, "Privacy Impact Assessments: International experience as a basis for UK Guidance," *Computer Law & Security Review*, vol. 24, no. 3, pp. 233 – 242, 2008.

[22] OPCD. (2011, Dec.) "Privacy Impact Assessments," Office of the Privacy Commissioner of Canada, Canada. [Online]. Available: http://www.priv.gc.ca/resource/fs-fi/02_05_d_33_e.asp

[23] DHS. (2010, Jun.) "Privacy Impact Assessments: The Privacy Office Official Guidance," Dept. of Homeland Security. [Online]. Available: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf

[24] EC. (2011, Jan.) "Privacy and Data Protection Impact Assessment Framework for RFID Applications," European Commission (EC). [Online]. Available: http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf

[25] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," Special Publication 800-144, NIST, December 2011.

[26] L. Marinos and A. Sfakianakis, "ENISA threat landscape," Tech. Rep., ENISA, 2012.

[27] CSA. (2013, Mar.) "Cloud Controls Matrix," Cloud Security Alliance, v.1.4. [Online]. Available: http://cloudsecurityalliance.org/research/ccm/

[28] CSA. (2011, Jan.) "Consensus assessments initiative questionnaire," Cloud Security Alliance. [Online]. Available: http://cloudsecurityalliance.org/research/cai/

[29] S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services," in *Cloud 2009: ICSE Workshop on Software Engineering Challenges of Cloud Computing*. Vancouver, IEEE, 2009, pp. 44–52.

[30] ISO/IEC. "Information technology - Security techniques - Privacy framework," ISO/IEC 29100:2011, 2011.

[31] APEC. (2005, Dec.) "APEC privacy framework," APEC Secreteriat. [Online]. Available: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

[32] PIPEDA. (2000, Apr.) "Personal Information Protection and Electronic Documents Act," S.C. 2000, c. 5. [Online]. Available: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/

[33] European Commission . (2012) "Proposal for a directive of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. . [Online]. Available:http://ec.europa.eu/justice/data-protection/document/review2012/com201210en.pdf

[34] (2012, Feb.) "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," White House. [Online]. Available: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[35] APEC. (2011, Sep.) "Cross-border privacy enforcement arrangement," APEC Data Privacy Sub-Group, San Francisco, USA. [Online]. Available: http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_010.pdf

[36] L. Moerel, "Binding corporate rules," Ph.D. dissertation, Tilburg University, 2011.

[37] CIPL. (2009, Oct.) "Data protection Accountability - the essential elements: A document for discussion," Center for Information Policy Leadership. [Online]. Available: http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf

[38] CNIL. (2012, Jun.) "Methodology for privacy risk management," Commission Nationale de l'Informatique et des Libertés? [Online]. Available: http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf

[39] C. Castelluccia, P. Druschel, S. Fischer Hübner, A. Pasic, B. Preneel, and H. Tschofenig. (2011, Feb.) "Privacy, accountability and trust - challenges and opportunities," ENISA. [Online]. Available: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pat-study/at_download/fullReport

[40] S. Pearson, "Toward accountability in the cloud," *Internet Computing, IEEE*, vol. 15, no. 4, pp. 64–69, 2011.

[41] ——, "Privacy management in global organisations," in *Proceedings of the 13th IFIP TC 6/TC 11 international conference on Communications and Multimedia Security*, ser. CMS'12. Berlin, Heidelberg: Springer-Verlag, 2012, pp. 217–237.

[42] CIPL. (2010, Oct.) “Accountability Project (Galway Project),” Center for Information Policy Leadership. [Online]. Available: http://www.informationpolicycentre.com/accountability-based_privacy_governance/

[43] (2013, Jul.) “Cloud Accountability Project - A4Cloud,” http://www.a4cloud.eu/