Towards the design of secure and privacy-oriented Information Systems in the Cloud: Identifying the major concepts

Christos Kalloniatis
Cultural Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, University Hill, GR81100 Mytilene, Greece, chkallon@aegean.gr

Haralambos Mouratidis
Secure and Dependable Software Systems (SenSe) research cluster, School of Computing, Engineering and Mathematics, University of Brighton, h.mouratidis@brighton.ac.uk

Manousakis Vassilis
Cultural Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, University Hill, GR81100 Mytilene, Greece, ct08081@ct.aegean.gr

Shareeful Islam
School of Architecture, Computing and Engineering, University of East London, U.K., shareeful@uel.ac.uk

Stefanos Gritzalis
Information and Communication Systems Security Laboratory, Department of Information and Communications Systems Engineering, University of the Aegean, GR83200 Samos, Greece, sgritz@aegean.gr

Evangelia Kavakli
Cultural Informatics Laboratory, Department of Cultural Technology and Communication, University of the Aegean, University Hill, GR81100 Mytilene, Greece, kavakli@ct.aegean.gr

Category

Research Paper

Towards the design of secure and privacy-oriented Information Systems in the Cloud: Identifying the major concepts

Abstract

Cloud computing is without a doubt one of the most significant innovations presented in the global technological map. This new generation of technology has the potential to positively change our lives since on the one hand it provides capabilities that make our digital lives much easier, than before, while on the other hand it assists developers in creating services that can be disseminated easier and faster, than before, and with significantly less cost. However, one of the major research challenges for the successful deployment of cloud services is a clear understanding of security and privacy issues on a cloud environment, since the cloud architecture has dissimilarities comparing to the traditional distributed systems. Such differences might introduce new threats and require different treatment of security and privacy issues. Nevertheless, current security and privacy requirements engineering techniques and methodologies have not been developed with cloud computing in mind and fail to capture the unique characteristics of such domain. It is therefore important to understand security and privacy within the context of cloud computing and identify relevant security and privacy properties and threats that will support techniques and methodologies aimed to analyze and design secure cloud based systems. The contribution of this paper to the literature is two-fold. Firstly, it provides a clear linkage between a set of critical cloud computing areas with security and privacy threats and properties. Secondly, it introduces a number of requirements for analysis and design methodologies to consider for security and privacy concerns in the cloud.

Towards the design of secure and privacy-oriented Information Systems in the Cloud: Identifying the major concepts

1. Introduction

The last few years, a new generation of technology has positively invaded our lives providing a number of capabilities that has made our digital behavior much easier than before. This technology is commonly known as "cloud computing". Various well-known services such as email, instant messaging, and web content management, are among the many applications that can be offered via a cloud environment. Although many of these services and applications were offered, through the Internet, before the cloud era; cloud computing environments offer greater degree of scalability, flexibility, and resource pooling thus elevating its use, leading to its great expandability and applicability noted nowadays [1].

While the degree of Internet users that enroll and access cloud based services rises dramatically every day, recent surveys reveal the uncertainty and instability of cloud environments. In June 2009, a survey conducted by a document management software company revealed, that 41% of senior IT professionals don't know what cloud computing really is [2]. From the remaining 59% of IT professionals, who stated that they know what cloud computing is, 17% of them understand cloud computing to be internet-based computing while 11% believe it is a combination of internet-based computing, software as a service (SaaS), software on demand, an outsourced or managed service and a hosted software service. The remaining respondents understand cloud computing to be a mixture of the above. One of the innovations that cloud computing introduced and played a key role in its rapid development is the use of virtualisation as a way for providing three basic types of services: software, platform and infrastructure. However, most of the recent studies [3-7] have identified a number of security and privacy challenges uniquely to the cloud. Although, typical security and privacy concerns, such as data protection, unauthorised access, data handling and traceability, are the same as in traditional distributed systems, but the solutions required and the requirements introduced by those in a cloud context are very different than those used in traditional systems.

When engineering software systems, it is necessary to identify and model respective security and privacy properties based on the system specific context so that appropriate security and privacy requirements can be identified and analysed. The elicited security and privacy requirements should be implemented within the system, which should enclose all the necessary measures for dealing with possible security and privacy threats that will cause harm to its assets or users. A number of research efforts [8-11] have already contributed to the area of identifying and analyzing security and privacy requirements for the development of software systems. However, these works have not been developed for cloud-based systems. On the other hand, industry-led reports [1, 2, 12] have been published discussing security and privacy issues within the context of cloud computing. However, most of these reports provide a list of security and/or privacy issues without providing a clear linkage with relevant security and privacy properties and threats. Moreover, they do not explicitly discuss any set of requirements that are essential for analysis and design methodologies to incorporate, to support security and privacy analysis for cloud based systems.

This paper makes a number of contributions. Figure 1 provides an overview of our contributions. On the one hand, we discuss a number of security and privacy properties that are applicable to the cloud. Our work in that area is based on the highly influential and important report from the Cloud Security Alliance (CSA) [13] and work from an EU report on cloud computing [14]. However, our work introduces a number of security and privacy properties that are not discussed in these reports. On the other hand, we provide a clear linkage between those properties and relevant security and privacy threats. In particular, based on the list of threats published by CSA [3] and Gartner [15], we discuss how each of the security and privacy properties can be linked to specific threats. Finally, we provide set of requirements that we consider important for any development methodology that supports analysis and design of security and privacy in the cloud. Although, we do not claim that the list of presented requirements is final (on the contrary we believe it is work in progress), we believe the list provides a good starting point for any developers that would like to consider inclusion of cloud security and privacy analysis in their methodology. As shown in Figure 1, we start with cloud computing areas and conclude with list of requirements based on the security and privacy properties, threats and critical areas.

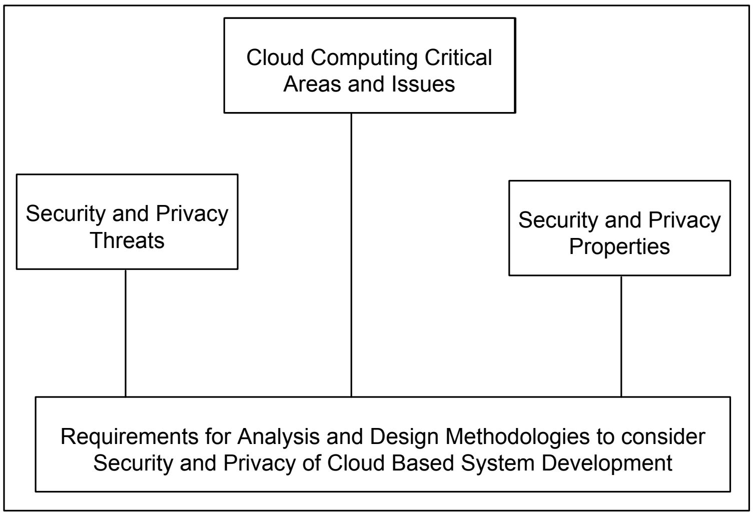
Cloud Computing Critical Areas and Issues
Security and Privacy Threats
Security and Privacy Properties
Requirements for Analysis and Design Methodologies to consider Security and Privacy of Cloud Based System Development

Figure 1. Overview of the contribution

Section 2 provides a brief overview of the basic cloud-computing characteristics. In section 3, the most critical cloud computing areas are presented along with security and privacy threats. In section 4, the major security and privacy properties are discussed and a clear linkage is provided between issues, threats and properties. Moreover, a set of requirements is presented for methodologies based on the linkage of issues, threats and properties in section 5. Section 6 presents related work both on software engineering methods both in the fields of traditional systems as well as cloud oriented. Finally, section 7 presents areas for future work and concludes the paper.

2. Cloud Computing main characteristics

Cloud computing is the delivery of computing and storage capacity as a service [12] to a community of end-recipients. Cloud computing entrusts services with a user's data, software and computation over a network, following a logical diagram as shown in Figure 2. Cloud computing providers offer their services according to three fundamental models [16-18]: a) Infrastructure as a Service (IaaS), where users rent use of servers provided by one or more cloud providers; b) Platform as a Service (PaaS), where users rent use of servers and the system software to use in them; and c) Software as a Service (SaaS), where users rent also application software and databases. In the cloud, IaaS is the most basic and each higher model abstracts from the details of the lower models as it is graphically shown in Figure 3.

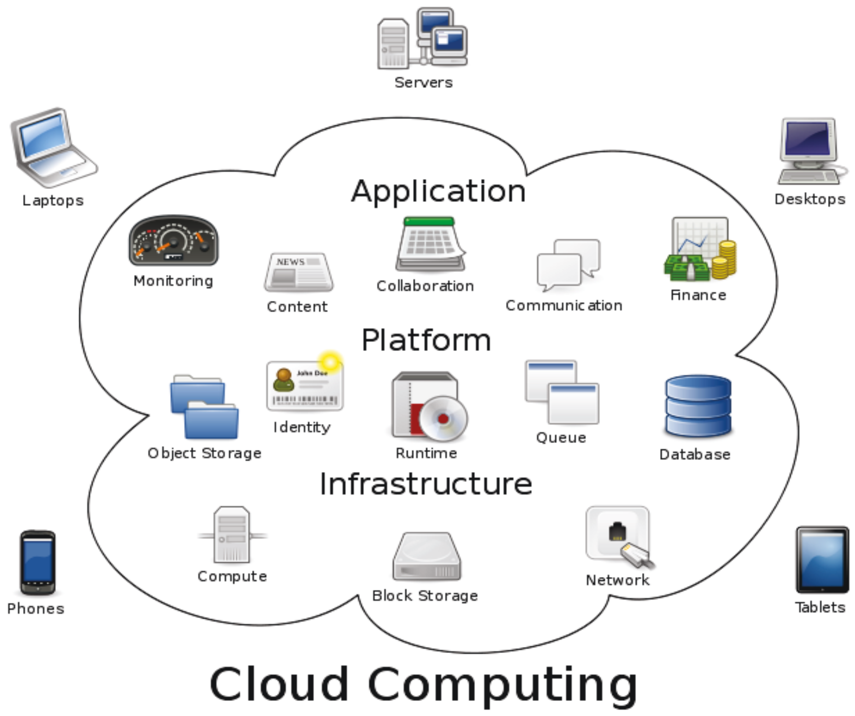

Figure 2. Cloud Computing Logical Diagram

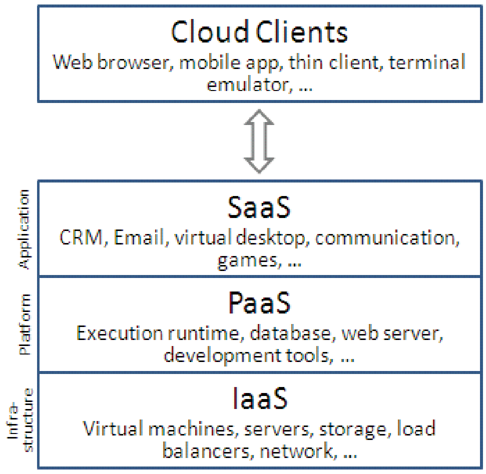
Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

Figure 3. Cloud Computing Layers

Cloud computing provides the following characteristics:

a) *Agility,* which improves users' ability to re-provision technological infrastructure resources;

b) *Cost,* which is reduced since infrastructure is typically provided by a third party and does not need to be purchased for one-time or infrequent intensive computing tasks. Also the cost of IT skills is lowered since in-house implementation is avoided [19];

c) *Virtualisation*, which is the basic technology used in cloud environments allowing servers and storage devices to be shared thus increasing utilization. Applications are usually being migrated from one server to another depending on the capacity and usage of the cloud providers' infrastructure;

d) *Multitenancy*, which enables the sharing of resources and cost across a large pool of users allowing centralization of infrastructure, increment of peak-load capacity and systems' utilization and efficiency improvement [20];

e) *Reliability,* which is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery [21];

f) *Scalability* and *elasticity*, which support the on-demand provisioning of resources on a fine-grained self-service basis near real-time without users having to engineer for peak loads [22-23];

g) *Device and location independence*, which support users to access cloud services from anyplace through a web-browser regardless of the device they are using or the location they are accessing the service from [24].

h) *Maintenance,* which is easier since there is no software installation on each user's machine and the services' sources are managed and updated from single third party.

It is worth mentioning, that although the combination of the above characteristics is what provides the various advantages of cloud computing, it is the same combination that introduces new security and privacy challenges and requires different solutions. The following section provides an analysis of the critical areas and major threats that exist in cloud environments.

3. Critical Areas and Threats of Cloud Computing

Building new services in the cloud or even adopting cloud computing into existing business context in general is a complex decision involving many factors. Enterprises and organizations have to make their choices related to services and deployment models as well as to adjust their operational procedures into a cloud oriented scheme combined with a comprehensive risk assessment practice resulting from their needs. In doing so, it is important to have a clear understanding of the critical areas, with respect to security and privacy, of a cloud computing solution. This section provides an overview of the critical areas of cloud computing and security and privacy threats that can affect to the cloud based system context.

3.1 Critical Areas of Cloud Computing

We performed a systematic review [25] of the literature, which started by identifying studies that consider cloud-computing areas, alongside security and privacy as domain specific key words. We focused on areas that are important to cloud-based systems, such as virtualization, interoperability, regulatory compliance, and identity management. We followed these key words to specifically search the literature. We also identified relevant literature from major research databases such as Elesevier, IEEE Xplore, SpringerLink, ACM Digital Library, and Google scholar. We considered only peer-reviewed papers and considered citations and place of publication of individual papers as inclusion criteria besides key words. Our results indicated that there is no much literature that focuses on identifying critical areas of cloud computing. A report of the Cloud Security Alliance (CSA) recommended a list of critical areas of cloud computer that match with our key words and we decided to select this work for the critical areas [13]. The areas recommended by CSA are mainly focused on governance and operations issues considering both provider and user perspectives. For instance, strategic and policy issues are addressed through governance domains, while the operational domains deal with security concerns and implementation techniques within the Cloud architecture. In the rest of the section we discuss these areas, focusing our discussion in the context of information systems development methodologies and techniques.

a) *Cloud Computing Architectural Framework*

This domain focuses on providing a conceptual framework and description of concepts used in cloud. Cloud Computing architecture is analyzed from the aspect of IT and security professionals. This sub areas are considered, i.e., a complete lexicon of terminologies used, requirements and challenges of cloud's architecture in order security to be implemented, and a taxonomy model that involves cloud computing services and architectures. The architecture framework includes unique cloud characteristics such as virtualization technologies and multi-tenancy for the cloud service and deployment model.

b) *Governance and Enterprise Risk Management*

Governance is related to the organization and entails the control and supervision over the operational and procedural activities of the cloud services. In particular, issues like policies, procedures, application development standards, design, legal issues, service monitoring, testing and implementation are activities that organization employees are involved with. However, cloud migration requires examining policies and legal issues extensively with the new type of dependencies and business models. Threats relating to agreement breaches, cloud providers transparency, sensitive data protection need adequate attention. Organization should have the ability to govern and measure the enterprise risks considering the strategic and operational activities.

c) *Legal Issues: Contracts and Electronic Discovery*

Cloud architecture poses legal issues that mainly concern its usage. Both providers and customers need to comply with existing regulatory requirements and Service Level Agreements (SLAs) between the user and provider. Legal issues consider the protection requirements relating to SLA/contractual obligation, privacy, laws and legislation. Note that before adapting cloud into the existing business context, organization should perform due diligence by evaluating its existing practice, organizational needs, and constraints to identify the requirements. Periodic monitoring, testing and evaluating of the migrated entities are also necessary. Finally the area considers the electronic document identification. Security issues are critical for the e-discovery.

d) *Compliance and Audit*

Legal compliance is a significant challenge for cloud-based systems. Due to the nature of the domain, service models and ubiquitous morphology organization needs to deal with the issues like, evaluation of compliance issues that is affected by deploying cloud. Legal and regulatory law issues that a cloud provider has to conform depend on the location of their services. Therefore several operational functions, like data lifecycle management, physical infrastructure requirements, electronic discovery, security and privacy obligations, etc. are affected, in a way that customer's security and privacy could be violated. The area focuses on some guideline necessary during the audit for the compliance. Both internal and external audit and control play necessary role for cloud from user and provider perspectives.

e) *Information Management and Data Security*

Data and is one of the centre parts of cloud computing. Users store data on the provider system that is managed by the provider, therefore, data protection within a shared environment is important. This area considers identification and control of data. Data protection is achieved through network protection both virtual and physical, data integrity, data segregation, data sanitization, data backup, hardware and data cryptography. Solid computation techniques, strong isolation, proper hardware maintenance, sanitization and strong cryptography are factors that should be taken into account in the whole data lifecycle management [26-29]. Insecure interfaces and Application Programming Interfaces (APIs), malicious insiders, shared technology issues, data loss or leakage, data location and recovery are the main threats related to this security issue. Information management deals with process and policies relating to usage such as create, store, use, share, archive, and destroy of information and governing that usage. Therefore both internal and external users' identify and access control is necessary for the information management [14]. This area should also cover preventing data from unauthorized access during migrating data into cloud as well as data loss prevention.

f) *Portability and Operability*

Cloud's dynamic model brings a great level of scalability to an organization in terms of infrastructure and computation. This area considers balance of services among multiple providers and move of data and service from one platform to another, in particular when an organization desires to change the provider due to some specific reasons. Therefore, creation of standard file formats by every cloud provider is important to support portability. An individual file format may result in lack of interoperability and portability between cloud providers, in case a client decides to migrate from one vendor to another. However portability requirements varies for different cloud models for instance in IaaS, it is necessary to understand how virtual machine image should capture and map with new provider, for private cloud interoperability should exist between common hypervisor.

g) *Traditional Security, Business Continuity and Disaster Recovery*

This area is under the operating issues of the cloud. The inherent security issues due to the cloud characteristic need to identify, assess and control for the business continuity. Appropriate security measure through a defense in depth is necessary to control the risks and to ensure confidentiality, integrity and availability of information and other critical assets. In particular, services must be constantly available to the users and if interrupted, a solid recovery system should be ready for recovery and business continuity. Availability is important and could result in a business close down, if cloud services continuity is break down [4, 29]. There are many reasons for the continuity breakdown such as DDoS attacks, hardware failure, and physical disaster. Long-term Viability and Lack of Recovery are the threats that this issue is associated. Finally, data backup and disaster recovery in cloud should support reliable data protection and transition if anything fails. Therefore, fully virtualized storage structure, scalable file system and recovery application is necessary for the business continuity and disaster recovery.

h) *Data Center Operations*

Data center certainly is one of the main components for the cloud operation as the organization mission or application hosted in the data center. Issues such as, evaluation of provider's data center architecture and operational procedures, data center dissemination are key element need adequate attention for the data center operation. On-going services and long-term stability relying on the proper identification of fundamental and other common data center characteristics, as well as other ones, as far as users are concerned. The area also considers physical requirements based on the different standards and regulatory requirements and service management process, location of data center.

i) *Incident Response, Notification and Remediation*

Incident response is necessary for any information security management system. For cloud based system, there should have an efficient and effective incident response facility. However cloud computing does not require a separated incident response facility, but the existing process should appropriately map the program, process and tools to the specific operating environment. The incident response practice can vary from provider to provider. Therefore, gap analysis is necessary on this context. In case of a security incident, proper actions should be made in order to discover under what circumstances the incident happened. Because of cloud's architecture (traditional borders, high scalability, multi-tenancy, dynamic migration), it is difficult to perform digital forensics and determine attack's vectors. A solid forensics system should be able to perform incident verification, attack analysis, remediation and restoration. The threat that is linked to the issue is investigate support [4, 30]. An examination of incident response lifecycle is necessary including detecting and handling the incident, SLA integrated with incident response, within this area.

j) *Application Security*

This area deals with the security issues throughout the life time of an application from design to deployment and maintenance into cloud. Threats that an application is going to exposed to in cloud environment is higher comparing to compare to traditional data centre. Therefore, an application needs to ensure security from both internal and external malicious environment. In particular, the level of the access of employees or cloud clients, to physical and virtual assets, can take advantage of them in such a way that data confidentiality could be compromised or even control of cloud services could be taken, without the risk of detection [3, 4, 29]. The area includes issues like authentication, authorization of the user to access the application, monitor the application, a secure SDLC, security assurance program, application penetration testing, and other relevant areas.

k) *Encryption and Key Management*

Data should be encrypted, if necessary, in any form of usage so that it can prevent potential data leakage that is particularly critical in cloud environment. Context aware encryption or format preserving encryption is commonly used in cloud deployment. Key management is a difficult process in cloud computing, in particular within the multi tenancy model. This area considers issues like storage and safe guarding of keys, key management practice, trusted cryptographic services are relevant for this context.

l) *Identity, entitlement and Access Management*

Considering traditional computing, identity management is changed in cloud by including entitlement in the access management process. In particular, cloud service and application use various sources to identity it users, entitlement management provides decision-making process for authorizing access to the system, process, and data within cloud. This area covers all types' identity that are relevant for the domain such as users, device, code, organization, and agents. Key points for the identify of all entities are strength of identity and attributes, should provide greater flexibility in cloud internally within the organization boundaries or external public cloud. The access in cloud can be network, system, application, process, and data. The entitlement process should link with the user business requirements and security requirements into a set of rule to govern access to different entities of the cloud. Issues arise when an organization attempts to extend its identity procedures and policies; this area helps the organization to verify if it is ready to migrate to a cloud-oriented Identity Enterprise Architecture.

m) *Virtualization*

Virtualization is one of the fundamental technologies used in the cloud infrastructure. It allows the cloud infrastructure to be shared among multiple users but logically separated area through hypervisor technology to support multi tenancy and better server utilization. Hypervisor is important in order to maintain the security, integrity and privacy of users and overall system context [29, 31]. A VM's actions must be restricted to the level that has been granted from the contract agreement. Escaping from a VM to another VM, or to the hypervisor is an unwanted situation. Virtual network traffic is not visible to the physical network security devices as a consequence it is difficult to detect and control possible intrusions [4]. Hypervisor needs to be completely isolated from actions from and to the hypervisor in order for the system to be completely safe. VM also poses threats from cohabitation techniques that referred to the IP pattern recognition techniques, just to achieve co-residency with the victim's VM and launch a series of attacks [32]. Vulnerability or a mis-configuration in virtualization or in hypervisor's kernel may result in system compromise and take down the whole cloud. Isolation needs also to be examined from another point of view, that of purpose limitation. Rights and roles should be established in order for the level of access to be determined for the cloud employees, this way data usage should be limited to what is necessary [14]. Malicious insiders, shared technology issues and data loss or leakage are the threats related to this issue. Therefore VM specific security requirements and up-to-date security policies for the VM are necessary for this area.

n) *Security as a Service*

Security is one of the main concerns in cloud computing and present strong barrier for the cloud adaption. Generally in a SLA, standard security framework should specify which security services are provided and how. This area considers enterprise security for the cloud. Issues like visibility of user security control, proper credential and background check, protect data leakage in VM instances need adequate attention under this area. Security obligations from incident detection to proper access management are deposited on a trusted third party. The benefit of this service is that the user has the ability to choose the appropriate security service and not necessary to rely on providers' choices, that is almost entirely cut out from security implementation procedures and techniques. Security measures should be taken to protect both client and provider from possible attacks.

3.2 Major threats in Cloud Computing

To identify relevant threats, we have followed the same literature review approach described in the previous section. We have focused on several papers that consider security and privacy threats in the Cloud. An overview of the papers that we examined is provided in the related work section. However we have decided to define a list of threats based on the reports of CSA [3] and Gartner [15], because these works are comprehensive and there is a link that can be provided between the identified threats and the critical areas described in the previous section. Our analysis identified 14 different threats. It is important to indicate that only some of these threats are specific to cloud computing (see for example threat 1) while most of the threats can also be found in traditional distributed systems. We have focused however our discussion, of the identified threats, in the context of cloud computing.

a) 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 compute power to perform illegal activities, all the above combined with Inadequate identity management[1] and lack of know-how[2] converts cloud from a 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.

b) 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, to build upon these and offer services to their

[1] Partial anonymity through weak registration.

[2] Limitations on fraud detection capabilities.

customers, so as a result security and availability are crucial. 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.

c)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 applicability on IaaS, PaaS and SaaS service models.

d) Threat #4: Shared technology issues

Virtualization is the concept that cloud computing notion is built upon. Dynamic provisioning of services in multi-tenant environment due to hardware virtualization (e.g., CPU, 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 to be completely addressed to prevent any type of data leakage. For instance, side channel can instant new virtual machine to retrieve user data. The specific threat is matched with the Data Center Operations and Virtualization domains and has applicability on IaaS service model.

e) 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 Authentication, Authorisation and Accounting (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

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

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

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.

f) Threat #6: Account or Service Hijacking

Phishing frauds, vulnerabilities exploitation, software exploitation or even user's personal choices (reused passwords) are methods that can achieve results, in a cloud environment, as hijacking is concerned. 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.

g) 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.

h) 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.

i) Threat #9: Regulatory Compliance

Cloud providers are obliged to follow laws and regulations of each country the 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.

j) Threat #10: Data Location

Security, privacy and data lifecycle procedures are strictly related to the country that 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.

k) 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.

l)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.

m) 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

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

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 domains and has applicability on IaaS, PaaS and SaaS service models.

n) Threat #14: Long-term Viability

Cloud provider should have safety measures in case that something breaks its service continuity (bankruptcy, Denial of Service (DoS) 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.

3.3. Matching Threats with Cloud Service Models and Critical Areas

It is necessary to understand how the identified threats link with the cloud models and cloud areas, so that appropriate security and privacy properties can be justified to address the threats. This section provides the linking between the threats with cloud service models and critical areas.

Table 1 presents the result of the matching between threats and cloud service models. It should be noted that the matching of threats 1-7 to the relevant service models has been done by CSA [3], while we have improved on that work by adding the matching of threats 8-14 to the service models. Focusing on threats 8-14, it is clear that some threats are applicable to all service models. Privileged use access covers all service models, because is referred to the fact that certain employees have access rights to the cloud's services and as a result customer's data due to the nature of their work. Data location threat covers all service models, because data lifecycle process happens from these three models and it's important for users to know each country's laws and regulations as this subject is concerned. Long term viability is applicable to all service models, because it describes that cloud services should be functional all the time and providers should be clear about the procedures that are followed, when are no longer able to provide them.

Some of the threats are more applicable to IaaS such as shared technology issues, due to flaws of the virtualization technology. Lack of recovery can directly affect on unavailability of platform and software as a service. Regulatory compliance covers Paas and SaaS service models, due to the fact that cloud providers should comply with each country's regulations as specific cloud matters are concerned. Lack of segregation threat, is a virtualization flaw that causes problems to vm isolation that's why only matches PaaS and SaaS service models. Lack of recovery is a common problem in cloud environments and is referred to the inability of the provider to provide a recovery system for the data from a possible attack or a disaster. That's the reason that matches only with the last two service models. Investigate support covers only the PaaS and SaaS layers, because if an incident occurs in the cloud, a digital forensics system should provide instant information from the investigation in these layers.

Table 1. Matching Threats with Cloud Service Models

	IaaS	PaaS	SaaS
CSA[3]			
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
Gartner[15]			
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 provides between the threats and the critical cloud areas. Providing such matching is important for two reasons. Firstly, it enables information system methodology and techniques developers to understand what critical areas their work needs to cover in order to provide analysis and support for the specific threats. For example, if a method developer is interested in developing a method that supports analysis of the Shared Technology Issues threat, they need to make sure their work supports areas such as Data Centre Operations and Virtualisation. Secondly, it enables software engineers to have a foundation for threat analysis for their specific systems based on the relevant properties and security policies of their system. For example, as illustrated on the table, threats to the Identity and Access Management are Data Loss or Leakage and Account or Service Hijacking. Some threats affect several areas. For instance, threats relating to data location certainly affect governance, legal and compliance areas. Therefore, as stated previously, we need to control a identify and analyse threat and its consequences if that affect to a critical area that is relevant from the user perspective.

Table 2. Matching Threats with Critical Cloud Areas

	Governance and Enterprise Risk Management	Legal Issues: Contracts and Electronic Discovery	Compliance and Audit	Information Management and Data Security	Portability and Operability	Traditional Security, Business Continuity and Disaster Recovery	Data Center operations	Incident Response, Notification and 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							

4. Security and Privacy Properties and Threats

As indicated above, it is important to identify the set of security and privacy properties that are related to cloud computing environments. We have used the existing literature for eliciting the relevant security and privacy properties such as the European Commission Draft Report on Security Issues in Cloud Computing [14], CSA report [13], NIST guideline [33] and other relevant literature. Moreover, we have used our previous work in that area [5,11, 34-39] and we have also identified new concepts based on our analysis of the critical areas presented in the previous section. Finally we link these properties with the threats and issues relating to critical areas in cloud.

4.1 Security and Privacy Properties in Cloud

For each property, we provide a brief explanation along with graphical illustration of the property. It is worth mentioning that we have identified two different types of properties, those that can also be found in traditional distributed systems security/privacy, such as Availability, and those are that are unique to the cloud context, such as Isolation. However, our discussion below focuses on how all these properties can be understood within the context of cloud computing.

a) Isolation

The property of isolation refers to the complete seal of user's data inside the Cloud computing environment. Due to multi-tenant environments, cloud-computing resources are introduced to risks related to information disclosure. As a result strong isolation must be achieved inside the cloud environment as shown in Figure 4. Isolation addresses data disclosure in two ways: limit the point of view and support hypervisor hardening [14].

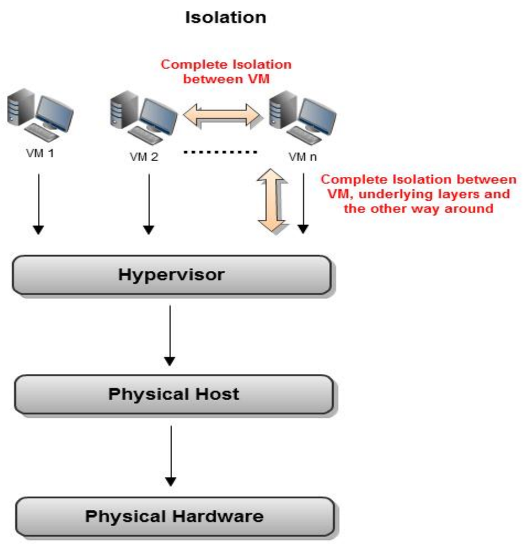
Isolation
Complete Isolation between VM
VM 1
VM 2
VM n
Complete Isolation between VM, underlying layers and the other way around
Hypervisor
Physical Host
Physical Hardware

Figure 4. Isolation Example

b) Provenanceability

This property refers to a Virtual Machine's (VMs) provenance mapping. Building a VMs background tree makes it easier to get information about its parent image. Figure 5 depicts the VM tree from parent VM to child VM. 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 [31].

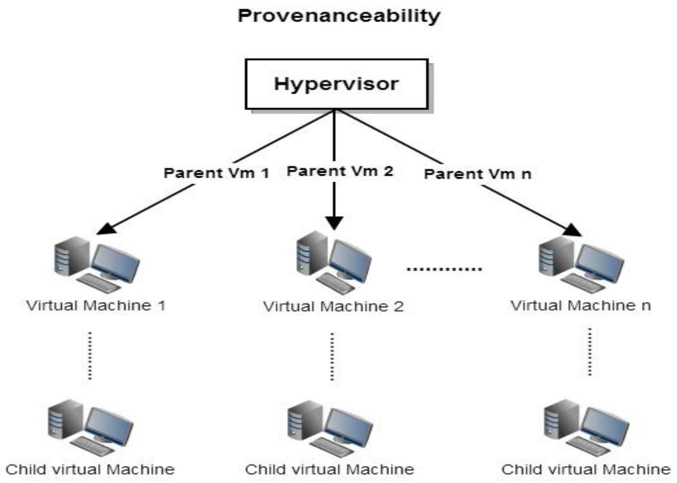

Figure 5. Provenaceability Example

c) Traceability

This property 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 this is also true for cloud-based systems. Many cases have been documented for privacy violations due to inappropriate handling of data deletion (documents, photos, etc.). As such, traceability aims to reassure cloud clients that their data has been completely deleted or stay invisible and anonymized through the ability of tracing them among data repositories as shown in Figure 6.

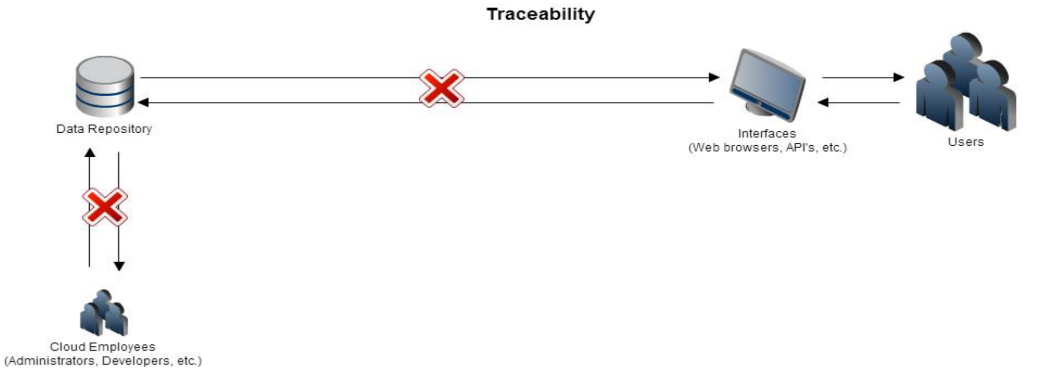
Traceability
Data Repository
Interfaces
(Web browsers, API's, etc.)
Users
Cloud Employees
(Administrators, Developers, etc.)

Figure 6. Traceability Example

d) Availability

The availability property refers to the ability to support continuous service as per the agreement and reduce the factors that can break such continuity such as security attacks (for example DoS attacks), physical disasters and/or hardware failure. Unavailability of service or data can have severe impact on the customer business. Figure 7 provides an example of availability.

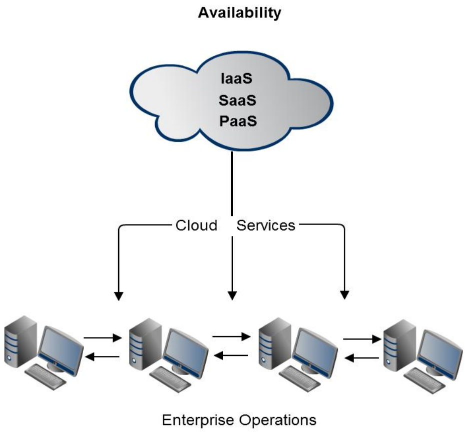

Figure 7. Availability Example

e) Integrity

Integrity refers to the ability to avoid clients' data unauthorized modification. In particular , all data must be modified in a legitimate way by legitimate authority. According to EU directives [14], cloud providers must assure users that their data has not been tampered while it was passed through the whole data life cycle.

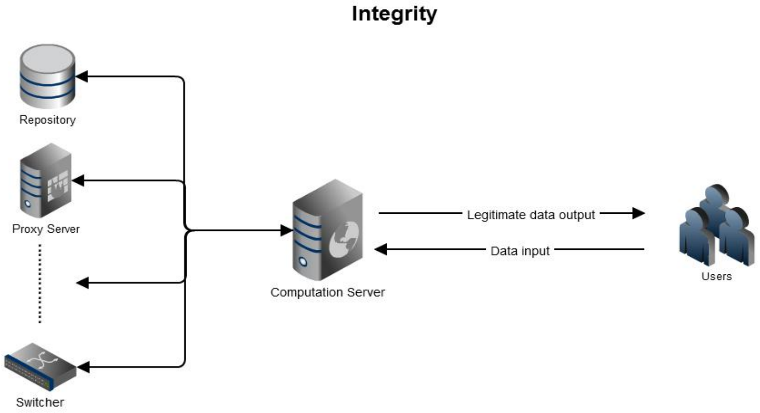

Figure 8. Integrity Example

f) Confidentiality

The confidentiality property derives from the fact that cloud is multi-tenancy environment and many of its resources are shared. That raises concerns about the data that communicates within a cloud, from the cloud provider to the client, and vice versa. Figure 9 shows different phases of data from it generation to destruction and confidentiality needs to be ensured all these phases. Encryption techniques and authorization and authentication mechanisms can support data's confidentiality [14].

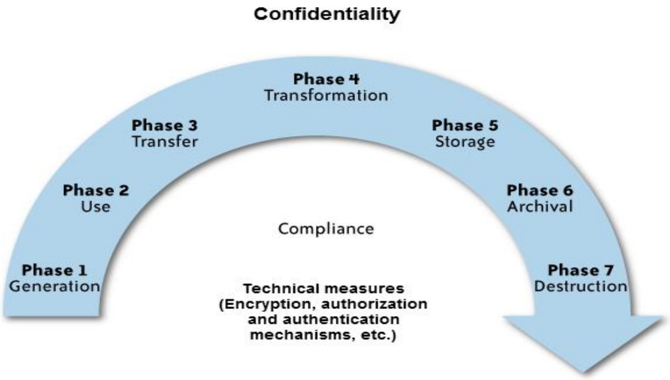

Figure 9. Confidentiality Example [40]

g) Transparency

The transparency property refers 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 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 [14-15]. As shown in Figure 10, provider should provide report to ensure the transparency about the activities that handle critical user assets.

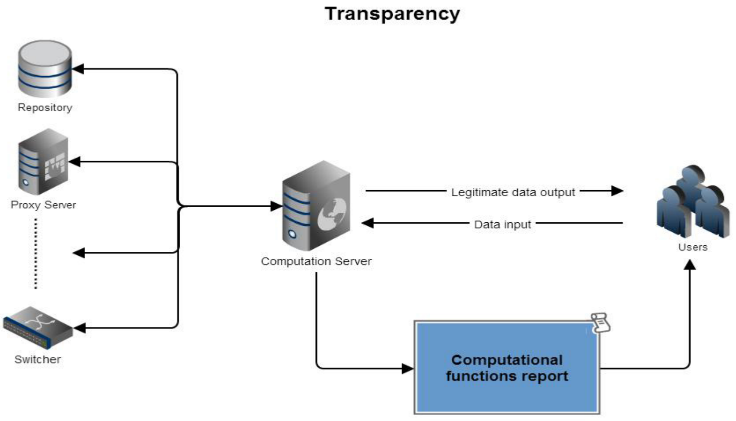

Figure 10. Transparency Example

h) Intervenability

The Intervenability property refers to the fact that users should be able to process their data despite the cloud's service architecture as shown in Figure 11. 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 [14].

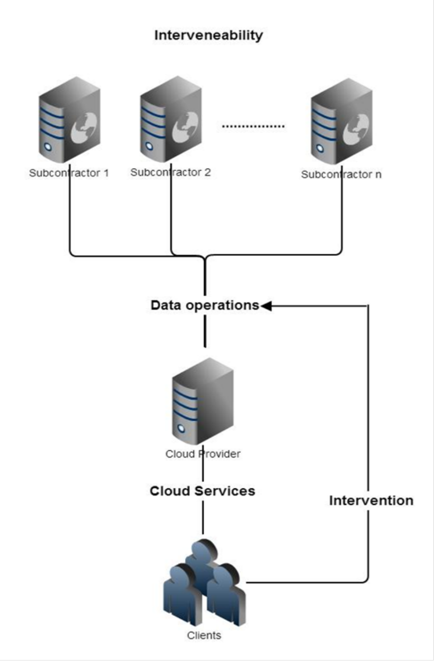

Figure 11. Intervenability Example

i) Portability

The Portability property aims to achieve data transferability, 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. Figure 12 depicts how portability can be achieved among different providers using the same data. 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 [14].

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

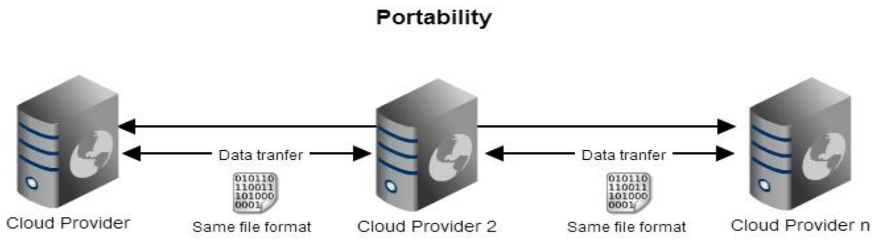

Figure 12. Portability Example

j) Accountability

The Accountability property is referred to the fact that, cloud providers should provide information anytime about an incident. Figure 13 provides an example about accountability within the cloud environment. 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 any incident, what an entity did and when, just to trace malicious actions from the whole cloud infrastructure [14].

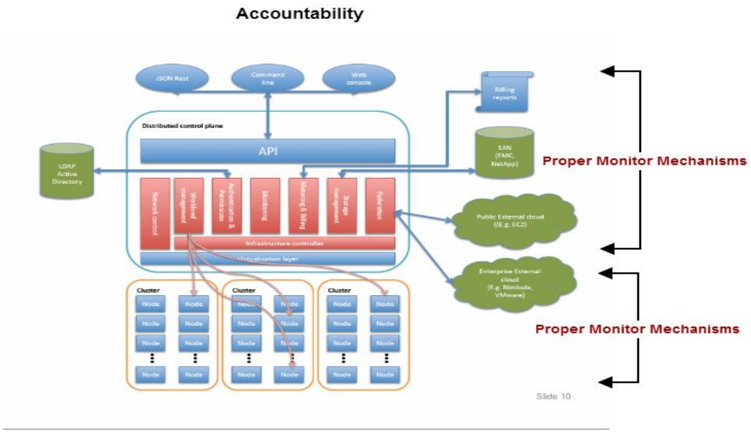

Figure 13. Accountability Example [41]

k) Identification

The Identification property has a twofold role. Firstly to protect both the user that accesses a resource or service within the cloud as well as the user's data stored in the cloud.

[7] International services residual.

Secondly to allow only authorized people to access those data. Specifically, when an external user accesses, as shown in Figure 14, a service the cloud provider should check if this service requires users' identification or not. In the first case the user will have to be authenticated and authorized to access the specific service. In the second case Identification requirement will work oppositely thus preventing the cloud provider from storing any identifiable or traceable information regarding the external user. It should be noted that user anonymity is not ensured since this is not an anonymity service, just a transaction without providing identities. If anonymity is also required then the respective requirement described below, should also be applied.

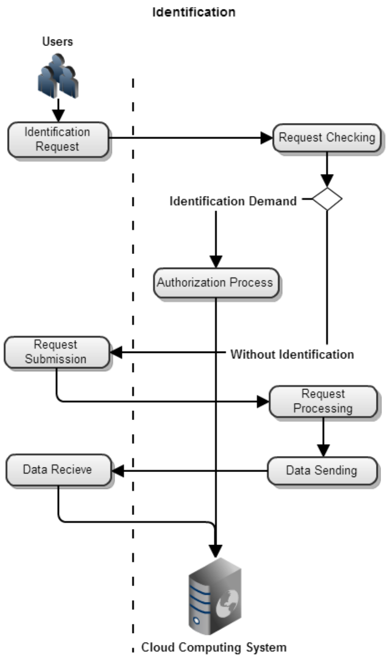

Figure 14. Identification Example

l) Authentication

The authentication property is necessary to ensure that only eligible users have access to various cloud services. Similar to the traditional distributed system, cloud provider only grant permission to the legitimate user as shown in Figure 15. Therefore, providers should also ensure protection from possible attackers who fail to prove their identity to the cloud service provider.

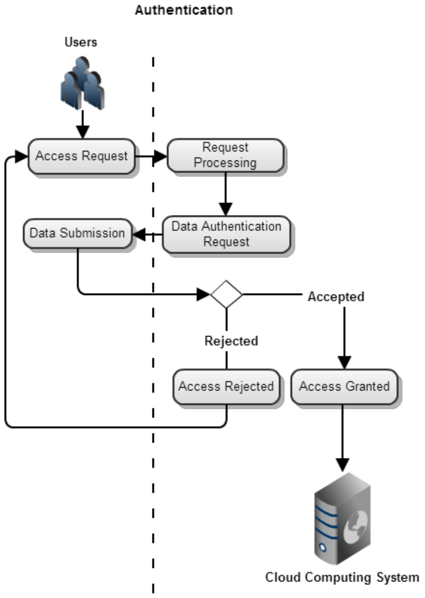

Figure 15. Authentication Example

m) Authorisation

Authorisation follows authentication. Specifically, users' private data should only be accessed by authorized users. When a user submits a request to the cloud provider, as shown in Figure 16, the nature of the request should first be checked since it is not legal for example to ask from that user to login for a service that identification is not needed. If the user requests specific services or access to data that need authorisation then she should pass the authentication process and then, according to her rights, get the privileges for accessing or not the specific service or data.

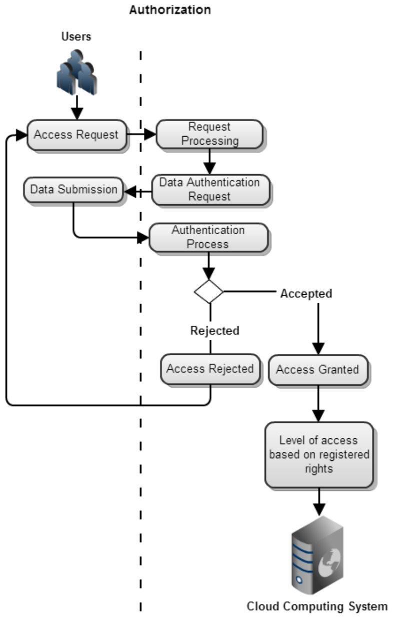

Figure 16. Authorization Example

n) Data Protection

The aim of this property is to ensure that every transaction involving personal data is realized according to the organisation's privacy regulations and Directive 95/46/EU [42] regarding the processing of personal data and the free movement of such data. When a user tries to access private data, an identification process is triggered for identifying the user and for granting her with the rights of reading, processing, storing, or deleting private data. Subsequently, if the user asks to perform any of the above tasks the cloud provider checks whether this complies with the privacy regulations and the request is either granted or denied, accordingly. Thus, there are two intermediate "inspections" before actually a user is able to perform various tasks on other users' private data.

o) Anonymity

The property anonymity means the state of being anonymous or virtually invisible, and having the ability to operate online without being tracked [43]. Therefore, anonymity is the ability of a user to use a resource or service without disclosing his/her identity [44] as shown in Figure 17. A formal definition for anonymity is given by A[41]. Let RU denote the event that an entity U (e.g. a user) performs a role R during an event E. Let A denote an attacker and NCA the set of entities that are not cooperating with A. An entity U is called anonymous in role R for an event E against an attacker A if for each observation B that A can make the following relation holds: $\forall U' \in NC_A{:}0 < P(R_{U'}|B) < 1$. The outcome of the above definitions is that anonymity serves the great purpose of hiding personal identifiable information when there is no need of revealing them. Browsing the Internet only for collecting information is one of many issues that anonymity plays a significant role and must be attained.

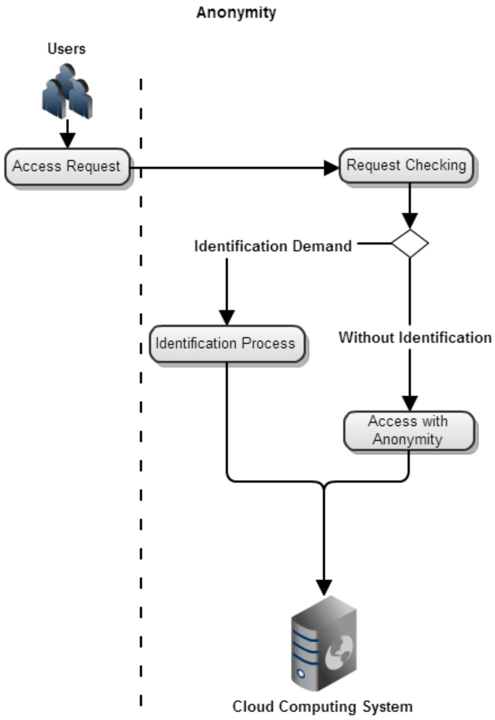

Figure 17. Anonymity Example

p) Pseudonymity

Pseudonymity is the user's ability to use a resource or service by acting under one or many pseudonyms, thus hiding his/her real identity. However, under certain circumstances the possibility of translating pseudonyms to real identities exists. Pseudonyms are aliases for a user's real identity such as shown in Figure 18. Users are allowed to operate under different aliases. Nevertheless revelation of user's real identity occurs when acting unlawfully. Pseudonymity has characteristics similar to anonymity in that user is not identifiable but can be tracked through the aliases he/she uses [43]. Pseudonymity is used for protecting user's identity in cases where anonymity cannot be provided (e.g. if the user has to be held accountable for his/her activities [44-45].

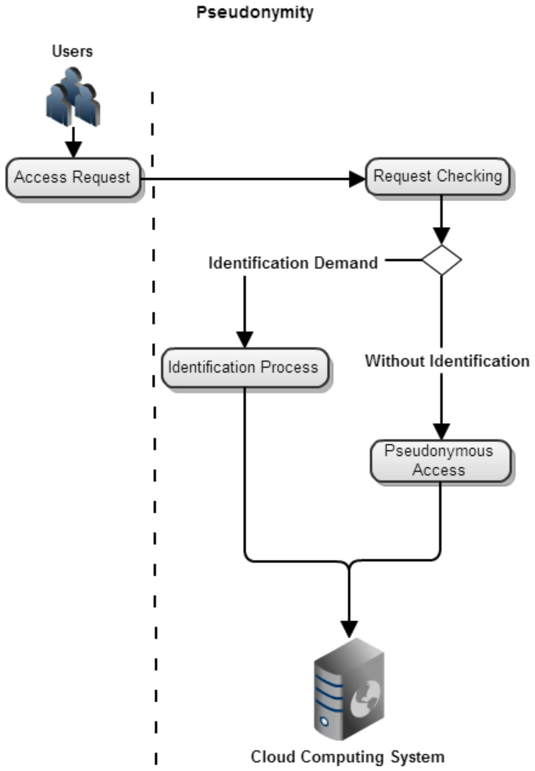

Figure 18. Pseudonymity Example

q) Unlinkability

The property unlinkability expresses the inability to link related information [43]. In particular, unlinkability is successfully achieved when an attacker is unable to link specific information with the user that processes that information. Also unlinkability can be successfully achieved between a sender and a recipient. In that case unlinkability means that though the sender and recipient can both be identified as participating in some communication, they cannot be identified as communicating with each other. A. Pfitzmann in [46] addresses unlinkability in the following formal way. Figure 19 provides an example of unlinkability. Let $X_{E,F}$ denotes the event so that E and F have a corresponding characteristic X. Two events E and F are unlinkable in regard of a characteristic X for an attacker A, if for each observation B that A can make, the probability that E and F are corresponding in regard of X given B is greater than zero and less than one: $0 < P(X_{E,F}/B) < 1$. The ability to link transactions could give a stalker an idea of your daily habits or an insurance company an idea of how much alcohol your family consumes over a month. Ensuring unlinkability is vital for protecting user's privacy.

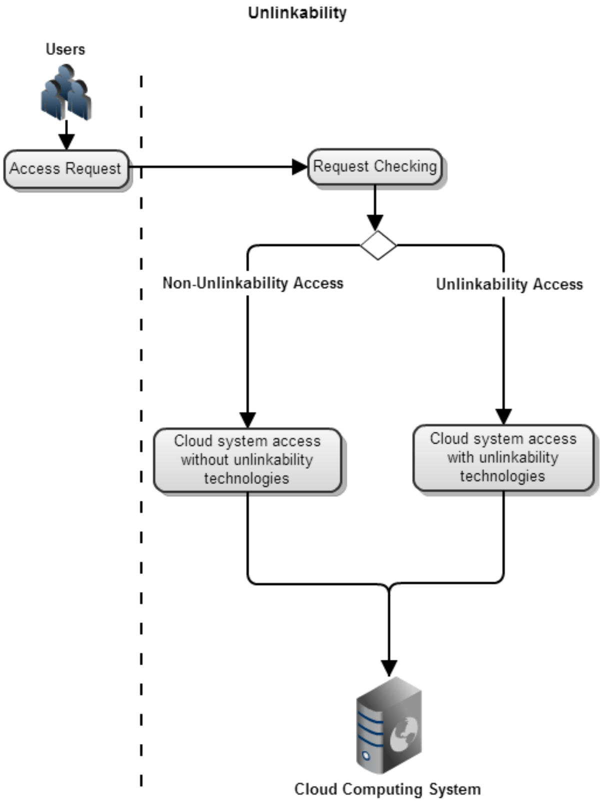

Figure 19. Unlinkability Example

r) Unobservability

Unobservability protects users from being observed or tracked while browsing the Internet or accessing a service. Unobservability is similar to unlinkability, shown in Figure 20, in the sense that the attacker aims to reveal users identifiable information by observing rather than linking the information he/she retrieves. A formal representation of unobservability is stated as follows [46]. An event E is unobservable for an attacker A if for each observation B that A can make, the probability of E given B is greater than zero and less than 1. $0 < P(E|B) < 1$

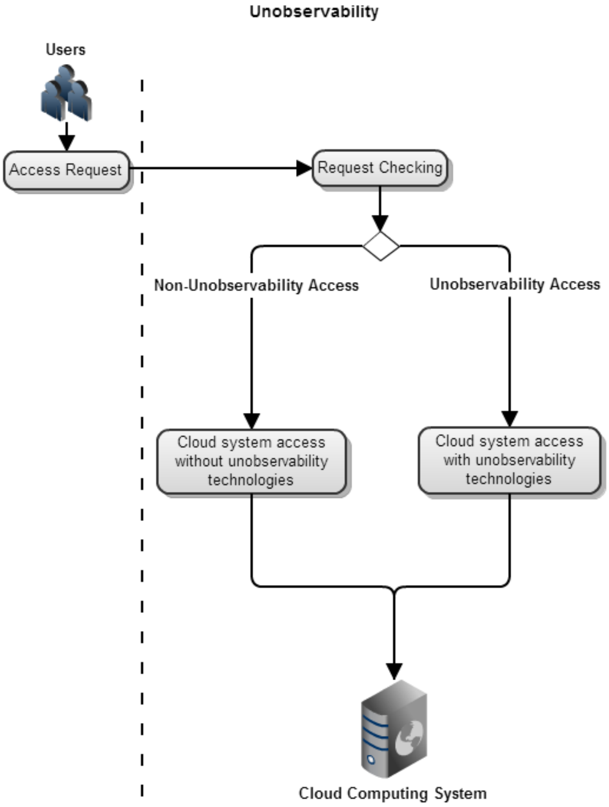
Unobservability
Users
Access Request
Request Checking
Non-Unobservability Access
Unobservability Access
Cloud system access without unobservability technologies
Cloud system access with unobservability technologies
Cloud Computing System

Figure 20. Unobservability Example

4.2 Cloud Security and Privacy Properties and Threats

In order to make the above set of properties useful to method developers, we present a matching between the presented properties and the various threats discussed in previous sections, as shown in Table 3. Note that we use IAA to denote identification, authentication and authorisation in the table. In particular, we identify relevant security and privacy properties can address the threats based on the issues relating to critical areas. In the last column a number of technical security and privacy properties are mentioned that can be realised for resolving the security or privacy issue of the listed cloud threats. Thus, through this table it can be easily seen which are the basic security and privacy areas, which threat has an impact on which area and how the new security and privacy concepts identified before can be matched in order to provide proper guidance to analysts when considering the implementation of secure and privacy oriented services in the cloud.

The basic security properties such as confidentiality, integrity, and authentication are necessary to address the threats that relates with compliance, insiders, data protection. Data plays a central role for the cloud based system context and organisations and individuals would have to hand in their personal and organizational data into service providers over which they have no control. Therefore, data needs appropriate protection throughout its phases from generation to distribution from all possible threats and most of the security and privacy properties are applicable on this occasion. We need to understand the dependency chain relating to API considering all these properties for the data protection. It is necessary to have reliable service availability, thus cloud services should have continuity so that lack of recovery and long term viability do not pose any service interruption. Client side protection needs user's IAA specifically strong access control mechanism is required. Similar forensic activities need IAA and accountability for the proper investigation of any malicious activities. Property like portability is necessary to handle issues relating to vendor or data lock-in. Privacy properties such as anonymity, unlinkability, and unobservability are necessary where we need to appropriate protection of sensitive information. For instance, data protection or protect from any insider attack it is necessary to provide adequate technical and organizational measure for the preservation of the privacy properties. Transparency of user activities is also necessary for addressing the threats relating to insiders. Furthermore, provenanceability besides anonymity and isolation are necessary to address the threats such as shared technology, data leakage & lack of segregation relating to virtualization. Depending on the organizational specific context, it is necessary to determine and in-depth analysis of relevant security and privacy properties to support the needs. However, users should define their security best practice and practice effective information security management system to obtain the maximum benefit for the cloud migration.

5. Requirements for a Methodology to Support Security and Privacy Analysis

Based on our analysis of the critical issues of cloud computing (Section 3.1), the security and privacy threats in the cloud (Section 3.2) and the security and privacy properties related to the cloud (Section 4), we have identified a number of challenges that make the integration of requirements and design analysis into the development stages of a software systems development methodology considering cloud based system. These are:

- Challenge 1: A clear understanding of security and privacy issues requires determining the organisational needs and reasoning for migrating to a cloud based solution.

- Challenge 2: Different cloud based deployment models require different security and privacy mechanisms.
- Challenge 3: A clear association should be supported between analysis and design.
- Challenge 4: Different cloud providers provide different mechanisms to support security and privacy properties.
- Challenge 5: It is important to have a clear association between properties, threats and mechanisms.

To support the above challenges, we have defined a set of requirements that an analysis and design methodology should support. It is worth mentioning that we do not include on our list requirements that are required from any software systems methodology, such as for example being clear and structured and include well defined concepts and stages, but we only focus on a list of requirements related to modeling and analysis of security and privacy related concerns. We have identified the following requirements:

- Requirement 1: It should include concepts from both cloud and organization areas such as actor, organizational goals, dependencies, infrastructure, information management, portability, application during the analysis for the development of cloud based system. This supports understanding of organizational needs for migrating into the cloud (response to Challenge 1);
- Requirement 2: It should provide techniques to select appropriate cloud deployment models. The selected model shall support organizational needs, requirements and shall address the identified threats and risks. Selection of deployment model needs to analyse the different deployment models considering all constraints and portability of organizational data or infrastructure into cloud (Response to Challenge 2).
- Requirement 3: It should enable the usage of a defined set of concepts and notations during the analysis and design process, to support a unified analysis and a clear connection between requirements analysis and design solutions (Challenge 3).
- Requirement 4: It should allow developers to evaluate cloud providers. The selection should be based on degree of satisfaction of requirements, mechanisms, and organizational needs and the selected deployment model (Challenge 4).

- Requirement 5: It should consider relevant security and privacy properties, threats, and risks and be able to identify appropriate measures and mechanisms to control security and privacy threats and risks and satisfy the security and privacy properties (Challenge 5).
- Requirement 6: It should provide mechanisms to clearly identify a linkage between security and privacy issues and relevant threats and properties. To support an easy facilitation of such linkage we have identified, in Table 3, an association between security and privacy issues, and the threats and properties we have presented in the previous sections. Although we do not claim the list to be extensive nor final, we believe it can be used as a starting point and be modified and/or extended as required (Challenge 5).

Table 3 Matching Security and Privacy Properties with respective cloud threats and issues within critical areas

Threats **Issues of critical area**	#1: Abuse and Nefarious Use of Cloud Computing	#2: Insecure interfaces and APIs	#3: Malicious Insiders	#4: Shared technology issues	#5: Data Loss or Leakage	#6: Account or Service Hijacking	#7: Unknown Risk Profile	#8: Privileged user access	#9: Regulatory Compliance	#10: Data Location	#11: Lack of Data Segregation	#12: Lack of Recovery	#13: Investigate Support	#14: Long-term via.	**Security/ Privacy Properties**
Compliance									x						Confidentiality Transparency Intervenability Data Protection
Governance							x		x					x	Intervenability Accountability
Insiders	X		x		x			x							Isolation Confidentiality Integrity Anonymity IAA Unlinkability Transparency
Cloud Service's continuity												x		x	Availability
Operational and procedural visibility									x						Transparency

Virtualization and Hypervisor flaws			x	x	x			x			x				Isolation Anonymity Provenanceability
Virtual and Physical network protection			x	x	x			x							Anonymity Data Protection Unlinkability Unobservability
Client – Side protection		x				x									Traceability Anonymity IAA Data Protection Pseudonimity Unlinkability
IdM and Access Process		x	x			x		x							Authentication Authorization Identification
Data protection		x	x	x	x					x		x			Confidentiality Integrity Isolation Transparency Traceability Anonymity IAA Pseudonimity Unlinkability Unobservability
Vendor or Data Lock-in	X		x									x			Portability
Forensics													x		Accountability IAA
Imponderables							x								Confidentiality Intervenability Anonymity Pseudonimity Unlinkability
Cohabitation technics.			x	x			x	x							Isolation Anonymity

6. Related Work

Our work focuses on the integration of cloud computing and security and privacy. This section presents works that are related to our work. We first discuss requirements engineering methods that consider security and privacy issues then related work within the cloud-computing domain.

There are works that focus on the development of requirements engineering methods to support security and privacy issues during the development of software systems. Mouratidis & Giorgini [47] proposed Secure Tropos, an extension of Tropos methodology, which employs the concepts of security constraints, secure dependency, and secure goal amongst others. The approach supports the analysis of security from the Requirements Engineering phase. Houmb et al. introduced the SecReq approach to elicit, analyse and trace security requirements, starting from the requirements engineering phase to design [39]. A misuse case driven approach is used to establish visual links between use cases and misuse cases for eliciting security requirements at an early stage of the development [10]. PriS is a requirements engineering method that incorporates privacy requirements as organisational goals that need to be satisfied and adopts the use of privacy process patterns as a way to: (a) describe the effect of privacy requirements on business processes; and (b) facilitate the identification of the system architecture that best supports the privacy-related business processes [35, 48]. Islam et al. use natural language patterns, with the Hohfeld legal taxonomy, to extract security requirements from laws and combine them with the ISO/IEC policies and finally trace the identified requirements into the secure system design [49-50]. Four methodological activities are used to evaluate existing security and privacy requirements for legal compliance [51]. The approach in particular prioritizes the requirements and establishes traceability links from requirements to legal texts. A model based process is proposed to support security and privacy requirements engineering using a set of concepts such as goal, actor, constraint, and threat [11].

On the other hand, there are works that focus on the security and privacy issues related to the cloud-computing domain. Mulazzani et al. [52] demonstrate that attackers can exploit data duplication techniques to access customer data by obtaining hash code of the stored file. A decision support tool based on cost and benefits and risk is proposed for the public IaaS cloud migration [53]. The cost modelling tool enables users to model IT infrastructure using UML. A goal-driven approach is introduced to support analysis of security and privacy risks of cloud based system [5]. Goals, threats and risks are considered from three main components data, service/application, and technical and organisational measures. Some works identify the security and privacy threats. For instance, Pearson identify that privacy threats differ depending on the type of cloud scenario and lack of user control, potential unauthorized secondary usage, data proliferation are more dominate in public cloud [6]. Side-channel attack can instantiate new VMs of a target virtual machine so that the new VM can potentially monitor the cache hosted on the same physical machine [7]. There are four possible places where faults can occur in cloud computing: provider-inner, provider-across, provider user and user-across [54]. It is necessary to address any fault arising from these places within the cloud infrastructure.

The above works are important in the field of security modeling. However, while various modeling methods have been presented through these works, none deals with the combination of security and privacy requirements elicitation and none has identified any list of requirements needed by analysis and design methods to support security and privacy in the cloud. Thus, our work aims on contributing to that gap.

7. Conclusions and future steps

A computing Cloud represents a dynamic environment with many different stakeholders involved in various levels and services, all aiming to provide new and highly innovative services to users and companies. However, the rapid development of this technology has emerged new security and privacy concepts that need to be considered when designing security and privacy related services and systems.

The main aim of this paper is to provide a clear linkage among cloud computing areas, threats within the areas and security and privacy properties. To achieve that aim, we considered a list of security and privacy properties that address threats to critical cloud computing areas. A secondary aim was to provide an initial set of requirements for analysis and design methodologies that are developed in order to consider cloud security and privacy as part of their development process. We believe such requirements would help to develop systematic engineering methodologies for the cloud-computing context and enable analysis and design of critical areas, threats and identified security and privacy properties. As future work, we aim to integrate those requirements into our previous work and develop methodologies that support the security and privacy analysis and design of cloud-based systems. Additionally, we plan to evaluate the applicability of our work, in particular how the identified security and privacy properties support user needs for migration into a cloud and what implementation techniques could support the implementation of the security and privacy properties.

References

[1] Microsoft Technical report: Privacy in the cloud computing era, a Microsoft perspective, November 2009, Microsoft Corp, Redmond, USA [Last access 12/08/2012]

[2] Version One Survey Results: Cloud Confusion amongst IT Professionals, 24 June 2009, http://www.versionone.co.uk/news/cloud-of-confusion-amongst-it-professionals.php [Last access 08/09/2012]

[3] Cloud Security Alliance "Top Threats to Cloud Computing V1.0". https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf Retrieved 2012-09-22. [Last access 09/01/2013]

[4] S. Subashini, & V. Kavitha, , "A survey on security issues in service delivery models of cloud computing", Journal of Networks and Computer Applications, Vol 34, No.1, p.p. 1-11, 2011

[5] S. Islam, H. Mouratidis, & E. Weippl, "A Goal-driven Risk Management Approach to Support Security and Privacy Analysis of Cloud-based System", Book chapter Security Engineering for Cloud Computing: Approaches and Tools, IGI global publication, 2012.

[6] S. Pearson, & A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing", 2nd IEEE International Conference on Cloud Computing Technology and Science, pp 693 – 702, UK. IEEE Computer Society, 2010.

[7] C. Gong, J. Liu, Q. Zhang, H. Chen, & Z. Gong, "The Characteristics of Cloud Computing", Proceedings of the 2010 39th International Conference on Parallel Processing Workshops, IEEE Computer Society Washington, DC, USA, 2010.

[8] H. Mouratidis, C. Kalloniatis, S. Islam, M. P. Huget, S. Gritzalis, "Aligning Security and Privacy to support the development of Secure Information Systems, Journal of Universal Computer Science, Vol. 18, No. 12, pp. 1608-1627,2012

[9] C. Kalloniatis, E. Kavakli, S. Gritzalis, "Security Requirements Engineering for eGovernment Applications: Analysis of Current Frameworks", In proceedings of the 3rd International Conference on Electronic Government(EGOV'04), pp.66-71, ,2004,Springer Lecture Notes in Computer Science.

[10] G. Sindre,& A. L. Opdahl, A. L., "Eliciting security requirements with misuse cases", Requirements Engineering Journal, Vol. 10, No.1, p.p. 34–44, 2005.

[11] S. Islam, H. Mouratidis, C. Kalloniatis, A. Hudic, & L. Zechner, "Model Based Process to Support Security and Privacy Requirements Engineering", International Journal of Secure Software Engineering (IJSSE), Vol. 3, No 3, September, IGI global publication, 2012.

[12] Cloud Computing. Academic Room. [last access 16/06/2012]

[13] Cloud Security Alliance "Security Guidance for Critical Areas of Focus in Cloud Computing V3.0". https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf. [Last access 09/01/2013]

[14] EU opinion 05/2012 on Cloud Computing , 2012[Last access 09/09/2012]

[15] J. Heiser, & M. Nicolett, "Assessing the Security Risks of Cloud Computing", white paper, Gartner group, ID Number: G00157782, ,2008 [Last access 09/01/2013]

[16] R. Baburajan, The Rising Cloud Storage Market Opportunity Strengthens Vendors, infoTECH, 2011. It.tmcnet.com,[last access 02/12/2012]

[17] Z. Kerravala, Yankee Group, Migrating to the cloud is dependent infrastructure, Tech Target. Convergedinfrastructure.com.[last access 2011-12-02]

[18] W. Voorsluys, J. Broberg, & R. Buyya,. Introduction to Cloud Computing. Cloud Computing: Principles and Paradigms. 2011. New York, USA: Wiley Press. pp. 1–44. ISBN 978-0-470-88799-8.

[19] Defining Cloud Services and http://www.cloudreviews.com/blog/what-is-hot-in-cloud-computing Cloud Computing. IDC. 2008-09-23. [Last access 09/01/2013]

[20] "Jeff Bezos' Risky Bet", Business Week, http://www.businessweek.com/stories/2006-11-12/jeff-bezos-risky-bet, [Last access 09/01/2013]

[21] King, Rachael, Cloud Computing: Small Companies Take Flight, http://www.businessweek.com/stories/2008-08-04/cloud-computing-small-companies-take-flightbusinessweek-business-news-stock-market-and-financial-advice Businessweek. [Last access 09/12/2012]

[22] Defining and Measuring Cloud Elasticity, KIT Software Quality Departement. http://digbib.ubka.uni-karlsruhe.de/volltexte/1000023476. [Last access 13/08/2012]

[23] Economies of Cloud Scale Infrastructure. Cloud Slam 2011. [Last access 13/05/2012]

[24] Farber, Dan. The new geek chic: Data centers. http://news.cnet.com/8301-13953_3-9977049-80.html CNET News. [Last access 22/08/2012]

[25] B. Kitchenham, & S. Charters, Guidelines for performing Systematic Literature Reviews in Software Engineering, Version 2.3. EBSE Technical Report. University of Keele and Durham University,2007.

[26] M. Zhou, R. Zhang, W. Xie, W. Qian, & A. Zhou, Security and Privacy in Cloud Computing: A Survey, In Proceeding of 6th IEEE International Conference on Semantics, Knowledge and Grids, 2010.

[27] J.Szefer, & R. B. Lee, “A Case for Hardware Protection of Guest VMs from Compromised Hypervisors in Cloud Computing”, ICDCS Workshops, p.p. 248-252, 2011.

[28] X. Yu & Q. Wen “A view about cloud data security from data life cycle”, International Conference on Computational Intelligence and Software Engineering (CiSE), IEEE, p.p. 1-4, 2010.

[29] F. Sabahi , “Cloud computing threats and responses” , in Proceeding of 3rd IEEE International Conference on Communication Software and Networks (ICCSN), 2011

[30] B. Grobauer, T. Schreck, “Towards Incident Handling in the Cloud: Challenges and Approaches”, In proceedings of the ACM workshop on Cloud computing security workshop (CCSW 2010), ACM New York, p.p. 77-86, ISBN: 978-1-4503-0089-6, 2010.

[31] J. Wei, X. Zhang, G. Ammons, V. Bala, & P. Ning, “Managing Security of Virtual Machine Images in a Cloud Environment”, Proceedings of the ACM workshop on Cloud computing security, p.p. 91-96, New York, ISBN: 978-1-60558-784-4, 2009

[32] T. Ristenpart, E. Tromer, H. Shacham, & S. Savage “Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds”, Proceedings of the 16th ACM conference on Computer and communications security (CCS 2009), ACM New York, p.p. 199-212, ISBN: 978-1-60558-894-0, 2009.

[33] T. Grance & W. Jansen, Guidelines on Security and Privacy in Public Cloud Computing, National Institute of Standards and Technology, 2011 [last access 18/01/2013].

[34] C. Kalloniatis, E. Kavakli, & S. Gritzalis, "PriS Methodology: Incorporating Privacy Requirements into the System Design Process", Proceedings of the SREIS 2005 13th IEEE International Requirements Engineering Conference – Symposium on Requirements Engineering for Information Security, J. Mylopoulos, G. Spafford (Eds.), August 2005, Paris, France,

[35] C. Kalloniatis, E. Kavakli, E. & S. Gritzalis, “Addressing privacy requirements in system design: The PriS method”, Requirements Engineering Journal, Vol. 13, No. 3, p.p. 241-255, 2008.

[36] C. Kalloniatis, E. Kavakli, E. Kontellis (2010) "PRIS tool: A case tool for privacy-oriented Requirements Engineering", Journal of Information Systems Security, Vol. 6, No. 1, pp. 3-19, AIS

SIGSEC, University of the Aegean, E-Vote: An Internet-based electronic voting system. University of the Aegean, Project Deliverable D 7.6, IST Programme 2000#29518, 21/11/2003, Samos

[37] E. Kavakli, C. Kalloniatis, P. Loucopoulos, & S. Gritzalis, (2006) "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, Vol. 16, No 2, pp.140-158

[38] C. Kalloniats, E. Kavakli, S. Gritzalis., "Dealing with Privacy Issues during the System Design Process", 5th IEEE International Symposium on Signal Processing and Information Technology, December 18-21, 2005, Athens, Greece

[39] S. H. Houmb, S. Islam, E. Knauss, J. Jürjens, & K. Schneider, Eliciting Security Requirements and Tracing them to Design: An Integration of Common Criteria, Heuristics, and UMLsec. Requirements Engineering Journal, 15(1):63–93, March. Springer-Verlag, 2010.

[40] "Cloud Security and Privacy: What Is the Data Life Cycle?", Programming 4 Us, http://mscerts.programming4.us/ [Last access 29/10/2012]

[41] "CloudTP", Nibula Cloud Comptuing http://cloudtp.com/thought-leadership/cloud-vendor-evaluations/cloud-computing-emerging-companies/nimbula-cloud-computing, [Last access 29/10/2012]

[42] European Parliament and the Council: Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and of the free movement of such data. October 1995.

[43] J.C. Cannon, Privacy, What Developers and IT Professionals Should Know. Addison-Wesley, 2004

[44] S. Fischer-Hübner, IT-Security and Privacy, Design and Use of Privacy Enhancing Security Mechanisms. Lecture Notes in Computer Science, Vol. 1958. Springer-Verlag, Berlin Heidelberg New York, 2001

[45] Pfitzmann, B., Waidner, M., Pfitzmann, A.: Rechsicherheit trotz Anonymität in offenen digitalen Systemen. Datenschutz und Datensicherheit(DuD) No. 6, 243-253 (Part 1), No. 7 305-315 (Part 2), 1990.

[46] A. Pfitzmann, Diensteinte-grierende Kommunika-tionsmnetze mit teilnehmerüberprüfbaren Datenschutz. Informatik-Fachberichte 234. Springer-Verlag, Berlin Heidelberg New York, 1990

[47] H. Mouratidis, & P. Giorgini, , " Secure Tropos: A Security-Oriented Extension Of The Tropos Methodology", International Journal of Software Engineering and Knowledge Engineering, © World Scientific Publishing Company 2006.

[48] E. Kavakli, S. Gritzalis, and C. Kalloniatis, C., "Protecting Privacy in System Design: The Electronic Voting Case", Transforming Government: People, Process and Policy, Vol. 1,No. 4, p.p. 307-332, 2007.

[49] C. Kalloniatis, E. Kavakli, S. Gritzalis, "Methods for Designing Privacy Aware Information Systems: A review", Proceedings of the PCI 2009 13th Pan-Hellenic Conference on Informatics, pp.185-194, V. Chrysikopoulos, N. Alexandris, C. Douligeris, S. Sioutas (Eds.), September 2009, Corfu, Greece, IEEE CPS Conference Publishing Services, 2009.

[50] Islam, S., Mouratidis, H., & Wagner, S., "Toward a framework to elicit and manage security and privacy requirements from laws and regulation", In Proceeding of Requirements Engineering: Foundation for Software Quality(REFSQ), Lecture Notes in Computer Science, Volume 6182/2010, pp.255-261, 2010.

[51] A.K. Massey, P.N. Otto, L.J. Hayward, & A. I. Antón, "Evaluating existing security and privacy requirements for legal compliance", Requirements Engineering Journal, Vol 15, No1, Springer-Verlag, 2010.

[52] M. Mulazzani, S. Schrittwieser, M. Leithner, M. Huber, & E. Weippl. “Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space”. Proceedings of Usenix Security, 2011.

[53] A. Khajeh-Hosseini, I. Sommerville , J. Bogaerts, , & P. Teregowda, “Decision Support Tools for Cloud Migration in the Enterprise”, In proceeding of IEEE 4th International Conference on Cloud Computing. IEEE Computer Society, 2011.

[54] B. Grobauer, & T. Walloschek, & E. Stocker, “Understanding Cloud Computing Vulnerabilities”, IEEE Security & Privacy Magazine, Vol. 9, No. 2, pp. 50-57, 2011.