INTERNATIONAL
HELLENIC
UNIVERSITY

Security Classification of Data for Cloud Environments

Student Name: Areti Bania

SID: 3301120013

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Information and Communication Systems

NOVEMBER 2013

THESSALONIKI – GREECE

INTERNATIONAL HELLENIC UNIVERSITY

Security Classification of Data for Cloud Environments

Student Name: Areti Bania

SID: 3301120013

Supervisor:		Assistant Professor. Vasileios Katos
Supervising Members:	Committee	Assoc. Prof. Name Surname
		Assist. Prof. Name Surname

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Information and Communication Systems

NOVEMBER 2013

THESSALONIKI – GREECE

Abstract

This dissertation was written as a part of the MSc in ICT Systems at the International Hellenic University. Specifically, this master thesis focuses on describing what cloud computing is and addresses the top security risks and threats while adopting a cloud provider. Besides analyzing in general the security risks and threats, it further examines data security in the cloud during the different stages of the data life cycle and, taking these aspects into consideration, a comparison of different cloud providers is presented. Finally, the last part of the master thesis, describes the development of a wizard that can help a stakeholder to choose a cloud provider based on his needs and the provided security features.

I would like to express my gratitude to my supervisor Prof. Vasileios Katos for his useful comments, remarks and help throughout this period. Furthermore, I would like to thank Dr. Efstratios Kontopoulos. Without his supervision and constant help this dissertation would not have been possible. Last but not least, I would like to thank my family for always being on my side.

Areti Bania

6 November 2013

Contents

1 Introduction

Many debates are made during the last years on whether cloud computing is a new technology or a technology that is based on traditional technologies that were gradually evolved. After many argues and scientific researches, the scientific community has concluded that cloud computing isn't a new technological revolution but instead is the result of a continuous evolution of existing technologies in the last fifty years.

Specifically, Jeffrey Voas, a computer scientist at the US *National Institute of Standards and Technology* (*NIST*), states that cloud computing, as we know it today, has passed through six phases during all these years. Figure 1 depicts those stages, starting with the use of mainframes in the 50's, where a user could access the mainframe by using a terminal. Later, they were replaced by the personal computer (PC). Then the advent of the local networks enabled the communication between different computers and, when the Internet was established, it changed the ways of communication and sharing. During the fifth stage, grid computing was introduced, where computer power and data storage capacity was shared over the Internet, eventually leading to cloud computing as we know it today [38].

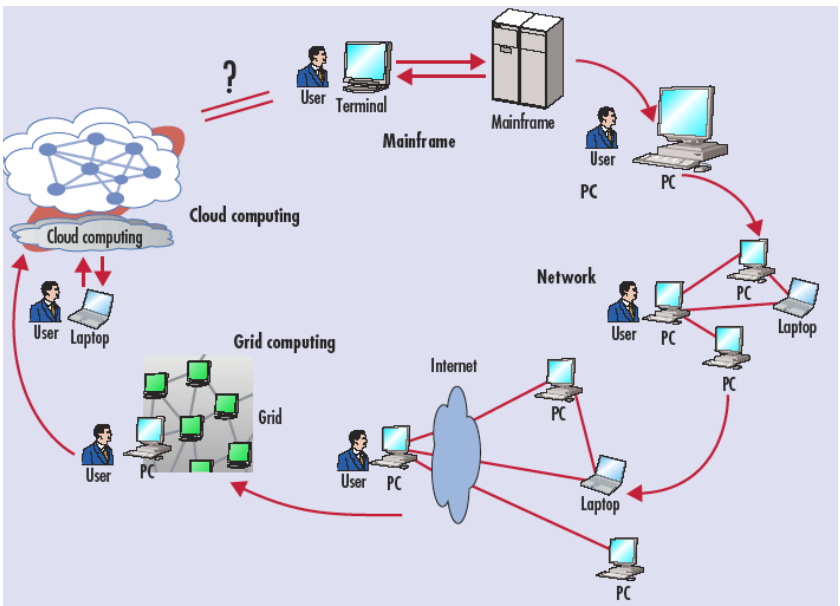

Figure 1: The Evolution of Cloud Computing [38]

Cloud computing is a technological trend that has radically changed the way we perceive information technology services today and the way we do business. Particularly, cloud computing provides on demand self-service, broad network access, resource pooling, rapid elasticity and measured service. Consequently, an increasing number of organizations and businesses have already adopted a cloud, or they intend to, given that it reduces capital and IT costs, improves the operational flexibility and gives a vital advantage towards their competitors.

However, cloud computing, just as any traditional information system, faces many security risks and threats, such as Lock-in, Loss of governance, Compliance risks, Isolation failure and Data protection risks. Some of these risks are inherited from conventional IT computing, while others are explicitly related to it. Thus, a secure cloud environment should mitigate these risks, by adhering to the fundamental principles of information security, i.e. Confidentiality, Integrity and Availability (CIA triad). Concerning individuals who wish to migrate their business to a cloud provider, these factors should be taken into consideration, in order to achieve the optimal security assurance.

Nevertheless, one of the key challenges that security experts are still concerned about is the protection of data in cloud environments. Malicious attackers can easily explore new ways to launch attacks to the cloud provider, compromising that way the stored data. Security experts suggest that, in order to achieve the optimal data protection, the IT departments of organizations and businesses have to closely examine all the stages of the data lifecycle and the ways data are accessed and processed from applications and individuals. The data lifecycle, together with the appropriate security techniques, such as data encryption, data classification and access management should be adopted in each phase, in order to mitigate the security risks as much as possible.

At this point, it should be mentioned that, since many resources are invested in protecting the confidentiality, availability and integrity of data, organizations and businesses should assess their risk tolerance by adopting a risk assessment approach, before moving their data to a cloud provider. The risk assessment should not only focus on information assets but also it should take into account how this information is used, stored and processed and what are the threats and vulnerabilities that may occur, avoiding that way the exposure of vital data to potential threats. Even though

many risk assessment methodologies are proposed, Octave Allegro is a really promising risk based information security assessment.

Having examined all the aforementioned issues, it is concluded that selecting the suitable cloud provider isn't as easy as it seems. With so many diverse cloud deployment choices that can be combined with the three service models, a stakeholder should determine the most appropriate one, taking into consideration not only the various security and privacy requirements but also the legal, regulatory and operational requirements. Particularly, since the operation of most organizations and businesses relies on the management of data, and especially confidential data, there are no margins for errors or security breaches. Consequently, given that malicious attackers and nefarious insiders constantly explore new ways to manipulate systems, there is no question that data are no longer safe and only by taking a holistic approach to security can a cloud environment be considered safe.

To that end, the objective of this dissertation is to examine thoroughly what cloud computing is, to analyze in depth the existing service models combined with the various deployment models, to understand not only the security risks this newborn technology involves but also to comprehend the specific security risks when choosing to adopt a cloud and to indicate how the optimum data protection can be achieved when choosing to mitigate to a cloud. Furthermore, a methodology is proposed for allowing a stakeholder, by answering a series of questions, to make an informed decision concerning which service model to choose and consequently which cloud provider best fits his need.

Thus, Chapter 2 contains a general analysis of cloud computing together with its five essential characteristics and points out the three service models, SaaS, PaaS, IaaS and the four deployment models. In addition, the top security risks and threats in Cloud Computing are analyzed. Chapter 3 examines the security of data in a cloud environment during data lifecycle and emphasizes on the security measures that should be applied to every phase of data lifecycle in order to achieve the optimum data protection. Chapter 4 examines further the three service models and a comparison among fifteen cloud providers is made, in order to implement a Java wizard that will recommend to a stakeholder a cloud provider that can cover his need based on certain security features. Finally, Chapter 5 concludes the dissertation and gives an initial outline of ideas for further improvements and directions of work.

2 Cloud Computing

As the global economic crisis has infected the public and private sector, many companies, in order to deal with the strict budgets and at the same time to continue being competitive, moved to cloud environments, saving approximately 45% of operational and infrastructure resources. Many analysts have predicted that the size of this market will reach $150 billion by 2013 and by 2016 they expect a 130% increase. To this end, in order to evaluate this trend, it has to be understood what cloud computing is and how it works.

2.1 What is Cloud Computing

Many researchers tried to give a formal definition about what cloud computing really is and many debates were made about this issue. If we tried to give a general definition, we would say that cloud computing isn't just a single system, it is a system that comprises many technologies and models. However a definition that is generally accepted by the community is made by the U.S. National Institute of Standards and Technology (NIST) that defines Cloud computing as" *a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*." (Mell & Grance, 2011) [1].

In other words, NIST defines cloud computing by analyzing five essential characteristics: 1) On-demand self-service, 2) Broad network access, 3) Resource pooling, 4) Rapid elasticity**,** 5) Measured service, three service models: 1) Software as a Service (SaaS), 2) Platform as a Service (PaaS), 3) Infrastructure as a Service (IaaS) and four deployment models: 1) Private cloud, 2) Community cloud, 3) Public cloud, 4) Hybrid cloud [1]. All these factors are analyzed in respective subsections later on.

Figure 2 visualizes the NIST Visual Model of Cloud Computing Definition [2].

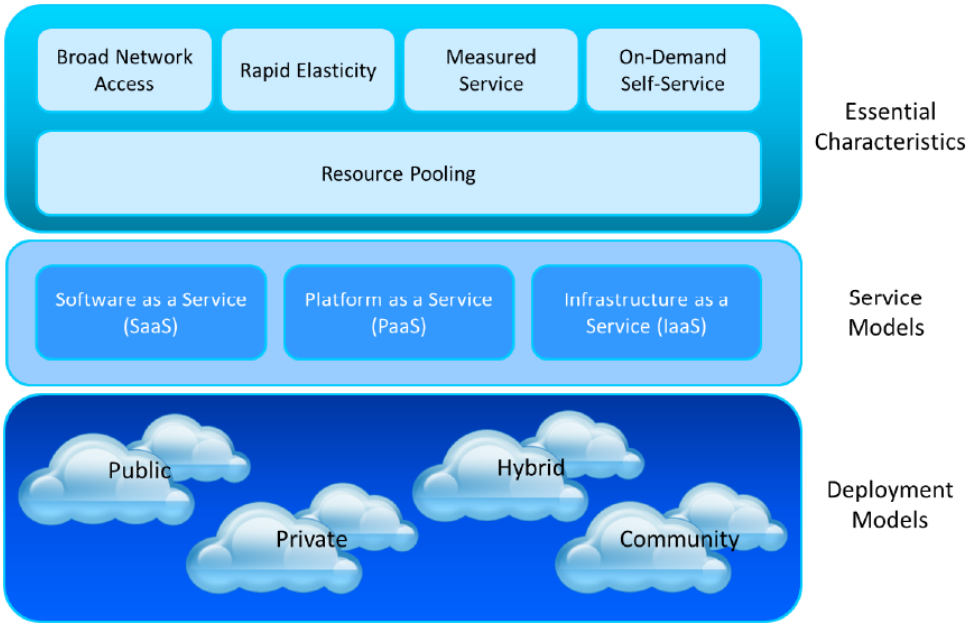

Figure 2: Visual Model of Cloud Computing Definition [2]

In general, these kinds of systems are based on the client-server model. Figure 3 depicts a physical view of how a cloud provider can be accessed by different clients. As can be observed, a cloud provider consists of a grid of computers in a network that is in position to provide their services to clients. Therefore, this grid is able to serve clients that are already accessing the cloud and using its resources, clients that want to initiate access and those who terminate their access to the cloud.

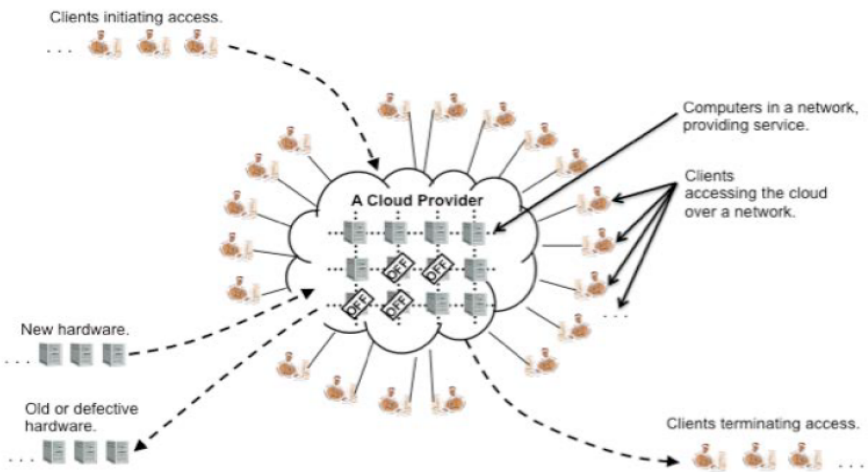

Figure 3: A general view of Cloud environment [2]

The main goal of each cloud provider is to maximize the provided services, but at the same time to try to minimize the costs. Hence, a cloud provider can embody new hardware, revoke old or deficient hardware and turn off computers during periods with small demand [2].

2.1.1 Five Essential Characteristics

These characteristics are critical for cloud computing, since they define the advantages of using this kind of systems and also they signify the similarities and differences compared to traditional computing systems. In detail, the five essential characteristics are: [5] [6]

1) *On-demand self-service:* This characteristic defines that a client can use a cloud provider on demand without any interaction between the two of them, giving the ability to the client to exploit capabilities such as computation and storage as needed. This way both client and cloud providers decrease costs and are more efficient.
2) *Broad network access:* This characteristic defines that a client can have access and make use of all capabilities of a cloud provider through network, enabling the connectivity of many different computing platforms such as laptops, mobiles, printers and PDAs. However, the use of this three-tier architecture of platform connectivity may lead to some delays.
3) *Resource pooling:* This characteristic defines that resources, such as storage and virtual machines, are pooled in order to provide the best service according to the client's demands. In order to achieve this optimum performance, the resources can be allocated to different locations unfamiliar to clients.
4) *Rapid elasticity:* This characteristic defines that a cloud provider can administrate their resources efficiently, having the ability to expand or reduce the resources quickly and automatically, serving client needs effectively.
5) *Measured service:* This characteristic defines that all accessible services that a cloud provider makes available to clients can be monitored, controlled and measured, giving the ability to clients to be charged only for the allocated resources used.

2.1.2 Three Service Models

These three cloud models usually are referred to as *the SPI model*, where *S* stands for Software, *P* stands for Platform and *I* stands for Infrastructure. At this point, it should be noted that *Infrastructure as a Service* (*IaaS*) is the core of the three service models, while *Platform as a Service* (*PaaS*) sits upon IaaS and adds one more layer of Integration and Middleware and *Platform as a Service* (*PaaS*) is built upon PaaS. Figure 4 depicts this stack of service models and it can be observed that each stack inherits the capabilities but also the information security issues and risks (from the stacks below it) [3].

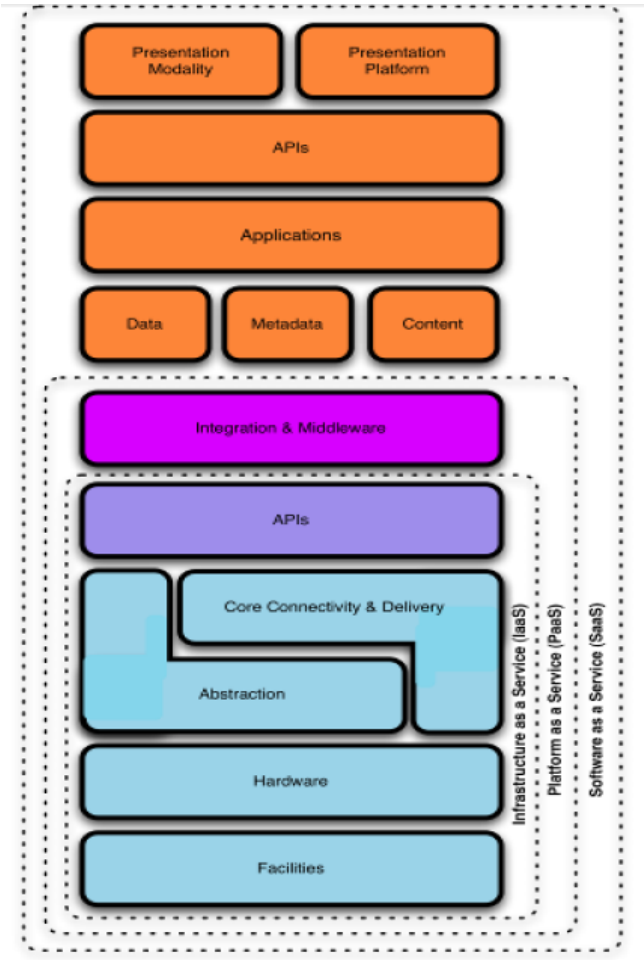

Figure 4: Cloud Reference Model diagram [3]

1) *Software as a Service (SaaS):* Is a model of service delivery that is able to provide to consumers individual software packages such as online word processing**.** This kind of cloud model does not permit the consumer to control

cloud infrastructure except from some limited configuration settings of the applications. Some vendor examples are Zoho Suite, Apple's MobileMe, Google Docs, Facebook, Windows Live and LinkedIn.

Figure 5 briefly illustrates the interaction between clients and the SaaS cloud model [2]. This simplified model depicts how a cloud provider serves two clients C_1 and C_2. Specifically, the provider offers a variety of applications that can be used by the clients over the internet. For instance, C_1 uses two applications (B and C) and C_2 uses one application (C). In order to be executed, the used applications utilize execution resources, such as physical computers or virtual machines that the cloud provider is in position to offer. Thus, client C_1 uses execution resource 1 for application B and execution resource 2 for application C, whereas client C_2 for the same application uses execution resource 3.

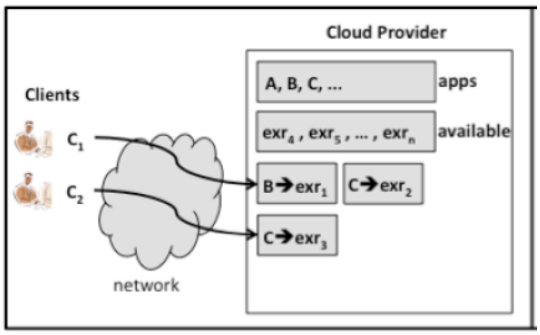

Figure 5: SaaS Client-Provider Interaction [2]

2) *Platform as a Service (PaaS):* Is a model of service delivery that provides consumers with a complete operating system and software package, in order to deploy new applications using APIs. Similarly with SaaS, the consumer has no control over the cloud infrastructure, but has overall control of the applications. Some vendor examples are Google App Engine, Microsoft Azure, Intuit QuickBace and force.com.

   Figure 6 briefly depicts the interaction between clients and the PaaS cloud model. In general, the cloud provider consists of applications, development tools such as programming languages, interfaces and compilers and execution resources. In particular, Figure 6A shows the interaction between a client and

a PaaS environment. Similarly to the SaaS environment, the client uses two applications (B and C) that are executed by the execution resources 1 and 2. Figure 6B and Figure 6C demonstrate how the cloud provider can serve a developer and a client. The developer uses the development tools, while the client uses the applications that are executed by the execution resources. The output of the development tools usage is added to the cloud provider as a new application. Finally Figure 6D illustrates that an administrator configures the application that was made by the developer in the previous figure and a client at this point is able to use both the new and old applications.

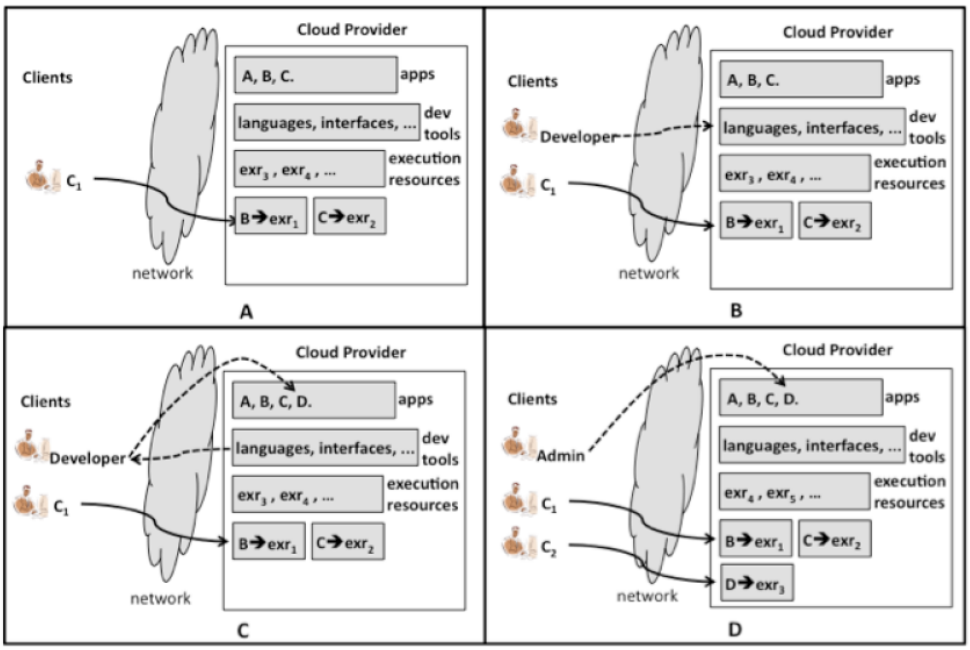

Figure 6: PaaS Client-Provider Interaction [2]

3) *Infrastructure as a Service (IaaS):* Is a model of service delivery that is able to provide to consumers mainly infrastructure services such as storage, network capacity etc. As the abovementioned models, the consumer isn't permitted to control cloud infrastructure, but can control operating systems, storage and applications. Some vendor examples are Amazon EC2 and S3, Sun Microsystems Cloud Services, Terremark, Dropbox.

   Figure 7 briefly illustrates the interaction between clients and the IaaS cloud model. Currently, the cloud provider consists of virtual machines available to be utilized by clients.

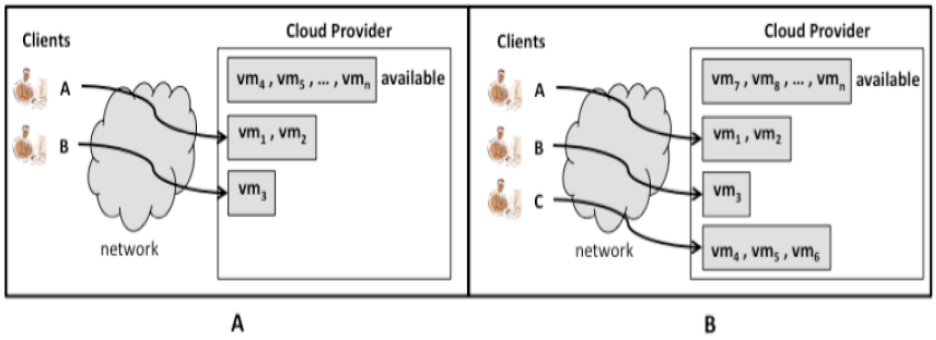

Figure 7: IaaS Client-Provider Interaction [2]

For example, in Figure 7A client A has access to two virtual machines, while client B has access to one virtual machine. In addition, in Figure 7B we can observe a new client entering the cloud provider, in order to use virtual machines and the allocations of the available machines of the provider.

Figure 8 depicts the control that a cloud consumer and a cloud provider have over a cloud environment for each of the three models. On the whole, one can say that, whenever the control of the cloud provider is high, the control of the cloud consumer is correspondingly narrow. At this point, it is also worth mentioning that a cloud consumer can have control only to the three top layers of the cloud environment, whilst the cloud provider has full control over the bottom two [4].

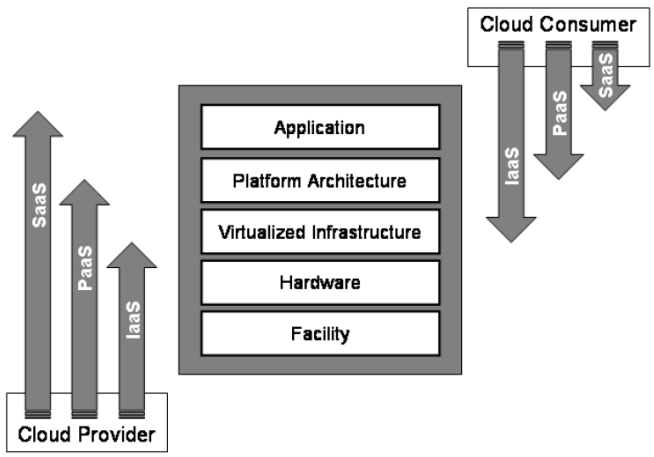

Figure 8: Control among Cloud Service Models [4]

2.1.3 Deployment Models

For all three service models described above there are also several deployment models. Specifically, a service model can be represented to users in any of the four deployment models [5].

1) *Private cloud:* Is a deployment model that can be used solely by a single organization. Private clouds are also known as internal clouds. It is managed and owned by organizations or third party providers and it can be on or off - premise of the organization's data center. Figure 9 illustrates a simplified concept of a private cloud.

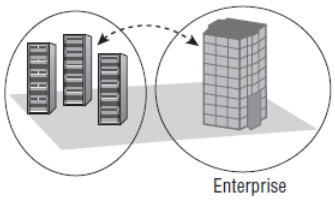

Figure 9: Private Cloud [5]

2) *Community cloud:* Is a deployment model, where multiple organizations that have overlapping concerns share the same cloud infrastructure. It may be located on any member's premises, but a significant issue arises concerning the managing of this cloud due to undetermined ownership.
3) *Public cloud:* Is a deployment model that can be used by individuals or enterprises over the Internet. Public clouds are also known as "*externals*". They are managed and owned by organizations that sell cloud services and are external to consumers. Figure 10 depicts a simplified concept of a public cloud.

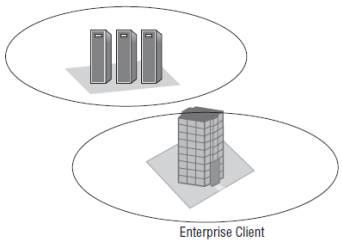

Figure 10: Public Cloud [5]

4) *Hybrid cloud:* Is a combination of at least two of the private, community and public clouds. The clouds that belong to a hybrid cloud continue to retain their characteristics and use uniform technologies, in order to permit data and application portability. For instance, an organization can store sensitive data to the private cloud and non-sensitive data to a public cloud. Figure 11 illustrates a simplified concept of a hybrid cloud.

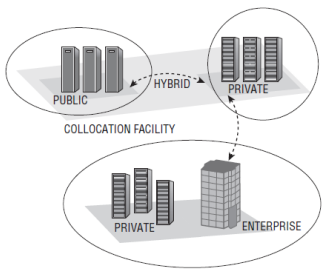

Figure 11: Hybrid Cloud [5]

Table 1 summarizes the main points of the four deployment models. The term "management" implies who should be responsible for issues such as governance, security and compliance with policies and standards. Furthermore, "trusted" and "untrusted" consumers are terms to indicate which of them can be considered part of the organizations and which cannot. [3]

Table 1: Deployment models [3]

	Infrastructure Managed By	Infrastructure Owned By	Infrastructure Located	Consumed By
Public	Third Party Provider	Third Party Provider	Off- Premise	Untrusted
Private/ Community	Organizations Or Third Party Provider	Organizations or Third Party Provider	On- Premise or Off Premise	Trusted
Hybrid	Both Organizations & Third Party Provider	Both Organizations & Third Party Provider	Both On-Premise & Off- Premise	Trusted & Untrusted

2.2 Cloud Security Objectives and Services

Cloud computing, just as any traditional information system, faces many risk issues. Some of these risks are inherited from conventional IT computing, while the rest are explicitly related to it. The next sections explore the objectives and services of cloud information security and study how these affect the security of a cloud.

2.2.1 Cloud Security Objectives

The three fundamental principles that apply to any information system are known to security experts as *the CIA triad*, where *C* stands for *confidentiality*, *I* stands for *integrity* and *A* stands for *availability*. In order for an information system to be considered as a secure information system, it should comply with these three principals. When the triad is violated, then we have to deal with *Disclosure*, *Alteration* and *Destruction*, known as *DAD*.

At this point, in an attempt to have a better insight of the aforementioned three principals and to understand their importance, a brief description of the CIA triad is provided:

- *Confidentiality*: This principal indicates who is authorized to have access to information or data. For example, absence of this principal may occur, when an unauthorized employee reveals information to a competitive company.

Ways to protect confidentiality are via security protocols, authentication services and data encryption.

- *Integrity*: This principal specifies that information or data should not be modified by unauthorized individuals, or authorized individuals should not proceed to unauthorized modifications of information or data. For instance, absence of this principle may occur, when an employee accidentally or intentionally modifies information or data. Ways to protect integrity is by using firewalls, intrusion detection services and communications security management.
- *Availability*: This principal ensures that an authorized individual can have immediate access to system, whenever this is needed. For instance, absence of this principal may occur during *denial-of-service* attacks, known as *DoS*. Some ways to protect the availability is via appropriate networking security mechanisms or fault tolerance concerning data availability.

2.2.2 Cloud Security Services

Besides the CIA triad principals, there are four additional security objectives that are equally important: *Authorization*, *Authentication*, *Accountability* and *Auditing*. These concepts are described briefly below [5]:

- *Authentication*: Identification and Authentication are concepts that guarantee that, when an individual logs into a system, the credentials used indeed correspond to the specific user. Identification is especially important for authentication and authorization.
- *Authorization*: This principal determines the rights and privileges that an individual has to the system and its resources. It is important for every organization to determine the levels of the employees' authorization to the system, in order to mitigate the exposure of critical information and data.
- *Accountability*: This principal ensures that a user of a cloud system won't be able to deny his actions or behaviors. Accountability can be supported for instance with the use of logs or via audit trails that can provide information such as the date and time of a transaction and who was involved in the transaction. The description of this principal implies that accountability correlates with non-repudiation.

- *Auditing*: The two basic methods of auditing are: a) System Audit and b) Monitoring. The primary goal of these methods is to conserve operational assurance by evaluating periodically (or just once) the security of the system or by monitoring user activities. It should be mentioned that the Information Systems Audit and Control Association has established some standards that apply specifically to cloud environments.

Figure 12 depicts six information security requirements in terms of service models and deployment models of a cloud environment. The 'X' mark indicates that a specific requirement is mandatory while the '*' mark indicates that the requirement is optional [8] [9]. For instance, in a Hybrid cloud, availability is optional for all three service models, in a Private cloud it is mandatory for all three service models and in a Public cloud it is mandatory for IaaS and PaaS, while it is optional for the SaaS service model.

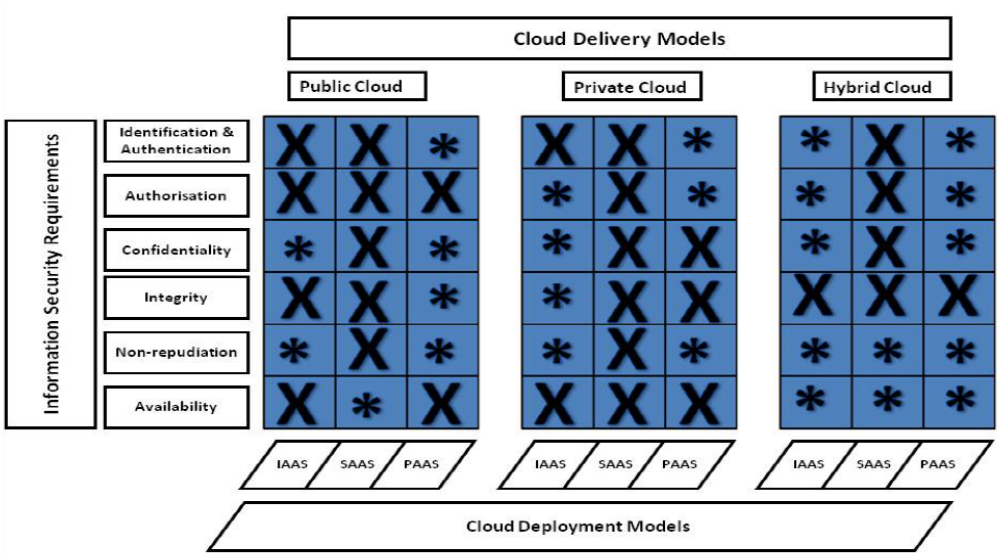

Figure 12: Information Security Requirements [8]

It is important to understand that in cloud computing the levels of security are affected by the type of cloud (e.g. Public, Private or Hybrid) and by the service model (e.g. SaaS, IaaS, PaaS). Generally, it could be argued that Public clouds require more careful security planning, whereas Private clouds require less, since they are similar to conventional systems. Concerning the service models, in SaaS environments the security levels are negotiable between the cloud provider and the client and the

outcome is the contract of service, in IaaS environments the provider is responsible for the security levels of infrastructure and abstraction layers, while the client is responsible for the remainder of the stack. Finally, in PaaS environments the provider is responsible for the security levels of the platform and the client is responsible for the security levels of applications. Either way, a secure cloud environment should mitigate risks by adopting the CIA triad and ensure access by taking into consideration the authentication, authorization, accountability and auditing.

2.3 Security Risks and Threats in Cloud Computing

Adopting a cloud provider has obviously numerous benefits, however, those who have already shifted to this kind of solution, or intend to do so, have to understand and take into consideration the vulnerabilities and security threats, in order to achieve the optimal security assurance.

2.3.1 Top Security Risks

In an attempt to identify the potential security risks that may be involved in cloud environments, a classification into three main categories has been addressed: 1) *Policy and Organizational Risks*, such as Lock-in, Loss of governance, Compliance risks, Cloud service termination or failure, 2) *Technical Risks*, such as Isolation failure, Cloud provider malicious insider, Management interface compromise, Insecure or incomplete data deletion, 3) *Legal Risks*, such as Risk from changes of jurisdiction, Data protection risks and Licensing risks. Furthermore, the levels of security risks may vary depending on the type of cloud architecture.

Table 2 presents briefly the most common security risks in clouds and the level of the corresponding risk. However, the emphasis will be on analyzing only the top security risks of each class.

Table 2: Security Risks [6]

Security Risks		
Category	**Risk**	**Level of Risk**
Policy & Organizational Risks	Lock-in	High
	Loss of governance	High
	Compliance challenges	High
	Loss of business reputation due to co-tenant activities	Medium
	Cloud service termination or failure	Medium
	Cloud provider acquisition	Medium
	Supply chain failure	Medium
Technical Risks	Resource exhaustion	Medium
	Isolation failure	High
	Cloud provider malicious insider	High
	Management interface compromise	Medium
	Intercepting data in transit	Medium
	Data leakage on up/download, intra-cloud	Medium
	Insecure or ineffective deletion of data	Medium
	Distributed denial of service (DDoS)	Medium
	Economic denial of service (EDOS)	Medium
	Loss of encryption keys	Medium
	Undertaking malicious probes or scans	Medium
	Compromise service engine	Medium
Legal Risks	Subpoena and e-discovery	High
	Risk from changes of jurisdiction	High
	Data protection risks	High
	Licensing risks	Medium

Therefore, according to the research of the *European Network and Information Security Agency* (*ENISA*) [6], the top security risks based on the level of their risk are:

- *Lock-in*: Lock-in is a term to describe the portability and interoperability among different platforms. In other terms, customers cannot easily migrate their data from one cloud provider to another, since cloud API's aren't standardized yet; hence there is no guarantee on successful migration. Therefore, the lack of standard technologies could cost the reputation of an organization and raise many issues about personal data [11].
- *Loss of governance:* The adoption of a cloud provider from an individual or an organization leads to relinquishing the control to the provider causing security issues. Even though between the client and the provider there is a *Service-Level Agreement* (*SLA*), a gap in security still exists. Consequently, the lack of roles and responsibilities, the unclear ownership and the lack of information on jurisdictions could lead to a severe impact on complying with the three fundamental principles of security requirements.
- *Compliance challenges*: Organizations, before moving to a cloud provider, depend on specific technologies, certifications and standards. By adopting a cloud provider, organizations have to rely on the cloud provider's technologies, certifications and standards, but there is no guarantee of compliance with the organization's requirements.
- *Isolation failure*: The main characteristic of cloud environments is the ability to provide to users a shared infrastructure, such as common network, capacity and storage. However the lack of resource isolation and the lack of reputational isolation lead to a failure of separating this shared infrastructure, making it vulnerable to attacks such as SQL injections or guest hopping attacks.
- *Cloud provider malicious insider*: Three different types of malicious insiders in clouds have been identified: 1) the imposter cloud provider administrator, 2) the employee that seeks for system weaknesses in order to exploit them and 3) the insider that uses cloud resources to perform malicious attacks. These three types of malicious insiders can violate the confidentiality, integrity and availability of information systems [12].
- *E-discovery*: Refers to a process where electronically stored information may be used as evidence in the Court of Law. Although the existent Federal Rules of

Discovery can cover a large percentage in personal computing affairs, they cannot effectively cover cloud computing. The main reason is because cloud environments lack resource isolation and cloud providers don't provide their clients with clear information about storage jurisdiction. Consequently, this could lead to disclosure of client data to third parties and the unintentional violation of regulations [13].

- *Risk from changes of jurisdiction*: One of the main issues concerning cloud computing is that the client isn't in a position to determine where the servers of the chosen provider are physically located. Moreover, usually their data are held in different jurisdictions, giving rise to serious legal issues, especially when the servers are located in high-risk countries. This lack of information on jurisdiction could lead to a dispute between the two parties and may affect personal data as they are defined by the European Data Protection Directive.
- *Data protection risks*: European law specifies that the individual who is responsible for protecting the data is the data controller. The data controller remains legally responsible, even when he assigns the data processing to third parties. Therefore, the client in the role of data controller is the only responsible individual to check if the processing of the data is carried out in a lawful way. If the client fails to meet this requirement, he will face the applicable legal sanctions of the country in which this processing occurred [14] [15].

2.3.2 Top Threats in Cloud Computing

According to a survey by the *Cloud Security Alliance* (*CSA*), security specialists acknowledge nine severe top threats to cloud security. These threats focus mainly to the first abovementioned characteristic (on demand) of cloud computing. Thus, based on their severity, the nine threats are [7] [9]:

1) *Data Breaches*: This threat indicates that if a cloud database isn't secure enough and there is a flaw in a client's account, then a malicious intruder can easily have access not only to this account and data but also to every client of the cloud. Unfortunately, this threat affects all three service models (PaaS, SaaS and IaaS) and violates one of the three fundamental principles of information security, confidentiality, while 91% of experts believe that this threat is still relevant. Figure 13 depicts the risk matrix of data breaches based on actual and perceived risk.

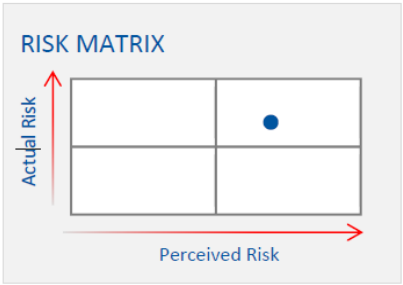

Figure 13: Data Breaches Risk Matrix [7]

2) *Data Loss*: Data losses in the cloud may occur due to many causes. Besides the activity of hackers, data could be lost as a result of natural disasters or unintentional deletion by the provider. Even though both cloud providers and clients should take efficient measures, such as backups, to prevent these losses, this survey specifies data loss as the second most severe threat. Figure 14 illustrates the risk matrix of data loss based on actual and perceived risk.

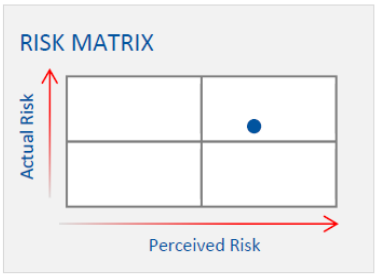

Figure 14: Data Loss Risk Matrix [7]

It should be noted that this threat may exist on all three service models and, in addition to data losses, there is a violation of the CIA triad and particularly a violation of availability. 91% of the experts claim that this threat is still relevant.

3) *Account Hijacking*: Stolen credentials and passwords are the main reason for this threat making cloud providers vulnerable to attackers. This threat in 2010 was relatively low in ranking, but in 2013 it occupies the 3rd place. Figure 15 depicts the risk matrix of account hijacking based on actual and perceived risk demonstrating how critical it is.

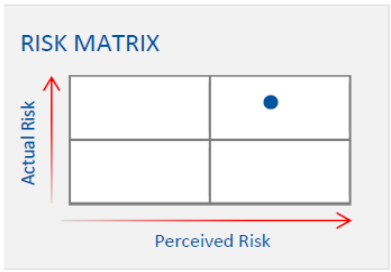

Figure 15: Account Hijacking Risk Matrix [7]

In addition, this threat affects all three service models (PaaS, SaaS and IaaS), violates all three CIA fundamental principles and 87% of experts declare that it is still relevant.

4) *Insecure APIs*: The basic benefit of service models is that they can provide clients with the ability to use existing applications or to deploy new applications using APIs. However, the security of cloud providers depends on how secure these applications are. In case of weak APIs, various security issues can arise and affect the CIA triad of information security.

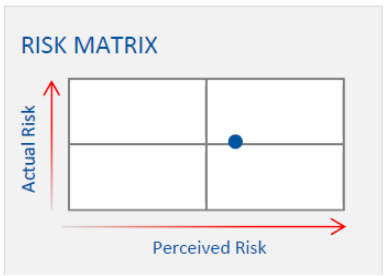

Figure 16: Insecure APIs Risk Matrix [7]

Figure 16 illustrates the risk matrix of insecure APIs based on actual and perceived risk. This threat still exists today, but fortunately occupies the 4th place in 2013, while 90% of experts claim that it is still relevant. Additionally, it should be highlighted that this threat may exist on all three service models and violates all three fundamental principles of information security.

5) *Denial of Service* (*DoS*): This kind of threat is a common attack by malicious intruders, where they prevent the clients to have access to their data and

applications. From the clients' side this appears as a slowdown of the system, making them question whether adopting a cloud environment was eventually a good practice.

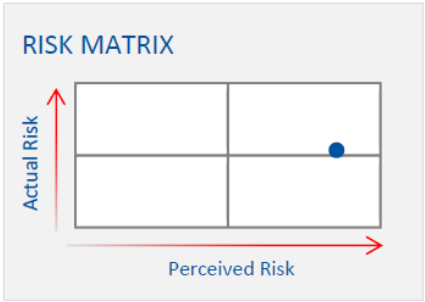

Figure 17: Denial of Service Risk Matrix [7]

Figure 17 depicts the risk matrix of denial of service, indicating that this risk should be considered as one of the top threats, while 81% of experts believe that this threat is still relevant. Furthermore, denial of service may exist on all three service models and can affect the availability of the system violating the CIA triad.

6) *Malicious Insiders*: This term implies any individual who has authorized access to a system and thereupon access to data and intentionally violates the three principals of information systems (confidentiality, integrity and availability). It is obvious that this threat can exist to all three service models.

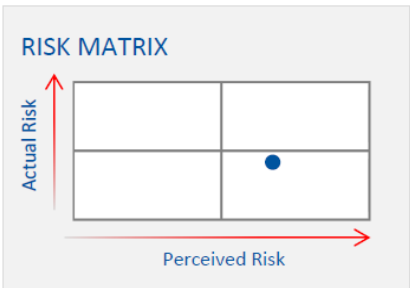

Figure 18: Malicious Insiders Risk Matrix [7]

Figure 18 illustrates the risk matrix of malicious insiders. It should be noted that even though in 2010 this threat was in 3rd place, at the moment it occupies

the 6th place. Nevertheless 88% of experts claim that this threat is still relevant.

7) *Abuse of Cloud Services*: The main advantage of cloud computing is that it can offer massive computing power to its clients. However, a malicious intruder may exploit this advantage and use cloud resources to perform attacks such as DDoS attacks. This kind of threat affects mainly the two service models, IaaS and PaaS and, while in 2010 it was the top threat to cloud computing, today it occupies the 7th place. However the 84% of experts indicate that this threat is still relevant.

8) *Insufficient Due Diligence*: Cloud computing is a new and really promising technology that offers low costs, efficient services and better security management. In order to take advantage of these promises, individuals and organizations adopt a cloud provider that might increase the security risk, without comprehending this new environment and its operation.
Figure 19 depicts the risk matrix of insufficient due diligence and obviously this threat affects all three service models, while 81% of the experts believe that this threat is still relevant.

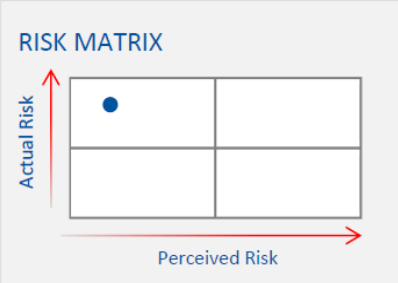

Figure 19: Insufficient Due Diligence Risk Matrix [7]

9) *Shared Technology Issues*: Cloud computing serves its clients by providing a common infrastructure and applications. However, a single vulnerability or a misconfiguration can raise security issues not only to individuals but can compromise the security of the entire cloud. This threat can affect all three service models, since cloud providers aren't in the position to offer strong isolation.

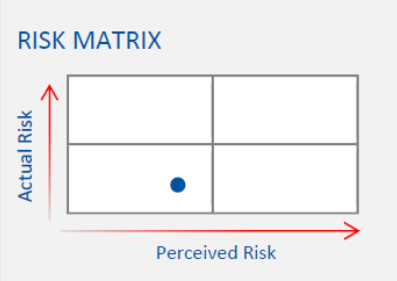

Figure 20: Shared Technology Issues Risk Matrix [7]

Figure 20 presents the risk matrix of shared technology issues and it should be mentioned that while this threat occupied the 4th place in 2010, today it occupies the last place, even though 82% of the experts believe that this threat is still relevant.

Table 3 summarizes the aforementioned top threats in cloud computing. The first column illustrates the name of the threat, followed by the service models that are being affected, the third column includes the affected CIA triad principles, the fourth column examines if the threat is still relevant and, finally, the last two columns present the rankings of the threat for 2010 and 2013.

Table 3: Top Threats in Cloud Computing

Threat	Service Model	Risk Analysis	Threat Still Relevant	Threat Ranking in 2010	Threat Ranking in 2013
Data Breaches	IaaS PaaS SaaS	Confidentiality	Yes	5th	1st
Data Loss	IaaS PaaS SaaS	Availability Accountability	Yes	5th	2nd

Threat	Service Model	Risk Analysis	Threat Still Relevant	Threat Ranking in 2010	Threat Ranking in 2013
Account or Service Traffic Hijacking	IaaS PaaS SaaS	Authenticity Integrity Confidentiality Accountability Availability	Yes	6th	3rd
Insecure Interfaces and APIs	IaaS PaaS SaaS	Authenticity Integrity Confidentiality	Yes	2nd	4th
Denial of Service	IaaS PaaS SaaS	Availability	Yes	N/A	5th
Malicious Insiders	IaaS PaaS SaaS	—	Yes	3rd	6th
Abuse of Cloud Services	IaaS PaaS	N/A	Yes	1st	7th
Insufficient Due Diligence	IaaS PaaS SaaS	—	Yes	7th	8th
Shared Technology Vulnerabilities	IaaS PaaS SaaS	—	Yes	4th	9th

2.4 Summary

Throughout this section, an attempt was made to analyze what cloud computing is and how it works. In simple terms, it could be said that cloud computing is the technology that delivers via the Internet computer resources at the user's discretion, such as storage, servers, networking and applications. There are three types of service models, Software as a Service is the appropriate model for those who wish to utilize applications that are running on a cloud infrastructure using a variety of devices.

Platform as a service is the appropriate model for those who want to develop or deploy applications by utilizing the available programming languages and tools on a cloud infrastructure. Infrastructure as a Service is the appropriate model for those who want to rent computer resources (e.g. hardware, networking, and storage) instead of buying them.

For these three service models there are also several deployment models. The term deployment model implies the location of the physical servers and who carries the responsibility of those servers. Hence, the three main deployment models that were examined are Public, Private and Hybrid clouds. Consequently, it can be derived that, similarly to any traditional information system, Cloud computing face many security risks and threats. Some of these risks are inherited from conventional IT computing, while the rest are explicitly related to it. Specifically, it has been addressed that Policy and Organizational Risks Technical Risks and Legal Risks may compromise the confidentiality, integrity and availability of the system.

3 Data Security in the Cloud

Data security in cloud environments is a major area of concern, since many organizations are still skeptical about adopting a cloud provider due to data security concerns and privacy issues. Traditional data security can cover many aspects of this technology, however, due to multi-tenancy, elasticity and the architecture of clouds, new security strategies should be adopted. To that end, it is vital to examine the security measures that should be applied to every phase of data lifecycle, in order to achieve the optimum data protection.

3.1 The Data Security Lifecycle

One of the key challenges that security experts have to deal with is the protection of data in cloud environments. However, in order to achieve the optimal data protection, organizations have to closely examine all the stages of data lifecycle and how data are accessed and processed by applications and individuals alike.

Figure 21 [10] illustrates these six phases of data lifecycle: 1) *Create*, 2) *Store*, 3) *Share*, 4) *Use*, 5) *Maintain* and 6) *Destroy*. Even though the phases appear to be linear, actually when a piece of data is created it can move around among different phases or even skip some. For instance, not all created data are deleted during the Destroy phase [3].

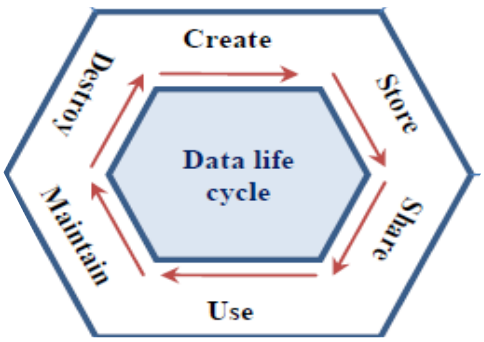

Figure 21: Data Lifecycle [10]

1) *Create:* This phase indicates, beyond the creation of new data, the alteration or the update of existing data.

2) *Store:* Just after the creation, alteration or update of data, the data lifecycle indicates the storage of data in a repository.
3) *Share:* This phase indicates that data can be shared and exchanged among users.
4) *Use:* This phase indicates that data can be accessed and processed among users.
5) *Maintain:* This phase indicates that data can be archived or backed-up. In the first case the original data that are no longer in use are stored long term and in the second case copies of the original data are stored in case of damage or loss.
6) *Destroy:* This phase indicates the permanent deletion of data. A way to accomplish this in cloud environments is by using methodologies such as *Crypto Shredding* [3] where all encryption keys and protocols are destroyed.

However, this lifecycle of data doesn't contain two main aspects of cloud environments, namely, the locations where the data are stored and who and how can have access to the data. In other words, the movement of data between different storage locations and operating environments has to be examined and also who is authorized to have access and what devices and channels he uses in order to take adequate security measures towards minimizing potential security risks.

Furthermore, Microsoft's white paper "*Guide to Data Governance for Privacy, Confidentiality, and Compliance-Managing Technological Risks*" [16] introduces a new phase to the existing data lifecycle model, the *Transfer* phase. By this term, it is implied that a piece of data can be either copied or removed from its original location and transferred to another location, indicating the creation of a new lifecycle. Security experts consider this phase equally important for data security and privacy with all the other phases, since it involves additional security risks. For instance, what physical means are used for transferring the data (e.g. Internet, private network), should data be encrypted before the transfer and during the transfer and does the recipient have the same security policies in order to protect the data?

Figure 22 depicts how data can be accessed by different devices in different locations and environments and how these layers are interconnected. The low level layer contains the external and internal devices, such as laptops and smart-phones that are used as access devices, the middle level layer illustrates the traditional infrastructure with the aforementioned data lifecycle and the top level layer contains the cloud and

hosting services together with the corresponding data lifecycles. Consequently, it is derived that data may exist in a location, may be transferred between different locations or between external providers [17]

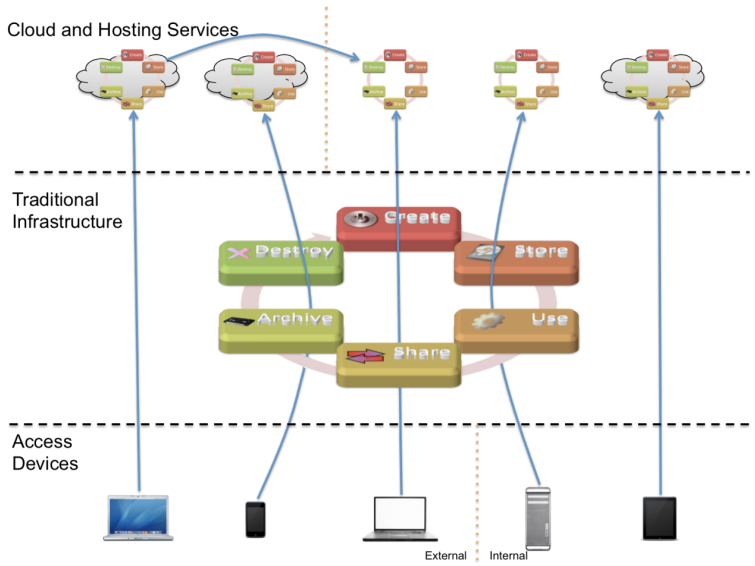

Figure 22: Cloud Access Devices and Locations [17]

The next step that should be taken into consideration is to map every phase of data lifecycle with the techniques that can be used, in order to mitigate the security risks as much as possible. To that end, Figure 23 presents the data lifecycle together with the appropriate techniques that should be adopted in each phase. The detailed presentation of the aforesaid techniques is given in the next sections.

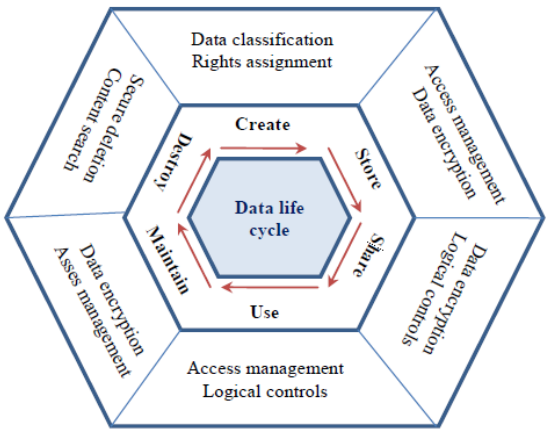

Figure 23: Ensuring data security in cloud [10]

3.2 Data Security during Create Phase

As mentioned earlier, during the first phase of data lifecycle the creation, alteration and update of digital content is addressed. Specific risks involved in this phase have to do, mainly, with the unauthorized creation and access of data. A proposed technique to prevent these risks is the classification of data and the assignment of rights or permissions.

3.2.1 Data Classification

Data Classification is a process, where structured and unstructured data are classified manually or automatically by an authorized administrator based on the organization's application logic or by tagging and labeling. Data classification is vital for any organization, not only in order to achieve the best possible security protection by enhancing the fundamental principles of the CIA triad (see Section 2.2), but also, for giving a competitive advantage to every organization, by providing information concerning the sensitivity or the substantiality of data. In addition, it has to be clarified that not all data are equally important to organizations, thus, during classification the sensitivity of loss or disclosure of data needs to be considered.

On the above basis, a classification scheme regarding data and its applicability to cloud contains respectively four classes to achieve the optimal confidential and availability levels and three classes to achieve the optimal integrity levels. The confidentiality classes are: 1) *Public*, where information isn't classified and can be publicly shared without affecting the organization or the employees (e.g. advertising leaflets, press releases), 2) *Internal*, (default) where information requires more careful classification planning (e.g. internal documents and memos) and it may be accessed only by the organization's personnel, 3) *Confidential*, where the information can be accessed only by authorized individuals and the likelihood of disclosure will affect the organization (e.g. financial information and risks, product strategy) and 4) *Strictly Confidential* that contains critical information about the organization and an unauthorized disclosure will lead to severe impact for the organization (e.g. clients or personnel identifying data). The main goal of these classes is to enhance the confidentiality of data and to protect them from unauthorized or accidental disclosure. Table 4 presents the four confidential levels together with a brief description of the required protection [20].

Table 4: Confidentiality levels [20]

Confidentiality	Suggested Protection
Public	No need for taking protection measures since information is available to general public.
Internal (Default)	Access control mechanisms, authentication mechanisms and encryption mechanisms are recommended to prevent unauthorized access and to protect information that is transferred outside the organization.
Confidential	Increased access control mechanisms, access rights should be reviewed occasionally, increased authentication mechanisms, narrow physical access.
Strictly Confidential	Transferred data should be encrypted, strict authentication mechanisms, strict access control mechanisms, restricted physical access.

The integrity classes are: 1) *Basic*, where in case of alteration, loss or destruction of data the impact will be insignificant for the organization and it will require correction at the administrative level, 2) *Trusted* (default), where the alteration, loss or destruction of data will lead to a significant impact for the organization and legal measures for correction might be applied, 3) *Guaranteed*, where the alteration, loss or destruction of data will have a huge impact to the organization, both in economic and legal terms. The main goal of these categories is to enhance the integrity of data and to protect them by an unauthorized, accidental modification or deletion [10] [18]. Table 5 presents the three integrity levels together with a brief description of the suggested protection measures [20].

Table 5: Integrity levels [20]

Integrity	Suggested Protection
Basic	Basic access control mechanisms should be implemented and protection of unauthorized changes of information is recommended.

Integrity	Suggested Protection
Trusted (default)	Data traceability techniques should be applied in order to monitor authorized and unauthorized modifications and increase the security measures for control access.
Guaranteed	Use of cryptographic hash functions and cryptographic signatures to enhance tamper-proof evidence in order to serve a better protection to information.

Concerning availability, the four classes are: 1) *Bronze*, where the cloud provider offers the best minimum security protection, in order to achieve 99% of availability, without the provision of penalties in case of failing to meet this goal, 2) *Silver*, where the cloud provider implements continuity plans with the provision of penalties in cases of failure, in order to achieve 99,9% of availability, 3) *Gold*, where the cloud provider implements continuity plans and offers protection against (*Distributed Denial of Service*) *DDoS* attacks with the provision of penalties, in order to achieve 99,9% of availability and 4) *Platinum*, where the cloud provider uses continuity plans and offers protection against DDoS attacks with the provision of penalties in case of failing to meet this goal, in order to achieve 99,9% of availability. It should be noted that Gold and Platinum levels don't permit unplanned outages; also at Gold level the permitted disruption of unplanned internet connectivity varies from zero to one while at Platinum level it isn't permitted at all. Table 6 presents the four availability levels together with a brief description of the suggested protection measures [21].

Table 6: Availability levels [21]

Availability	Suggested Protection
Bronze	Antivirus and malware protection, Network and firewall isolation, Data retention and deletion management, Secure protocols for remote administration.
Silver	Network intrusion prevention, Control access to logs, Implementation of continuity plan.
Gold	Penetration testing, Isolation of hardware, Encrypted communication and authentication.

Availability	Suggested Protection
Platinum	Encryption of data in flight and in rest, prohibition, and Cloud provider's employees should not have administrative access.

Furthermore, since data don't have the same value within the organization and in order to define which data will be classified and which won't, some classification criteria should be specified. The most common classification criterion is *Value*, which determines if a piece of information/data is important to the organization and accordingly if it should be classified or not. Other criteria are: i) *Age*, where the classification should be lowered if the value of the information decreases, ii) *Useful Life*, where the information should be declassified if it is considered obsolete and iii) *Personal Association*, where information that involves individuals or is protected by law should be classified [5].

A research from the SANS Institute [19] proposes a six-step approach to data classification in order to implement a valid classification system. The steps are: 1) Identify the data resources that need to be protected, 2) Identify data protection measures, 3) Identify data classes, 4) Map data measures to data classes, 5) Classify data and 6) Repeat as needed. By executing step 1 the organization will be in a position to have a holistic view about its resources, such as data location, data owners, data custodians etc. At the second step, depending on the organization's goals, the desired data protection measures such as authentication, encryption, intrusion detection etc. will be chosen. Also at the next step, the labels of the classes such as public, private etc. will be chosen. The fourth step indicates the mapping of steps 2 and 3. At the fifth step data classification is performed and, if the categorization is not possible for all data, the execution of the sixth step is proposed. Table 7 presents the aforementioned steps together with a brief description of each step.

Table 7: SANS Institute six-step approach to data classification [19]

Steps	Description
Step 1: Identify the data resources that need to be protected	Data resources may be derived from surveys, questionnaires and reports.

Steps	Description
Step 2: Identify data protection measures	Data protection measures may be derived from the goals and security policies of the organization, data administrators or regulatory laws.
Step 3: Identify data classes	The most common data classes are labeled as Public, Private and Confidential. Other main classes are Confidentiality, Integrity, and Availability.
Step 4: Map data protection measures to data classes	Assign the identified data protection measures with the classes that have been chosen.
Step 5: Classify data	The classification labels and the measures are applied to resources.
Step 6: Repeat as needed	If the classification fails to accommodate all sources then the iteration of steps is recommended.

3.2.2 Right management-Assign rights

Assign of rights is a process where rights are applied to data, in accordance with their classification. The main purpose of assigning rights is to narrow the access to data, resources, such as devices and locations, of individuals or groups that the corresponding rights have been assigned to. Therefore this process can be accomplished by using two technical methods:

1) *Label Security* that adds a label to data so as to protect rows of data, columns of data or both. Hence, when a user tries to access these data, his security label is compared to security label of data, determining whether access is permitted or not. It should be noted that the security labels are determined by the security policies of the organization. Table 8 presents a simple example of Security labeling, indicating that the data in the first row of the table is marked as sensitive.

Table 8: Simple example of Security Labeling

ID	Last Name	First Name	Country	Label
01	Jones	Mary	Greece	Sensitive

2) *Enterprise Digital Rights Management* (*DRM*) that protects sensitive digital data from a potential malicious attack by managing rights to digital data. Thereupon, the main purpose of DRM is to protect the confidentiality of data, to prevent data leaks and thefts, by applying security policies that control the level of access to data by individuals or groups in the organization or by business partners.

Table 9 presents the three service models, SaaS, PaaS and IaaS in relation to data classification and assigned rights during create phase. It is derived that data classification in the SaaS service model is entirely controlled by the cloud provider, however, in some cases SaaS may offer label technologies, but the customer has to come to an agreement with the provider. In a PaaS service model, classification depends on the availability of APIs and the development environments. The customer should contact the PaaS provider in order to implement security controls. In the IaaS service model, classification is supported but depends on the available methods of the cloud provider. For example, if data labels aren't provided, the customer can manually implement them [23].

Table 9: Data classification and Assign rights in Service Models [23]

Service models	Assign rights
Software as a Service (SaaS)	Controlled by cloud provider
Platform as a Service (PaaS)	Depend on the availability of APIs and development environments
Infrastructure as a Service (IaaS)	Depend on the availability of the cloud provider

3.3 Data Security during Store Phase

One of the main advantages of cloud computing is the ability to provide to individuals and to organizations the option to store their data to a cloud environment. However, before adopting a cloud provider, it is essential to comprehend that certain security issues (such as unauthorized data access during transmissions, data losses and legal issues due to different location of jurisdiction) may arise during the transfer of data to a cloud provider or during the transit between cloud providers or other environments. A proposed control to prevent these risks and amplify the confidentiality, integrity and availability of data is Access Management and Data Encryption.

3.3.1 Access Management

Access control is a mechanism that ensures data confidentiality, integrity and availability in cloud environments. The basic concept of access control is the *principle of least privilege*, indicating that a user, in order to perform a task, should be able to have access only to the necessary information and resources in order to prevent data leakage, theft of credentials and encryption keys and privilege escalation. The term "user" implies any individual involved in a cloud environment e.g. cloud customers, cloud employees, system administrators and applications.

The control measures can be divided in three main categories: 1) *Physical controls* that involve the security of the buildings and its equipment (e.g. protection of servers and laptops, building protection), 2) *Logical controls* that involve the protection of the information by restricting access to users (e.g. encryption, access control lists) and 3) *Administrative controls*, containing all the policies and procedures concerning the behavior of the employees towards the sensitive information of the organization (e.g. security awareness program, work habit checks) [28].

The access control models that apply to Logical and Administrative measures are: 1) Mandatory Access Control (Mac), where the access rights are determined by a central authority or policies by using label mechanisms and a set of interfaces. In order to specify the policies of the Mac model, the *Bell-LaPadula Confidentiality* and *Biba Integrity* security models [22] can be used. Table 10 presents those models and the corresponding security rules.

Table 10: Security rules for Mac [22]

Model	Rules	
Bell-LaPadula Model	No read up	No write down
Biba Model	No read down	No write up

Specifically, the Bell-LaPadula confidentiality model defines two rules: i) *Simple security rule*, where a subject cannot read an object with a higher security level, ii) *Property star* (∗-property), where the subject cannot write to an object with a lower security level. The Biba Integrity model defines as well two similar rules: i) The *Simple Integrity Axiom*, where a subject cannot read an object with lower integrity level, ii) The *Star Integrity Axiom* (*), where a subject cannot write to an object with a higher integrity level. At this point, it should be noted that the system administrator is responsible for access permissions and users have no authority to change the access controls (Rule Based Access Control). 2) *Discretionary Access Control* (*DAC*), where, unlike the Mandatory access control, the user (subject) has the authority to specify what objects should be accessible only by him. For that purpose, the use of Access Control Lists determines the privileges of a user to a specific resource. In particular, a matrix, containing rows that represent the subjects and columns that represent the object, can appoint what actions may be performed by a subject to an object.

Table 11: Example of Access Control Lists

	Object	
	File 1	File 2
Subject	User. Mary: rw	Group.*: r; Group.groupA: rx

Table 11 presents an example of Access Control Lists, where the user (Mary) can read and write file 1, whereas regarding file 2 all the groups can read it but especially group A can also execute it.

3) *Non-Discretionary Access Control* (*NDAC*), where the rules are specified at the discretion of the user. A significant advantage of this model is that in an organization

with multiple employees, the control access is based on the position of the employee within the organization. *Separation of Duty* (*SoD*) can assist this kind of access and also protects the confidentiality, integrity and availability of data by preventing conflicts of interest among the employees and by detecting security breaches, information theft and fraud [22].

3.3.2 Data encryption

Data encryption combined with other security controls can incur significant results to data protection and security during storage phase. Since there are many encryption algorithms, they can be classified in two categories for convenience: *Symmetric algorithms* that share the same encryption and decryption key (e.g. Triple data encryption algorithm) and *Asymmetric algorithms*, where the encryption key is different from the decryption key. However, to ensure maximum data security protection, it should be examined what measures should be adopted during data migrating to cloud, data in transit to cloud and between different providers or environments and data within the cloud.

Particularly, data migrations to cloud can be protected not only by using the traditional security methods but also by using *Database Activity Monitoring* (*DAM*) and *File Activity Monitoring (FAM)* [3] [24]. These methods should be used prior to migration to clouds, in order to prevent unauthorized movement of data. Specifically, DAM is able to monitor and audit in real time all the performed activities in database platforms, indicating an unauthorized activity or policy violation. FAM is a similar method with DAM, but focuses mainly on the interaction of users with files [25]. During the migration of organizational data to the cloud, the indicated method is the use of *URL filters* that can prevent unauthorized individuals to connect to cloud and *Data Loss Prevention (DLP)*, contrary to URL filters that are a technology focusing on the content of data rather than its destination. Its main goal is to protect and prevent the unauthorized access of sensitive data, minimizing the intentional or unintentional data leaks [26].

Data in transit to clouds (e.g. movement of data from an organization to a cloud provider and movement of data between cloud providers) can be protected using three- level encryption: 1) *Client/Application Encryption*, where data are encrypted prior to the transmission into the cloud provider, 2) *Link/Network Encryption*, where

encryption techniques, such as Secure socket layer, Transport layer security, Virtual private network, ensure the transmission of data through a secure network. 3) *Proxy-Based Encryption*, where the transmitted data are sent to a proxy thereafter gets encrypted and finally the encrypted data are transmitted to the cloud storage.

Data within the cloud (movement of data within the cloud provider) can be protected using different encryption methods for each service model:

- IaaS Service Model has two storage models: *Object storage* is a file repository that can be accessed via using APIs (e.g. Amazon S3) and *Volume storage* is a virtual hard drive (e.g. Amazon EBS). Table 12 presents the encryption methods that can be applied to the corresponding IaaS storage models. It can be observed that, for both storage models, some of the aforesaid encryption techniques are used. Concerning the encryption methods for Object storage, File/Folder encryption and Enterprise Digital Rights Management (EDRM) uses the traditional encryption techniques or the EDRM in order to encrypt files or folders before the storage. As for the encryption methods in Volume storage, Instance-managed encryption encrypts data at instance using a key that is stored in the volume storage. Externally managed encryption encrypts data at instance but the difference from the instance managed encryption is that the key is created externally upon request.

Table 12: IaaS Encryption

IaaS Encryption	
IaaS storage models	**Encryption methods**
Object Storage	• File/Folder encryption and Enterprise Digital Rights Management • Client/Application encryption • Proxy encryption
Volume Storage	• Instance managed encryption • Externally managed encryption • Proxy encryption

- PaaS service models cover various technologies such as APIs and Database as a service so the encryption methods diversify. Generally, it could be supported that the main encryption methods used by most of the providers are Client/application encryption, where the data can be encrypted in PaaS application, Database encryption where the data is encrypted in the database, Proxy encryption and a variety of other encryption methods such as APIs built into the platform.
- SaaS service model supports mainly application level encryption, but can implement all the aforementioned encryption methods, using keys per customer, in order to enhance multi- tenancy, one of the main characteristics of clouds. Since the encryption is offered and managed by the SaaS provider, the customer should get informed about the methods and encryption keys [3].

In addition, an Open Data Center Alliance research [18] about Data encryption and the levels of confidentiality, integrity and availability suggests that it is crucial to encrypt the transmitted data/application from an organization to a cloud storage, if it has been classified as confidential or strictly confidential, whether these data are in transit, in rest or in use. Furthermore, concerning integrity, they suggest the use of a system integrity check combined with digital certificates and if the integrity is vital for the organization the data encryption should be tamper-proof. Regarding the availability of data during the transit between cloud providers or other environments, the encryption key should be available to the recipient and in general cloud providers should always keep the primary and alternative encryption keys secure.

3.4 Data Security during Use Phase

During this phase, clients are able to interact with data either via direct/abstract access (e.g. Dropbox) or by using cloud applications (web based or client applications). In order to achieve and enhance the confidentiality, integrity and availability of data during this phase, certain controls should be applied. Specifically, the proposed controls during the Use phase are Access management and Logical controls. Some of these controls were introduced during the other two phases, so the focus will now be on the applicability of these controls to this phase. Furthermore, at this point it should be mentioned that controls such as Activity monitoring of databases, applications and

files, even though they aren't cloud specific, they can support the protection of data with proper handling.

Access management, just like during Create and Share phase, plays an important role during the interaction of data by the users. The proposed techniques Assign rights and Access control were presented correspondingly in sections 2.2.1 and 2.2.2. However, during this phase additional rights and controls are enforced, in order to facilitate users to perform supplementary activities, such as copying, printing or modifications of data.

The basic goal of Logical controls is to protect information and computer resources by restricting access to unauthorized users. To that end, Sans Institute [27] signify that logical controls should include Audit trails, smart cards, passwords, antivirus and access control software [30].

Regarding the service models, in SaaS, data security during use phase depends on the availability of security controls that are provided, in PaaS data security depends on the deployment of the provider, while IaaS provides the most flexible environment to enforce various data security controls.

3.5 Data Security on Share Phase

During this phase users have the ability to exchange data among them. This procedure is more complex than the traditional sharing of data, since users exchange data in a cloud environment, where external security controls can't track these data. To that end, the proposed controls are Data encryption and Logical controls, in order to exchange data securely and to ensure confidentiality, availability and integrity of data. Data encryption was discussed in detail in section 2.3.2 and since the exchange of data among different environments is included in this phase (e.g. applications, databases and clouds), the network connection should be encrypted by using standard network protocols. For instance, the IaaS service model uses Virtual private networks, in order to facilitate the exchange of data.

Logical controls were introduced in sections 2.3.1 and 2.4.2 and still apply in this phase. Concerning the service models, data security during Share phase depends on the PaaS provider, for the SaaS model it is encapsulated within the application, whereas IaaS service models use Virtual private networks [28].

3.6 Data Security on Maintain Phase

During Maintain or Archive phase the data that are no longer in use are transferred to long term storage. In other words, this phase deals with data recovery and archiving. The main controls that should be taken into consideration during this phase and in order to facilitate the security of data are Data encryption and Asset management. The main concern of both traditional and non-traditional environments, such as cloud environments, is to track the location of the archived data that are encrypted or the unencrypted sensitive data. Asset management is a tool that can provide this control and ensure the availability of data. Generally, cloud providers can offer this control to their customers, but in the cases where personal handling of archived data is needed, users should themselves implement an asset management.

Data encryption was introduced during Store phase, and particularly when data are in transit, in rest and in use. During this stage, the encrypted data that are no longer in use are moved into archived storage together with the corresponding encryption keys. In case of unencrypted data, the aforementioned encryption techniques may be applied and depend on the devices that data will be archived; database, tape or storage encryption may be used.

With respect to service models, data security during maintain or archive phase depend on the PaaS or SaaS provider, whereas for the IaaS provider data security is similar to traditional archived storage [29].

3.7 Data Security on Destroy Phase

During this stage, data that are no longer in use should be permanently deleted together with the corresponding encryption keys. The controls that are used in the Destroy phase should ensure that deleted data or copies of deleted data are no longer accessible. However, due to complexity of cloud environments, the controls used during this phase can't guarantee that data is unrecoverable, but they can assure to mitigate the risk of retrieval. Thus, the main controls that are used during Destroy are *Crypto-shredding, Secure deletion* and *Content Discovery*. Crypto-shredding is a technique that ensures the permanent destruction not only of data but also the destruction of the associated encryption keys regardless of the physical location.

Regarding Secure deletion, two proposed methods are the *Disk/Free Space Wiping*, where proper software and hardware ensures the deletion on hard disks or any other media and the *Physical Destruction* using either Degaussing processes, where data becomes unreadable by applying a reverse magnetizing force on storage devices [31] or Physical destruction of storage devices by grinding and shredding.

Content Discovery is a tool that uses content analysis techniques, in order not only to scan the storages and identify the location of sensitive data, but also to ensure that the destroyed data or copies of them cannot be retrieved. Data loss prevention (DLP) and Content Monitoring and Protection (CMP) are tools that have the ability to scan files and databases.

Concerning the service models during the Destroy phase, in the SaaS model the deletion of data depends entirely on the cloud provider, in the PaaS model the limitations in deletion of data are similar to SaaS and depend on the deployment of the PaaS application, while the IaaS model is more flexible, supporting all three controls and for the virtual machines there is the option to overwrite data [3] [29].

3.8 Risk Assessment of Data Security

The need of accessible data is a critical point in every organization and many resources are invested in protecting the confidentiality, availability and integrity of data. Therefore, before moving their data to a cloud provider, organizations should take into consideration and assess their risk tolerance by implementing a risk assessment approach, avoiding that way the exposure of vital data to potential threats. To that end, over the last years, many risk assessment methodologies were proposed, without focusing primarily on information assets. The *Octave Allegro* approach, though, takes into account not only information assets, but also examines how this information is used, stored and processed and what are the threats and vulnerabilities that may occur.

Figure 24 [32] depicts the eight steps that should be implemented during four stages.

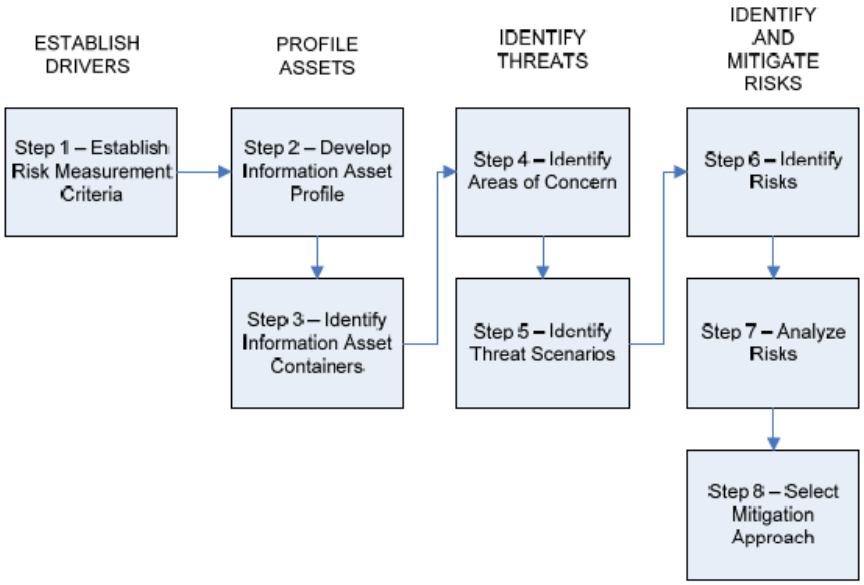

Figure 24: Octave Allegro Steps [32]

First stage, Establish Drivers, contains Step 1, where the Risk Measurement Criteria are established. Second stage, Profile Assets, contains two steps, where in Step 2 the Information Asset Profile is developed and in Step 3 the Information Asset Containers are identified. Third stage, Identify threats, contains two steps, where in Step 4 and Step 5 various Areas of concern and Threat Scenarios are identified, respectively. The last stage, Identify and Mitigate Risks, contains 3 steps, where in Step 6 and Step 7 the Risk are identified and analyzed and in Step 8 the appropriate Mitigation approach is selected. The analytical presentation of the aforementioned areas will follow.

- *Establish Drivers*

This term implies the designation of the organization's drivers (e.g. goals, success factors) that will be used, in order to estimate the outcome of a potential risk to the organization. The risk measurement criteria that will be established should reflect the areas that the organization considers as significant. For instance, those criteria can be financial, legal, productivity issues etc. Table 13 presents an indicative example of risk measurement criteria for legal penalties. Specifically, the impact area is Lawsuits and, depending on the values that will be given from the organization, it can be Low, Moderate or High.

Table 13: Allegros Risk Measurement Criteria Worksheet [32]

Risk Measurement Criteria for Legal Penalties			
Impact Area	**Low**	**Moderate**	**High**
Lawsuits	Fines less than _____€	Fines between _____€ and _____€	Fines greater than _____€

Afterwards, the impact areas should be prioritized by ranking from the most important to the less important. Table 14 presents an example of the execution of Step 2. The Priority column should be filled indicating how important the impact area to the organization is. For example, if Legal Penalties is considered the first priority in the organization, it should be marked by 3 since there are only 3 impact areas. This prioritization will be used then to calculate the relative risk score.

Table 14: Allegro's Impact Area Prioritization Worksheet [32]

IMPACT AREA PRIORITIZATION	
Priority	**Impact area**
2	Financial
1	Productivity
3	Legal Penalties
N/A	User defined

- *Profile Assets*

During this stage the information assets, either in physical (e.g. CDs, papers) or electronic forms (e.g. files, databases) of the organization are defined. In order to implement a successful risk assessment, the profile of assets should contain only information that is critical to the organization and will later assist in identifying threats and vulnerabilities. An information asset should be considered critical if the disclosure, modification, loss or destruction of information will have a severe impact to the organization. Specifically, the critical information asset profile should contain six areas that should be filled: 1) *Critical Asset*, where the asset is defined, 2) *Rationale for Selection*, where the reason for selecting this asset is described, 3)

Description, where the critical information is described analytically, 4) *Owner*(*s*), where the owner(s) of the specific information asset is defined, 5) *Security Requirement*, where the security requirements, such as confidentiality, integrity and availability, are assigned to the information assets and 6) *Most Important Security Requirement*, where the most important security requirement is selected for the specific information asset. The next step is to identify information asset containers, namely identifying the place where the information asset is stored, transported or processed (e.g. hardware, software, servers, network, people or physical objects such as piece of paper). By mapping the information assets with the containers, the boundaries of the examined risks will be defined.

- *Identify threats*

During Step 4, concerns that may threaten the organization's information asset should be identified. However, since the areas of concern may vary, the security requirements for information assets specified in the previous step should be taken into consideration, in order to mitigate the list. Subsequently, during Step 5 the areas of concern are expanded into threat scenarios. A threat scenario consists of an actor, a motive, an access mean and an outcome and can be represented as a threat tree. For instance, an employee (actor) accidently (motive) deletes a file leading to loss of information (outcome).

Figure 25 presents an example of threat tree, where an actor accidental or deliberate violates the security requirements leading to disclosure, modification, interruption and destruction or loss of information asset.

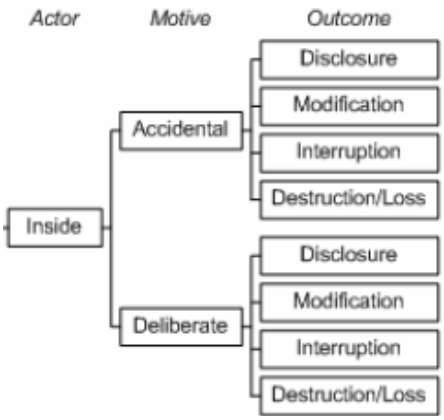

Figure 25: Graphical representation of threat trees [32]

Furthermore, during this phase it is recommended to use probabilities to each identified threat scenario, in order to help the risk mitigation prioritization during the next steps. Since data/information can't be measured, the use of qualitatively probability is suggested, such as "High" if the scenario could occur, "Neutral" if the scenario may occur and "Low" if the scenario is unlikely to occur.

- *Identify and Mitigate Risks*

During Step 6, the identification of risk is implemented. Specifically, the impact of the occurrence of the aforesaid scenarios is examined. For instance, if an employee accidently accesses another employee's medical record, the organization (threat scenario) will face legal issues, such as lawsuits and a resulting fine of 50.000 € (impact). A simple risk equation indicates that if the impact is added to the threat then it is possible to identify the risk.

In Step 7, a relative risk score is performed by assigning values such as "High", "Medium" or "Low" to the impact areas of the threat scenario.

Table 15: Indicative example of assign values to impact areas

Impact Area	**Impact Value**
Financial	Average
Productivity	Low
Legal Penalties	High

Table 15 presents the Impact areas together with the corresponding Impact values. At this point, it should be noted that for Legal Penalties the Impact Value was assigned as High because a threshold of 20.000 € as an upper limit was assumed (see Table 13).

Finally, the relative score is computed by multiplying the Ranking of each Impact area with the Impact Value. Table 16 presents the aforesaid procedure and it should be noted that since the Impact Values are in qualitative form, quantitative values are assigned (High-3, Average-2 and Low-1).

Table 16: Indicative example of computing the relative score [32]

Impact Area	Ranking	Impact Value	Score
Financial	2	Average (2)	4
Productivity	1	Low (1)	1
Legal Penalties	3	High (3)	9
		Total Score	14

Having computed the relative score, the next step requires the categorization of the risk. During this procedure the collaboration of many departments is needed, in order to have a balanced and cost effective mitigation strategy. The most common categorization method indicates sorting the risks from the highest to lowest and then assigning them to corresponding Pools. For instance Pool 1 will contain the risks with the highest score and Pool 4 will contain the risks with the lowest score.

Table 17: Relative Risk Matrix [32]

Relative Risk Matrix			
Probability	**Risk Score**		
	30 to 45	**16 to 29**	**0 to 15**
High	Pool 1	Pool 2	Pool 2
Medium	Pool 2	Pool 2	Pool 3
Low	Pool 3	Pool 3	Pool 4

Table 17 presents an indicative Risk Matrix and how the risks depending on the range of their relative score are assigned to Pools.

The final step of the risk assessment is to select a mitigation approach. Table 18 presents an indicative mitigation approach for each Pool. However, the final decision for the mitigation approach should be taken by considering the organization's needs.

Table 18: Indicative Mitigation approach [32]

Pool	Mitigation approach
Pool 1	Mitigate

Pool	Mitigation approach
Pool 2	Mitigate or Defer
Pool 3	Defer or Accept
Pool 4	Accept

3.9 Summary

This chapter has examined ways to achieve the optimal data protection in cloud environments. Even though traditional data security can cover many aspects of this technology, new security strategies should be adopted. To that end, it is recommended that organizations should closely examine all stages of the data lifecycle and apply specific security measures. Specifically, the measures that should be adopted are classification of data and assignment of rights or permissions in the Create phase, encryption of data and access management in the Store Phase, data encryption and logical controls in the Share phase, access management and logical controls in the Use phase, data encryption and asset management in the Maintain phase and Crypto-shredding, Secure deletion and Content Discovery in the Destroy phase.

Moreover, it is suggested that, before moving their data to a cloud provider, organizations should assess their risk tolerance by implementing a risk assessment policy, avoiding the exposure of vital data to potential threats. Over the last years, many risk assessment methodologies were proposed, unfortunately without focusing primarily on information assets. The Octave Allegro approach, in contrast to other risk assessment methodologies, takes into account not only information assets, but also examines how this information is used, stored and processed and what are the threats and vulnerabilities that may occur. Only when stakeholders understand these issues, can an informed decision be made about which deployment and service models are appropriate for their business in the light of risk tolerance.

4 Choosing a Cloud Provider

Nowadays, choosing the right cloud provider among thousands of really promising providers takes a lot of time, effort and searching. Over the last decade, Software as a Service (SaaS) was the prominent service model, covering a wide range of consumer needs, while Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) gained recognition only recently. According to Forrester Research [33], the global cloud market will raise from a $40.7 billion in 2011 to $241 billion in 2020. Figure 26 [33] illustrates this phenomenon, indicating that from $47.22 billion market size in 2013 SaaS will reach $132.57 billion in 2020, from $4.38 billion market size in 2013 PaaS will reach $11.91 billion in 2020 and from $4.99 billion market size in 2013 IaaS will reach $4.78 billion in 2020. To that end, it is predicted that Software as a Service will conquer the global market, since an increasing number of large, medium and small organizations and businesses have already adopted a SaaS cloud provider or are considering moving their services to a SaaS provider. Concerning the other two service models, their revenue in the global market remains in the same level having a slightly upward trend.

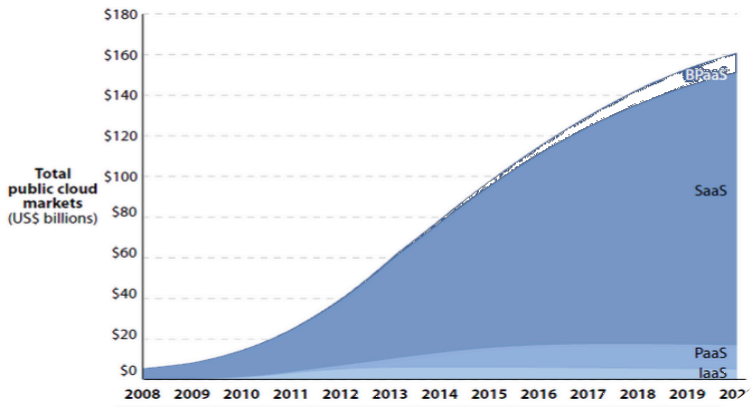

Figure 26: Global Cloud Market Size [33]

Nevertheless, at this point, an attempt is made to meet the special needs of customers with the security risks of cloud computing. Thus, this section focuses on the implementation of a wizard that will assist individuals, organizations and business to

make the proper choice in adopting a cloud provider based not only on their needs but also based on the security issues involved.

4.1 Further Analysis of the Three Service Models

Choosing a suitable service model requires an in-depth analysis and knowledge of the characteristics and flaws, in order to evaluate if the corresponding model can satisfy certain requirements, such as compliance, reliability and security issues. In Chapter 2, the three service models were briefly presented, so further research is necessary in an attempt to detect the similarities and differences of those models. On the above basis, a first attempt is to understand who uses each layer, what services are available and the outcome of using them. Figure 27 depicts the three layers, indicating that SaaS is suitable for end users, who can complete their business tasks via using services such as email, office automation, virtual desktop and social networking.

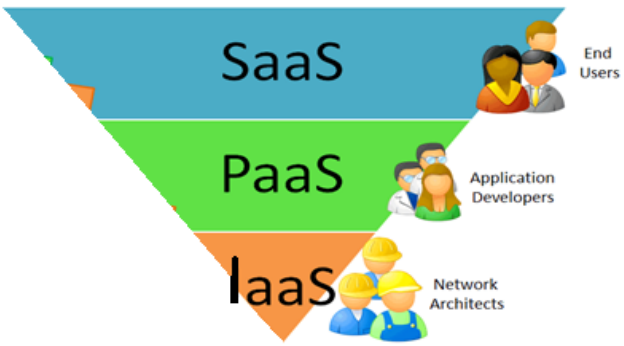

Figure 27: Service models stuck

PaaS is the appropriate service model for application developers, who can create and deploy applications destined for end users by using programming languages and tools that are supported by the provider. IaaS is the appropriate model for network architects and system managers in general, who can create platforms for application testing, development and deployment by using storage, networks and other fundamental computing resources that are supported by the provider. Table 19 presents the general characteristics of each service model as they were analyzed in Section (2.1).

Table 19: General characteristics of service models

Consumers	Available Services	Outcome
End users	Communication (e-mail), Collaboration (e-meeting), Enterprise Resource Planning (ERP), CRM	Complete business or personal tasks
Application developers	Development and Testing, Integration, Application Platform, Databases	Create or deploy applications for end users
System managers	Virtual machines, Cloud management, Storage, Networking	Create platforms

4.1.1 Software as a Service (SaaS)

Generally, SaaS provides all the available applications that are running on a cloud infrastructure and the end user may utilize these services through a web server using a variety of devices. It is worth mentioning that end users may be individuals that use the applications for personal reasons, employees of an organization that are authorized to have access to the organization's software applications and administrator developers in order to configure the developed applications. At this point, it should be noted that the end user manages only specific configuration settings of the used applications, whereas the cloud provider is responsible for everything else. Figure 28 [2] depicts the cloud providers' and subscribers' responsibilities in a traditional software stack, where the cloud provider has total control of the middleware (provides user authentication, identity management etc.), operating system and hardware layer and the cloud provider admin has control of the applications. The cloud subscriber has no control over the last three layers and has limited control in the application level.

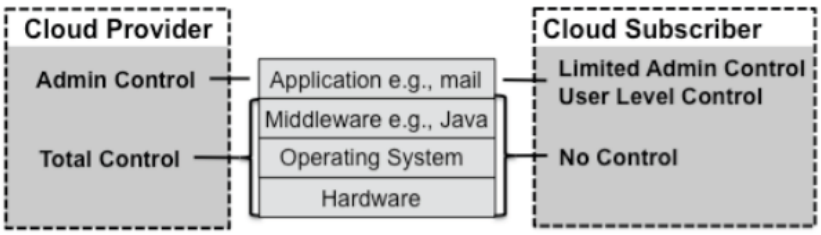

Figure 28: Cloud providers and subscribers responsibilities [2]

Specifically, a user should be able to exchange data over a secure internet connection, in order to exploit the advantages of this model. Hence, the use of cryptography is strongly recommended. This procedure requires the exchange of a shared key between the user's browser and the cloud server, using a standard protocol such as SSL [Net96], in order to achieve the encryption of the communication. When a secure communication is established, the cloud provider and the user can exchange their credentials safely, using mainly an account name and a password.

Furthermore, the functionality of the abovementioned service model isn't the only criterion that should be taken into consideration when choosing a cloud provider. Another aspect that should be examined are the benefits for the consumers and the potential risks that this procedure involves. Towards this direction, the identified benefits that should be examined are five:

1) *Very Modest Software Tool Footprint*: SaaS applications differentiate from the traditional software applications not only because they do not require installation but also because they minimize the risk of misconfiguration due to bare minimum footprints on the user's device.
2) *Efficient Use of Software Licenses*: A single license can accommodate users' needs on multiple devices reducing that way license management and the cost of purchasing additional licenses.
3) *Centralized Management and Data*: An efficient management of data by providing services such as disaster recovery, compliance, and security protection can be achieved by the centralization of data, a service offered by the SaaS model.
4) *Platform Responsibilities Managed by Providers*: As it was examined in detail, a user can exploit the available applications without having to worry about security issues, back-ups, maintenance and operational issues. The provider is responsible for all these tasks.
5) *Savings in Up-front Costs*: By using the SaaS model, a user can utilize the applications for a certain amount that is determined by the corresponding provider, without worrying about up-front costs for the acquisition of equipment.

However, the drawbacks and the various concerns should be examined before adopting a cloud provider. Specifically, a research that was conducted by the National Institute of Standards and Technology [2] detects four main areas of concern:

1) *Browser-based Risks*: The communication between the server's cloud provider and the client's browser is encrypted but certain risks may arise leading to information disclosure (e.g. message traffic or the size of the message can reveal information). In addition, attacks such as man-in-the-middle can lead to hijacking consumer's resources. Compromise of user's data may also be performed from a browser that was contaminated by a malicious web page and afterwards the same browser was used to access SaaS applications.
2) *Network Dependence*: In order to access SaaS applications, a user should be connected to the Internet. Hence, the availability of these applications depends on a consistent and continuously accessible network. However, neither the cloud provider nor the end users are able to guarantee network availability.
3) *Lack of Portability between SaaS Clouds*: Each cloud provider offers specific services to the end users, such as customized user interfaces, application settings, add-ons and data extensions, making the transition from one cloud provider to another a non-trivial task.
4) *Isolation vs. Efficiency (Security vs. Cost Tradeoffs):* Isolation is a key point in SaaS models, since applications simultaneously serve multiple users. In order to achieve the optimum separation of end users and to enhance security, performance and availability, approaches like using separate virtual machines for running applications or separate physical computers are recommended, even though the cost is high. While in the aforesaid approach, users utilize copies of the applications and data are saved in separate databases, a more efficient approach is to reengineer SaaS applications in a way that an application would be in a position to serve multiple users and save the data in a combined database. However this approach may enhance efficiency but involves security risks since malicious actions of a user would degrade the performance of other users.

Table 20 summarizes the aforesaid benefits and concerns that should be taken into consideration when choosing a cloud provider.

Table 20: SaaS Benefits and Concerns [2]

SaaS Benefits and Concerns	
Benefits	**Concerns**
Scalability	Browser-based Risks and Risk Remediation
Accessibility	Performance-Network Dependence
Upgradeability	Integration-Lack of Portability between SaaS Clouds
Resilience	Security risks- Isolation vs. Efficiency
Cost savings	

SaaS applications can deliver their application services to a wide range of areas and are recommended in areas with a reliable network and specific characteristics such as low latency and sufficient bandwidth to serve users' needs. Nevertheless this service model shouldn't be used in certain areas. Mainly, it should be avoided in real time and critical software and in cases where extremely large data should be processed [2] [35].

4.1.2 Platform as a Service (PaaS)

The PaaS service model provides all the available programming languages and tools to facilitate the user for developing or deploying applications destined for end users. While in the SaaS model the user has minimum control over the underlying infrastructure and security, in PaaS the user has control over the deployed applications and the provider is responsible for everything else. Concerning security issues, Hewlett-Packard Development Company [34] states that PaaS provides the optimum security balance concerning the responsibilities of the customers and providers. Figure 29, illustrates providers' and subscribers' responsibilities in a traditional software stack, where the cloud provider has total control over the operating system and hardware, the cloud provider admin shares the responsibilities with the cloud consumer for the middleware layer and the cloud consumer admin has control of the applications.

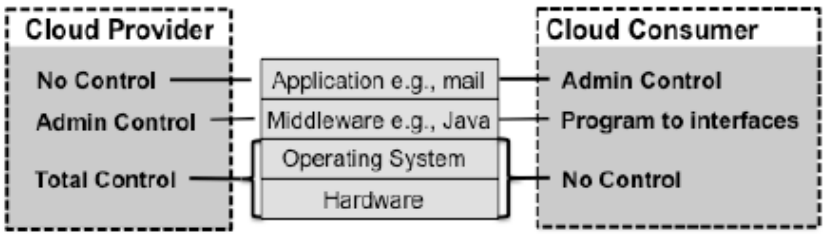

Figure 29: Cloud providers and subscribers responsibilities [2]

Besides the functionality of the specific service model, another aspect that should be examined, are the benefits that could be exploited by the consumers and the potential risks that this procedure involves. Towards this direction, the identified benefits are similar to the SaaS service model (Section 3.1.1) and the various issues and concerns are categorized to those that are similar to SaaS and those that are specific to PaaS. Specifically, a research that was conducted by NIST [2] defines that PaaS's similar issues and concerns with the SaaS model are: 1) Browser-based Risks and Risk Remediation, 2) Network Dependency and 3) Isolation vs. Efficiency, where those that concern specifically PaaS are: 1) Lack of Portability between PaaS Clouds, especially when new applications are deployed, 2) Event-based Processor Scheduling, where the task completion and task arrival events are defined by scheduling and 3) Security Engineering of PaaS Applications, where the use of cryptography is recommended since PaaS applications access the network.

4.1.3 Infrastructure as a Service (IaaS)

In IaaS the user can create platforms for application testing, development and deployment using storage, networks, and other fundamental computing resources that are supported by the provider. The end user manages network, servers, operating systems and storage and the provider is responsible only for the underlying cloud infrastructure. While in PaaS the security is the responsibility of both users and providers, Hewlett-Packard Development Company [34] states that in IaaS the security of the operating system, middleware, and application is the user's responsibility. Figure 30 depicts the cloud providers' and subscribers' responsibilities in a traditional software stack, where the cloud provider has total control of the hardware layer and the administrative control over the hypervisor layer is shared with the cloud consumer's requests in order to create and manage new virtual machines.

The cloud consumer is responsible and has total control over the top three layers, namely the applications, middleware and guest operating systems.

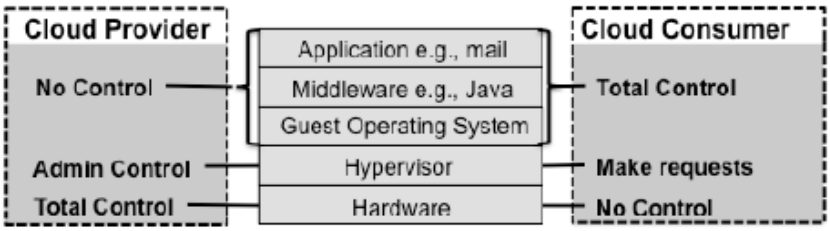

Figure 30: Cloud providers and subscribers responsibilities [2]

Even though IaaS functionality is an important aspect when choosing a service model, another aspect that should be examined are the benefits for the consumers and the potential risks that this approach involves. Towards this direction, the identified benefits are similar to SaaS and PaaS, namely savings in the up-front costs. Particularly, a research that was conducted by NIST [2] defines that, besides the savings in the up-front costs, the end user can exploit full control of the computing resource through administrative access to virtual machines. Furthermore, end users can utilize computing resources such as storage, virtual machines and bandwidth by renting them and via the compatibility and portability that IaaS offers, conventional network applications can also run from IaaS virtual machines.

The various issues and concerns that should be taken into consideration when choosing a service model are categorized to those that are similar to the SaaS and PaaS models and those that are specific to the IaaS model. The similar issues and concerns are: 1) *Browser-based Risks and Risk Remediation* and 2) *Network Dependency*. Those that concern specifically the IaaS model are: 1) *Virtual Machine Sprawl*, where an out of date virtual machine may be compromised 2) *Robustness of VM-level Isolation*, where the isolation of virtual machines should be carefully implemented in order to avoid a malicious attack, 3) *Dynamic Network Configuration for Providing Isolation*, where the proper configuration of the network should protect users from interference between the different networks of other users, 4) *Data Erase Practices*, where data erase policies in shared resources may be time consuming in an environment that users change often and 5) *Verifying Authenticity of an IaaS Cloud*

Provider Web Site, where the end user is responsible to verify the identity of the cloud site, even though cryptography is used to establish a secure connection.

4.2 The Cloud Wizard

Since the global cloud industry has started to mature and became very competitive, an increasing number of organizations and businesses are thinking to migrate their operations to a cloud. However, choosing the proper cloud provider is a difficult process and many aspects should be taken into consideration, given that the market offers a variety of service providers that can cover different needs. Therefore, this cloud wizard can help a stakeholder to make the appropriate decision concerning which service model to choose and consequently which cloud provider best fits his needs.

4.2.1 A general approach of the Cloud Wizard

The wizard was implemented in Java by using NetBeans IDE 7.3.1 and Java Developer Kit (JDK) 7. Concerning the questions used in the wizard, they were derived by examining the characteristics of the service models and the analysis of five cloud providers for each corresponding service model. Specifically, since the stakeholder should take an informed decision when choosing a cloud provider depending on various security and privacy requirements but also on legal, regulatory and operational requirements, the questions focus on three main areas: (1) Security features, (2) Compatible operating systems and languages, (3) Supported services and Cost. Table 22 in Appendix A presents the questions that were used to determine the proper service model, SaaS, PaaS or IaaS, while Table 23, Table 24 and Table 25 in Appendix A presents the questions for the corresponding cloud providers. The parentheses in both cases indicate the respective service models and cloud providers that correspond to each question.

The wizard is divided in two parts. The first part contains six general questions and, depending on the user's answers (at this point the user should be able to choose only one answer among three answers), one of the three models (SaaS, PaaS, IaaS) will be chosen. The second part contains twenty questions for each service model, but depending on the chosen service model of the first part, only the respective question set will be presented to the user. Thus, at the end of the first part, the answers will be

computed and the result will then determine the question set that will be presented to the end-user. For instance if the user has selected more A's, then the service model that best fits his needs is SaaS and the corresponding questions for SaaS cloud providers will be presented. If he selects more B's, it corresponds to the PaaS service model and the corresponding questions for PaaS cloud providers will be presented and, finally, if he selects more C's, it corresponds to the IaaS service model and the corresponding questions for IaaS cloud providers will be presented.

Regarding the cloud providers, the scope of choosing a limited number of providers is to be able to highlight the similarities and differences of each representative of the service models. To that end, having examined the SaaS characteristics and in order to implement the wizard, specific SaaS providers will be examined. A thorough research made by Gartner, Inc [36], indicates the most popular SaaS providers for Sales Force Automation. Figure 31 depicts the most popular SaaS providers by classifying them to Challengers, Leaders, Niche players and Visionaries. It should be noted that since SaaS providers cover a wide area of services, the research will focus only to SaaS providers for customer relationship management (CRM).

Figure 31: Gartner's most popular SaaS providers for Sales Force Automation [36]

To that end, the five SaaS providers that will be examined and analyzed are:

- *Sales Cloud Professional Edition*

Sales Cloud is an application launched from salesforce.com, a global cloud computing enterprise that specializes in customer relationship management products. It was established in 1999 and covers Asia Pacific, America, Europe and Middle East. Their datacenters are certified with SAS 70 II, ISO 2700, SysTrust and EU Safe Harbor. Table 26 in Appendix B presents the main characteristics of Sales Cloud Professional Edition [39] [40].

- *Microsoft Dynamics CRM Online*

Microsoft Dynamics CRM Online is a customer relationship management application that has been launched by Microsoft, the largest software company globally. It was established in 1975 and covers Asia Pacific, America, Europe, Middle East and Africa. Their datacenters are certified with HIPAA, ISO 27001, EU Model Clauses and EU Safe Harbor. Table 27 in Appendix B presents the main characteristics of Microsoft Dynamic CRM Online [41] [42].

- *SugarCRM Professional*

SugarCRM Professional is a customer relationship management application launched by SugarCRM, a relatively young company. It was established in 2004 and covers Asia Pacific, America, Europe. Their datacenters are certified with SAS 70 II and U.S.-EU Safe Harbor. Table 28 in Appendix B presents the main characteristics of SugarCRM Professional [43] [44].

- *Zoho CRM Enterprise Edition*

Zoho CRM Enterprise Edition is a customer relationship management application that has been launched by Zoho, another relatively young company. It was established in 2005 and covers Asia Pacific and North America. Their datacenters are certified with U.S.-EU Safe Harbor. Table 29 in Appendix B presents the main characteristics of Zoho CRM Enterprise Edition [45].

- *NetSuite CRM+*

NetSuite CRM+ is a customer relationship management application that has been launched by NetSuit, an awarded vendor for financial management. It was established in 1998 and covers Asia Pacific, America and Europe. Their datacenters are certified with SAS 70 Type II, PCI-DSS, and EU-US Safe Harbor. Table 30 in Appendix B presents the main characteristics of NetSuite CRM+ [46] [47].

Regarding to PaaS providers, Gartner, Inc evaluation for the best PaaS providers isn't published yet; therefore, in order to choose the providers that will represent this category a thorough research was made. Hence, the criteria for the selection were based taking into consideration Gartners, Inc. classification of providers, i.e. Challengers, Leaders, Niche players and Visionaries.

To that end, the five PaaS providers that will be examined and analyzed are:

- *Google App Engine*

Google App Engine is a platform that has been launched by Google initially in 2008, for developing and hosting applications. Google's datacenters cover North and South America, Asia and Europe and they are certified with SAS70 II, SSAE 16 II, and ISAE 3402 Type II. Table 31 in Appendix C presents Google's App Engine main characteristics [48].

- *Microsoft Windows Azure*

Microsoft Windows Azure is a platform launched by Microsoft in 2010, for developing and hosting applications. Google's datacenters cover North America, Asia, Europe and Oceania and are certified with ISO/IEC 27001:2005, SOC 1 and SOC 2 SSAE 16/ISAE 3402 and HIPPA. Table 32 in Appendix C presents the main characteristics of Microsoft Windows Azure [49] [50].

- *Engine Yard Cloud*

Engine Yard Cloud is a platform for creating and hosting applications that has been launched by Engine Yard in early 2006. Engine Yard datacenters cover North America, Tokyo, Japan, Dublin and Australia and are certified with CISSP, SAS 70 II and ISO 27002:2005.

Table 33 in Appendix C presents the main characteristics of Engine Yard Cloud [51] [52].

- *Force.com*

Force.com is a platform for creating and deploying applications that has been launched by Salesforce and covers Asia Pacific, America, Europe and Middle East. Their datacenters are certified with SAS 70 II, ISO 2700, SysTrust and EU Safe Harbor. Table 34 in Appendix C presents the main characteristics of Force.com [53].

- *AT&T Synaptic*

AT&T Synaptic is a platform for creating and hosting applications that has been launched by AT&T, one of the largest telecommunications companies founded in 1983. AT&T datacenters cover America, Europe and Asia and are certified with ISO 27001, SAS 70, SysTrust, Payment Card Industry (PCI) and Data Security Standard (DSS). Table 35 in Appendix C presents AT&T main characteristics [54] [55].

Furthermore, in order to select the most prominent IaaS providers, Gartner, Inc [37] performed a detailed research that indicates the most popular IaaS providers [95]. Figure 32 illustrates the IaaS Leaders, Challengers, Niche players and Visionaries providers.

Figure 32: Gartner's most popular IaaS providers [37]

To that end, the five IaaS providers that will be examined and analyzed are:

- *Amazon EC2*

Amazon EC2 is the main part of Amazon's cloud computing platform that has been launched by Amazon, one of the largest companies globally in the electronic

commerce, founded in 1983. Amazon datacenters cover North America, Europe and Asia Pacific and they are certified with ISO 27001, SAS 70, SOC 2, SOC 3, HIPAA, Payment Card Industry (PCI) and Data Security Standard (DSS). Table 36 in Appendix D presents the main characteristics of Amazon EC2 [56] [57]

- *Rackspace Cloud*

Rackspace Cloud that delivers infrastructures to businesses of all sizes has been launched by Rackspace Inc, an IT hosting company that was founded in 1998. Rackspace datacenters cover North America, Europe and Asia Pacific and they are certified with ISO 27001, ISO 27002, SAS 70, SOC 2, SOC 3, Safe Harbor, HIPAA, Payment Card Industry (PCI) and Data Security Standard (DSS). Table 37 in Appendix D presents the main characteristics of Rackspace Cloud [58].

- *Verizon Terremark*

Verizon Terremark that offers advanced infrastructure and managed services has been launched by Terremark Worldwide Inc, an IT hosting company that was founded in 1980. Terremark datacenters cover North and South America, Europe and they are certified with ISO 27001, ISO 27002, Payment Card Industry (PCI) and Data Security Standard (DSS). Table 38 in Appendix D presents the main characteristics of Verizon Terremark [59].

- *ThinkGrid Ceano*

ThinkGrid Ceano, that offers advanced infrastructure and managed services, has been launched by ThinkGrid, an IT company that was founded in 2008. ThinkGrid datacenters cover America, Europe and Australia and they are certified with SSAE16, SAS70 or ISO27001. Table 39 in Appendix D presents the characteristics of ThinkGrid Ceano [60] [61].

- *GoGrid*

GoGrid is a “pure” infrastructure-as-a-service provider that was founded in 2008. GoGrid datacenters cover North America and West Europe and they are certified with SAS70 Type II. Table 40 in Appendix D presents the main characteristics of GoGrid [62].

Table 21 presents the summary of the top cloud providers that were presented in this section and are analyzed in Appendix B, Appendix C and Appendix D.

Table 21: Summary of the Top Cloud Providers

Service Provider Type	Cloud Provider Name
SaaS	Sales Cloud Professional Edition Microsoft Dynamics CRM Online SugarCRM Professional Zoho CRM Enterprise Edition NetSuite CRM+
PaaS	Google App Engine Microsoft Windows Azure Engine Yard Force.com 4.3.5 AT & T Synaptic
IaaS	Amazon EC2 Rackspace Verizon Terremark ThinkGrid GoGrid

4.2.2 The Implementation of the Cloud Wizard

As already mentioned, the Cloud Wizard was implemented in Java using NetBeans IDE 7.3.1 and Java Developer Kit (JDK) 7. Java is a powerful language that enables a developer to code pretty much everything by just using the applicable libraries. To that end, the implementation of the wizard was based on the NetBeans platform, where by choosing NetBeans Modules a wizard is created that contains the basic source structure and some default files. It should be noted that the user can select the Registration Type of the wizard (i.e. custom or new file), the Wizard Step Sequence (i.e. static or dynamic) and finally the Number of Wizard Panels. For the specific wizard the "Custom" option has been selected for the Registration Type, for the Wizard Step Sequence "Dynamic" has been selected and the number of panels was set to 68.

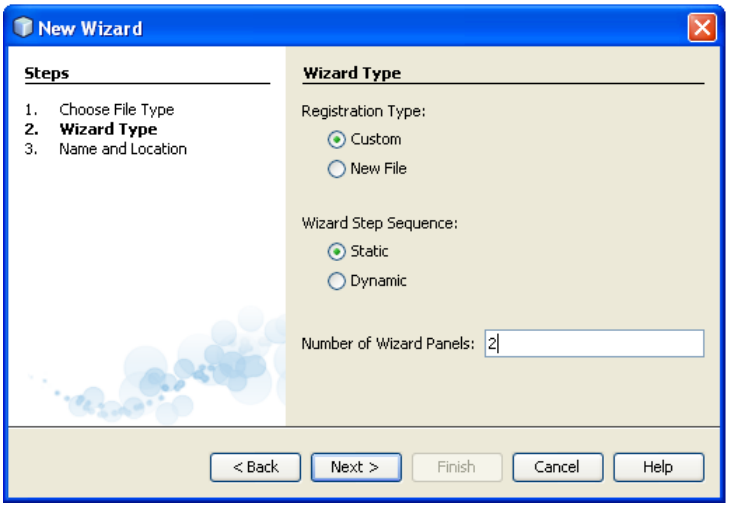

Figure 33: Creating the Wizard

Figure 33 illustrates the fields that should be filled by the user in order to create the general interface and the initial classes of the wizard. Then, by pressing "Next", the user is able to specify the name of the Class and from the drop down list to select the main package. By pressing "Finish" the user would be able to see in the left corner under the tab "Projects" the created project as shown in Figure 34.

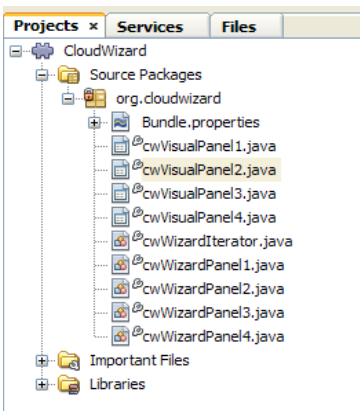

Figure 34: Wizard Project

During the next step the user should design the interfaces for each panel. As depicted in Figure 34, for each created panel there is a Visual Panel that corresponds to a graphical user interface (GUI) and a Wizard Panel that plays basically the role of the controller, in order to process users' data e.g. retrieve data. The design of the interfaces is taking place in the Visual Panels. Concerning the definition of each of

the panel controllers, the getComponent method had to be specified, in order to return the corresponding graphical user interface that the controller should work with. Figure 35 depicts the way that each panel controller should be by default.

```
@Override
public questionsVisualPanel3 getComponent() {
    if (component == null) {
        component = new questionsVisualPanel3();
    }
    return component;
}
```

Figure 35: Define the panel controllers

Furthermore, when creating the infrastructure of the wizard, a class that is being created by default is the Iterator. This class plays a significant role when implementing a dynamic wizard, since it is responsible for defining the sequence of the panels and the indexing of the selected panel. Even though this class contains by default a simple way of how these panels should be accessed, the redefinition of the default sequence was necessary. Based on the aforementioned approach in Section 4.2.1, when a user completes the first 6 questions, his answers are counted and the corresponding questions of the cloud providers will be presented. To that end the first step was to initialize the panels and determine the initial index and sequence.

To that end, the initial Index and Sequence is illustrated in Figure 36.

```
initialIndex = new String[]{
    steps[0], steps[1], steps[2], steps[3], steps[4],
    steps[5], steps[6], steps[67]
};
initialSequence = new WizardDescriptor.Panel[]{
    allPanels[0], allPanels[1], allPanels[2], allPanels[3], allPanels[4]
    allPanels[5], allPanels[6], allPanels[67]
```

Figure 36: Initial Index and Sequence

However, at this point it is vital to mention that in order to count the answers of the user during the 6 first steps and the proper question set to be presented, a new class by

the name QueryObserver had to be created. Figure 37 depicts the creation of this class and how the answers of the users are counted.

```
public QueryObserver() {
    System.out.println("QueryObserver Created");
    queries = new HashMap<Integer, Integer>();
    ready = false;
}

public static String calculateObserver() {
    String result = "";

    int countSaas = 0;
    int countPaas = 0;
    int countIaas = 0;

    Iterator<Integer> iter = queries.keySet().iterator();

    while (iter.hasNext()) {
        Integer key = iter.next();
        if(queries.get(key) == 1) {
            countSaas++;
        } else if(queries.get(key) == 2) {
            countPaas++;
        } else if(queries.get(key) == 3) {
            countIaas++;
```

Figure 37: QueryObserver

Figure 38 depicts, based on the previous count, the question set that will be presented to user.

```
if((countSaas > countPaas) && (countSaas > countIaas)) {
    result = "saas";
} else if((countIaas > countSaas) && (countIaas > countPaas)) {
    result = "iaas";
} else if((countPaas > countSaas) && (countPaas > countIaas)) {
    result = "paas";
```

Figure 38: Define the Question Sets

During the next steps, the definition of the Indexing and the Sequence of the 3 different question sets (SaaS, PaaS, IaaS) should be determined. For instance, for the SaaS question set, the panels that should be accessed are the initial 6 and the last one (Summary) together with the specific SaaS questions from question 7 to 26. Figure 39 depicts SaaS Indexing and Sequence.

```
saasIndex = new String[]{
    steps[0], steps[1], steps[2], steps[3], steps[4],
    steps[5], steps[6], steps[7], steps[8], steps[9],
    steps[10], steps[11], steps[12], steps[13], steps[14],
    steps[15], steps[16], steps[17], steps[18], steps[19],
    steps[20], steps[21], steps[22], steps[23], steps[24],
    steps[25], steps[26], steps[67]
};
saasSequence = new WizardDescriptor.Panel[]{
    allPanels[0], allPanels[1], allPanels[2], allPanels[3], allPanels[4],
    allPanels[5], allPanels[6], allPanels[7], allPanels[8], allPanels[9],
    allPanels[10], allPanels[11], allPanels[12], allPanels[13], allPanels[14],
    allPanels[15], allPanels[16], allPanels[17], allPanels[18], allPanels[19],
    allPanels[20], allPanels[21], allPanels[22], allPanels[23], allPanels[24],
    allPanels[25], allPanels[26], allPanels[67]
```

Figure 39: SaaS Index and Sequence

Figure 40 presents the Indexing and Sequence of the PaaS questions.

```
paasIndex = new String[]{
    steps[0], steps[1], steps[2], steps[3], steps[4],
    steps[5], steps[6], steps[27], steps[28], steps[29],
    steps[30], steps[31], steps[32], steps[33], steps[34],
    steps[35], steps[36], steps[37], steps[38], steps[39],
    steps[40], steps[41], steps[42], steps[43], steps[44],
    steps[45], steps[46], steps[67]
};
paasSequence = new WizardDescriptor.Panel[]{
    allPanels[0], allPanels[1], allPanels[2], allPanels[3], allPanels[4],
    allPanels[5], allPanels[6], allPanels[27], allPanels[28], allPanels[29],
    allPanels[30], allPanels[31], allPanels[32], allPanels[33], allPanels[34],
    allPanels[35], allPanels[36], allPanels[37], allPanels[38], allPanels[39],
    allPanels[40], allPanels[41], allPanels[42], allPanels[43], allPanels[44],
    allPanels[45], allPanels[46], allPanels[67]
```

Figure 40: PaaS Index and Sequence

While, Figure 41 depicts the IaaS Indexing and Sequence.

```
iaasIndex = new String[]{
    steps[0], steps[1], steps[2], steps[3], steps[4],
    steps[5], steps[6], steps[47], steps[48], steps[49],
    steps[50], steps[51], steps[52], steps[53], steps[54],
    steps[55], steps[56], steps[57], steps[58], steps[59],
    steps[60], steps[61], steps[62], steps[63], steps[64],
    steps[65], steps[66], steps[67]
};
iaasSequence = new WizardDescriptor.Panel[]{
    allPanels[0], allPanels[1], allPanels[2], allPanels[3], allPanels[4],
    allPanels[5], allPanels[6], allPanels[47], allPanels[48], allPanels[49],
    allPanels[50], allPanels[51], allPanels[52], allPanels[53], allPanels[54],
    allPanels[55], allPanels[56], allPanels[57], allPanels[58], allPanels[59],
    allPanels[60], allPanels[61], allPanels[62], allPanels[63], allPanels[64],
    allPanels[65], allPanels[66], allPanels[67]
```

Figure 41: IaaS Index and Senquence

During the previous steps, the definition of the Indexing and Sequence were made; at this stage, the sequence of the corresponding question sets is defined. Figure 42 depicts the definition of the setSequence.

```
private void setSequence(String sequence) {
    String[] contentData;

    if (sequence.equals("saas")) {
        currentPanels = saasSequence;
        contentData = saasIndex;
    } else if (sequence.equals("paas")) {
        currentPanels = paasSequence;
        contentData = paasIndex;
    } else {
        currentPanels = iaasSequence;
        contentData = iaasIndex;
    }

    wizardDesc.putProperty(WizardDescriptor.PROP_CONTENT_DATA, contentData);
```

Figure 42: Define setSequence

While in Figure 43 it is defined how the next panel should be accessed. It should be noted that the WizardDescriptor.PROP_CONTENT_DATA and the WizardDescriptor.PROP_CONTENT_SELECTED_INDEX are properties of the wizard API.

```
@Override
public void nextPanel() {
    if (!hasNext()) {
        throw new NoSuchElementException();
    }
    if (index == 6) {

        setSequence(QueryObserver.calculateObserver());


    }
    index++;
    wizardDesc.putProperty(WizardDescriptor.PROP_CONTENT_SELECTED_INDEX, index);
}
```

Figure 43: Define nextPanel

The final step contains the creation of an action, by using the New Action Wizard, which will be used in order to start the wizard. Throughout the steps of the New Action Wizard, the user should choose as an Action Type the field Always Enabled, in the GUI Registration step, as a position from the drop down list the field HERE-New Project… should be chosen and, finally, during the last step the user should specify the name of the class. Figure 44 depicts the steps that should be followed so as to create an action to start the wizard.

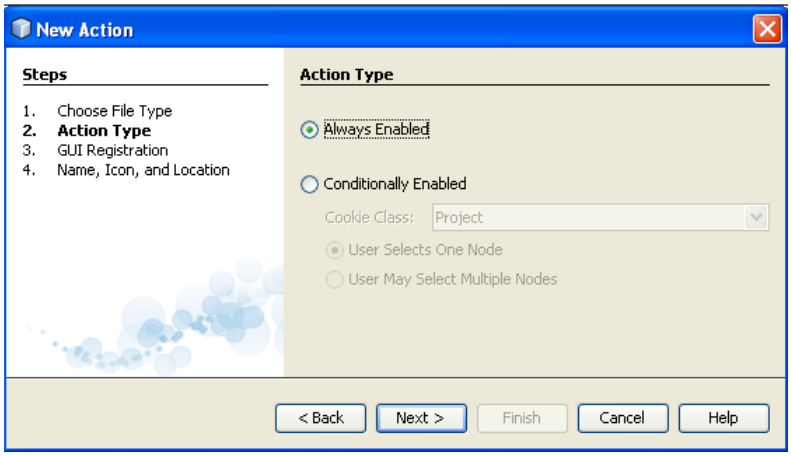

Figure 44: New Action Wizard

Specifically, when the created Action is invoked, the wizard should start and the user should be able to use it. Figure 45 depicts how the wizard is invoked

```
questionsWizardIterator iterator = new questionsWizardIterator();
WizardDescriptor wizardDescriptor = new WizardDescriptor(iterator);
iterator.initialize(wizardDescriptor);

wizardDescriptor.setTitleFormat(new MessageFormat("{0} ({1})"));
wizardDescriptor.setTitle("Cloud Wizard");

Dialog dialog = DialogDisplayer.getDefault().createDialog(wizardDescriptor);
dialog.setVisible(true);
dialog.toFront();

boolean cancelled = wizardDescriptor.getValue() != WizardDescriptor.FINISH_OPTION;

if (!cancelled) {
    System.out.println("CANCELLED");
```

Figure 45: Invoke the wizard

After running the application (via Run→Run Project or by just pressing F6), a new window will appear and by pressing Tools→Open Question Wizard the Cloud Wizard will be ready for use. Figure 46 depicts the Cloud Wizard Interface. At the left side of the window the user can observe the various steps of the wizard, while at the center of the window a series of questions should be filled. It should be noted that, since the wizard is dynamic, a user should be able to review previous answers by pressing "Back" or skip questions by pressing "Next".

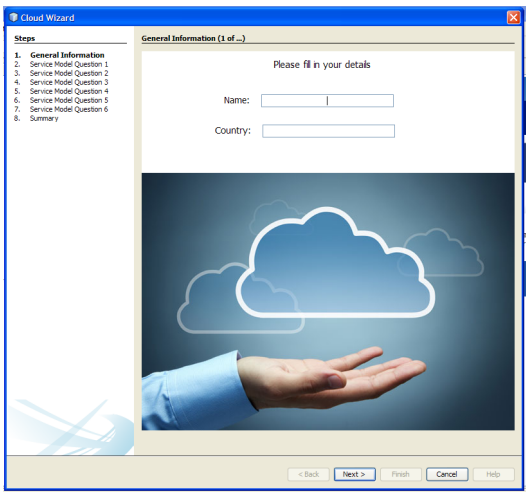

Figure 46: Cloud Wizard Interface

Figure 47 depicts SaaS questions after having completerd the 7 steps.

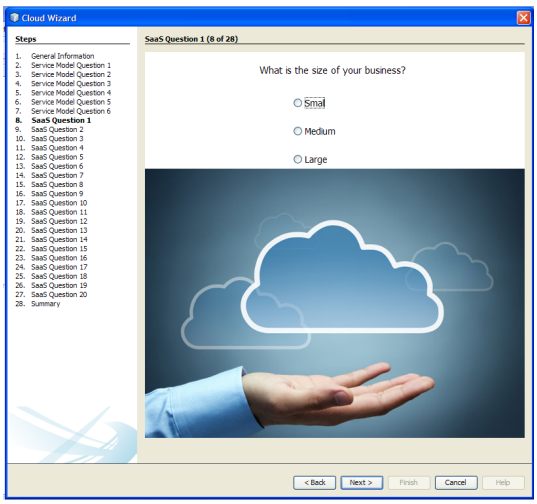

Figure 47: Clouds Wizard SaaS Questions

Figure 48 illustrates the end of the cloud wizard, where the user is informed regarding the appropriate cloud provider, based on his answers.

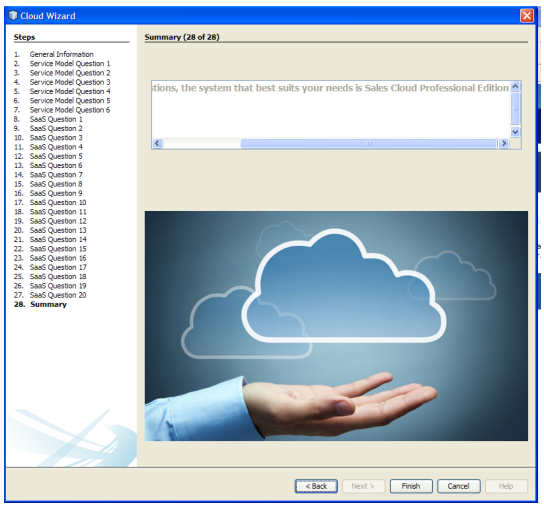

Figure 48: End of Cloud Wizard

4.3 Summary

This chapter focused on the implementation of a wizard that will assist individuals, organizations and businesses to make the proper choice in adopting a cloud provider, based not only on their needs but also on various security, privacy, legal, regulatory and operational requirements. Initially, an in depth analysis was made for the three service models in an attempt to detect the similarities and differences of those models. Then, the characteristics of the various cloud providers that were used in the wizard were analyzed and, finally, a description of the Java implementation was presented.

5 Conclusions

Since the creation of the first mainframes till the adoption of a cloud, significant technological developments have occurred that changed the information technology sector and marketplace. During all these years, the aim has been to provide to multiple users the ability to share computer resources, via common infrastructures and applications. Even though this concept originated around the 60's, only in 1999 did Salesforce.com manage to deliver applications via Internet to the end users. One year later, Amazon launched Amazon Mechanical Turk, a cloud suite that was able to provide not only software applications but also storage and computation facilities. Nowadays, since the computing landscape has changed radically, IT researchers believe that in the near feature everything will be, by some means, connected to a cloud.

However, although there is so much talking going on about this newborn technology, there are still some issues that are ambiguous, making many individuals skeptical about adopting a cloud provider. Therefore, throughout this study, an attempt was made to analyze what cloud computing is and how it works. Thus, having examined scientific papers and reports, it could be said in simple terms that cloud computing is the technology that delivers computer resources at the user's discretion via the Internet, such as storage, servers, networking and applications. Individuals or organizations and businesses can choose among three types of service models. Software as a Service (SaaS) is the appropriate model for those who wish to utilize, through a browser, applications that are running on a cloud infrastructure using a variety of devices. Platform as a service (PaaS) is the appropriate model for those who want to develop or deploy applications destined for end users, by utilizing the available programming languages and tools on a cloud infrastructure. Infrastructure as a Service (IaaS) is the appropriate model for those who want to rent computer resources (e.g. hardware, networking, and storage) instead of buying them.

In addition, it has been defined that for these three service models there are also several deployment models. The term "deployment model" implies the location of the physical servers as well as who carries the responsibility of those servers. Hence, the three main deployment models that were examined are Public, Private and Hybrid

clouds. In Public clouds the resources are owned by a third party and can be accessed by the public. Even though this model can reduce the upfront costs, data control and management is an aspect that should be taken into consideration. Private cloud is the model where the resources are owned by an organization and can be accessed only by the members of the organization. Data control and management in this case is subject to internal security measures in contrast to Public clouds. Hybrid cloud is the model that combines Public with Private clouds, enabling migration between them and offering the advantage of Public cloud for low cost and the protection of data in Private clouds.

Consequently, it can be derived that, similarly to any traditional information system, the Public, Private and Hybrid models face many security risks and threats. Some of these risks are inherited from conventional IT computing, while the rest are explicitly related to the models. Specifically, it has been addressed that Policy and Organizational Risks (such as Lock-in, Loss of governance, Compliance risks), Technical Risks (Isolation failure, Cloud provider malicious insider, Insecure or incomplete data deletion) and Legal Risks (Risk from changes of jurisdiction, Data protection risks and Licensing risks) may compromise the confidentiality, integrity and availability of the system.

Particularly, it has been addressed that Data protection is a major area of concern when adopting a cloud provider. Traditional data security can cover many aspects of this technology, however, due to multi-tenancy, elasticity and the architecture of clouds, new security strategies should be adopted. Hence, in order to achieve the optimal data protection, organizations have to closely examine all stages of the data lifecycle and how data are accessed and processed by applications and individuals alike. During all stages of the data lifecycle, specific security measures should be applied. For instance, the following are proposed: classification of data and assignment of rights or permissions in the Create phase, encryption of data and access management in the Store Phase, data encryption and logical controls in the Share phase, access management and logical controls in the Use phase, data encryption and asset management in the Maintain phase and Crypto-shredding, Secure deletion and Content Discovery in the Destroy phase.

Moreover, the need for accessible data has led organizations to make significant capital investments, in order to protect the confidentiality, availability and integrity of

the data. Thus it is suggested that, before moving their data to a cloud provider, organizations should assess their risk tolerance by implementing a risk assessment methodology, avoiding the exposure of vital data to potential threats. Over the last years, many risk assessment methodologies were proposed, unfortunately without focusing primarily on information assets. Since this is the era of Big Data and information is vital to organizations and businesses, the primary goal is to protect data, especially its sensitive subsets. The Octave Allegro approach, in contrast to other risk assessment methodologies, takes into account not only information assets, but also examines how this information is used, stored and processed and what are the threats and vulnerabilities that may occur. Only when stakeholders understand these issues, can an informed decision be made about which deployment and service models are appropriate for their business in the light of risk tolerance.

Accordingly, choosing a suitable cloud requires a depth analysis and knowledge of the characteristics and the flaws and, also given that the cloud market can offer a variety of service providers that can cover different needs, choosing the proper cloud provider is a difficult process and many aspects should be taken into consideration. To that end, a cloud wizard was implemented, in order to assist a stakeholder to take the proper decision concerning which service model to choose and consequently which cloud provider best fits his needs, depending on various security and privacy requirements but also on legal, regulatory and operational requirements. Both coarse-grained and fine-grained decision making approaches were used, since at the first stage it has to be determined in general which service model best fits stakeholders' needs and at the second stage a more detailed approach was needed with the intention of determining the specific cloud provider.

5.1 Future Work

Although the implementation of the Cloud wizard was successful in addressing the appropriate cloud provider to the end user, further investigation and research could be made. Initially the wizard could be expanded by including a wider variety of cloud providers, giving this way the opportunity to the stakeholders to consider more sophisticated cloud providers based on their specific business needs. Likewise, more questions could be added in the wizard concerning the Confidentiality, Integrity and Availability of each cloud provider. These questions will determine the Service Level

Agreement of each cloud provider and will establish a more thorough approach in demonstrating the appropriate cloud provider. Finally, a web-based version of this Cloud Wizard would definitely make it further approachable to interested end-users.

5.2 Final Remarks

Concluding, it could be said that Cloud computing indeed is a technological area that stills grows and nobody in the next few years can accurately predict how this trend will change the way we do business. Nevertheless, whatever the future might bring and besides cloud differences in functionality and complexity, nobody can deny the major impact in information technology, in industry and mainly in our everyday life.

Bibliography

[1] P. Mell and T. Grance, *The NIST Definition of Cloud Computing,* Vols. 800-145, National Institute of Standards and Technology, 2011.

[2] L. Badger, T. Grance, R. Patt and J. Voas, *Cloud Computing Synopsis and Recommendations,* Vols. 800-146, National Institute of Standards and Technology, 2012.

[3] C. Hoff and R. Mogull, *Security Guidance for Critical Areas of Focus in Cloud Computing,* vol. 3, Cloud Security Alliance, 2011.

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

[5] R. Krutz and R. Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley Publishing, Inc., 2010.

[6] D. Catteddu and G. Hogben, "Cloud Computing: Benefits, risks and recommendations for information security," European Network and Information Security Agency, 2009.

[7] C. T. T. W. Group, "The Notorious Nine Cloud Computing Top Threats in 2013," Cloud Security Alliance , 2013.

[8] S. Ramgovind, M. Eloff and E. Smith, "The management of security in Cloud computing," in *Information Security for South Africa (ISSA)*, 2010.

[9] M. Sutton and D. Hubbard, *Top Threats to Cloud Computing,* vol. 1, Cloud Security Alliance, 2010.

[10] M. Mircea, "Addressing Data Security in the Cloud," *World Academy of Science, Engineering and Technology,* vol. 66, 2012.

[11] R. Katz, A. Konwinski and D. Patterson, "Above the Clouds: A Berkeley View of Cloud Computing," Berkeley, 2009.

[12] W. Claycomb and A. Nicol, "Insider Threats to Cloud Computing: Directions for New Research Challenges," in *Computer Software and Applications Conference*

(COMPSAC), 2012 IEEE 36th Annual, 2012.

[13] A. Araiza, "Electronic Discovery in the Cloud," Duke Law & Technology Review, 2011.

[14] D. Dowling, "International Data Protectionand Privacy Law," in *International Corporate Practice*, Practising Law Institute, 2012.

[15] W. Party, "ARTICLE 29 DATA PROTECTION," European Commission, 2012.

[16] J. Salido and P. Voon, "A Guide to Data Governance for Privacy, Confidentiality, and Compliance," *ISACA,* vol. 6, 2010.

[17] R. Mogull, "Data Security Lifecycle 2.0," Securosis, 2011.

[18] A. Caballero, A. Shvartz, B. Li, C. Gévaudan, I. Lamont, M. Mahabhaleshwar and T. Hirschmann, "Data Security Framework Rev 1.0," Open Data Center Alliance,, 2013.

[19] S. Fowler, "Information Classification - Who, Why and How," SANS Institute, 2003.

[20] E. Simmons and J. Sedayao, "Compute Infrastructure as a Service REV 1.0," Open Data Center Alliance, 2012.

[21] O. D. C. A. Usage, "Provider Assurance Rev. 1.1," Open Data Center Alliance, 2012.

[22] V. C. Hu, D. F. Ferraiolo and R. Kuhn, "Assessment of Access Control Systems," National Institute of Standards and Technology Interagency, 2006.

[23] R. Mogull, "Cloud Data Security Cycle: Create (Rough Cut)," Securosis, 2009.

[24] R. Mogull, "Understanding and Selecting a Database Activity Monitoring Solution," SANS Institute, 2011.

[25] R. Mogull, "Understanding and Selecting a File Activity Monitoring Solution," Securosis, 2011.

[26] P. Kanagasingham, "Data Loss Prevention," SANS Institute, 2008.

[27] O. Nilsen, "Protection of Information Assets," SANS Institute, 2002.

[28] R. Mogull, "Cloud Data Security: Share (Rough Cut)," Securosis, 2009.

[29] R. Mogull, "Cloud Data Security: Archive and Delete (Rough Cut)," Securosis, 2009.

[30] R. Mogull, "Cloud Data Security: Use (Rough Cut)," Securosis, 2009.

[31] N. S. Agency, "Evaluated Products List - Degausser," Department of defence USA, 2012.

[32] R. A. Caralli, J. F. Stevens, L. R. Young and W. R. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," CERT, 2007.

[33] S. Ried and H. Kisker, "Sizing The Cloud-Understanding And Quantifying The Future Of Cloud Computing," Forrester, 2011.

[34] R. Los, "Is PaaS the optimal cloud service model option for security?," Hewlett-Packard Development Company, 2012.

[35] B. Kepes, "Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS," Rackspace Company, 2013.

[36] R. P. Desisto and P. Stakenas, "Magic Quadrant for Sales Force Automation," Gartner, Inc. , 2013.

[37] L. Leong, D. Toombs, B. Gill, G. Petri and T. Haynes, "Magic Quadrant for Cloud Infrastructure as a Service," Gartner, Inc., 2013.

[38] J. Voas and J. Zhang, "Cloud Computing: New Wine or Just a New Bottle?," *IEEE Internet Computing,* Vols. 1520-9202 /9, 2009.

[39] force.com, "Secure, private, and trustworthy:enterprise cloud computing with Force.com," Salesforce, 2010.

[40] Salesforce, "Sales Cloud Overview," [Online]. Available: http://www.salesforce.com/sales-cloud/overview/.

[41] "Microsoft Dynamics CRM," 2013. [Online]. Available: http://www.microsoft.com/en-xm/dynamics/crm.aspx.

[42] "Microsoft Dynamics CRM Online security and service continuity guide," Microsoft, 2013.

[43] "Sugar Professional CRM," Sugar, 2013. [Online]. Available:

https://store.sugarcrm.com/product/professional.

[44] "Sugar Crm Edition Comparison," SugarCrm, 2013.

[45] "Understanding Zoho CRM," Zoho CRM, 2013.

[46] "NetSuite CRM+ A Powerful CRM That Drives The Complete Customer Lifecycle," Netsuite, 2011.

[47] "NetSuite ERP The World's #1 Cloud ERP Solution," NetSuite, 2011.

[48] "Overview of App Engine Features," Google Developers, 2013.

[49] "Technical Overview of the Security Features in the Windows Azure Platform," Microsoft, 2013.

[50] "Windows Azure Trust Center," Microsoft, 2013.

[51] "Security Practices -Engine Yard Cloud," Engine Yard, 2013.

[52] "Engine Yard- Product Datasheet," Engine Yard, 2013.

[53] S. Bobrowski, "Protecting Your Data in the Cloud," Salesforce, 2013.

[54] "AT&T Synaptic Compute as a Service," AT&T, 2013.

[55] "AT&T Managed Security Services-Help detect, deter and mitigate the damage of cyber attacks," AT&T, 2013.

[56] "Amazon Elastic Compute Cloud (Amazon EC2)," Amazon Web Services, 2013.

[57] "Amazon Web Services -Overview of Security Process," Amazon Web Services, 2013.

[58] "Managed Security Overview," Rackspace, US Inc, 2013.

[59] "Verizon Terremark Security Services," 2013. [Online]. Available: http://www.terremark.com/services/security-services.aspx.

[60] "ThinkGrid Ceano Virtual Server Infrastructure (IaaS)," ThinkGrid, 2013.

[61] "Virtual Server Infrastructure Datasheet," ThinkGrid, 2013.

[62] "GoGrid Security Overview," GoGrid, 2013.

[63] "Compare Cloud Computing Providers," 2013. [Online]. Available: http://cloud-computing.findthebest.com/.

Appendix A: Service Model Questions

Table 22: Service model questions

6 Questions for Service Models
1) What's your motive in adopting a cloud provider? a) Personal or Business use (SaaS) b) To develop applications (PaaS) c) Business use (IaaS) 2) What do you expect to use the cloud provider for? a) To use applications running on a cloud infrastructure (SaaS) b) To create web applications on a cloud infrastructure (PaaS) c) To outsource the hardware needs on a cloud infrastructure (IaaS) 3) You would prefer to: a) Simply use applications and let the rest of the aspects (e.g. OS, middleware etc) be managed by the cloud vendor (SaaS) b) Manage applications yourself and let the cloud vendor manage everything else (PaaS) c) Manage applications yourself, as well as data, operating system, middleware and runtime (IaaS) 4) You are interested in: a) Accessing the applications from a variety of devices, in the office or on the go (SaaS) b) Application testing or development (PaaS) c) Extra data space for processing power (IaaS) 5) What services will you utilize by adopting a cloud provider? a) Applications like Office 365 (SaaS) b) Development tools and/or databases (PaaS) c) Virtual servers, storage, networking and operating systems (IaaS) 6) Concerning security issues, you would prefer to have: a) Minimum control over security (SaaS) b) A shared responsibility with the vendor (PaaS) c) Full control over security (IaaS)

Table 23: SaaS Questionnaire

20 Questions for SaaS
1) What is the size of your business? a) Small (1) (2)(3)(5) b) Medium (1)(2)(3)(5) c) Large (4) (5)
2) What operating systems do you use? a) Windows (1)(2)(4)(5) b) Linux (1)(4)(5) c) Mac OS X d) Cross Platform (2)(3)
3) Choose the industry category that best describes your business a) Education (1)(3)(5) b) Financial (1)(2)(3)(4) c) Government (1) d) Manufacturing (1)(2)(4)(5) e) Health and Social Services (2)(3) f) Media (1)(2)(3)(4)(5) g) Non-Profit (1)(3)(5) h) Professional Services (3)(4)(5) i) Retail (2)(5)
4) Choose the desired Sales Automation features a) Billing/Invoicing (1)(2)(4)(5) b) Contact History (1)(2)(4)(5) c) Contact Manager (1)(2)(3)(4)(5) d) Contact Scheduler (1)(2)(4)(5) e) Customer Database (2)(3)(4)(5) f) Lead Management (1)(2)(3)(4)(5) g) Lead Tracking (1)(3)(4)(5)
5) Choose the desired Collaboration features a) Chat (1)(2)(3)(4) b) Mail Merge (1)(2)(3)(4)(5) c) Mobile Access (1)(3)(4)(5) d) Remote Access (2)(4)(5) e) Remote Tracking (3) (4)(5)
6) What kind of support do you wish to have? a) 24/7 (1)(2)(3)(5) b) Blog (1)(2)(3)(4) c) Email (1)(2)(3)(5)

d) Forums (2)(3)(4)
e) Help Desk (3)(5)
f) Live Chat (3)(4)(5)
g) Phone (1)(2)(3)(5)
h) Recorded demos (1)(2)(3)(4)
i) Remote training (1)(2)(3)(5)

7) What kind of access control do you wish to have in order to protect system and resources from unauthorized access?
   a) Field-level security (1)(3)(4)
   b) Group Creation and Management (1)(2)(3)(4)(5)
   c) Roles/Organizational Hierarchy (1)(2)(5)
   d) Security Admin Profiles (1)(5)

8) Do you wish the cloud provider to have restore and recovery capabilities in case of e.g. cyberattacks, equipment failures or natural disasters, in order to protect your data?
   a) Yes (1)(2)(3)(4)(5)
   b) No ()-disaster recovery

9) Do you wish the cloud provider to ensure protection and isolation of sensitive data in cases of malicious attacks such as SQL injections or guest hopping attacks?
   a) Yes (1)(2)(3)
   b) No (4)(5)-Data isolation

10) Do you wish the cloud provider to have physical and environmental security measures of their data centers to prevent unauthorized physical access or damage of the stored information?
   a) Yes (1)(2)(3)(4)(5)
   b) No ()-Physical Security

11) Do you wish the cloud provider to collect metrics and automatically trigger alerts when a faulty condition, e.g. unauthorized attempt to access data, is detected?
   a) Yes (1)(2)(3)(4)(5)
   b) No () –Monitoring

12) Do you wish the cloud provider to ensure the secure transfer of data from your enterprise to cloud and from cloud to cloud?
   a) Yes (1) (2)(3)(4)(5)
   b) No () –Security for data exchange

13) Do you wish the cloud provider to have an effective backup strategy?
   a) Yes (1)(2)(3)(4)(5)
   b) No () –Backup

14) What kind of security certifications and standards do you wish the cloud provider to have?
    a) ISO 27001 (1)
    b) ISO 27002 (2)
    c) PCI-DSS (5)
    d) HIPAA (2)
    e) SAFE HARBOR (1)(2)(3)(4)(5)
    f) SAS 70 II (1)(3)
    g) SysTrust (1) (5)

15) Would you like the cloud provider to perform compliance audit in order to protect your data and adhere to regulatory guidelines?
    a) Yes (1)(2)(3)(4)(5)
    b) No ()-Compliance audit

16) In order to avoid malicious attacks like denial of service, man in the middle, network sniffing, port scanning and cross site scripting, that may compromise your business and data would you like the cloud provider to have adequate network level security?
    a) Yes (1)(2)(3)(4)(5)
    b) No ()-Network layer security

17) Since data may be held in different jurisdiction raising legal issues, choose the geographic location that you want your data to be stored.
    a) South America (1)(2)(3)(5)
    b) North America (1)(2)(3)(4)(5)
    c) Europe (1)(2)(3)(5)
    d) Asia Pacific (1)(2)(3)(4)(5)
    e) Middle East (1)(2)

18) Would you like your data to be encrypted while in rest, in use or in transit?
    a) Yes (1)(2)(5)
    b) No (3)(4)-Encryption

19) Would you like the cloud provider to offer a stable Service Level Agreement (SLA) in order to mitigate security or functional issues?
    a) Yes (2)(3)(4) (5)
    b) No (1)-SLA

20) What is the monthly budget that you are willing to pay?
    a) 0-20 $ (4)
    b) 21-40 $ (3)
    c) 41-60 $ (2)
    d) 61-150 $ (1)(5)

Table 24: PaaS Questionnaire

20 Questions for PaaS
1) What operating systems do you use? a) Cent OS (2) b) Debian (2) c) Debian Linux (2) d) Fedora (2) e) Gentoo Linux (3) f) Linux Operating Systems (1) (3)(4)(5) g) Oracle Enterprise Linux (2) h) Windows Server 2003 (2) i) Windows Server 2008 (1)(2)(4)(5)
2) What programming languages do you want to use? a) Basic (2) b) C# (2) c) Java (1)(2)(3)(4)(5) d) Php (1)(2)(3)(4)(5) e) Python (1)(2)(4) f) Ruby (2)(3)(4)(5) g) Visual Basic (2)
3) Since data may held in different jurisdiction raising legal issues, choose the geographic location that you want your data to be stored. a) South America (1)(4)(5) b) North America (1)(2)(3)(4)(5) c) Europe (1)(2)(4)(5) d) Asia Pacific (1)(2)(3)(4)(5) e) Middle East (4)
4) Would you like the cloud provider to offer a stable Service Level Agreement (SLA) in order to mitigate security or functional issues? a) Yes (1)(2)(3)(5) b) No (4) –SLA
5) What kind of security certifications and standards do you wish the cloud provider to have? a) ISO 27001 (1)(4)(5) b) ISO 27002 [3] c) PCI-DSS (5) d) HIPAA (2)(5) e) SAFE HARBOR (1)(3)(4) f) SAS 70 II (1)(3)(4)(5) g) SysTrust (4)(5)

h) SSAE 16 II (1) (2)
i) ISAE 3402 Type II (1) (2)

6) In order to avoid malicious attacks like denial of service, man in the middle, network sniffing, port scanning and cross site scripting, that may compromise your data would you like the cloud provider to have adequate network level security?
   a) Yes (1)(2)(3)(4)(5)
   b) No ()-Network layer security

7) Do you wish the cloud provider to have physical and environmental security measures of their data centers to prevent unauthorized physical access or damage of the stored information?
   a) Yes (1)(2)(3)(4)(5)
   b) No ()-Physical Security

8) Would you like the cloud provider to perform compliance audit in order to protect your data and adhere to regulatory guidelines?
   a) Yes (1)(2)(3)(4)(5)
   b) No ()-Compliance audit

9) Do you wish the cloud provider to collect metrics and automatically trigger alerts when a faulty condition, e.g. unauthorized attempt to access data, is detected?
   a) Yes (1)(2)(3)(4)(5)
   b) No () –Monitoring

10) Do you wish the cloud provider to have restore and recovery capabilities in case of e.g. cyberattacks , equipment failures or natural disasters, in order to protect your data?
   a) Yes (1)(2)(3)(4)(5)
   b) No ()-disaster recovery

11) Do you wish the cloud provider to have an effective backup strategy?
   a) Yes (1)(2)(3)(4)(5)
   b) No () –Backups

12) Do you wish the cloud provider to maintain a strict privacy policy to help protect customer data?
   a) Yes (1)(2)(3)(4)(5)
   b) No –Critical data privacy

13) Do you wish the cloud provider to take all adequate measures in order to protect your data?
   a) Yes (1)(2)(3)(4)(5)
   b) No – Data protection

14) What kind of access control do you wish to have in order to protect system and resources from an unauthorized access?
    a) Authentication controls (1)(2)(3)(4)(5)
    b) Authorization controls (1)(2)

15) Would you like the cloud provider to ensure that a platform can be transferred from a failing data center to a healthy one in order to provide nearly uninterrupted service to cloud customers?
    a) Yes (1)(2)(3)(4)(5)
    b) No -Failover features

16) Do you wish the cloud provider to allow you scale your computational resources dynamically and predictably?
    a) Yes (1)(2)(3)(4)
    b) No (5)–Autoscaling

17) Is it important for you that the cloud provider has virtual private servers?
    a) Yes (2)(3)(5)
    b) No (1)(4)

18) Would you like the cloud provider to support the isolation of virtual machines?
    a) Yes (2)(3)(5)
    b) No (1)(4)

19) What kind of support do you wish to have?
    a) Phone (2)(3)(4)
    b) Forums (1)(2)(3)(4)(5)
    c) 24/7 (2)
    d) Urgent response (2)
    e) Online resources (1)(2)(3)(4)(5)
    f) Live Chat (3)(4)
    g) Knowledge base (3)(4)
    h) Online guides (1)(3)(4)

20) What is the monthly budget that you are willing to pay?
    a) 0-100 $ (4)(5)
    b) 100-200 $ (1)(3)
    c) 200-500 $ (2)

Table 25: IaaS Questionnaire

20 Questions for IaaS

1) What operating systems do you use?
   a) Cent OS (1)(2)(3)(5)
   b) Debian (1)(5)
   c) Debian Linux (2)(3)(4)(5)
   d) Fedora (1)(2)
   e) Gentoo Linux (1)(2)
   f) Red Hat Enterprise Linux (1)(2)(3)(4)(5)
   g) Oracle Enterprise Linux (1)(4)
   h) Ubuntu Linux (1)(2)(3)(5)
   i) Windows Server 2003 (1)(3)(4)(5)
   j) Windows Server 2008 (1)(2)(3)(1)(4)(5)

2) What programming languages do you want to use?
   a) All (1)(3)(5)
   b) APL (1)(3)(5)
   c) C++ (1)(3)(4)(5)
   d) Java (1)(2)(3)(5)
   e) Php (1)(2)(3)(5)
   f) Python (1)(2)(3)(5)
   g) Ruby (1)(2)(3)(5)
   h) Win Dev (1)(3)(5)

3) Since data may be held in different jurisdiction raising legal issues, choose the geographic location that you want your data to be stored.
   a) South America (3)(4)
   b) North America (1)(2)(3)(4)(5)
   c) Europe (1)(2)(3)(4)(5)
   d) Asia Pacific (1)(2)(3)
   e) Middle East (3)

4) Would you like the cloud provider to offer a stable Service Level Agreement (SLA) in order to mitigate security or functional issues?
   c) Yes (1)(2)(3)(4)(5)
   d) No ()

5) What kind of security certifications and standards do you wish the cloud provider to have?
   a) ISO 27001 (1)(2)(3)(4)
   b) ISO 27002 (2)(3)
   c) PCI-DSS (1)(2)(3)
   d) HIPAA (1)(2)
   e) SAFE HARBOR (1)(2)()
   f) SAS 70 II (1)(2)(4)(1)(5)
   g) SysTrust ()()

h) SSAE 16 II (1) (2)(4)(5)

6) In order to avoid malicious attacks like denial of service, man in the middle, network sniffing, port scanning and cross site scripting, that may compromise your data would you like the cloud provider to have adequate network level security?
   a) Yes (1)(2)(3)(4)(5)
   b) No ()-Network layer security

7) Do you wish the cloud provider to have physical and environmental security measures of their data centers to prevent unauthorized physical access or damage to the stored information?
   a) Yes (1)(2)(3)(4)(5)
   b) No ()-Physical Security

8) Would you like the cloud provider to perform compliance audit in order to protect your data and adhere to regulatory guidelines?
   a) Yes (1)(2)(3)(4)(5)
   b) No ()-Compliance audit

9) Do you wish the cloud provider to collect metrics and automatically trigger alerts when a faulty condition, e.g. unauthorized attempt to access data, is detected?
   a) Yes (1)(2)(3)(4)(5)
   b) No () –Monitoring

10) Do you wish the cloud provider to have restore and recovery capabilities in case of e.g. cyberattacks , equipment failures or natural disasters, in order to protect your data?
   a) Yes (1)(2)(3)(4)(5)
   b) No ()-disaster recovery

11) Do you wish the cloud provider to have an effective backup strategy?
   a) Yes (1)(2)(3)(4)(5)
   b) No () –Backups

12) Do you wish the cloud provider to maintain a strict privacy policy to help protect customer data?
   a) Yes (1)(2)(3)(4)(5)
   b) No –Critical data privacy

13) Do you wish the cloud provider to take all the adequate measures in order to protect your data?
   a) Yes (1)(2)(3)(4)(5)
   b) No – Data protection

14) What kind of access control do you wish to have in order to protect system and resources from an unauthorized access?
    a) Authentication controls (1)(2)(3)(4)(5)
    b) Authorization controls (1)(2)(3)(4)

15) Would you like the cloud provider to ensure that a platform can be transferred from a failing data center to a healthy one in order to provide nearly uninterrupted service to cloud customers?
    a) Yes (1)(2)(3)(4)(5)
    b) No -Failover features

16) Do you wish the cloud provider to allow you scale your computational resources dynamically and predictably?
    a) Yes (1)(2)(3)(4)(5)
    b) No ()–Autoscaling

17) Is it important to you that the cloud provider has virtual private servers?
    a) Yes (1)(2)(3)(4)(5)
    b) No ()()

18) Would you like the cloud provider to support the isolation of virtual machines?
    a) Yes (1)(2)(3)(4)(5)
    b) No ()()

19) What kind of support do you wish to have?
    a) Phone (1)(2)(3)(4)(5)
    b) Forums (1)(2)(3)(5)()
    c) 24/7 (1)(2)(3)(4)(5)
    d) Urgent response (1)(2)(3)(5)
    e) Online resources (2)(3)(4)(5)()
    f) Live Chat (2)(3)(4)(5)
    g) Diagnostic Tools (1)()
    h) Online guides (1)(2)(4)

20) What is the monthly budget that you are willing to pay?
    a) 0-20 $ (4)(5)
    b) 21-40 $ (1)(3)
    c) 41-60 $ (2)

Appendix B: SaaS Providers

Table 26: Sales Cloud Characteristics [63]

Sales Cloud Professional Edition	
Price	
$65/User/ Month	
Industry Solutions	
Education	Yes
Financial	Yes
Government	Yes
Health and Social Services	No
Manufacturing	Yes
Media	Yes
Non-Profit	Yes
Professional Services	No
Retail	No
Business size	
Small	Yes
Medium	Yes
Large	No
Platform	
Windows	Yes
Linux	Yes
Mac	No
Mac OS X	No
Cross Platform	No
Security Features	
Data Encryption	Yes
Field-level security	Yes

Group Creation and Management	Yes
Roles/Organizational Hierarchy	Yes
Security Admin Profiles	Yes
Audit Compliance	Yes
Security for Data Exchange	Yes
Data Isolation	Yes
Disaster Recovery	Yes
Backups	Yes
Physical Security	Yes
Network level security	Yes
Security Monitoring	Yes
SLA	N/A
Integration	
Data Import/Export	No
Knowledge Base Integration	No
Legacy Integration	Yes
Product catalog Integration	Yes
Collaboration Features	
Chat	Yes
Mail Merge	Yes
Mobile Access	Yes
Remote Access	No
Remote Tracking	No
Sales Automation Features	
Billing/Invoicing	Yes
Contact History	Yes
Contact Manager	Yes
Contact Scheduler	Yes
Customer Database	No
Lead Management	Yes

Lead Tracking	Yes
Support Features	
24/7	Yes
Blog	Yes
Email	Yes
Forums	No
Help Desk	No
Live Chat	No
Phone	Yes
Recorded demos	Yes
Remote training	Yes

Table 27: Microsoft Dynamic CRM Online Characteristics [63]

Microsoft Dynamics CRM Online	
Price	
$44/User/ Month	
Industry Solutions	
Education	Yes
Financial	Yes
Government	Yes
Health and Social Services	Yes
Manufacturing	Yes
Media	Yes
Non-Profit	Yes
Professional Services	No
Retail	Yes
Business size	
Small	No
Medium	No
Large	Yes

Platform	
Windows	Yes
Linux	No
Mac	No
Mac OS X	No
Cross Platform	No
Security Features	
Data Encryption	Yes
Field-level security	No
Group Creation and Management	Yes
Roles/Organizational Hierarchy	Yes
Security Admin Profiles	No
Audit Compliance	Yes
Security for Data Exchange	Yes
Data Isolation	Yes
Disaster Recovery	Yes
Backups	Yes
Physical Security	Yes
Network level security	Yes
Security Monitoring	Yes
SLA	99.9
Collaboration Features	
Chat	Yes
Mail Merge	Yes
Mobile Access	Yes
Remote Access	Yes
Remote Tracking	Yes
Sales Automation Features	
Billing/Invoicing	Yes
Contact History	Yes

Contact Manager	Yes
Contact Scheduler	Yes
Customer Database	Yes
Lead Management	Yes
Lead Tracking	Yes
Support Features	
24/7	No
Blog	Yes
Email	No
Forums	Yes
Help Desk	Yes
Live Chat	Yes
Phone	No
Recorded demos	No
Remote training	No

Table 28: SugarCRM Professional Characteristics [63]

SugarCRM Professional	
Price	
$35/User/ Month	
Industry Solutions	
Education	Yes
Financial	Yes
Government	No
Health and Social Services	Yes
Manufacturing	No
Media	Yes
Non-Profit	Yes
Professional Services	Yes
Retail	No

Business size	
Small	Yes
Medium	Yes
Large	No
Platform	
Windows	No
Linux	No
Mac	No
Mac OS X	No
Cross Platform	Yes
Security Features	
Data Encryption	No
Field-level security	Yes
Group Creation and Management	Yes
Roles/Organizational Hierarchy	No
Security Admin Profiles	No
Audit Compliance	Yes
Security for Data Exchange	Yes
Data Isolation	Yes
Disaster Recovery	Yes
Backups	Yes
Physical Security	Yes
Network level security	Yes
Security Monitoring	Yes
SLA	99,5%
Collaboration Features	
Chat	Yes
Mail Merge	Yes
Mobile Access	Yes
Remote Access	No

Remote Tracking	Yes
Sales Automation Features	
Billing/Invoicing	No
Contact History	No
Contact Manager	Yes
Contact Scheduler	No
Customer Database	Yes
Lead Management	Yes
Lead Tracking	Yes
Support Features	
24/7	Yes
Blog	Yes
Email	Yes
Forums	Yes
Help Desk	Yes
Live Chat	Yes
Phone	Yes
Recorded demos	Yes
Remote training	Yes

Table 29: Zoho CRM Enterprise Edition Characteristics [63]

Zoho CRM Enterprise Edition	
Price	
$20/User/ Month	
Industry Solutions	
Education	No
Financial	Yes
Government	No
Health and Social Services	No
Manufacturing	Yes

Media	Yes
Non-Profit	No
Professional Services	Yes
Retail	No
Business size	
Small	No
Medium	No
Large	Yes
Platform	
Windows	Yes
Linux	Yes
Mac	No
Mac OS X	Yes
Cross Platform	No
Security Features	
Data Encryption	No
Field-level security	Yes
Group Creation and Management	Yes
Roles/Organizational Hierarchy	No
Security Admin Profiles	No
Audit Compliance	Yes
Security for Data Exchange	Yes
Data Isolation	N/A
Disaster Recovery	Yes
Backups	Yes
Physical Security	Yes
Network level security	Yes
Security Monitoring	Yes
SLA	99,5%
Collaboration Features	

Chat	Yes
Mail Merge	Yes
Mobile Access	Yes
Remote Access	Yes
Remote Tracking	Yes
Sales Automation Features	
Billing/Invoicing	Yes
Contact History	Yes
Contact Manager	Yes
Contact Scheduler	Yes
Customer Database	Yes
Lead Management	Yes
Lead Tracking	Yes
Support Features	
24/7	No
Blog	Yes
Email	No
Forums	Yes
Help Desk	No
Live Chat	Yes
Phone	No
Recorded demos	Yes
Remote training	No

Table 30: NetSuite CRM+ Characteristics [63]

NetSuite CRM+
Price
$129/User/ Month
Industry Solutions
Education — Yes

Financial	No
Government	No
Health and Social Services	No
Manufacturing	Yes
Media	Yes
Non-Profit	Yes
Professional Services	Yes
Retail	Yes
Business size	
Small	Yes
Medium	Yes
Large	Yes
Platform	
Windows	Yes
Linux	Yes
Mac	No
Mac OS X	Yes
Cross Platform	No
Security Features	
Data Encryption	Yes
Field-level security	No
Group Creation and Management	Yes
Roles/Organizational Hierarchy	Yes
Security Admin Profiles	Yes
Audit Compliance	Yes
Security for Data Exchange	Yes
Data Isolation	N/A
Disaster Recovery	Yes
Backups	Yes
Physical Security	Yes

Network level security	Yes
Security Monitoring	Yes
SLA	99,5%
Collaboration Features	
Chat	No
Mail Merge	Yes
Mobile Access	Yes
Remote Access	Yes
Remote Tracking	Yes
Sales Automation Features	
Billing/Invoicing	Yes
Contact History	Yes
Contact Manager	Yes
Contact Scheduler	Yes
Customer Database	Yes
Lead Management	Yes
Lead Tracking	Yes
Support Features	
24/7	Yes
Blog	No
Email	Yes
Forums	No
Help Desk	Yes
Live Chat	Yes
Phone	Yes
Recorded demos	No
Remote training	Yes

Appendix C: PaaS Providers

Table 31: Google App Engine Characteristics [63]

Google App Engine	
Price	
Base Plan Cost	$150/month
Security Features	
Authentication controls	Yes
Authorization controls	Yes
Backups	Yes
Critical Data Privacy	Yes
Data Protection	Yes
Failover Features	Yes
Physical Security	Yes
Network layer security	Yes
Audit Compliance	Yes
Monitoring	Yes
Disaster recovery	Yes
Isolation of VMs	No
Service Level Agreement (SLA)	Yes
Autoscaling	
Yes	
Virtual Private Servers	
N/A	
Compatible OS	
Cent OS	No
Debian	No
Debian Linux	No
Fedora	No

Gentoo Linux	No
Linux Operating Systems	Yes
Oracle Enterprise Linux	No
Windows Server 2003	No
Windows Server 2008	Yes
Supported Programming Languages	
BASIC	No
C#	No
Java	Yes
PHP	Yes
Python	Yes
Ruby	No
Visual Basic	No
Supported Services	
Phone	No
Forums	Yes
24/7	No
Urgent Response	No
Online Resources	Yes
Live Chat	No
Knowledge Base	No
Online Guides	Yes

Table 32: Microsoft Windows Azure Characteristics [63]

Microsoft Windows Azure	
Price	
Base Plan Cost	$500/month
Security Feauters	
Authentication controls	Yes
Authorization controls	Yes

Backups	Yes
Critical Data Privacy	Yes
Data Protection	Yes
Failover Features	Yes
Physical Security	Yes
Network layer security	Yes
Audit Compliance	Yes
Monitoring	Yes
Disaster recovery	Yes
Isolation of VMs	Yes
Service Level Agreement (SLA)	Yes
Autoscaling	
Yes	
Virtual Private Servers	
Yes	
Compatible OS	
Cent OS	Yes
Debian	Yes
Debian Linux	Yes
Fedora	Yes
Gentoo Linux	No
Linux Operating Systems	No
Oracle Enterprise Linux	Yes
Windows Server 2003	Yes
Windows Server 2008	Yes
Supported Programming Languages	
BASIC	Yes
C#	Yes
Java	Yes
PHP	Yes

Python	Yes
Ruby	Yes
Visual Basic	Yes
Supported Services	
Phone	Yes
Forums	Yes
24/7	Yes
Urgent Response	Yes
Online Resources	Yes
Live Chat	No
Knowledge Base	No
Online Guides	No

Table 33: Engine Yard Characteristics [63]

Engine Yard	
Price	
Base Plan Cost	$150/month
Security Features	
Authentication controls	Yes
Authorization controls	No
Backups	Yes
Critical Data Privacy	Yes
Data Protection	Yes
Failover Features	Yes
Physical Security	Yes
Network layer security	Yes
Audit Compliance	Yes
Monitoring	Yes
Disaster recovery	Yes
Isolation of VMs	Yes

Service Level Agreement (SLA)	Yes
Autoscaling	
Yes	
Virtual Private Servers	
Yes	
Compatible OS	
Cent OS	No
Debian	No
Debian Linux	No
Fedora	No
Gentoo Linux	Yes
Linux Operating Systems	Yes
Oracle Enterprise Linux	No
Windows Server 2003	No
Windows Server 2008	No
Supported Programming Languages	
BASIC	No
C#	No
Java	Yes
PHP	Yes
Python	No
Ruby	Yes
Visual Basic	No
Supported Services	
Phone	Yes
Forums	Yes
24/7	No
Urgent Response	No
Online Resources	Yes
Live Chat	Yes

Knowledge Base	Yes
Online Guides	Yes

Table 34: Force.com Characteristics [63]

Force.com	
Price	
Base Plan Cost	$75/month
Security Features	
Authentication controls	Yes
Authorization controls	No
Backups	Yes
Critical Data Privacy	Yes
Data Protection	Yes
Failover Features	Yes
Physical Security	Yes
Network layer security	Yes
Audit Compliance	Yes
Monitoring	Yes
Disaster recovery	Yes
Isolation of VMs	No
Service Level Agreement (SLA)	N/A
Autoscaling	
Yes	
Virtual Private Servers	
-	
Compatible OS	
Cent OS	No
Debian	No
Debian Linux	No
Fedora	No

Gentoo Linux	No
Linux Operating Systems	Yes
Oracle Enterprise Linux	No
Windows Server 2003	No
Windows Server 2008	Yes
Supported Programming Languages	
BASIC	No
C#	No
Java	Yes
PHP	Yes
Python	Yes
Ruby	Yes
Visual Basic	No
Supported Services	
Phone	Yes
Forums	Yes
24/7	No
Urgent Response	No
Online Resources	Yes
Live Chat	Yes
Knowledge Base	Yes
Online Guides	Yes

Table 35: AT&T Characteristics [63]

AT&T Synaptic	
Price	
Base Plan Cost	$75/month
Security Features	
Authentication controls	Yes
Authorization controls	No

Backups	Yes
Critical Data Privacy	Yes
Data Protection	Yes
Failover Features	Yes
Physical Security	Yes
Network layer security	Yes
Audit Compliance	Yes
Monitoring	Yes
Disaster recovery	Yes
Isolation of VMs	Yes
Service Level Agreement (SLA)	Yes
Autoscaling	
No	
Virtual Private Servers	
Yes	
Compatible OS	
Cent OS	No
Debian	No
Debian Linux	No
Fedora	No
Gentoo Linux	No
Linux Operating Systems	Yes
Oracle Enterprise Linux	No
Windows Server 2003	No
Windows Server 2008	Yes
Supported Programming Languages	
BASIC	No
C#	No
Java	Yes
PHP	Yes

Python	No
Ruby	Yes
Visual Basic	No
Supported Services	
Phone	No
Forums	Yes
24/7	No
Urgent Response	No
Online Resources	Yes
Live Chat	No
Knowledge Base	No
Online Guides	No

Appendix D: IaaS Providers

Table 36: Amazon EC3 characteristics [63]

Amazon EC2	
Price	
Base Plan Cost	$51.24/month
Security Features	
Authentication controls	Yes
Authorization controls	Yes
Backups	Yes
Critical Data Privacy	Yes
Data Protection	Yes
Failover Features	Yes
Physical Security	Yes
Network layer security	Yes
Audit Compliance	Yes
Monitoring	Yes
Disaster recovery	Yes
Isolation	Yes
Service Level Agreement	Yes
Autoscaling	
Yes	
Virtual Private Servers	
Yes	
Compatible OS	
Cent OS	Yes
Debian	Yes
Debian Linux	No
Fedora	Yes

Gentoo Linux	Yes
Red Hat Enterprise Linux	Yes
Oracle Enterprise Linux	Yes
Ubuntu Linux	Yes
Windows Server 2003	Yes
Windows Server 2008	Yes
Supported Programming Languages	
All	Yes
APL	Yes
C++	Yes
Java	Yes
PHP	Yes
Python	Yes
Ruby	Yes
Win Dev	Yes
Supported Services	
Phone	Yes
Forums	Yes
24/7	Yes
Urgent Response	Yes
Online Resources	No
Live Chat	No
Diagnostic Tools	Yes
Online Guides	Yes

Table 37: Rackspace Cloud Characteristics [63]

Rackspace	
Price	
Base Plan Cost	$58.40/month
Security Features	

Authentication controls	Yes
Authorization controls	Yes
Backups	Yes
Critical Data Privacy	Yes
Data Protection	Yes
Failover Features	Yes
Physical Security	Yes
Network layer security	Yes
Audit Compliance	Yes
Monitoring	Yes
Disaster recovery	Yes
Isolation	Yes
Service Level Agreement	Yes
Autoscaling	
Yes	
Virtual Private Servers	
Yes	
Compatible OS	
Cent OS	Yes
Debian	No
Debian Linux	Yes
Fedora	Yes
Gentoo Linux	Yes
Red Hat Enterprise Linux	Yes
Oracle Enterprise Linux	No
Ubuntu Linux	Yes
Windows Server 2003	No
Windows Server 2008	Yes
Supported Programming Languages	
All	No

APL	No
C++	No
Java	Yes
PHP	Yes
Python	Yes
Ruby	Yes
Win Dev	No
Supported Services	
Phone	Yes
Forums	Yes
24/7	Yes
Urgent Response	Yes
Online Resources	Yes
Live Chat	Yes
Diagnostic Tools	No
Online Guides	Yes

Table 38: Verizon Terremark Characteristics [63]

Verizon Terremark	
Price	
Base Plan Cost	$33/month
Security Features	
Authentication controls	Yes
Authorization controls	Yes
Backups	Yes
Critical Data Privacy	Yes
Data Protection	Yes
Failover Features	Yes
Physical Security	Yes
Network layer security	Yes

Audit Compliance	Yes
Monitoring	Yes
Disaster recovery	Yes
Isolation	Yes
Service Level Agreement	Yes
Autoscaling	
Yes	
Virtual Private Servers	
Yes	
Compatible OS	
Cent OS	Yes
Debian	No
Debian Linux	Yes
Fedora	No
Gentoo Linux	No
Red Hat Enterprise Linux	Yes
Oracle Enterprise Linux	No
Ubuntu Linux	Yes
Windows Server 2003	Yes
Windows Server 2008	Yes
Supported Programming Languages	
All	Yes
APL	Yes
C++	Yes
Java	Yes
PHP	Yes
Python	Yes
Ruby	Yes
Win Dev	Yes
Supported Services	

Phone	Yes
Forums	Yes
24/7	Yes
Urgent Response	Yes
Online Resources	Yes
Live Chat	Yes
Diagnostic Tools	No
Online Guides	No

Table 39: ThinkGrid Ceano Characteristics [63]

ThinkGrid Ceano	
Price	
Base Plan Cost	$33/month
Security Features	
Authentication controls	Yes
Authorization controls	Yes
Backups	Yes
Critical Data Privacy	Yes
Data Protection	Yes
Failover Features	Yes
Physical Security	Yes
Network layer security	Yes
Audit Compliance	Yes
Monitoring	Yes
Disaster recovery	Yes
Isolation	Yes
Service Level Agreement	Yes
Autoscaling	
Yes	
Virtual Private Servers	

Yes	
Compatible OS	
Cent OS	No
Debian	No
Debian Linux	Yes
Fedora	No
Gentoo Linux	No
Red Hat Enterprise Linux	Yes
Oracle Enterprise Linux	Yes
Ubuntu Linux	No
Windows Server 2003	Yes
Windows Server 2008	Yes
Supported Programming Languages	
All	No
APL	No
C++	Yes
Java	No
PHP	No
Python	No
Ruby	No
Win Dev	No
Supported Services	
Phone	Yes
Forums	No
24/7	Yes
Urgent Response	No
Online Resources	Yes
Live Chat	Yes
Diagnostic Tools	No
Online Guides	Yes

Table 40: GoGrid Characteristics [63]

GoGrid	
Price	
Base Plan Cost	$57.60/month
Security Features	
Authentication controls	Yes
Authorization controls	No
Backups	Yes
Critical Data Privacy	Yes
Data Protection	Yes
Failover Features	Yes
Physical Security	Yes
Network layer security	Yes
Audit Compliance	Yes
Monitoring	Yes
Disaster recovery	Yes
Isolation	Yes
Service Level Agreement	Yes
Autoscaling	
Yes	
Virtual Private Servers	
Yes	
Compatible OS	
Cent OS	Yes
Debian	Yes
Debian Linux	Yes
Fedora	No
Gentoo Linux	No
Red Hat Enterprise Linux	Yes
Oracle Enterprise Linux	No

Ubuntu Linux	Yes
Windows Server 2003	Yes
Windows Server 2008	Yes
Supported Programming Languages	
All	Yes
APL	Yes
Java	Yes
PHP	Yes
Python	Yes
Ruby	Yes
Win Dev	Yes
Supported Services	
Phone	Yes
Forums	Yes
24/7	Yes
Urgent Response	Yes
Online Resources	Yes
Live Chat	Yes
Diagnostic Tools	No
Online Guides	No