Migrating into the Cloud: Identifying the Major Security and Privacy Concerns

Christos Kalloniatis[1], Vassilis Manousakis[1], Haralambos Mouratidis[2], and Stefanos Gritzalis[3]

[1] Department of Cultural Technology and Communication, University of the Aegean, University Hill, GR 81100 Mytilene, Greece
chkallon@aegean.gr, ct08081@ct.aegean.gr
[2] School of Architecture, Computing and Engineering, University of East London, Docklands Campus, 4-6 University Way, E16 2RD, London, U.K.
haris@uel.ac.uk
[3] Information and Communication Systems Security Laboratory, Department of Information and Communications Systems Engineering, University of the Aegean, GR 83200, Samos, Greece
sgritz@aegean.gr

Abstract. Cloud Computing is without a doubt one of the most significant innovations presented in the global technological map. The number of potential users enrolling and using cloud services increases exponentially on a daily bases. The great demand from online users for cloud services along with the reduced operational costs that the latter offers has motivated many organisations and companies to consider migrating organizational services, data and applications on the Cloud. However, despite the various positive characteristics of all cloud service models like reduced costs, better availability insurance, on demand data storage and computation power, cloud migration may hinder various security and privacy issues that need to be considered before an organization or company decides to move on to the Cloud. This paper aims to reveal the major security and privacy concepts for all three cloud service models and through a systematic analysis to guide the organization's stakeholders in deciding which service model best fits their needs based on their security and privacy requirements.

1 Introduction

According to National Institute of Standards and Technology (NIST), Cloud Computing delivers three different types of services to the end users that derive from three different models. The delivery models are IaaS, PaaS and SaaS, each one of them providing three distinct types of resources, like virtual infrastructure resources, application platforms and software services. Each delivery model is considered as separate layer that is depended from each other and with IaaS being the foundation, PaaS sits on top of IaaS and SaaS sits on top of PaaS. So, as the end users combine different type of services for implementing their requirements, they need to consider the various combined security and privacy threats that are behind these services.

C. Douligeris et al. (Eds.): I3E 2013, IFIP AICT 399, pp. 73–87, 2013.

Another factor that should be considered is the impact of deployment model on privacy and security measures. Security and privacy risks seem to have larger impact on public, hybrid and community cloud, compared to the rest of the deployment models. On the other hand, cloud consumers should keep in mind that while private cloud deployments are theoretically safer, still the same security and privacy threats do apply. The only difference is the users' group that the model is based on. In this deployment model, users starting from the administrator down to the simple one are trusted, but this does not imply a more secure and privacy oriented model.

In general, the more low level services the client requests the more responsible for security and privacy is, but still the cloud vendor has an important role on managing and implementing security and privacy measures even in low levels of abstraction.

The various innovations that cloud computing introduced in its operational environment vary from the traditional "trusted" environment where today's information systems rely on. These innovations hinder new security and privacy concepts that need to be identified in order to protect the traditional systems when migrating to cloud environments. This is exactly the scope of the specific paper. Specifically, in section 2 the critical cloud threats are presented as they have been examined from the respective literature. At the end of section two an analysis of the respective threats along with the cloud critical areas and cloud service models is conducted. In section 3 the description of the newly identified security and privacy concepts are described along with respective case diagrams. At the end of section 3 a matching between the newly concepts and their applicability on the cloud service models is presented in order to reveal the linkability and influence on every concept on the respective service model. This matching can also assist in informing the cloud users about what they should consider when migrating to the cloud as far as security and privacy requirements are considered, by matching them with each cloud service model separately without omitting of course to make a solid research for the above mentioned scenarios that meet their needs.

2 Critical Threats in Cloud Computing

In order to identify the major security and privacy cloud concepts an analysis of the major threats in cloud computing was conducted. The threats identified are based on the identified issues of the Cloud Security Alliance (CSA) report [1] as well as the ones from Gartner presented in [2] and mentioned in [3].

2.1 Threat #1: Abuse and Nefarious Use of Cloud Computing

Abuse and nefarious use of cloud benefits derive from the result of several reasons. For example, the constant advertisement of cloud's advantages result in attraction of more and more users in order to test their services, only to make cloud a giant pool of potential victims and attackers that want to exploit cloud vulnerabilities or even use cloud's computing power to perform illegal activities, all the above combined with Inadequate identity management[1] and lack of know-how[2] converts cloud from a

[1] Partial anonymity through weak registration.
[2] Limited of fraud detection capabilities.

ubiquitous and convenient resource pool, into an unsafe place to migrate someone's business vital operations. Several examples of this kind of usage are hosting of Zeus botnet, Trojan horses, Microsoft and Adobe PDF exploits, etc. The specific threat is matched with data center operations and Incident Response, Notification and Remediation domains and has applicability on IaaS and PaaS service models.

2.2 Threat #2: Insecure Interfaces and APIs

A variety of software interfaces and APIs are in use in order for the cloud services to be managed by the customers. Several actions like, management, provisioning, orchestration and monitoring are carried out through them. Customers, organizations and third parties interact with general cloud services through APIs, in order to process in implementing various services for their customers. Thus security and mainly availability of these APIs are of critical importance in the cloud environment. Confidentiality, integrity, availability and accountability are some of the issues that organizations are exposed through vulnerable APIs and interfaces[3]. The specific threat is matched with the application security domain and has applicability on IaaS, PaaS and SaaS service models.

2.3 Threat #3: Malicious Insiders

A malicious insider is a realistic scenario that a client cannot take immediate action. Opaque processes and procedures, not strict access to cloud's resources both physical and virtual, deficient monitoring, policy incompliance and improper employee hiring standards and in general lack of transparency are creating an attractive environment that could enable a potential adversary to gain control over cloud services and tamper data that rely on them. The specific threat is matched with the Governance and Enterprise Risk Management as well as with the Traditional Security, Business Continuity and Disaster Recovery domains and has an applicability on IaaS, PaaS and SaaS service models.

2.4 Threat #4: Shared Technology Issues

Virtualization is the concept that cloud computing notion was build. Dynamic provisioning of services in multi-tenant environment due to hardware virtualization (e.g., CPU,GPU, RAM, Disk partitions etc.) are promising advantages. On the other hand, the underlying infrastructure does not offer strong isolation between tenants, and as a result a virtualization hypervisor was implemented to fill this gap but still the issue has not completely addressed. As a matter of fact there are several examples like Joanna Rutkowska's Red and Blue pill and Kortchinksy's CloudBurst presentations that impact other tenants operations, tamper with data, network traffic, etc. The specific threat is matched with the data center operations and virtualization domains and has applicability on IaaS service model.

[3] Hidden filed manipulation, reusable tokens or passwords, clear-text authentication or transmission of content, improper authorizations, etc.

2.5 Threat #5: Data Loss or Leakage

Due to cloud's architecture the threat of data compromise increases. Data loss or leakage (through virtualization flaws) can cause unrecoverable damage and serious implications[4]. Insufficient AAA controls and encryption and software keys, system and operational failures, data lifecycle management challenges, compliance issues, vendor and client reliability are examples that derive from this threat. The specific threat is matched with the Information management and data security, the encryption and key management as well as the identity and access management domains and has applicability on IaaS, PaaS and SaaS service models.

2.6 Threat #6: Account or Service Hijacking

Phishing frauds, vulnerabilities exploitation, software exploitation or even user's personal choices (reused passwords) are methods that can lead to various threats in a cloud environment as for example hijacking. The damage that could cause a breach in terms of eavesdropping, tampering, service confidentiality, integrity and availability, is great. The specific threat is matched with the governance and enterprise risk management, the incident response, notification and remediation as well as the identity and access management domains and has applicability on IaaS, PaaS and SaaS service models.

2.7 Threat #7: Unknown Risk Profile

Seemingly insignificant factors about security should be considered by organizations. Software versions, updates, compliance, security practices and design, log files, information about the co-tenants, maintenance, who has access to the data or who is responsible or what data will be disclosure in case of an incident, how the data are stored in case of an incident, etc., all the above mentioned constitute an Unknown risk profile that companies should carefully weight. The specific threat is matched with the governance and enterprise risk management, the legal issues: contracts and electronic discovery, the data center operations as well as the incident response, notification and remediation and has applicability on IaaS, PaaS and SaaS service models.

2.8 Threat #8: Privileged User Access

Migrating to a cloud solution may result in loss of physical control over the organization operations and functions. Concerns as far as, "who" has access to data and the procedures in general, which are the hiring requirements, which is the level of access are posed. The specific threat is matched with the governance and enterprise risk management, compliance and audit and identity and access management domains and has applicability on IaaS, PaaS and SaaS service models.

[4] Brand and reputation damage to compliance violations and legal ramifications, etc.

2.9 Threat #9: Regulatory Compliance

Cloud providers are obliged to follow laws and regulations of each country where respective cloud services are reside from. Each country has different regulations as far as certain[5] procedures are done and the customer should be completely aware of them only to take his decisions. The specific threat is matched with the governance and enterprise risk management and compliance and audit domains and has applicability on IaaS, PaaS and SaaS service models.

2.10 Threat #10: Data Location

Security, privacy and data lifecycle procedures are strictly related to the country that the respective cloud services reside from. For example large datacenters may reside on foreign countries that have different jurisdictions specifications and regulations compared to the client's country. Client should be aware of that and make explicitly clear to the vendor the demands they have in mind. The specific threat is matched with the governance and enterprise risk management and compliance and audit and legal issues domains and has applicability on IaaS, PaaS and SaaS service models.

2.11 Threat #11: Lack of Data Segregation

Multi-tenancy in cloud computing is a basic concept that raises questions about the level of isolation between the tenants. Data should be completely isolated through the entire data lifecycle in order for the client to be protected. The specific threat is matched with the encryption and key management and virtualization domains and has applicability on PaaS and SaaS service models.

2.12 Threat #12: Lack of Recovery

In case of a disaster a solid recovery system should be in preparedness, just to restore services and data in their previous healthy state. The specific threat is matched with the traditional security, business continuity and disaster Recovery, incident response, notification and remediation domains and has applicability on PaaS and SaaS service models.

2.13 Threat #13: Investigate Support

In case of a security violation a properly configured forensics system should be ready, in order to examine the causes and the circumstances of the incident. Such actions are difficult due to cloud's nature, but provider should be ready to deal with this kind of emergencies. The specific threat is matched with Security as a Service and incident response, notification and remediation domain and has applicability on IaaS, PaaS and SaaS service models.

---

[5] Data processes, security and privacy procedures, etc.

2.14 Threat #14: Long-Term Viability

Cloud provider should have safety measures in case that something breaks tis service continuity (bankruptcy, DDoS attacks, etc.). Customer's data not only should be available in those situations, but there should be in their last healthy state. The specific threat is matched with portability and operability and traditional security, business continuity and disaster recovery domains and has applicability on IaaS, PaaS and SaaS service models.

CSA has also issued a report [4] regarding the cloud critical areas, with Cloud Architecture included, that Cloud providers and users should take into account, related both to strategic and tactical Security and Privacy pain points that exist in a Cloud environments and falls into any combination of cloud service and deployment model. The domains are divided into two main categories, governance and operations. Strategic and policy issues are addressed through governance domains, while the operational domains deal with security concerns and implementation techniques within the Cloud architecture. The critical areas are: a) Cloud Computing Architectural Framework, b) Governance and Enterprise Risk Management, c) Legal Issues : Contracts and Electronic Discovery, d) Compliance and Audit, e) Information Management and Data Security, f) Portability and Operability, g) Traditional Security, Business Continuity and Disaster Recovery, h) Data Center operations, i) Incident Response, Notification and Remediation, j) Application Security, k) Encryption and key management, l) Identity and Access Management, m) Virtualization and n) Security as a Service.

The matching between the aforementioned threats and the respective cloud service models is presented in table 1. In table 2 a matching between the aforementioned threats and the cloud critical areas is presented. These matching can assist the developers in identifying the possible drawbacks that will have to solve when deciding a cloud migration on a specific cloud model. Also this analysis assisted in the basic security and privacy concepts identification presented in section 3.

3 Security and Privacy-Oriented Concepts

This section describes the basic security and privacy properties that constitute the basic issues that need to be considered when a migration to the cloud needs to be established. The aim of this section is twofold. Firstly it aims on revealing and describing a number of concepts some of which are derived from the respective literature.

Secondly it aims on identifying the applicability of every concept on the respective cloud service model thus assisting the stakeholders on deciding which security and privacy properties need to be realised in order to satisfy their own goals on every cloud service model respectively. The concepts proposed are mainly derived from the European Commission Draft Report on Security Issues in Cloud Computing [5] as well as from our previous work presented in [6-13]. However, new concepts are also introduced and explained in order to form a complete set for covering all the respective cases.

Table 1. Matching Major Cloud Threats with Cloud Service Models

	IaaS	PaaS	SaaS
Threat #1: Abuse and Nefarious Use of Cloud Computing	x	x	
Threat #2: Insecure interfaces and APIs	x	x	x
Threat #3: Malicious Insiders	x	x	x
Threat #4: Shared technology issues	x		
Threat #5: Data Loss or Leakage	x	x	x
Threat #6: Account or Service Hijacking	x	x	x
Threat #7: Unknown Risk Profile	x	x	x
Threat #8: Privileged user access	x	x	x
Threat #9: Regulatory Compliance		x	x
Threat #10: Data Location	x	x	x
Threat #11: Lack of Data Segregation		x	x
Threat #12: Lack of Recovery		x	x
Threat #13: Investigate Support		x	x
Threat #14: Long-term Viability	x	x	x

Table 2. Matching Threats with Critical Cloud Areas

	Gov. & Enterpr. Risk Manag.	Legal Issues	Compliance and Audit	Inform.Manag & Data Security	Portability and Operability	Traditional Security, Business Continuity & Disaster Recovery	Data Center operations	Inc. Resp., Notific. & Remediation	Application Security	Encryption and key management	Identity and Access Management	Virtualization	Security as a Service
Threat #1: Abuse and Nefarious Use of Cloud Computing							x	x					
Threat #2: Insecure interfaces and APIs									x				
Threat #3: Malicious Insiders	x					x							
Threat #4: Shared technology issues							x					x	
Threat #5: Data Loss or Leakage				x						x	x		
Threat #6: Account or Service Hijacking	x							x			x		
Threat #7: Unknown Risk Profile	x	x					x	x					
Threat #8: Privileged user access	x					x							
Threat #9: Regulatory Compliance	x	x	x										
Threat #10: Data Location	x	x	x	x									
Threat #11: Lack of Data Segregation				x		x							
Threat #12: Lack of Recovery						x		x					
Threat #13: Investigate Support								x					x
Threat #14: Long-term Viability	x					x							

3.1 Isolation

The specific concept is referred to the complete seal of user's data inside the Cloud computing environment. Cloud computing resources sharing among a multi-tenant environment, poses the risk of any kind of information disclosure. As a result strong isolation must be achieved inside the cloud environment. Isolation is meant to address data disclosure in two ways, firstly, from purpose limitation point of view and secondly from the aspect of hypervisor hardening [5].

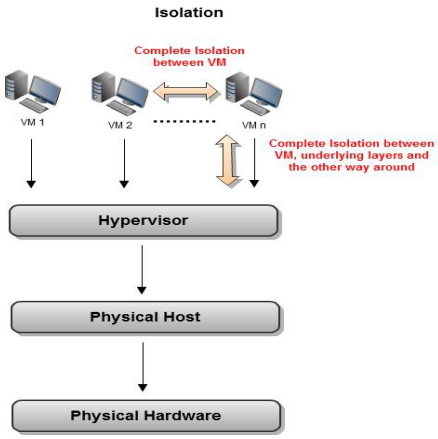

Fig. 1. Isolation Example

3.2 Provenanceability

The specific concept is referred to a vm's provenance mapping. Building a virtual machine's background tree makes it easier to get information about its parent image. The goal is to gather information about the reason of creating a new image, modifications, updates, vulnerabilities, etc. inside the cloud environment. The above, can be used to trace malicious actions of illegal content inside the vm image or let the owners know of a derived image that the parent image had for example a security problem [14].

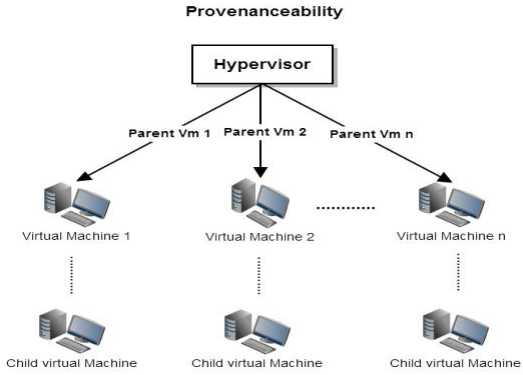

Fig. 2. Provenaceability Example

3.3 Traceability

Traceability concept aims to give the ability, for the data to be traced or not by the user. Data erasure is a major problem in web-based systems and still continues to

exist in clouds. Many cases have been documented for privacy violation due to improper data deletion (documents, photos, etc.). The traceability concept aims to reassure the clients that their data have been completely deleted or stay invisible and anonymized through the ability of tracing them among the data repositories.

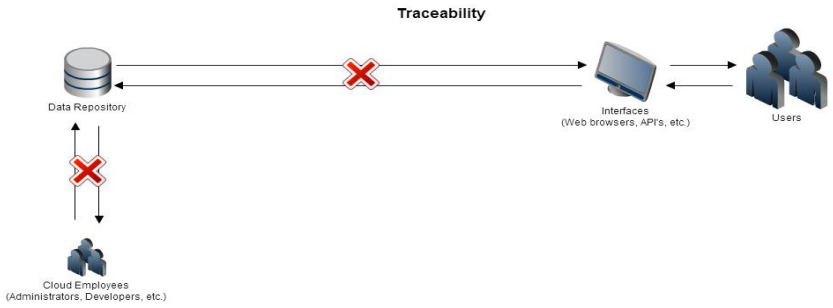

Fig. 3. Traceability Example

3.4 Availability

The specific concept tends to protect the system through specific procedures and techniques from meeting the above unwanted situations. Migration of enterprises operations to the cloud means that cloud provider is obliged to provide continuously the services to the specific enterprise no matter what. DoS attacks, physical disasters and hardware failure may result in breaking the continuity of service providing. That concept is to heal through specific procedures and techniques the above unwanted situations.

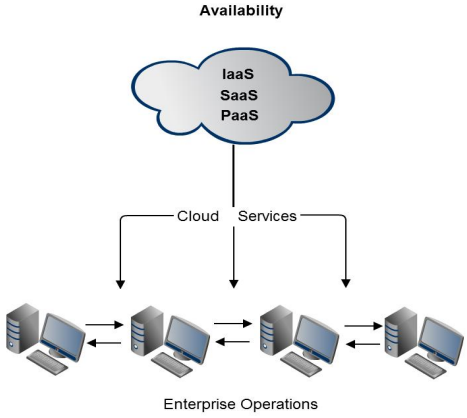

Fig. 4. Availability Example

3.5 Integrity

Integrity is referred to the fact that client's data remains in the exact form in which he send it in the first place. According to the EU directive [5], cloud providers must assure the user that his data have not got tampered while they were passing through the whole data life cycle. Integrity concept aims to provide to user assurances that their data have not been tampered somehow.

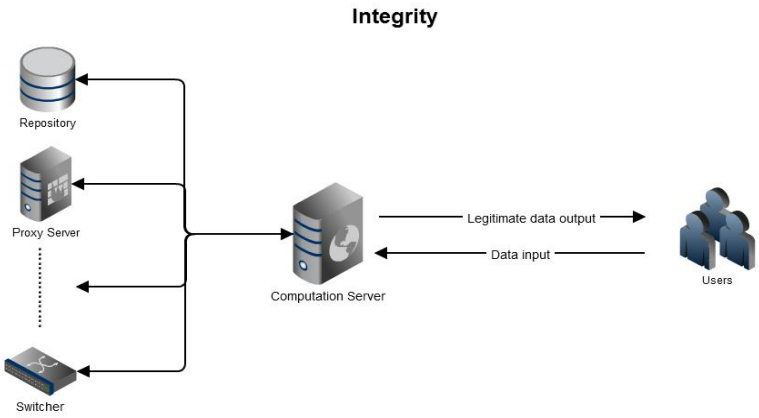

Fig. 5. Integrity Example

3.6 Confidentiality

Confidentiality issue derives from the fact that cloud is multi-tenancy environment and many of its resources are shared. That raises concerns about the data that travel inside the cloud, from the cloud provider to the client, and vice versa. Encryption techniques and authorization and authentication mechanisms, ensures that data's confidentiality is preserved [5].

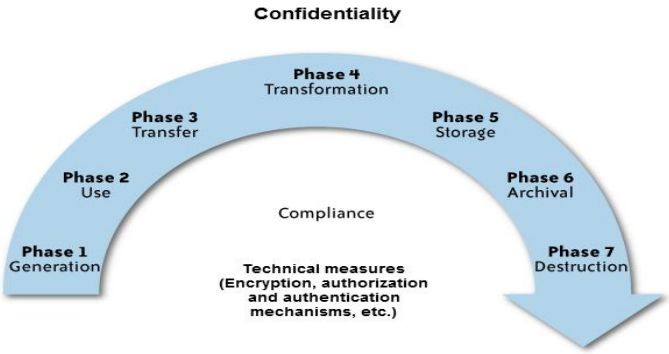

Fig. 6. Confidentiality Example

3.7 Transparency

Transparency concept is referred to the cloud vendor's obligation, to be completely clear about their procedures and functions. In order to preserve integrity and confidentiality of a client's data, transparency in several areas of cloud's procedures should exist. According to the EU directive, transparency must exist in regard to the contractors and subcontractors that cloud providers are related to and the internal cloud operations and procedures that the provider follows in certain circumstances [3, 5].

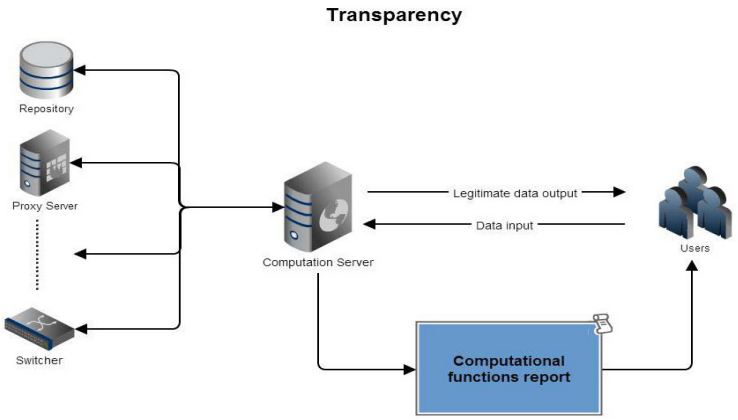

Fig. 7. Transparency Example

3.8 Intervenability

Intervenability concept is referred to the fact that, the users should be able to process their data despite the cloud's service architecture. A cloud vendor may rely on other provider's (subcontractor) services in order to offer his services. That should not be an obstacle for the user to intervene[6] to his data, in fact cloud vendor must be able to provide all the technical and organizational means to this goal including subcontractors [5].

3.9 Portability

Portability concept aims to achieve transferability as data are concerned, among different cloud providers and services. As we mentioned earlier data or vendor lock-in could result in lack of data portability and interoperability between different cloud services. The use of a standard format could impose obstacles in the transfer of personal data or even result in data disuse, due to the lack of compatibility, if a cloud vendor is bankrupted [5].

[6] Access, rectification, erasure, blocking and objection.

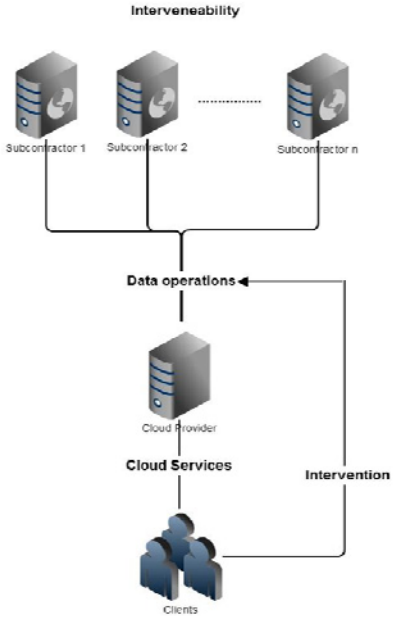

Fig. 8. Intervenability Example

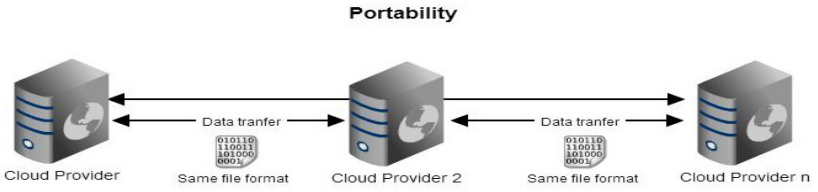

Fig. 9. Portability Example

3.10 Accountability

Accountability concept is referred to the fact that, cloud providers should provide information anytime about an incident. The cloud architecture[7] makes a complex form of an informational system. In terms of management and audit controls, this fact could result in very difficult manageability of incidents. A cloud provider should be able at any time to provide information about what an entity did and when, just to trace malicious actions from the whole cloud infrastructure [5].

[7] International services residual.

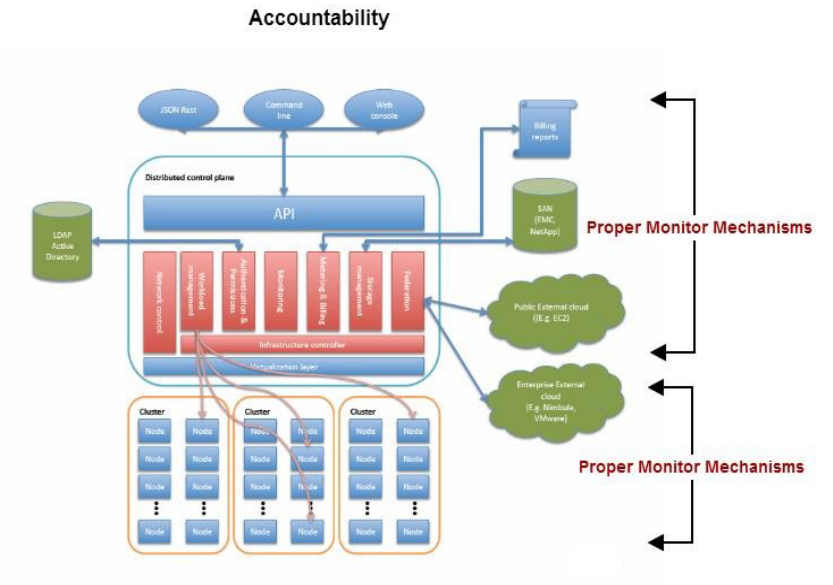

Fig. 10. Accountability Example

It should be mentioned that beside the above presented concepts other security and privacy properties do exist that can be taken under consideration when considering migrating an Information System to the Cloud. In [6-13] a number of security and privacy concepts are presented. These concepts have been presented for transforming privacy from a generic, mostly legal concept, to a technical requirement that analysts can enroll in the analysis and design process. These concepts also play a significant role in the migration process but due to space limitations are not presented analytically in this paper.

In the following table a matching between the aforementioned concepts and the cloud service models is presented. Based on the following table analysts can identify which are the security and privacy concepts belonging to their system and how these

Table 3. Matching Security and Privacy Properties with Cloud Services Models

	IaaS	SaaS	PaaS
Property #1: Isolation	x	x	x
Property #2: Provencability	x		
Property #3: Traceability		x	
Property #4: Availability	x	x	x
Property #5: Integrity		x	
Property #6: Confidentiality	x	x	x
Property #7: Transparency		x	
Property #8: Intervenability	x	x	x
Property #9: Portability		x	x
Property #10: Accountability	x	x	x

concepts can constitute an initial obstacle during the migration of a traditional system on a cloud environment. Usually when analysts consider the cloud migration their main goal is to decide on which service model they are interested in migrating to. The identified concepts and the respective matching is a start for creating a holistic process for assisting analysts on receiving the proper decisions.

4 Conclusions

Cloud computing environments offer great degree of scalability, flexibility and resource pooling thus elevating its use leading to its great expandability and applicability noted nowadays [15]. Many users, private companies and public organisations on a daily basis consider migrating their systems into the cloud in order to take advantage of these possibilities. However, cloud innovations hinder new undiscovered threats that analysis and users need to be considered before deciding the big change of cloud migration. This paper is an initial step on identifying a set of new concepts that need be realised in both cases either when migrating or developing from scratch information systems in cloud environments. The main contribution of the paper is the identification of various security and privacy concepts as well as the introduction of new ones under one framework. The identification was based on the threats revealed from the respective literature and extended with the introduction of some newly defined complementary concepts. Future steps include the transformation of these concepts on technical requirements and the design of a modeling process for applying these requirements on a real case scenario.

References

1. Cloud Security Alliance “Top Threats to Cloud Computing V1.0” (retrieved September 22, 2012), https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
2. Heiser, J., Nicolett, M.: Assessing the Security Risks of Cloud Computing, white paper, Gartner group, ID Number: G00157782 (published June 3, 2008)
3. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications 34(1), 1–11 (2010)
4. Cloud Security Alliance “Security Guidance for Critical Areas of Focus in Cloud Computing V3.0” (retrieved September 22, 2012), https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
5. Draft, EU Directive for Security issues in Cloud Computing (2012)
6. Kalloniatis, C., Kavakli, E., Gritzalis, S.: PriS Methodology: Incorporating Privacy Requirements into the System Design Process. In: Mylopoulos, J., Spafford, G. (eds.) Proceedings of the SREIS 2005 13th IEEE International Requirements Engineering Conference – Symposium on Requirements Engineering for Information Security. IEEE CPS, Paris (2005)
7. Kalloniatis, C., Kavakli, E., Gritzalis, S.: Addressing privacy requirements in system design: The PriS method. Requirements Engineering 13(3), 241–255 (2008)

8. Kalloniatis, C., Kavakli, E., Kontellis, E.: PRIS tool: A case tool for privacy-oriented Requirements Engineering. Journal of Information Systems Security 6(1), 3–19 (2010)
9. Kavakli, E., Kalloniatis, C., Loucopoulos, P., Gritzalis, S.: Incorporating Privacy Requirements into the System Design Process: The PriS Conceptual Framework. Internet Research, Special issue on Privacy and Anonymity in the Digital Era: Theory, Technologies and Practice 16(2), 140–158 (2006)
10. Kalloniats, C., Kavakli, E., Gritzalis, S.: Dealing with Privacy Issues during the System Design Process. In: 5th IEEE International Symposium on Signal Processing and Information Technology, Athens, Greece, December 18-21 (2005)
11. Mouratidis, H., Kalloniatis, C., Islam, S., Huget, M.P., Gritzalis, S.: Aligning Security and Privacy to support the development of Secure Information Systems. Journal of Universal Computer Science (2012)
12. Mouratidis, H., Giorgini, P.: Secure Tropos: A Security-Oriented Extension Of The Tropos Methodology. International Journal of Software Engineering and Knowledge Engineering (2007)
13. Mouratidis, Giorgini, P.: Security Attack Testing (SAT) - testing the security of information systems at design time. Inf. Syst. 32(8), 1166–1183 (2007)
14. Wei, L., et al.: Managing Security of Virtual Machine Images in a Cloud Environment (2009)
15. Microsoft Technical report: Privacy in the cloud computing era, a Microsoft perspective, Microsoft Corp., Redmond, USA (November 2009)