International Journal of Grid Distribution Computing
Vol.8, No.2 (2015), pp.285-308
http://dx.doi.org/10.14257/ijgdc.2015.8.2.25

Requirements Capture and Comparative Analysis of Cloud Security Techniques

[1]Manel Medhioub, [2]Mohamed Hamdi and [3]Tai-Hoon Kim

[1]Faculty of Economics and Management of Sfax
ESPRIT
[2]School of Communication Engineering
[3]Convergence Security Department, Sungshin Women's University
[1]manel.madhioub@esprit.tn, [2]mmh@supcom.tn, [3]taihoonn@empal.com

Abstract

Convergence and ubiquity are the key characteristics of tomorrow's service provision infrastructures. Today, Cloud architectures offer cost-efficient backbones that support transmission, storage, and computing of applications contents. These architectures can be used for business, scientific, and other computing purposes. However, the diversity of these services, delivered through Cloud infrastructures, increases its vulnerability to security incidents and attacks. The requirements for cost and complexity reduction make the design and development of protection mechanisms even more challenging. Furthermore, key design features such as confidentiality, privacy, authentication, anonymity, survivability, dependability, and fault-tolerance can be even more difficult to provide.

The aim of this paper is to present the state-of-the-art Cloud security and to explore research directions and technology trends to address the protection of Cloud infrastructures. To do so, we are going to explore the fundamental concepts of Cloud computing security, notably, its principles, vulnerabilities, requirements, and mechanisms.

Keywords: *Cloud computing security, attacks, threats, security mechanisms*

1. Introduction

Cloud Computing is clearly one of today's most enticing technology thanks to its cost-efficiency and flexibility. This technology eliminates the idea of setting up of excessively expensive computing infrastructure for the IT-based solutions and services that are needed in any business. It provides a flexible IT architecture that is accessible via internet for lightweight portable devices. In this way, the existing and new software are enhanced in both capacity and capability. It is also an ideal solution to test scenarios and potential proof of concepts with cost savings [1].

However, there are significant and persistent issues in Cloud Computing compromising its vision as a newly acquired IT model. When we adopt Cloud Computing solutions, we realize that many issues are essentially old problems in new settings but they may be more acute, for instance, virtual machine attacks and Web service vulnerabilities. Moreover, Cloud deployments face most of the same threats that conventional IT faces but also new challenges are being faced by potential Cloud computing adopters including reliable services and security. The security and privacy are the primary concerns for Cloud computing adopters. A study conducted by Ponemon Institute [2, 3] found that fifty-one percent of respondents think that the increased security risk is the main disadvantage with 56 percent.

ISSN: 2005-4262 IJGDC

There are various issues that need to be dealt with respect to security and privacy in a Cloud computing scenario. In this paper, the fundamental concepts of Cloud computing security will be explored, notably, its principles, vulnerabilities, requirements, and mechanisms.

2. Cloud Computing Basics

Before delving into the details related to the security of Cloud computing infrastructure, this section provides an overview on the fundamentals aspects related to the concept.

2.1. The Cloud Paradigm

The Cloud computing paradigm introduced by the US National Institute for Standards and Technology (NIST) refers to the development and implementation of models for enabling ubiquitous, convenient, on-demand access to a shared set 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 [4]. The Cloud Computing is based on five essential characteristics, three service models, and four deployment models.

The Cloud Computing has emerged as the natural evolution and integration of several fields. We present here the basic technologies that have contributed to this emergence:

- Outsourcing: In recent years, the option to outsource IT services to an external service provider has grown in importance due to a variety of positive aspects such as cost, quality, flexibility, and competitive advantages. It is simply the farming out of services to a third party, nonetheless, Cloud computing represents a new way to outsource IT resources.

- Virtualization: Virtualization is part of several trends in IT and it has been the underlying concept towards such a huge rise of Cloud Computing in the modern era. The term [6] refers to providing an environment able to render all the services, being supported by a hardware that can be observed on a personal computer, to the end users. In fact, the three forms of virtualization categorized as: Server, Storage and Network virtualization have lead to the evolution of Cloud computing.

For Cloud Computing, transition from using virtualization for server consolidation to using virtualization to produce a flexible on-demand infrastructure [7] has great value in rapid commissioning and decommissioning of servers. Virtualization also can deliver a degree of isolation and insulation from the effect of some forms of vulnerability risk.

- Resources sharing: In computing, a shared resource or network share is a device or piece of information on a computer that can be remotely accessed from another computer, transparently as if it were a resource in a local machine. The concept of resource sharing itself has been around for decades, as well as its problems, such as security, performance, availability, and administrative isolation.

2.2. Essential Characteristics

The Cloud Computing is based on five essential characteristics which are [4]:

- On-demand self-service: A consumer can unilaterally supply computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (*e.g.*, mobile phones, tablets, laptops, and workstations).

- Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Examples of resources include storage, processing, memory, and network bandwidth.
- Rapid elasticity: Consumers of Cloud resources can expend their use of computer resources (process, storage, bandwidth, and memory) as needed [5]. Capabilities can be elastically provisioned and released to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (*e.g.,* storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the offered service.

2.3. Service Models

Cloud Computing proposes three service models by which different types of services are delivered to the end user [27]. The different models have different strengths and are suitable for different customers and business objectives [2]. The three models are the SaaS, PaaS and IaaS. The three models are the SaaS, PaaS and IaaS, IaaS is the foundation of all Cloud services, with PaaS built upon it and SaaS in turn built upon it [6]:

2.3.1. Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS): provides fundamental computing resources such as processing, storage, and network where the client can deploy and run different software. The customer doesn’t have to own the infrastructure supporting services nor managing or controlling it. Virtualization plays a key role in this process [8] by having each server hosting multiple independent virtual machines (VMs) managed by a Virtual Machine Monitor (VMM) often referred to as a Hypervisor. IaaS services have enabled startups and other businesses to focus on their work without worrying much about the provisioning and management of infrastructure [27].

2.3.2. Platform as a Service (PaaS)

PaaS provides a set of programming languages, libraries, services and tools of development for deploying applications created by the customer, who is able to control and manage them. It offers developers a service that provides a complete software development lifecycle management [27], from planning to design to building applications to deployment to testing to maintenance.

2.3.3. Software as a Service (SaaS)

SaaS is a software deployment model where applications are running on a Cloud infrastructure and accessible from various client devices. The customer can apply limited user-specific application configuration settings but has no access control or management of the internal infrastructure. The SaaS model offers the customers with significant benefits [27], such as improved operational efficiency and reduced costs.

The proliferation of Cloud Computing services is illustrated by the number of applications that are being proposed in this context. Below is a list of Cloud-based services that have been often mentioned by researchers and scientists:

- Amazon Web Services (Public Cloud, IaaS): Arguably one of the most mature Clouds, launched in July 2002, didn't have IaaS offering, more like pieces of it. Its EC2, or Elastic Compute Cloud, which is classified as an IaaS offering launched officially (non-beta) in October 2008.
- Rackspace Cloud hosting: publicly launched in February 2008.
- GoGrid (Public Cloud, IaaS): Launched in April 2008.
- Salesforce.com (Public Cloud, SaaS, and PaaS): Although the company was launched in March 1999, Salesforces PaaS, Force.com started in January 2008.
- Google Apps Engine (Public Cloud, PaaS): was first publically launched in 2008 as beta version. GovCloud, Googles form of Google Apps that addresses and meets government security mandates was only launched in September 2009.

2.4. Deployment Models

Depending on the kind of Cloud deployment, the Cloud could offer limited private computing resources, or a remote access to a large quantity of resources. The different deployment models present a number of trade-offs in how customers can control their resources, the scale, cost, and availability of resources [2]. In providing a secure Cloud computing solution, it is important to decide on the type of Cloud deployment model to be implemented. These models are offered in four ways depending on the users' requirements, namely, a public, private, hybrid and community Cloud.

- A public Cloud: A public Cloud provides shared resources owned and managed by a third party over the internet for the general public. This model offers the greatest level of efficiency but it is less secure than the other Cloud models. Most of its benefits [9] are due to the large pool of available resources and to their geographical distribution.
- A Private Cloud: In private model, services and infrastructure are maintained by the company, a third party, or a combination of them. It offers the greatest level of security and control.
- A hybrid Cloud: It is a private Cloud that can extend to use resources in public Clouds. It provides virtual IT solutions through a mix of both these deployments.
- A community Cloud: In this model, the Cloud infrastructure is shared by several organizations with similar requirements and goals. They are bound together by standardized or proprietary technology that enables data and application portability.

In Figure 1, the lower layer represents the different deployment models of the Cloud namely private, community, public and hybrid Cloud deployment models. The delivery models are presented in the layer just above the deployment layer. The top layer shows the five characteristics which are on-demand self-service, multi-tenancy, ubiquitous network, measured service and rapid elasticity. It is important to make two points about the NIST Cloud Model. First, a customer or tenant can have greater security control over more resources as one move from SaaS to PaaS and again from PaaS to the IaaS service model.

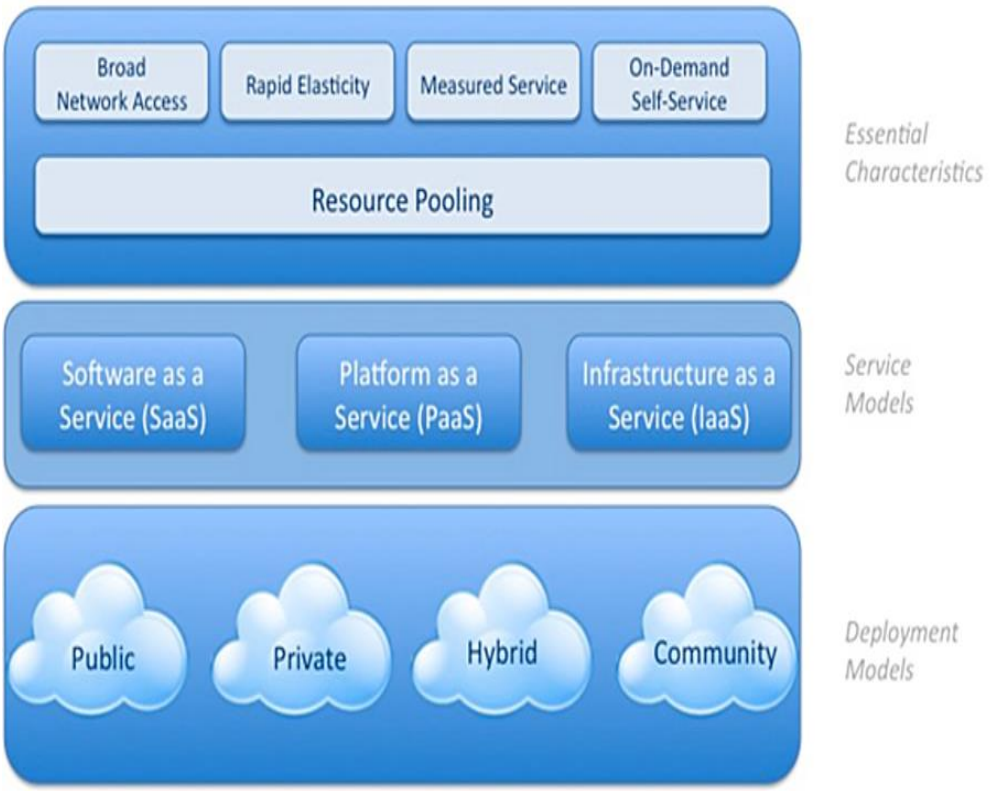

Figure 1. Visual Model of NIST Working Definition of Cloud Computing

Then, Cloud deployment impacts the degree of owner data/application control. A customer or tenant can achieve greater security control over more resources when moving from a public to a community Cloud, and, from a community to a private Cloud.

The Jericho Forum is an association maintained by the open group whose main focus is how protect Cloud network. This Forum has identified 4 criteria to differentiate Cloud formations from each other and the manner of their provision. The Cloud Cube Model [10] incorporates these 4 dimensions to satisfy different Cloud customer's needs as follows:

- Physical location of the data: Internal / External defines if the physical location of data will be inside or outside the organization's boundaries.
- Ownership: Proprietary/Open defines if the technologies are open or black box one.
- Security boundary: Perimeterised/ De-perimeterised Architectures: is a measure of whether the operation is inside or outside of traditional IT domain.
- Sourcing: Insourced / Outsourced defines if the services are controlled by the consumers or by third party.

Linthicum introduces more fragmentation into the Cloud model. 11 major categories [11] are considered as follows:

- Storage-as-a-service is the ability to leverage storage to any application that physically exists at a remote site.
- Database-as-a-service (DaaS) is the ability to leverage the services of a remotely hosted database and sharing it with other users.

- Information-as-a-service is the ability to consume any type of information, remotely hosted, through a well-defined interface such as an API.
- Process-as-a-service is a remote resource that can bind many resources together to form business processes.
- Application-as-a-service (AaaS), also known as software-as-a-service.
- Platform-as-a-service (PaaS).
- Integration-as-a-service is the ability to deliver a complete integration stack from Cloud, including interfacing with most of the features and functions found within traditional enterprise.
- Security-as-a-service: is the ability to deliver core security services remotely over the Internet.
- Management/governance-as-a-service (MaaS and GaaS) is the ability to manage one or more Cloud services and to enforce defined policies on data and services.
- Testing-as-a-service (TaaS) is the ability to test local or Cloud-delivered systems using testing software and services that are remotely hosted.
- Infrastructure-as-a-service (IaaS).

More recent applications have used the Cloud infrastructure for the provision of advanced services such as multimedia streaming [12], virtual reality [13], and robotics [14]. The richness of Cloud components and the complexity of the underlying architecture has considerably witnessed the proliferation of the services based on Cloud computing but it has also been at the origin of many malicious actions that will be described in the following section.

3. Cloud Computing Advantages

The success of Cloud Computing shows that it is suitable for startups, developers, research projects, and even e-commerce entrepreneurs. It is also an ideal solution to test scenarios and potential proof of concepts with cost savings. As a new model for IT, Cloud computing will be used to various advantages by competitors in the same industry, by vendors and providers of Cloud services, and by consumers and subscribers. Henceforth, as a new paradigm for computing, Cloud introduces challenges even as it offers advantages. In many ways, series of qualities that result from fundamental design and implementation decisions may have a direct impact on security [7].

The major benefits brought by Cloud computing, including resiliency, cost-effectiveness, data-centric storage, and scalability, will be highlighted.

3.1. Cost-efficiency

One of the key factors used by Cloud providers to promote their solutions is that the Cloud computing eliminates the requirements for acquiring a whole hardware/software architecture. In public deployment models, Cloud computing provides convenient rental of computing resources: users pay service fees while using a service. One of the central arguments for cost efficiency in public Cloud computing is that data centers (workloads) can be located where costs are the lowest.

The public Clouds have several advantages concerning return on investment for tools and security capabilities that are expensive and also expertise that user has to pay to properly implement and operate [7]. [2] In private deployment model, the beneficial effect of the economies is likely to be much less compared to public Clouds. The most direct approach is for a subscriber to acquire a data center in which he can deploy the Cloud management software or convert part or all of an existing data center. In this case, Cloud upfront costs are similar to those of a typical data center and the subscriber can acquire this latter for anticipated

workloads. For a community Cloud, if the organization plans to consume Cloud services only, the upfront costs appear to be modest. If the organization intends to provide Cloud services within the community Cloud, the costs appear to be similar to those for the private Cloud scenario.

In infrastructure as a Service, Cloud computing vendor's dedicated resources shared with contracted clients at a pay-per-use fee. This greatly minimizes the need for huge initial investment in computing hardware, networking devices and processing power. Computing resources can be added or released with better financial and functional flexibility than in an internal data center.

PaaS provides a low-cost way of developing and deploying applications. Clients using PaaS services transfer even more costs from capital investment to operational expenses. Outsourced and public SaaS Clouds allow the consumer to begin using an application without the upfront costs of equipment acquisition, but potentially with a recurring usage fee.

3.2. Scalability

Cloud Computing resources should look limitless and can be purchased at any time and in any quantity [19]. Public Clouds are generally unrestricted in their location or size. Additionally, they can generally use multi-tenancy without being limited by static security perimeters, which allows a potentially high degree of flexibility in the movement of consumer workloads to correspond with available resources [4]. Scaling to larger sets of subscribers and resources for public Clouds to achieve low costs and elasticity implies a large collection of potential attackers. Cloud elasticity entails continual reconfiguration in network and related controls from the Cloud Internet ingress through core switches and down to individual virtual machines (VMs) and storage. There are profound security implications to performing such dynamic changes to security controls. This elastic demands are also a sophisticated management infrastructure that continually reflects both desired and actual state of infrastructure configuration controls along with all resource allocation [7].

If an organization is large enough and supports a sufficient diversity of workloads, private Cloud may be able to provide elasticity to clients. But, at any specific time, a private Cloud has a fixed computing and storage capacity that has been sized to correspond to anticipated workloads and cost restrictions.

The Community Cloud is a social structure based on the community ownership of the infrastructure. Carrying with it a degree of economic scalability [15], without which there would be diminished competition and potential stifling of innovation as risked in public Clouds. Compared to a private Cloud, it is larger scale and better response to high peaks in resource demand [9].

When IaaS Cloud is public, it provides the ability to quickly rent and then release large numbers of VMs or other Cloud resources [9] without incurring the expense of purchasing and maintaining the necessary hardware. The on-demand dynamic and scalable resource allocation is the main motif behind the development and deployment of Cloud computing. PaaS application development frameworks typically provide design patterns supporting a high level of scalability. A variety of toolkits are structured to support large numbers of consumers, thus enabling PaaS applications to operate efficiently through large fluctuations in demand. Well-developed PaaS applications, particularly in public Cloud, can be quickly deployed to large numbers of consumers and provide very large quantities of data and processing services. Outsourced private or community PaaS Clouds can provide similar abilities; otherwise the scale is restricted by the data center resources [4].

SaaS environment are operated and supported by a scalable Cloud infrastructure. Scalability can even be more challenging on large scale SaaS systems with large

numbers of components. Hardware resources may be immediately available, but with a huge financial cost associated, and may not be an effective and elegant solution in case of inefficient design. Therefore, SaaS layer scalability depends on IaaS one.

3.3. Resilience

Resilience [7] is the ability of a system to provide and maintain an acceptable level of service in the face of faults unintentional, intentional, or naturally caused and deviations from normal operation. Managing resilience is more challenging for the Cloud than for traditional IT environments. It is important that resource elasticity is harmoniously managed for not only adding or releasing resource but also when it behaves badly or fails [7]. Reducing the effect of failures is a primary objective, but equally important is the ability to recover from disasters. Supporting operational resiliency requires a capability for managing operational risk.

The public Cloud option is able to provide a very resilient service with an associated satisfactory level of data assurance [9]. The resources implemented by a large provider and geographically distributed simplify the definition of business continuity and disaster recovery strategies [9]. In some cases, the internal expertise of the private Cloud provider and the available resources [9] may be less adequate to provide resilient service. The management of a Cloud computing service by a single company is in fact a single point of failure. The Community Cloud is not owned or controlled by any one organization, and therefore not dependent on the failure of any one organization. Because of the diversity of its supporting nodes, the Community Cloud ought to be robust and resilient to failure [15], and immune to failures of vendor Clouds. When occasionally failing doing, the unaffected nodes mobilize to compensate for the failure with minimal downtime.

IaaS guarantees more direct control but also leaves the customer fully responsible for the implementation of technical and procedural resilience measures [9]. The SaaS delivery model is clearly the solution that offers the customer less direct control over resilience parameters, but placing more control and responsibility in the hands of the provider [16]. The availability of a SaaS application depends on a reliable and continuously available network.

3.4. Data-centric Storage

In data-centric storage, all event data is stored by type at designated nodes in the network and can later be retrieved by distributed mobile access points in the network. Data storage is one of the fundamental and basic implementation of Cloud Computing. Under the hood, these are distributed storage systems running complex protocols to ensure that data is always available.

The Community Cloud would naturally require storage on its participating nodes, taking advantage of the ever-increasing surplus on most personal computers. Such varying requirements call for a combination of approaches, including distributed storage, distributed databases and key-value stores [15].

SaaS providers [17] may host the software in their own data centers or with co-location providers, or may themselves be outsourced to IaaS providers. If the SaaS provider is leveraging a public Cloud computing service, the SaaS service model implies that the majority of the data managed by an application resides on the servers of the Cloud provider [4] and that the enterprise data might be stored along with the data of other unrelated SaaS applications.

Table 1. Cloud Computing Advantages

	Cost-effectiveness	Scalability	resilience	data-centric storage
Public Cloud	+++	+++	+++	+
Private Cloud	+	+	+	+++
Community Cloud	++	++	++	++
IaaS	+++	+++	+	++
PaaS	++	+++	++	+
SaaS	++	++	+	+

4. Threats and risks of Cloud Computing Infrastructures

The rapid growing of the Cloud computing has also motivated malicious users to revise attacks techniques in order to cope with the features of Cloud infrastructures. This section highlights the security requirements that stem from the characteristics of Cloud computing architectures and gives a technical description of the most relevant attack scenarios.

4.1. Security Requirements for Cloud Computing

Adopting Cloud model results in losing control of both providers and customers of Cloud. The security architecture of the Cloud should be consistent and meeting the security requirements. In [7], a set of security requirements for Cloud computing has been enumerated:

- Service and data availability: Availability is one of the most critical security requirements in Cloud computing. It ensures an immediate and reliable access to Cloud and use of its systems by an authorized entity [18]. Availability can be affected temporarily or permanently by denial of service attacks, equipment outages, and natural disasters [18].
- Network reliability: Reliability can be described as a guarantee that the underlying technology can provide delivery of services. Network reliability is a key cornerstone for Cloud computing and Cloud services. Since a Cloud is accessed from public networks, the Cloud provider must be prepared to catastrophic loss of Internet backbone connectivity. The same concern should be a primary consideration for Cloud service consumers who entrust critical infrastructure to the Cloud.
- Confidentiality and privacy: Confidentiality is to ensure that user data which resides in the Cloud can be accessed only by authorized users or systems [18]. While the storage of user data on remote servers is not new, yet many organizations have not widely adapted the use of Clouds due to the concerns of confidentiality and privacy. In fact, Cloud computing has significant implications for the privacy of personal information and for the confidentiality of business and governmental information. A Cloud provider's terms of service, privacy policy, and location may have significant effects on the privacy and confidentiality protections of user's information. The increased number of parties, devices and applications and delegating data control to the Cloud increase in the risk of data compromise [18]. The Cloud computing industry would adopt better and clearer policies and practices, users would be more vigilant.

- Identity management: The provider's methods and procedures for managing user identities and their access to sensitive resources is one of the most critical elements of any Cloud initiative. Identity management is a primary mechanism for controlling access to data in the Cloud, preventing unauthorized uses, maintaining user roles, and complying with regulations [19]. It eliminates the need for sharing the passwords and supports a variety of user profiles. Identity management should also allow the user to appear anonymously [20] to the service provider while still making it possible to reveal true identity in the event of an investigation by a designated authority. Automating these processes can be a major management task. Currently the majority of Cloud computing systems provide digital identity for users to access their services. However, Cloud computing systems increase the difficulties faced by identity management systems by exposing a much larger attack surface to an intruder than a private network does [19].
- Disaster recovery and business continuity: Users and application providers should get insurance that the Cloud services persist in case of the occurrence of security incidents and disasters. The minimal core services that are mandatorily available should be specified in the continuity plan as well as the policy to use redundant systems. The recovery procedures should also be clearly addressed in order to minimize the downtime duration.
- Resilience: It is the ability of a system to provide and maintain an acceptable level of service in the face of faults unintentional, intentional, or naturally caused [21]. Reducing the effect of failures is a primary objective, but equally important is the ability to recover from disasters. Supporting operational resiliency requires a core capability for managing operational risk and this managing resilience is more challenging for the Cloud than for traditional IT environments.
- Cloud provider viability: The viability of the Cloud provider is an important factor when choosing a public Cloud. Concerns about provider viability are raised when proprietary interfaces are used to administrate the services accessible to the users.
- Risk tolerance: When the user puts information into Cloud, the amount of risk in this action should be estimated. The impact and the frequency of the identified threats should be used in providing an accurate prediction of the risk events. The amount of uncertainty should also be quantified in order to estimate the residual risk. The risk analysis process turns out to be more challenging in Cloud computing since many processes cannot be conducted as in traditional networks. For instance, information classification models should be adapted to cope with the context where multiple data, having different security levels uploaded by users having different access grants, should be managed in a single infrastructure.
- Cost-effectiveness: One of the key factors used by Cloud providers to promote their solutions is that they cost less than acquiring the whole hardware/software architecture. In the associated business model, users only pay for the services they actually exploit, without prior commitment, enabling cost reductions in IT deployment and a scalability of far greater resources. They are abstracted to users in order to appear unlimited, and presented through a simple interface that hides the back-office processes [22]. This assumption should not be affected by the security functionalities that should be provided to protect the Cloud-based services. Strong arguments should be given to the users to make them accept outsourcing the security of their data and application.
- Regulation and legislation compliance: When the data stored or transmitted through the Cloud architecture falls under regulatory compliance restrictions,

the appropriate deployment (private, public or hybrid) should first be determined. Privacy is a crucial issue in Cloud computing, especially with the proliferation of social web. Preventive countermeasures should be implemented to enforce the prohibition of any form of privacy violation. In addition, reactive mechanisms should be used to investigate the cases of privacy violation and take the necessary actions.

- Physical security: Physical security is important as any other security controls to protect the security and operation of the Cloud. Physical problems could cause a loss of availability which is one of the key principles of the security triad. The scope of issues in physical security including natural hazards, human actions, and disaster is significant. Physical access to the Cloud servers should be restricted. Control procedures as preventive measures or countermeasures should be applied against unauthorized access to the facility or to resources or information in the facility. System for protection of physical security should include individual security elements of environmental design, access control, monitoring, personnel identification and access controls as well as intrusion detection.
- Cloud-wide Time Service: Communicating computers that reside in different locations must be synchronized to the same time source. Their record and event timestamps need to be synchronized to a single source. Correct time information comes from authoritative national time standards and it's important for the correct operation of systems and authoritative system logs. A Cloud infrastructure is subjected to all manner of errors and made difficult to diagnose failures when clocks drift between network devices and/or computers.
- System and Network Auditing: Auditing is the process of reviewing and examining the authorization and authentication records in order to verify the compliance of different access control policies and to detect any system breaches [18]. Through the auditing of a Cloud system and network, Cloud provider grants significant control to tenants and manages the ongoing security. Maintaining record of past actions performed by Cloud customer, provider and user helps auditor to identify the modifications and deletion of entries. Relevant information including correct time, resolvable system, and user IDs and appropriate event codes and supporting information should be recorder with security events to perform the analyze of events. All audit events and logs shall be securely archived and controls must be implemented to protect the confidentiality, integrity, and availability of audit events, log and reporting. Audit difficulty is the effect of the lack of control in the Cloud and the distributed and the dynamic multitenant computing environment. Sufficient transparency in the operations of the Cloud provider should be provided also for auditing purposes [18].
- Security monitoring: Security monitoring is predicated on audit logs, network security monitoring and environmental data. It should be highly available and accessible in a secure manner. To trust in Cloud provider, the customer should be able to monitor access to the system and verify security enforcements. Security monitoring in Cloud infrastructure and services is based on the generation, collection, analysis, and reporting of security relevant event data. By the nature of a multi-tenant, security monitoring has additional importance for infrastructure control. Because of the demands of complex Cloud computing solutions, this requirement needs to become more sophisticated. In addition, effective security monitoring is necessary, provider response and security incidents or alerts should be closely tied together to effect a timely response.
- Incident Management: The goal of incident management is to minimize or contain the impact of events. This requirement should be transparent to the

customer and be in line with SLAs and the security policy. Incident management should support the customer's ability to identify and to report events to the provider. This process should include also procedures for managing incidents and situations by Cloud providers.

- Digital investigation in Cloud computing: Cloud computing systems rely on complex overlaying mechanisms that allow the implementation of ask hardware/software architectures. This elasticity poses a challenge to the forensics investigator due to the high volatility of resources such as disk space and memory. Moreover, the distribution of the Cloud infrastructure hardens the respect of agreements between users and providers since multiple legislations and regulations should be referred to [23, 24]. Cloud forensics will be among the topics that will be consistently addressed by researchers in the near future.

4.2. Vulnerabilities against Cloud Architectures

While the benefits are immense, Cloud Computing paradigm is still vulnerable to a large number of system failures. It has all the vulnerabilities associated with Internet applications, and additional vulnerabilities arise from virtualized, outsourced and multitenant resources [19].

4.2.1. Classification

These vulnerabilities prevent the users from adopting this technology and from trusting it. The first step to deal with vulnerabilities is classifying them. Vulnerability is a weakness that can be exploited by a threat, causing harm to the information systems or networks. In [25, 26], some vulnerabilities that are specific to Cloud computing have been pointed out.

Insecure API: Cloud Application Programming Interfaces (APIs) define an interface between a Cloud service and other entities and used by the customers to manage and interact with Cloud services [7]. Cloud services APIs vary from provider to provider, with both proprietary APIs and standards based APIs. Security weaknesses at APIs available to Cloud users are crucial since provisioning, management, orchestration, and monitoring are all performed using these interfaces. Cloud Provider publishes their API required to use services can invite attackers' attention to know the architecture and internal design details [28]. Moreover, the improper user of Cloud components may lead to the use of these components to conduct malicious actions against third victims. Today, these interfaces must be designed to protect against both accidental and malicious attempts.

Malicious Insiders: The provider's or user's site can be attacked by insider malicious employees. The risk of this dangerous security threat is amplified for consumers of Cloud services by the convergence of IT services and customers under a single management domain. In fact, the provider is outside the trusted domain of customer whose loses direct control over potentially business sensitive and confidential data. The level of access granted could enable attackers to collect confidential data or to misuse IT resources with little risk of detection. Additionally, general lack of transparency into provider process and procedure and a little visibility into the hiring standards and practices for Cloud users intensify this threat and affect customer trust on provider. Financial impact and productivity losses are also the ways a malicious insider can affect an organization [26].

Shared technology: Due to the nature of Cloud computing, Cloud users share pool of configurable and reliable computing resources in multi-tenant architecture. In fact, customers store and deliver their data on the same physical storage device without controlling the location. Due to this reason there is a high probability of one users' private data to be viewed by the other users. To handle such sensitive

situations, Cloud Provider should ensure proper data isolation providing security to the user data from any other user unauthorized access or attacks [28]. Although, the hypervisor allows multiple operating systems to be run on the same hardware platform at a same time. It turns out to be hard to keep track of all and hence maintaining all the operating systems secure is difficult. Effectively, a guest system may run a malicious code on the host system and bring the system down or take full control of the system and block access to other guest operating systems [26]. Share the network between tenant's results also in unpredictable performance and exposure to denial of service attacks. Legitimate tenants can run network-intensive workloads and protect against malicious tenants that launch denial of service attacks.

Data loss or leakage: Data loss or leakage can occur due deletion or alteration of records that can take place intentionally or unintentionally. Data deletion is more problematic in Cloud due to multi-tenancy. The architectural or operational characteristics of the Cloud environment increase the threat of data compromise. Data loss or leakage could impact customer trust and has financial and competitive implications. Data storage on unreliable media will be unrecoverable if data is lost. In the case of the inconsistent use of encryption keys, unauthorized parties will lead to the destruction of sensitive and confidential information.

Account or Service Hijacking: Unauthorized access to a system can be achieved by session hijacking. An attacker uses a valid session key or theft a cookie to hijack a session between a trusted client and network server. It is relevant to web application technologies weaknesses; the reuse of credentials and passwords amplifies the impact of this attack. Cloud solutions add a new threat to the landscape. With stolen credentials, attackers can eavesdrop on personnel activities, manipulate data and return falsified information. Account and service hijacking compromise the confidentiality, integrity and availability of Cloud computing services and data.

Abuse and Nefarious Use of Cloud Computing / Weak registration systems: By using a valid credit card, the Cloud customer can register and immediately begin using Cloud services including unlimited bandwidth and storage capacity. Otherwise, some providers offer their customers free limited trial period. By abusing the relative anonymity behind these registration and usage models, spammers, malicious code authors, and other criminals have been able to conduct their activities with relative impunity. Their impacts comprise password and key cracking, DDOS, launching dynamic attack points, hosting malicious data and botnet command and control.

Data locality: As businesses move towards the using and embracing of Cloud providers, the location of the data will become more and more important due to data privacy, legal, or regulatory demands [7]. For example, in many EU, certain types of data cannot leave the country because of potentially sensitive information. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (*e.g.*, country, state, or datacenter). Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architecture. On the other hand, data may not remain in the same data center, or within the same Cloud provider's systems. Data may even be stored in another country, incurring considerable concern [7].

Virtualized Environments: Due the Cloud virtualization, tenant's servers could reside on virtual machine within a resource pool shared by other customers of the same service provider. Since the hypervisor is the main resource of managing VMs and Cloud resources, attackers are targeting it to compromise and damage VMs and hardware. Isolation of VMs is necessary to maintain the security of users of the

same provider. In fact, virtualization expose them to the threat of malicious ones, vulnerability in one VM system can be exploited to attack other VM systems or the host systems. In addition, when VMs are connected to the host through virtual switch, intruders may be able to use a hacker technique to redirect packets going to or from the other VM for sniffing [29].

Table 2 shows how Cloud security vulnerabilities can be categorized based on impacted requirements.

Table 2. Impacted Security Requirement

Security threat	Impacted requirements
Insecure API	monitoring, confidentiality, service and data availability
Shared technology	confidentiality and privacy, system and network auditing, service and data availability
Abuse and nefarious use of Cloud computing	service and data availability, system and network auditing
Data loss or leakage	confidentiality and privacy, service and data availability, disaster recovery and business continuity, system and network auditing
Account or service hijacking	identity management, weak registration systems, service and data availability, system and network auditing
Malicious Insiders	confidentiality and privacy, service and data availability

4.2.2. True Story

Cloud is a much more inviting target for criminals than even company's traditional IT infrastructure. When companies outsource business processes, the Cloud provider is responsible for the security of any shared customer data [30]. Recent events expose the dark sides of Cloud computing for both businesses and consumers. This section discusses how already known attacks exploit Cloud service with weak security.

The case of the massive issue of Sony (a Cloud provider of entertainment services) [31] is sign that the Cloud industry may face new threats. The Sony breach is one of the biggest online data infiltrations that expose the personal data users of Sony's PlayStation Network, Sony Online Entertainment and Qriocity film and music service to potential identity theft. Sony disclosed on April 2011 that thieves had stolen account information of up to 77 million users on the PlayStation Network and Qriocity. A week later, the Sony Online Entertainment gaming service had also been breached, affecting an additional 24.6 million users. As a result Sony admitted that accounts appeared to be hijacked successfully and were subsequently locked down. In fact, hackers exploited known security vulnerability and use the stolen password data to gain access to user names, addresses, gender, birth dates and other information. The financial impact of the breach is estimated to be around 50 million dollars as a result of credit-card fraud, repairs to its network, marketing costs and reputational costs.

Epsilon is a Cloud-based online marketing service provider and a world's largest email service provider. In 2011, the breach of Epsilon has put the customers at risk from targeted phishing attacks. Spear phishing [34] occurs when a criminal sends an email convincing trusting readers to divulge identity information like social security numbers and credit card numbers. The breach fell to spear-phishing attacks which inject malicious code to a system through email attachments [32]. It affected data from 75 of Epsilon's client companies and exposed near 250 million customer emails. This case highlights that with the growth of Cloud services, one data breach can affect numerous organizations.

Cloud-based collaboration system Directors Desk Nasdaq system is designed to facilitate boardroom-level communications for 10,000 senior executives and company director [33]. In February 2011, attackers breached Directors Desk to have access to inside information which could sold to competitors or perhaps used to make beneficial stock market trades. Some analysts believe that the attackers probably exploit web application vulnerabilities to gained access or that internal staff conduct virtual insider trading to generate unfair profit.

Dropbox is an easy-to-use Cloud-storage service allowed approximately 25 million customers to store sensitive corporate information. In 2011, the Dropbox security breaches caused by an authentication code update highlights Cloud risks. For four hours, a site glitch leaves all of its customer data unprotected and exposed. Hackers used password exposed in breaches on another Web site to log into a Dropbox employee's account [34]. According to Dropbox less than a 100 accounts were accessed using this vulnerability and all accounts were accessed by a single individual.

In December 2009, a Zeus C&C server was hosted in Amazon EC2 Cloud delivering scalable compute capacity in the Cloud. Botmaster establishes a botnet by deploying bots from the original host to victims, it sets up Command and Control (C&C) server for collecting sensitive information from victim's machine. PCs will be infected with the malware and turned into zombies. Hackers were able to compromise a site on EC2 and use it as their own C&C operation. Then, a new variant of the Zeus banking Trojan has been spotted for infected machines. The issues included the inability of customers to access their data resulting in an interruption to their business and significant financial loss and even websites being shut down entirely.

Latest Yahoo data breach in 2012 [34] posted in clear text more than 400,000 username/password combinations. The account data was reportedly stored in an unencrypted state. The compromise involved a basic SQL-injection attack against an exposed Yahoo server. Yahoo confirmed that hackers had stolen credentials for Yahoo and other accounts, such as Google's Gmail and Microsoft's Hotmail. Password reuse across public and high-traffic social systems may have been the other motivation of this attack. The attack highlights the security' challenges of personal information.

In 2014, 80 million JP Morgan account holders have their records accessed in a Cloud related breach [35]. Personal information like names, addresses, email addresses and phone numbers of 76 million users and 7 million small businesses are accessed by the hackers. The bank said that the hackers didn't get any account information. It claims no unusual customer fraud is observed in the incident. Any user accessing the service, including websites and smartphone apps, are affected by the hack. Despite there being no evidence of fraudulent activity, JP Morgan stresses that the accessed information can still be abused by selling it to spammers.

These recent security breaches exploit vulnerabilities [36] present in the Cloud and affect organizations and customer as explain in the table 3.

Table 3. True Story

Event	Year	Affected customer	Vulnerabilities
Massive issue of Sony	2011	101.6 million	web application technologies weaknesses, Poor data control
breach of Epsilon	2011	250 million customer mails	Shared technology
Nasdaq system breach	2011	10,000 members	web application technologies weaknesses
Dropbox breach	2011	less than a 100 accounts	application technologies weaknesses
Amazon breach	2009	website in EC2' users	Weak registration systems, Malicious Insiders
Yahoo data breach	2012	400,000 username/password combinations	Poor data control for infected machines
JP Morgan Cloud server hack	2014	80 million accounts	web application technologies weaknesses

5. Attack Techniques against Cloud Infrastructure

The diversity of services that can be implemented based on Cloud computing is probably the major factor motivating the proliferation of attack techniques. In addition to financial gain, multiple aspects may be at the origin of malicious actions including organizational concurrence, political hacktivism, and privacy violation. In the following, a list of the most important attacks that can be conducted against Cloud infrastructures is given.

5.1. Attack on the Cloud

- Denial of service: According to multiple security survey reports [37], most of the attacks that are being conducted against information systems and communication networks belong to the Denial of Service (DoS) category. The major novelties regarding these attacks is that coordination is hybrid (*i.e.*, manual and automated) in the sense that public messages are broadcasted to Internet users to participate in the attack process. This allows users that do not have a technical background being involved in DoS attacks since they just have to download easy-to-use tools and

scripts. All what is required is time coordination so that the attack campaign puts down the victim resources. Perfect illustrations of such attacks scenarios are the operations conducted by the Anonymous groups against multiple governmental infrastructures. Other, and more technical, issues regarding these DDoS attacks are polymorphism and evasion. Multiple attacks vectors are sent to the victim infrastructures to enhance the efficiency of the DoS in terms of delay and probability of success. The most common vectors are:

- HTTP Get flood attack: targeting the web application resources and further modifying the target URL during the attack.
- TCP connection flood on port 80: targeting the web application resources
- SYN flood attack: targeting the server TCP/IP stack
- UDP flood attack: targeting network bandwidth resources
- Flooding attack: The computational servers in a Cloud system work with internal communication between them. The flooding attack [39] can engage the whole Cloud system just by interrupting the usual processing of one server. The attacker will overload the server through non-legitimate requests. To check the authenticity, CPU and memory will be consumed and legitimate services can starve. When server is overloaded, it transfers some of its jobs to a nearest service-specific server.

Evasion techniques are used by the attackers to bypass preventive and reactive security mechanisms. They break into four categories [38]

- Packet splitting: consists in splitting IP datagrams or TCP streams into non-overlapping fragments or segments. If the security system does not completely reassemble the IP fragments or TCP segments to restore the original application content, it may neglect an attack embedded in the content targeted at the victim host.
- Duplicate insertion: consists in inserting duplicate or overlapping segments (or IP fragments) to confuse the Intrusion Prevention Systems (IPSs) [38]. The efficiency of this technique depends on whether the victim handles the duplicate/ overlapping fragments as anomalies because the IPS lacks related information such as network topology and the victim's operating system.
- Payload mutation: Consists in transforming malicious packet payloads into semantically equivalent ones. The transformed payloads will look different from the signatures known and expected by the security system, so the attack can evade the detection.
- Shellcode mutation: consists in encoding a shellcode into polymorphic forms to evade a protection system that prevents/detects a shellcode according to the signatures extracted from one or a few variants of that shellcode.
- Accountability check problem: The payment method in a Cloud system is based on the recorded information about resources' use (duration of instance, amount of data transfer, and number of CPU cycles...). User accountability requires the linking of activities on an IT system to specific individuals and, therefore, requires the system to identify users. Customers should be satisfied and trust their charge for using the provider's services in order to build trust relationships in Cloud environment. When an attacker has engaged the Cloud with a malicious service or runs malicious code, the providers will charge the legitimate customer for a lot of computational power and storage [39]. Until the main cause of the resource usage is detected, the providers' business reputation still impacted.

  The most important attacks that can be performed at the application layer include SQL injection, Cross Site Scripting (XSS) attacks, and direct node injection [40].
- SQL injection attacks: is one type of attack which makes the entire data behind the web application and SaaS at risk. The attacker inserts into a standard SQL a

malicious code, gain unauthorized access to a database and become able to access sensitive information [6]. Sometimes the misunderstood input data allows web-site to be accessed by the SQL server. This lets attackers to have know-how of the functioning of the website and make changes into that.

- Cross Site Scripting (XSS) attacks [6]: Comparing to static web-sites, dynamic ones suffer from the security threats by providing multi-fold services to the users and get victimized by XSS attacks. When the attacker injects malicious scripts into Web contents, there is a high potential of intrusion into data. Some web pages or popups open up with the request of being clicked away to view the content contained in them. Curiosity users click on these hazardous links without verification and thus the intruding third party gets control over the user's private information or hack their accounts after having known the information available to them.
- Wrapping attack: The request made by the user from his VM through the browser is directed to the web server which generates a SOAP message. The body of the message contains the operation information supposedly signed by a legitimate user and the SOAP header should contain all the necessary information for the destination. The wrapping attack [39] consists of duplicate and sent the body of message to the server as a legitimate user. Using this privilege, the Signature value is duplicated by the attacker and used to check for the message. As a result, the adversary is able to interrupt the usual functioning of the Cloud servers and to run malicious code.
- Insider attacks: Insider attacks are the realization of the risk to companies, their data, their business partners and their long-term future caused by insiders becoming malicious and acting upon it. These attacks are orchestrated or executed by people that are trusted with varying levels of access to a company's systems and facilities. They also have intimate knowledge of the company's infrastructure which an external attacker would take a significant period of time to develop.
- Man-In-The-Middle/Cryptographic Attacks: Man in the Middle attacks is a class of traditional network attacks quite popular to SaaS. In such an attack, an intruder places himself between two users in communication. He can intercept and inject false information in data transferred between them. It is easier to target the application logic or framework of an application than the actual server behind the hardened network perimeter.

5.2. Attack using the Cloud

Cloud providers offer various types of services including unlimited bandwidth and storage capacity. These resources are available simultaneously to millions of customers anywhere in the world. However, the shared usage of resources raises new challenges. This part discusses how already known attack exploit Cloud service with weak security. Attackers can use Cloud as a platform to host malware and to crack passwords.

- Botnet: Botnet [41] is an example of attack running millions of infected computers, called bots, which upload spam and malware to thousands of computers. Botnets spread by systematically working through a list of IP addresses or dynamically scanning the machines and network space around them, seeking specific vulnerabilities.
- Cyber attack: Some Cloud service providers offer free limited trial periods that gives an opportunity for hackers to access the Cloud and use the computing power of Cloud to carry out powerful cyber attacks. Cloud can be used for attacks that are computationally expensive but highly parallelizable. For example, to perform a brute force attack on a number of passwords of that

magnitude requires tremendous computing power. Cyber attackers in "brute force attacks" send a constant stream of passwords at a computer system until it finds the correct code to enter. Unlimited Cloud resources enable attackers to successfully perform hash bruteforce and rainbow table generation.

- DDOS attack: The IaaS service supports a multitude of attacking machines. Using them together with specialized software ensures successful DDoS against target systems. This software should be responsible for intelligent loading of systems under attack.

6. Security Mechanisms

To deal with security issues, the Cloud provider must build up sufficient controls to provide such level of security. This part reviews the most important security mechanisms that have been proposed in the literature to protect Cloud computing systems.

6.1. Security Mechanisms for Cloud Computing

- Software isolation techniques: To reach the high scales of utilization and cost benefits and efficiencies desired, high degrees of multi-tenancy over large numbers of platforms are needed. Multi-tenancy in Cloud computing is typically done by multiplexing the execution of virtual machines from potentially different users on the same physical server. Applications deployed on guest virtual machines remain vulnerable to attack and compromise, much the same as their non-virtualized counterparts. Cloud providers have to ensure isolation of subscriber resources. Which is why we must understand the virtualization and other software isolation techniques that the Cloud provider employs.
- sHype [42]: The challenge is to share resources among VMs without compromising security. Hypervisors provide complete isolation between VMs, but it is not necessarily the best solution for efficient resource utilization and intercommunication between application workloads. sHype is a hypervisor security architecture that enables this secure resource sharing among VMs, it enforces Mandatory Access Control (MAC)-based security policy. MAC domains enable multiple coalitions to share a real resource by creating isolated virtual resources, it does not cause significant processing overhead. The sHype approach creates a flexible architecture with only around 11,000 lines of code.
- Mirage Image Management System [43]: VM images are shared by different and unrelated users in Cloud computing. Mirage Image Management System provides security and integrity of VM images. Each image in the repository has a unique owner, who can share images with trusted parties by granting access permissions. At publish time, filters remove or hide sensitive information from the publisher's original image. Mirage image management system implement a mechanism that tracks the derivation history of an image, it controls access to images and tracks the provenance of them. An image management system also ensure through image maintenance a periodic virus scanning of published images, that detect and repair vulnerabilities discovered.

6.2. Security Mechanisms for Cloud Storage

- Identity-based encryption: User data needs to be read by the intended users and protected from unauthorized access. To ensure securely share data for Cloud storage, cryptographic techniques have been researched. One fundamental technique is the identity-based encryption scheme, which enables a user specified by an identity to decrypt data. An Identity Based Encryption (IBE) system is a public key system where the public key can be an arbitrary string

such as an email address. A central authority uses a master key to issue private keys to identities that request them. The first construction for a hierarchical identity-based encryption (HIBE) system [42] was proposed by Gentry et al. It predefines user structure, and decryption keys are created following the structures. It is a generalization of IBE that mirrors an organizational hierarchy. An identity at level k of the hierarchy tree can issue private keys to its descendant identities, but cannot decrypt messages intended for other identities. A user can access a file only if the user's attributes satisfy the file's access structure.

- Process Isolation [42]: Data Protection focuses on the need of data privacy and isolation, as data from different customers resides on common data center in Cloud computing platforms. Data needs to be carefully treated so that it cannot be mixed with another user. Information flow control (IFC) tags data entering the system and isolates the data belonging to different users.
- Homomorphic encryption: Because the execution of programs is distributed by nature in Cloud computing, users cannot be certain where their input and output data is managed. This raises confidentiality and privacy issues that are not fully solved by existing security solutions. An approach proposed in [44] uses a homomorphic token with distributed verification of erasure-coded data towards ensuring data storage security. This approach supports dynamic operations on data blocks such as: update, delete and append without data corruption and loss. The application of Homomorphic encryption is an important brick in Cloud Computing security, this allows addressing the crucial problem of delivering a program that can be executed by a third-party without revealing confidential data. The uses of homomorphic encryption have also been assessed in other contexts where the confidential information is split into multiple pieces that are processed independently by multiple entities [45]. It lets anyone manipulate what is encrypted, even without knowing the secret key. It is a form of encryption where a specific algebraic operation performed on the plain text is equivalent to another (possibly different) algebraic operation performed on the ciphertext. Moreover, it is efficient against data modification and server colluding attacks as well as Byzantine failures. It achieves the storage correctness insurance as well as data error localization. However, it is still rather impractical due to its high computational complexity and large communication cost [46]. Malicious server location is possible using the tokens generated through homomorphic cryptosystems. However, granularity is the most important weakness of data isolation systems since the existing approaches are not efficient when the size of the data subject to attacks is small.

6.3. Security Mechanisms for Cloud Networking

- Border Gateway Protocol: In [47], a Border Gateway Protocol (BGP) architecture has been suggested to detect the cases where an autonomous system may announce itself wrongly as the destination for all the data that is being transferred over that network. This allows the implementation of anomaly detection and incident response mechanisms in Cloud computing environments. GRADUS tool can help to detect the source AS of the problem and respond. It also gives us the flexibility to run the secure BGP protocol on some of the autonomous systems in order to protect the whole network. The use of this approach should be accompanied by additional protection techniques since it is itself vulnerable to DoS attacks.
- Network segmentation: VMs from different customers may reside in the same physical network through which data traffic generated by VMs is transported. In order to overcome this issue, techniques as network virtualization through

VLAN or other logical network segmentation are applied. It segregates and isolates traffic among different user groups or subnets.

- Encryption mechanism: Customers will need to have a way to access their resources that are located within the Cloud and be able to manage those resources in a secure manner. Therefore, it is incumbent upon the Cloud provider to supply the customer with a management portal that is encrypted. Secure sockets layer (SSL) and transport layer security (TLS) would be the most common tool for Web traffic.

  Table 4 exposes different security requirements ensured through the adoption of each security mechanisms presented above.

Table 4. Security Mechanisms

Mechanisms/ Requirements	Software isolation techniques	sHype	Mirage Image	Homomorphic encryption	Process isolation	Border Gateway Protocol	Identity-based encryption
Service and data availability	-	-	+	++	+	-	-
Confidentiality and privacy	++	+	++	+++	+	+	++
Identity management	-	-	-	-	-	-	+
Disaster Recovery	-	-	+	-	-	+	-
Resilience	+	-	+	++	-	+	-
Risk tolerance	+	-	+	-	-	-	-
Cost effectiveness	+	++	+	-	+	+	+

8. Conclusion

Regardless of the various benefits provided by Cloud services, several privacy and security related questions have reduced the adoptability of Cloud. The diversity of the services delivered through Cloud infrastructures increases their vulnerability to security incidents and attacks.

Through this paper, we explain what Cloud computing is, including Cloud deployment models and service models and discuss Cloud advantages. We exposed Cloud security requirements and vulnerabilities afterwards we explore the attack techniques against Cloud infrastructure. The security mechanisms are then divided into three categories: computing, storage and networking.

References

[1] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication, vol. 800-144, **(2011)** December.
[2] "Flying Blind in the Cloud the State of Information Governance", Ponemon Institute, European Network and Information Security Agency, **(2010)**.
[3] "Security of Cloud Computing Providers Study", Ponemon Institute, **(2011)**.
[4] P. Mell and T. Grance, "The NIST Definition of Cloud Computing", National Institute of Standards and Technology, Information Technology Laboratory, **(2011)**.
[5] M. A. Morsy and J. Grundy. "An Analysis of the Cloud Computing Security Problem", Proceedings of APSEC 2010 Cloud Workshop, **(2010)** November 30, Sydney, Australia.
[6] R. Bhadauria, R. Chaki, N. Chaki and S. Sanyal, "A Survey on Security Issues in Cloud Computing", CoRR, vol. abs, **(2011)**.
[7] V. Winkler, Elsevier Inc, "Securing the Cloud Computer: Security Techniques and Tactics", **(2011)**.

[8] S. Kounev, P. Reinecke and F. Brosig, Springer Verlag, "Providing Dependability and Resilience in the Cloud: Challenges and Opportunities, Resilience Assessment and Evaluation", Dagstuhl Seminar **(2012)**.
[9] D. Catteddu, "Security & Resilience in Governmental Clouds - Making an informed decision", ENISA Re- port, **(2011)**.
[10] J. Forum, "Cloud Cube Model: Selecting Cloud Formations for Secure Collaboration", **(2009)** April.
[11] D. S. Linthicum, "Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide", Addison-Wesley Information Technology Series, **(2009)**.
[12] Z. Huang, C. Mei, L. E. Li and T. Woo, "CloudStream: delivering high-quality streaming videos through a cloud-based SVC proxy", IEEE Infocom, **(2011)** April, USA.
[13] C. M. Robertson, B. MacIntyre and B. Walker, "An Evaluation of Graphical Context as a Means for Ameliorating the Effects of Registration Error", IEEE Transactions on Visualization and Computer Graphics, vol. 15, **(2009)**.
[14] Y. Chen, Z. Du and M. Garcia-Acosta, "Robot as a Service in Cloud Computing". Proceedings of the 2010 Fifth IEEE International Symposium on Service Oriented System Engineering, **(2010)**, USA.
[15] G. Briscoe and A. Marinos. "Community cloud computing", Proceedings of the 1st International Conference on Cloud Computing, CloudCom, **(2009),** Beijing, China.
[16] R. Ghosh, F. Longo, V. Naik and K. Trivedi "Quantifying resiliency of Iaas cloud", In Reliable Distributed Systems", 29th IEEE Symposium on, **(2010)** November; New Delhi.
[17] S. Ramgovind, M. M. Eloff and E. Smith, "The Management of Security in Cloud Computing", Proceedings of Information Security for South Africa, **(2010)**.
[18] H. Tianfield, "Security issues in cloud computing", IEEE International Conference on Systems, Man, and Cybernetics (SMC), **(2012)**.
[19] B. Sosinky, Wiley, "Cloud Computing Bible", **(2011)**.
[20] A. Cavoukian, "Privacy in the Clouds" A White Paper on Information and Privacy Commissioner of Ontario, **(2008)**.
[21] D. Catteddu, "Security & Resilience in Governmental Clouds - Making an informed decision", ENISA report, **(2011)**.
[22] M. Armbrust, A. Fox, R. Gri_th, A. D. Joseph and R. Katz, "A View of Cloud Computing", Communications of the ACM, vol. 53, no. 4, **(2010)**.
[23] K. Ruan, J. Carthy, T. Kechadi and M. Crosbie, "Cloud forensics: An overview", Proceedings of the 7th IFIP International Conference on Digital Forensics, **(2011)**, USA.
[24] S. Zimmerman and D. Glavach, "Cyber Forensics in the Cloud", IA Newsletter, vol. 14, **(2011)**.
[25] M. Medhioub and M. Hamdi, "Security of Cloud Computing", IGI, **(2014)**.
[26] "Cloud Security Alliance", Top Threats to Cloud Computing, **(2013)**.
[27] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Proceeding of Journal of Network and Computer Applications, **(2011)**, UK.
[28] M. K.Srinivasan, K. Sarukesi, P. Rodrigues, M. S. Manoj and P. Revathy, "State of- the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment", Proceedings of the International Conference on Advances in Computing, Communications and Informatics- ACM, **(2012)**.
[29] R. L. Krutz and R. D. Vines, Wiley, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", **(2010)**.
[30] A. Webinar, "White Paper", The Liability Issues of Cloud Computing Service Providers, CNA, **(2012)**.
[31] J. Walter, "Latest Yahoo Data Breach Restates Need for Basic Security", **(2012)**.
[32] "Privacy Rights Clearinghouse", Datta Breaches: A Year in Review, **(2011)**.
[33] M. J. Schwartz, "Nasdaq server breach: 3 expected findings, informationweek", **(2011)**.
[34] J. Kincaid, "Dropbox Security Bug Made Passwords Optional For Four Hours", TechCrunch, **(2011)**.
[35] "CNN, PMorgan: 76 million customers hacked", **(2014)** October, http://money.cnn.com/2014/10/02/technology/security/jpmorgan-hack/.
[36] Cloud Security Alliance, "Top Threats to Cloud Computing", **(2010)**.
[37] Radware, "Global Application and Network Security Report", **(2011)**.
[38] T-H. Cheng, Y-D. Lin, Y-C. Lai and P-C. Lin, "Evasion Techniques: Sneaking through Your Intrusion Detection/Prevention Systems", IEEE Communications Surveys and Tutorials, Issue 99, **(2011)**, pp. 1-10.
[39] G. Kulkarni and N. Chavan, "Cloud Security Challenges", 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA), **(2012)**.
[40] M. Hamdi, "Security of Cloud Computing, Storage and Networking", IEEE International Conference on Collaboration Technologies and Systems (CTS), **(2012)**.
[41] A. Comazzetto, "Botnets: The Dark Side of Cloud Computing", Sophos, **(2012)**.

[42] T. Takahashi, "Enabling secure multitenancy in cloud computing: Challenges and approaches", In 2nd Baltic Congress on Future Internet Communications (BCFIC), **(2012)** April, Vilnius.
[43] J. Wei, X. Zhang, G. Ammons, V. Bala and P. Ning, "Managing security of virtual machine images in a cloud environment", Proceedings of the 2009 ACM workshop on Cloud computing security, **(2009)**.
[44] C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring Data Storage Security in Cloud Computing", In 17th International workshop on Quality of Service, **(2009)**, USA.
[45] M. Gomathisankaran, A. Tyag and K. Namuduri, HORNS: "A homomorphic encryption scheme for Cloud Computing using Residue Number System", In 45th Annual Conference on Information Sciences and Systems, **(2011)**, USA.
[46] C. Aguilar-Melchor, S. Fau, C. Fontaine, G. Gogniat and R. Sirdey, "Recent advances in homomorphic encryption", Proceedings of IEEE Signal Processing Magazine, **(2013)**.
[47] J. Karlin, S. Forrest and J. Rexford, Elsevier, "Autonomous Security for Autonomous Systems", Proceeding of Complex Computer and Communication Networks, vol. 52, no. 15, **(2008)**, NY, USA.

