Cloud Basics and Security

Eder Scheid, Bruno Rodrigues, Burkhard Stiller

Communication Systems Group CSG, Department of Informatics IfI,
University of Zürich UZH, Binzmühlestrasse 14, CH-8050 Zürich, Switzerland
[rodrigues¦rafati¦scheid¦stiller]@ifi.uzh.ch

Abstract

Cloud computing is a major technology in the Information and Communication Technology (ICT) due to its large computational capacity, which can be provisioned on demand. However, its security challenges, briefly overviewed in this document based on the different cloud service models, are the most important and challenging ones as they prevent companies from using or migrating their services to cloud computing platforms. To fully understand the nature of its security challenges, however, it is necessary to understand the basic aspects of cloud computing. In this sense, this document aims to introduce these basic cloud aspects, as well as the security challenges organized by service models, and their respective security recommendations.

1. Cloud Basics

On a daily basis, basic services such as water, electricity and telephone are charged according to their use by the consumer, i.e., a price is paid according to the personal or business demands of those who use these services. Cloud computing follows the same concept, making customers pay for the utilized computing services. This dynamism offered by cloud computing provided a continuous growth to the model, making it widely adopted by different companies and organizations in order to reduce costs provided by the traditional data center model. Conversely, this growth also exposes some of the shortcomings that the model has, among them that of security, which according to is one of the main factors for the adoption of cloud solutions.

Cloud computing is the result of a set of technologies that arrived at the market before a specific terminology had been established, which led several organizations

to establish their own definitions and characteristics related to cloud computing. Nonetheless, among the various terminologies the most accepted definition to describe is the one provided by NIST (SP 800-145):

> *"Cloud computing is a model that allows for ubiquitous, convenient, on-demand network access to a configurable set of shared computing resources that can be quickly provisioned and released with minimal management effort or service provider interaction."*

This definition concisely bases the purpose of cloud computing, determining that by any device with access to the Internet, which is convenient to the user and at any time, a set of physical or virtual computational resources must be available to the user, releasing or provisioning more resources according to its needs, *i.e.,* on-demand. In this regard, the major cloud computing characteristics are summarized as:

1. **On-demand service**: users can automatically define the provision of the computing capacity on-demand, such as server time and network storage, as needed, without human interaction with each service provider;
2. **Broad network access**: resources are available on the network and are accessed by the customer through various platforms, *e.g.*, mobile phones, and laptops;
3. **Resource pooling**: computing resources (storage, processing, memory, bandwidth and virtual machines) of the provider are grouped to serve multiple users. These resources (physical or virtual) are allocated dynamically and according to consumer demand;
4. **Rapid elasticity**: resources can be quickly provided to be scaled. The user has the impression that the available resources appear to be unlimited and can be acquired in any quantity, at any time;
5. **Measured service**: the cloud controls and optimizes the use of resources by providing metrics according to the type of service being provided. Both the provider and the consumer can monitor and control the use of resources.

These characteristics define the expected behavior from the services provided in cloud, providing in a combined manner, flexibility and availability along with a reduced cost for the user (in contrast to a traditional data center model). The resource pooling and rapid elasticity are characteristics related to the provision and

management of cloud resources to the user, characteristics of fundamental importance to the cloud, as these should convey the impression to the user that the resources of the cloud are unlimited. The characteristic that is responsible for assigning resources to the user is that of a resource pooling, which must always guarantee the availability of hardware required by the rapid elasticity, which manages the requests made by the user, allocating or releasing resources according to the customer's necessity.

The on-demand service characteristic is one of the most relevant for customers, as one does not need to hire a package of services that may not be completely used, or to hire another entire package in case of use. Thus, similarly to the model used in daily services, this characteristic ensures that only the resources used are charged. This type of service, called *pay-as-you-go* has become common in several areas, as one pays for the use of a service or resource and not a flat fee for a period of time as, for example, in traditional hosting.

Beside the different service models detailed in Section 2.2, there are different types of cloud deployment models whose choice of use depends on the particularities, business objectives, or type of information to be stored by each organization. Clouds are usually classified according to the location of the infrastructure and the access of its users. Hence, the location determines whether the resources are private (when they belong to a single organization), or public (when distributed across multiple organizations). NIST (SP 800-145) determines four types of deployment:

1. **Public**: characterized by exposing computational resources in the form of services that can be contracted by users. The cloud infrastructure is made available over the Internet to the general public or to a large industrial group and is managed by an entity that sells cloud services. For this reason, access restrictions regarding network management cannot be applied, and even less, apply authentication and authorization techniques;
2. **Private**: the cloud infrastructure is used exclusively by a single user or organization. It is usually built on a private data center and can be managed by the user/organization or by third parties. The members of the organization have exclusive use of computational resources, obtaining greater reliability and confidentiality regarding information and critical data.

Although it brings some conveniences for being in a private environment, this model requires internal management, increasing costs and leaving the system in a frozen in terms of automation of tasks such as updates;

3. **Community**: used when several organizations have similar requirements (security conditions, security policies, and others) and decide to share part of their infrastructure. This can be managed by organizations participating in the community or by a third party, in local or remote implementation;
4. **Hybrid**: any type of combination of two or more of the previous categories. It is characterized by behaving as a public cloud and also as a private cloud, combining these two concepts.

Each type of deployment has its benefit according to the objectives of those who are contracting the cloud service. Private clouds ensure greater security over stored assets and greater control over them since the cloud is maintained on a private network. Public clouds, offer greater efficiency for shared resources, but as it is exposed to the general public, their security must be efficient and well planned. The community approach can be understood as a cloud of clouds, in which organizations share their clouds and one can access the other, and finally, the hybrid approach that can combine the characteristics of two or more deployment approaches.

When choosing to use a private cloud, the organization keeps its data limited to an internal access ensuring that its level of security is “high”, since the management and use of the cloud are performed by the organization itself. When using a hybrid cloud, an organization allows its private cloud to communicate with a cloud (public or private) of unknown management, making the level of security a lower due to the exchange of data with an entity whose security policies are unknown. The public cloud is the type of cloud that has the lowest security level, as it is open to any user profile that knows the location of the service. For this reason, wider access restrictions cannot be applied regarding network management, and even less, apply authentication and authorization techniques.

2. General Scenario Overview

The “Cloud” – from now on simplified as cloud – is described as a set of online services, which are accessible across a network from almost all locations such that the service user is not aware of the physical location of these services. Note that one of these services may be “storage” such that a cloud may be considered as a

decentralized and distributed storage system, in which any data in electronic form – and at no specified format – can be stored. In turn, the data sharing principle across domains and platforms had seen an implementation of larger relevance, since technology-independent solutions (especially, independent of hardware differences and software/operating system alternatives) had been developed. The so-called cloud-based virtualization can help companies to reduce the number of machinery (typically counted as separates computers or systems) as well as software licenses they need to operate. Clouds regularly result in a more efficient and less costly way of performing re-occurring tasks and running dedicated businesses.

Almost all IT (Information Technology) resources (software and data as well as hardware) can be operated within the cloud. A program, an application, a service, a dedicated operating system, or an entire infrastructure can be “cloudified.” For instance, if a lawyer wants to set-up an IT infrastructure for handling his/her clients’ documents and data, the installation of appropriate software and services on local servers could be done. Alternatively, software, services, and a networking resource can be set-up in a cloudified manner to make them accessible to the lawyer only – under the assumption of appropriate access control schemes – or in case of needs third parties who are offered access credentials within the cloud. As shown in Figure 1, two lawyer’s offices 1 and 2 operate their local infrastructure for their employees. The cloudification made here enables the storage of the data with a so-called Cloud Provider (CP), who specializes in a reliable, trustworthy, and typically efficient write and read storage access. Thus, the data – typically organized in documents – are encrypted on the company’s side (indicated by the lock next to the document’s icon, while the keys known are only known to the lawyer’s office or even an individual user there) and transmitted across the network – here determined as the public Internet – in an encrypted manner. This example indicates that these two lawyer’s offices operate with their own separate keys (only known to each of them, generally only known to the lawyer’s office utilizing them), but do use the same CP’. These data are stored within the cloud provider’s infrastructure in a locked – encrypted – manner, such that the CP does not have a realistic chance to read the content of these data.

Even thought that the data from offices 1 and 2 are stored in the same CP infrastructure, office 1 cannot access the data from office 2 because it does not possess the key to decrypt the data; the same principle applies for office 2. If the CP infrastructure eventually compromised, the data leaked will not have any meaning

without the right decryption key. Note, as with all keying material as well as credentials used in the digital world, the likelihood to guess one such key is not zero, but highly unlikely, thus the risk is minimal if strong security mechanisms have been deployed. The same risk assessment holds basically true for any traditional safe deposit boxes, which need a number to be opened, which an attacker may have guessed or stolen beforehand.

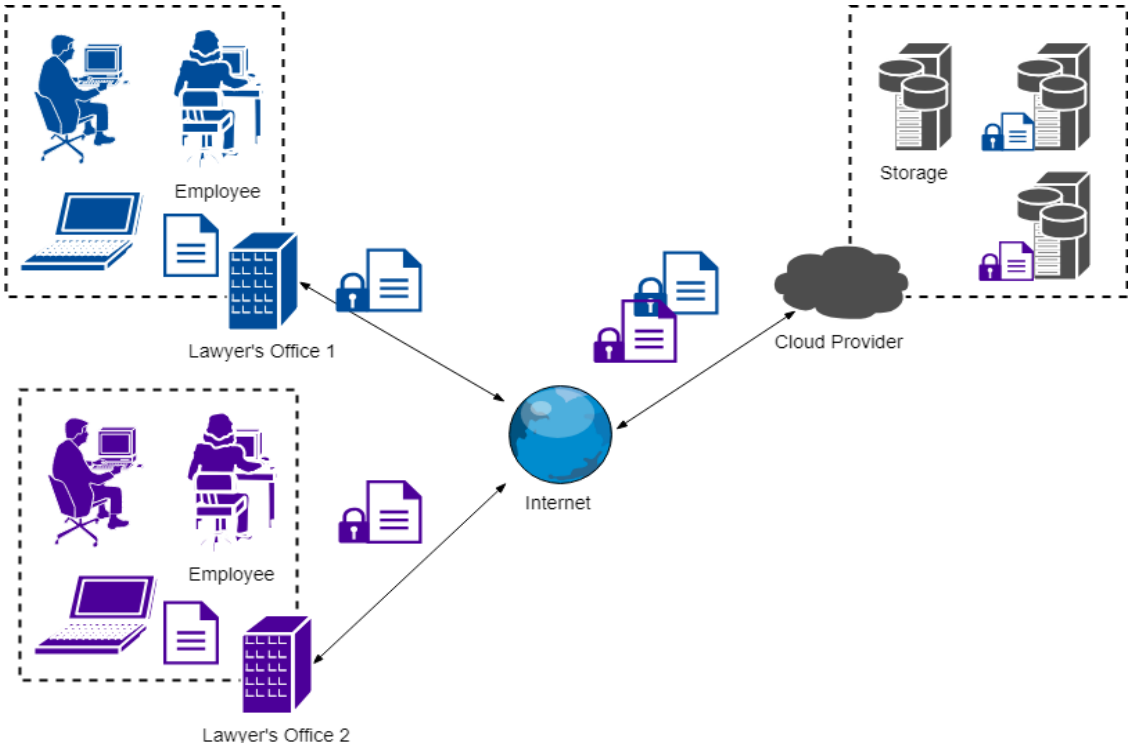

Figure 1: General Cloud-based Principle

2.1 Cloud Computing Models

Cloud service models refers to how the configurable set of cloud computing resources are organized and delivered to the user, i.e., how the entire manageable set of features can satisfy user conveniences. Among various commercial definitions for these service models, NIST, CSA and ENISA have defined as standard the categorization of these services into three main categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS), as seen in Figure 2.

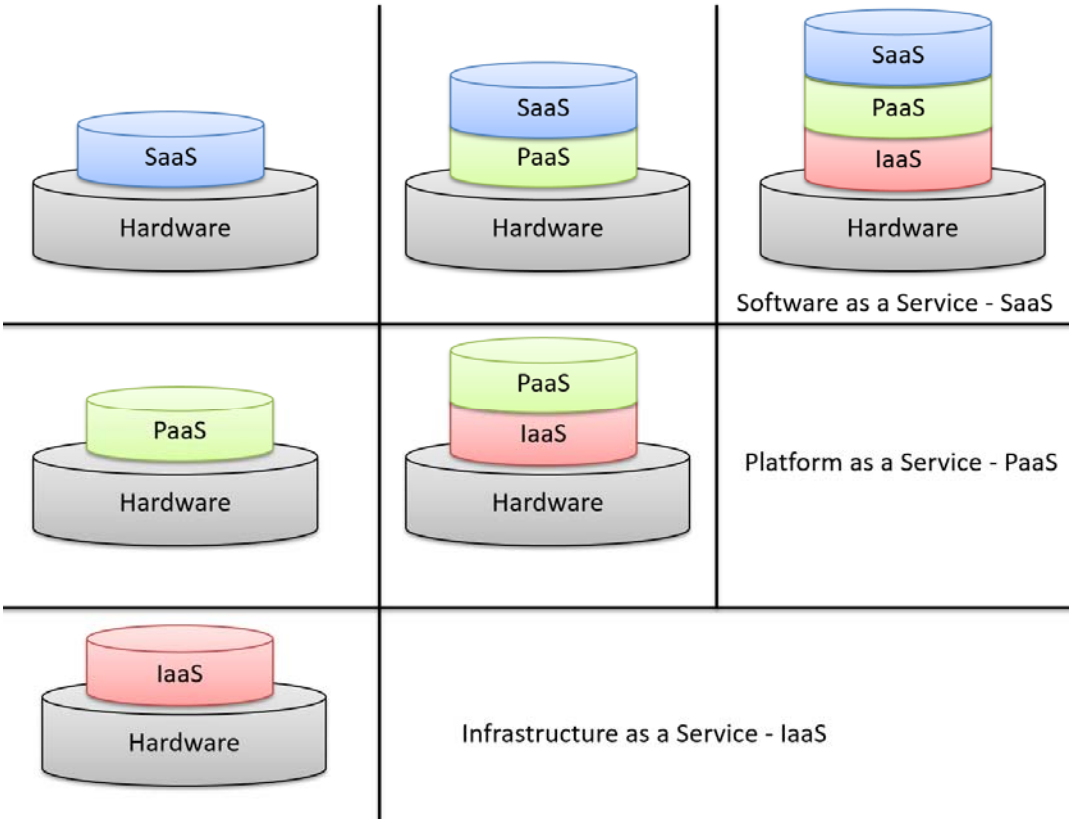

Figure 2: Cloud Computing Service Models

Figure 2 assists in the general understanding of how service models can be offered to a customer. Starting with the servers, the hardware on which all service abstractions are implemented. The IaaS model, being the most basic abstraction of the cloud services, is provisioned through Virtual Machines (VMs) in which the user can choose not only the configuration to be used, but also the type of service (compute, storage, networking). A VM is a software abstraction of a physical server providing the necessary environment (environment) to run user applications. In the IaaS model, a user is able to request one or multiple VMs that are hosted in one or multiple servers at the cloud provider infrastructure (c.f. hardware in Figure 2).

The PaaS model can be offered as a platform only, containing the support and management framework for cloud applications, or both PaaS and IaaS together. SaaS services can be offered in three different ways, only hosting an application, hosting an application combined with PaaS or SaaS, PaaS and IaaS.

These three service models characterize what can be offered in each cloud service abstraction layer, making more specific models to be encompassed in one or more of these three service categories. In addition, these service models can be grouped in different ways, as well as the resources to make them available, as shown in Figure 2. As such, it is possible to provide a cloud service from other cloud services or from a specific infrastructure for these purposes.

2.1.1 Software-as-a-Service (SaaS)

The software-as-a-service (SaaS) service model delivers the final cloud computing service, i.e., the consumer-ready web-based application. In this model a Lawyer's office does not manage or control the underlying layers of services, only the application itself (text processing, presentation slides) and all associated software and data are centrally stored, facilitating cloud management and support for applications.

2.1.2 Platform-as-a-Service (PaaS)

It has benefits for application developers as they can rent the hardware to deploy, test and make their applications available in tools and languages that are supported by the cloud provider. The purpose of this model is to reduce the costs and complexity of dealing with the hardware of the underlying layer. However, a major inhibitor of PaaS is the fact that applications developed in a PaaS usually "locked-in" with the vendor, causing applications to be "locked" only with a cloud provider. This fact deserves attention from potential users when choosing a PaaS solution.

2.1.3 Infrastructure-as-a-Service (IaaS)

It aims to deliver the cloud computing resources (e.g., compute, storage, networking) to meet users' needs, it is the most basic model of the services offered by the cloud. Lawyer's office, for instance, could use and/or deploy any software, including operating systems, as long as they do not control or manage the basic infrastructure of the cloud, they are also free to deploy and use applications.

IaaS is an interesting option when the business objective needs a computational infrastructure, such as a data center, but that maintaining this infrastructure is not necessary. The demand for these computational structures and the high price to maintain them generated a need for specialized IaaS providers, doing maintenance and management tasks (physical space, air conditioning,

connectivity, electricity, network, physical and logical security, among others) are left to the service provider and the user can focus directly on their business objective

2.2 Security Measures of Cloud Computing Models

Under the assumption that specifically lawyers' demands are considered to use the cloud storage service (Scenario 1) mainly, however, cloud-based computing technology alternatives are relevant as well (Scenario 2). Thus, word processing, data spreadsheet handling, and slide preparation software, may be operated on data stored within the cloud, too. In turn, the implementation alternatives for these two scenarios within the dedicated cloud computing model selected may follow explicitly the SaaS or IaaS path.

2.2.2 SaaS, PaaS and IaaS Security Measures

The choice of the service model has a great influence on the security measures over customer's data, as depicted in Figure 3.

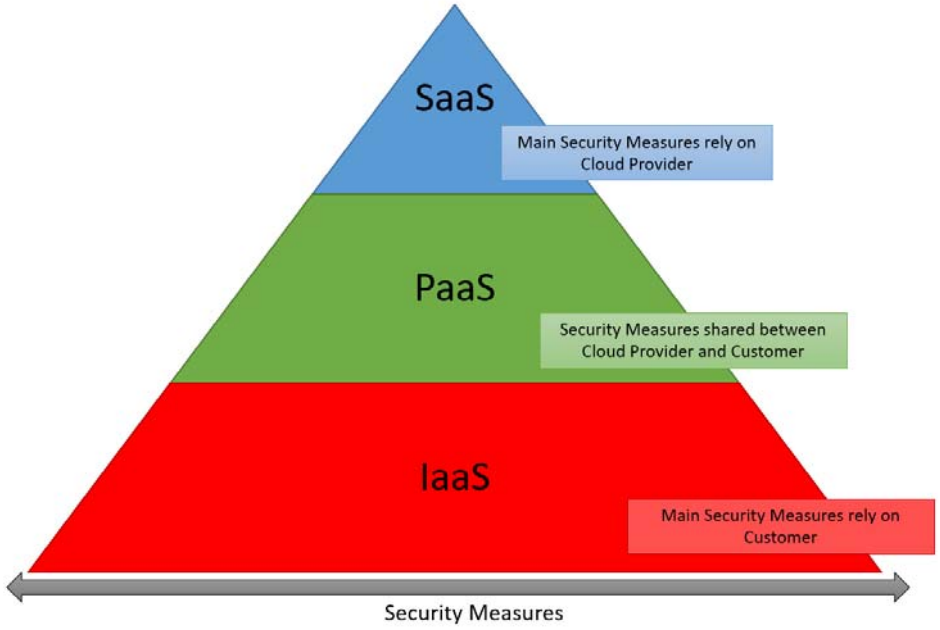

Figure 3: Service Models Shared Security Measures from Customer's point-of-view

- **IaaS**: the cloud provider provides one or more VMs to the customer, which has responsibility for all configuration and management of applications running on the (provided) infrastructure. Therefore, most of the measures regarding confidentiality and integrity rest on the customer configuration. It should be

noted, however, that there is still responsibility of the cloud provider to guarantee that the data stored in customer's VMs are not accessed by other users' VMs including the provider itself (confidentiality) and that this data is available whenever requested (availability).

- **PaaS:** the responsibility is shared since the infrastructure and the platform is delivered by the Cloud Provider and it is up to the customer to configure the environment in the cloud. In this regard, the responsibility is shared because the cloud provider should maintain customer's data and configuration confidential inside the infrastructure and available whenever the customer requires and the customer is responsible for the configuration of the platform and the safety implications they may cause.
- **SaaS:** the customer has a minimal security responsibility in contrast to IaaS and PaaS. In this model, all service configuration is transparent to the customer which is only responsible for the security of your access credentials to the service. Aspects of confidentiality (partial), integrity and availability are the sole responsibility of the service provider.

2.2.3 Scenario 1 Security Measures

Figure 4 indicates two dedicated instances of a suitable cloud storage model. The top indicates that the storage of the data itself may not be performed locally within the company anymore, but with a cloud provider. Here, the transmission across the network is performed in a secured – especially encrypted – manner, which utilizes an HTTPS (Hypertext Transmission Protocol Secure) approach under the exploitation of TLS (Transport Layer Security), which deploys a strong (128 bit) or even stronger (256 bit) key size.

TLS is the updated version of SSL (Secure Socket Layer) 3.0, which was deprecated by the IETF (Internet Engineering Task Force) in the document RFC7568. Thus, it is advised that all communication that relies on HTTPS must employ TLS as encryption protocol. The data itself reaches the cloud provider in Internet Protocol (IP) packets while being encrypted in transit. As soon as the cloud provider stores them in its local infrastructure, the data are encrypted with a local key of the cloud provider.

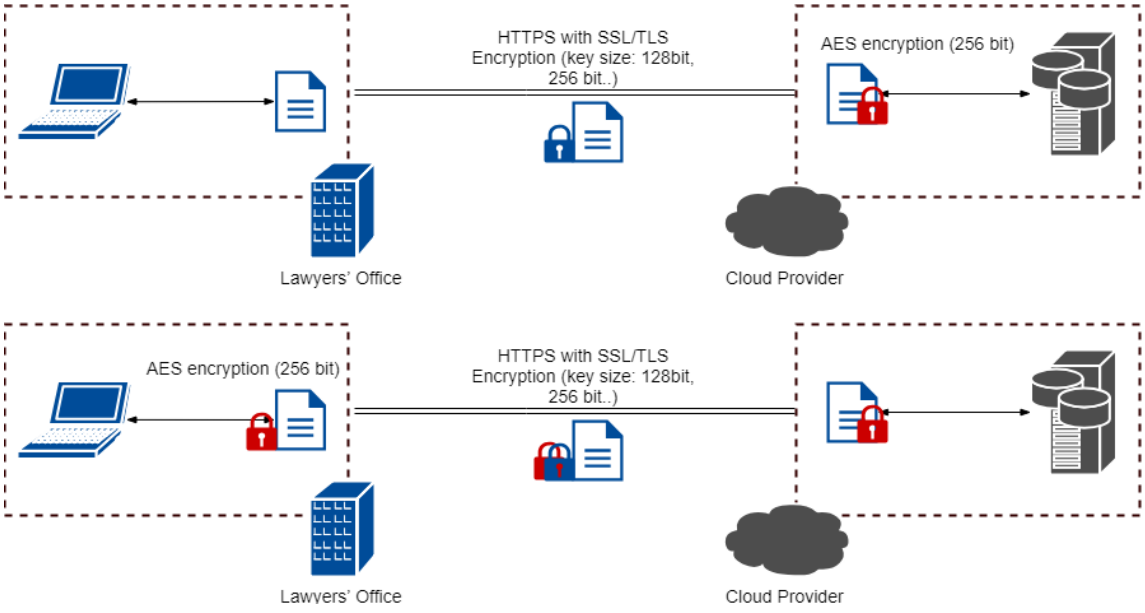

Figure 4: IaaS Cloud-based Storage with Different Key Management Approaches

Alternatively, the bottom part of Figure 2 indicates that already encryption of the data may be performed by the company before transmitting them across the network. Thus, the company only will have access to the data, as it is now responsible for the key management. All other steps for an encrypted transmission and the storage at the cloud provider's side remain unchanged, except for the fact that the cloud provider does not need to encrypt the data before their storage anymore. During transit, the data is protected twice – with the company's key and the HTTPS SSL/TLS key as deployed.

As cloud computing – especially cloud storage included – brings not only the advantages of the combination of different technologies but also several potential vulnerabilities. Technologies, such as virtualization mechanisms, have not been developed specifically for the cloud computing model, but they have been adapted to cloud computing to maximize the use of available resources.

2.2.4 Scenario 2 Security Measures

In Scenario 2, depicted in Figure 5, a Lawyers' Office could utilize tools, such as word processing, data spreadsheet handling, and slide preparation software in a SaaS model. In such a model, the cloud provider could host the software in a dedicated VM to the office. The data between the office and the cloud provider is transmitted using HTTPS with SSL/TLS. However, this data is not a file or document, as in Scenario 1, but it is information provided by the customer, such as actions in the

software (e.g., copy, paste, edit, new file, save, and so on). The document, once it is saved in the software, is encrypted and stored by the cloud provider using a different key for each customer. It is important to notice that in this SaaS model, the cloud provider may have access to the data saved in the document, but not other customers because the document is stored with different keys, providing data isolation. For instance, when using Google Docs suite, the content of documents are visible to the provider, but not to other customers using the service. Therefore, it is not a recommended service for customers that deal with sensitive, confidential documents.

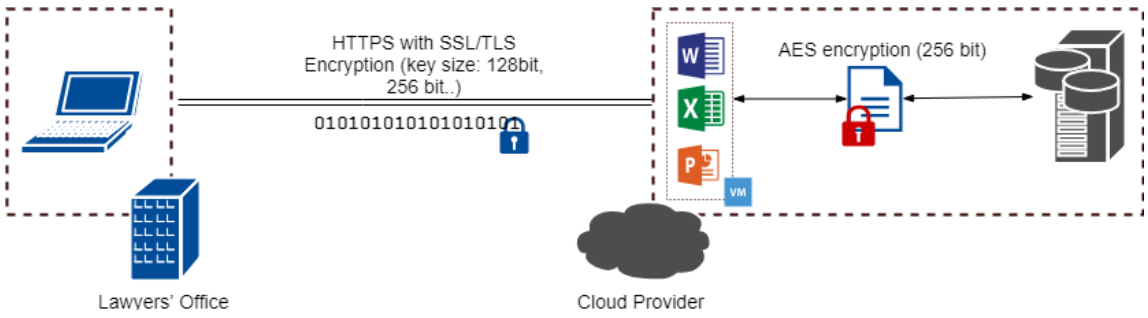

Figure 5: SaaS Cloud Provider with Security Mechanisms

2.3 Cloud Security Guidelines and Best Practices

These facts can lead to vulnerabilities – if no countermeasures are considered – that could expose stored data and could compromise the confidence in the cloud computing model and the cloud-based storage of data. A certain uncertainty regarding the reliability of the data stored in the model is considered a great obstacle for the adoption of cloud computing by many organizations and companies. Thus, cloud security is subject to several particular areas of research as well as part of commercially available cloud solutions, which propose adequate solutions to the set and wider range of security-related problems.

Note explicitly that a traditional storage of data within a lawyer's office was performed (a) on type writers, (b) later on desktops, and (c) in many cases laptops or mobile devices. While for (a) the paper-based documents had to store in safety-deposit boxes (either at the offices themselves or in the basement of a certain building with physical access mechanisms), desktop's security and mobile device's security is not only impacted by the IT approach applied (see above). It is heavily affected by the user's behavior, the lawyer or their employees, and the use of strong

credentials for logins, for data storage devices, or processing programs. While desktops typically do not leave offices and, thus, are under the same access control schemes as locally stored paper, laptops and mobile devices bear the risk of being stolen, while on travel, or being lost, while in transit, or being misused, while leaving them unattended and unlocked for a coffee break. Thus, the user's security understanding is the weakest part of the organizational aspects of any IT system, anf thus cloud services, too.

Therefore, the following security guidelines are evaluated concerning the list of the security concerns in the cloud storage model:

1. **NIST:** "*Guideline on Security and Privacy in Public Cloud Computing*" (JANSEN and GRANCE, 2011);
2. **CSA:** "*Security Guidance for Critical Areas of Focus in Cloud Computing v3.0*" (CSA, 2011);
3. **ENISA**: "*Benefits, Risks and Recommendations for Information Security*" (RYCK *et. al*, 2011).

3. NIST Security Guideline

The (JANSEN and GRANCE, 2011) guide states that organizations using a private cloud computing approach have a greater level of control over data. Thus, the document focuses on public cloud models. It provides an overview of cloud services, discussing cloud model benefits and problems from a security standpoint, indicating key security and privacy issues, and providing recommendations on outsourcing data to any cloud computing provider.

Key Points	Issues
1. Governance	
2. Compliance	**2.1** - Laws and regulations **2.2** - Data location compliance **2.3** – Electronic discovery
3. Trust	**3.1** – Internal Threats **3.2** – Data property **3.3** – Compound services **3.4** – Visibility **3.5** – Auxiliary data

Key Points	Issues
	3.6 – Risk management
4. Architecture	**4.1** - Monitor protection of VMs (hypervisor) **4.2** - Virtual network protection **4.3** - Auxiliary data protection **4.4** - Customer protection
5. Identity and Access Control	**5.1** – Authentication **5.2** – Access control
6. Software Isolation	**6.1** - VM quality monitor **6.2** - Tenant VM threats (co-tenant)
7. Data Protection	**7.1** - Data Isolation **7.2** - Secure Data Exclusion
8. Availability	**8.1** - Interruptions **8.2** – Denial-of-Service attacks
9. Accident Liability	

Items 1 and 2 deal with “Governance and Compliance”. Governance is the set of policies, functions, responsibilities, and processes that must be established to guide, direct and control how the organization uses technologies to achieve corporate goals, *i.e.*, a set of standards set to achieve a specific goal. Compliance covers topics that endeavor to verify that the organization meets the standards, laws, and regulations in question. Item 3 covers topics such as: Internal Threats (item 3.1), internal users or tenants that pose a risk to the ownership of the organization's internal data; Property Data (item 3.2) that are in the cloud and their intellectual property of the data residing in the cloud; the Visibility Gain (3.4) on the security controls used by the cloud provider; Risk Management (3.5).

Item 4 relates to architectural issues discussing software systems used in cloud computing. The description of security point initiates by warning that the introduction of virtual machine monitors (hypervisors, item 4.1) increases the attack surface in cloud computing compared to the traditional data center model. Subtopic 4.2 states that traffic over virtual networks should not be visible traditional network security tools such as firewalls, intrusion/prevention detectors, and so on. The need for special tools that are dedicated only to address these virtual networks is affirmed. In 4.3 it is stated that data on virtual machine images and cloud services may contain

information relevant to attackers and therefore require special care. Section 4.4 discusses the security of the client's web browser.

Identity and Access Control (item 5) focuses on the use of Security Assertion Markup Language (SAML), which is a standard for the exchange of authentication and authorization data between domains, and XACML (eXtensible Access Control Markup Language) for Access Control (item 5.2), which describes a policy language as well as a format for request and response messages. Item 6, Software Isolation, discusses threats that are related to the multi-tenancy feature (multi-tenant). The data protection approach (item 7) starts with highlighting the differences between the multi-tenancy model, in which the data of different users are placed in a single repository, and the multi-instance model in which each user uses and manages a separate data repository (item 7.1). After that, the issue of Safe Data Exclusion is addressed (item 7.2). In the discussion on Availability (item 8), a report was prepared on indirect threats from the sharing of the same cloud provider, with an organization that has a high potential to suffer a Denial-of-Service attack (DoS, item 8.2). As a result of multi-tenant support, these types of attacks can result in problems with the availability of cloud services. The last issue addressed is that of accident liability, which should result in an analysis to confirm the occurrence of an accident or determine the methods to provide the documentation with the necessary details and care to ensure traceability and that data integrity is maintained. In addition to the security issues survey, NIST also defined recommendations for each key point defined. The recommendations can be seen in the Table below.

Key Points	Recommendations
1. Governance	Increase organizational practices pertaining to policies, procedures, and standards used for application development and cloud service provisioning.
2. Compliance	Comprehend the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impacts on cloud computing initiatives, particularly those involving data localization, privacy and security controls, and more.
3. Trust	Ensure that service agreements have sufficient means to enable visibility into the privacy and security control processes and their performance. Clearly establish ownership rights over the data.

Key Points	Recommendations
	Establish a risk management program that is flexible enough to adapt constantly. Continuously monitor the state of information security to support risk management.
4. Architecture	Understand the lower layer technologies that the cloud uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the entire life cycle of the system and its components.
5. Identity and Access Control	Establish appropriate measures to ensure the security of authentication, authorization, and other identity and access control functions.
6. Software Isolation	Understand virtualization and other logical isolation techniques that the cloud provider uses in its multi-tenant architecture, and evaluate the risks involved for the organization.
7. Data Protection	Assess the competence of the cloud provider data management solutions for the organizational data involved, and the ability to access data, to protect stored, in transit, and in use data, and to exclude data.
8. Availability	Know forecasting and contract procedures for availability, data backup, disaster recovery, and ensure they adhere to the organization's continuity and contingency planning needs.
9. Accident Liability	Understand the forecasts and procedures in the contract for accident liability, ensuring that they comply with the requirements of the organization. Ensure that the provider has a transparent response and sufficient mechanisms to provide information before and during the accident.

4. Cloud Security Alliance Security Guideline

The CSA (Cloud Security Alliance) is a non-profit organization founded in late 2008 in an initiative to strengthen cloud computing security following an information security conference. Its founding members are mainly industrial representatives, corporations, associations such as Dell, HP, and eBay. One of its goals is to promote the adoption of best practices to promote security in cloud computing environments.

The guide begins with an editorial note that briefly describes the steps required to verify that an organization is ready for the transition to the cloud model. This editorial note consists of identifying and evaluating assets for cloud model deployment, mapping resources to verify possible deployment models (public/ private/hybrid), evaluating potential cloud providers, and more. The document identifies thirteen domains between these sections and several subtopics within these sections. The table below comprehends the domains and subtopics presented in the guideline.

Key Points	Issues
1 - Governance and Corporate Risk Management	**1.1** - Governance; **1.2** - Business Risk Management; **1.3** - Information Management; **1.4** - Management of Outsourcing.
2 - Legal Aspects: Contracts and Electronic Discovery	**2.1** - Legal Aspects; **2.2** - Contract Considerations; **2.3** - Questions Raised by Electronic Discovery.
3 - Compliance and Audit	**3.1** - Conformities; **3.2** - Auditing.
4 - Information Management and Data Security	**4.1** - Data Security; **4.2** - Location of the Data. **4.3** - Information Management; **4.4** - Data Security Lifecycle; **4.5** - Information Governance.
5 - Interoperability and Portability	**5.1** - Introduction to Interoperability; **5.2** - Introduction to Portability.
6 - Traditional Security, Business Continuity and Disaster Recovery	**6.1** - Internal Threats; **6.2** - Physical Security of Human Resources; **6.3** - Business Continuity; **6.4** - Disaster Recovery.
7 - Datacenter Operations	**7.1 –** Datacenter Operations.
8 - Liability for Accidents, Notices and Corrections	**8.1** - Cloud Characteristics that generate Responsibility on Accidents; **8.2** - Architectural Safety Model as Reference; **8.3** - Cycle of Examination of Responsibility on Accidents.
9 - Secure Applications	**9.1** - Safe Development Cycle; **9.2** - Authentication, Authorization and Compliance; **9.3** - Application Access Identity and Management; **9.4** - Invasion Tests for Applications.
10 - Key Management and Encryption	**10.1** - Data Encryption in Transit; **10.2** - Data Encryption at Rest;

Key Points	Issues
	10.3 - Data Backup Encryption; **10.4** - Secure Key Storage; **10.5** - Access to Key Storage; **10.6** - Backup and recovery of keys.
11 - Identity and Access Management	**11.1** - Identity Provisioning; **11.2** - Authentication; **11.3** - Federation; **11.4** - Authorization and Management of User Profiles.
12 – Virtualization	**12.1 -** Hypervisor architecture.
13 - Security as a Service	**13.1** - Ubiquity of the Service; **13.2** - Implementation Concerns; **13.3** - Benefits of Implementing Security as a Service; **13.4** - Diversity of Services that Can Be Categorized.

The Governance, item 1, and Business Risk Management are concerned with the organizational processes of information security. Service Level Agreements (SLAs) are discussed in detail in this area, specifying which security requirements should be specified in the SLA and enforced by a contract. For Risk Management, the document is cautioned not to evaluate only the cloud vendor, but also third parties (the services that are outsourced by the provider) with whom the provider is involved.

Items 2 and 3 are discussing compliance with government regulations, organizational standards, legal aspects (e.g., intellectual property, responsibilities), among others, establishing how these rules can influence the internal security of the organization. Section 4 describes several subtopics related to data manipulation, such as Security (Item 4.1), Location (item 4.2), Information Management (item 4.3), among others, establishing how data should be managed to avoid vulnerabilities that can expose the stored data. A discussion on Portability and Interoperability (item 5) begins with a specification of possible reasons to migrate the data to the cloud model, also states that cloud computing still lacks standardization of several factors, causing difficulty for the interoperability of services, and hence the difficulty of transition between cloud providers. It is worth highlighting the contribution of open source cloud platforms to this factor, which contributes to the increase of

interoperability between providers through the diffusion of their codes and interfaces (such as OCCI (Open Cloud Computing Interface)).

In item 6 the CSA researchers discuss the organization's Internal Threats, Disaster Recovery, Business Continuity claiming that the SLA alone is not enough to meet the user's needs for security, requiring a constant verification of the pillars of security (confidentiality, integrity, and availability). Datacenter Operations (item 7) primarily addresses the issues that should be considered when choosing the cloud provider, and CSA recommends attention to the following issues: auditing, availability, performance, patch management, compartmentalization, and support. In the discussion of the next issue, Responsibility on Accidents (item 8), an informational report on incident detection tools and analysis is developed to obtain information from the tools for incident prevention.

In Section 9, Secure Applications, the Application Development Cycle (item 9.1) is described and in the following subtopics techniques to ensure the security of information such as (Authentication, Authorization, and Conformities - item 9.2), identity management (item 9.3), among others. The CSA recommends it in this field, the vulnerability assessment through invasion tests (item 9.4) to ensure application security. In the topic on Encryption and Key Management (item 10), emphasis is given to the security of the communication between hosts, even with the internal communication in the network of the provider, warning that due to the characteristic of multi-tenancy the question of the management of keys it becomes even more complicated, and cloud consumer attention is needed in this regard.

Item 11 performs an introduction to cloud identity verification by identifying aspects that must be taken into account when implementing a cloud identity mechanism, highlighting the difficulty of scalability in the model. Also in this domain is explicitly dealt with Identity Provisioning (item 11.1), Authentication (item 11.2), among others. Item 12 addresses security issues related to virtual machines, the security of the hypervisor, and so on. The paper concludes with a discussion of Security as a Service (item 13), which highlights the differentiation of the cloud computing security model from the traditional data center model. The domain addresses issues such as implementation practices, benefits of implementing security as a service, and the variety of services that can be categorized as security as a service.

In addition to surveying the political/legal, and technical aspects surrounding the concept of cloud computing, the CSA made a recommendation for each topic covered, called domains in its document. The table below shows the security recommendation for each domain.

Key Points	Recommendations
1 - Governance and Corporate Risk Management	Reinvest money saved by cloud adoption to improve cloud provider security, applications, audits and audits. Metrics and standards to measure performance and effectiveness of information security management.
2 - Legal Aspects: Contracts and Electronic Discovery	Not found in document.
3 - Compliance and Audit	Use auditors specialized in the cloud model; Contracts must provide a third party review on metrics, SLAs, and conformities.
4 - Information Management and Data Security	Understand the storage architecture in question, choose the size of the data dispersion when available; monitor internal databases; encrypt all important data when performing a migration, among others.
5 - Interoperability and Portability	Comprehend how a VM can be captured and inserted into new cloud providers; identify and eliminate any specific extensions of cloud providers; understand the costs of migrating data from one server to another; among others.
6 - Traditional Security, Business Continuity and Disaster Recovery	Cloud consumers should not depend on a single provider; vendors of IaaS should have contracts with multiple platform vendors and have tools for quick recovery in case of incidents; Automatic data validation or allow users to perform through validation protocols; among others.
7 - Datacenter Operations	Possess management of processes, machines, practices, and software to understand and react to technology running within the datacenter; understand the mission of what is running within the datacenter; Understanding which parties should be responsible for the conformities set out in the SLA; among others.
8 - Liability for Accidents, Notices and Corrections	Cloud consumers should understand how providers define the events of interest in relation to security incidents and what events / incidents are reported to users; Consumers must have a means of communication with the provider in case of incidents; among others.
9 - Secure Applications	Perform risk analysis for the applications; detailed survey of attack vectors and risks in the cloud environment; seek to develop and maintain a secure software architecture; among others.
10 - Key Management and Encryption	Use good key management practices; Scope keys can be maintained on an individual and group level; use standard encryption algorithms, among others.

Key Points	Recommendations
11 - Identity and Access Management	All attributes used must have a level of trust; all attributes must be connected to an identity; developers should ensure that the services have import / export function following standards such as XACML; among others.
12 – Virtualization	Consumers should identify the type of virtualization that the provider uses; developers should encrypt VM images when they are not in use; VM's default settings must follow the minimum security requirements set; among others.
13 - Security as a Service	Developers should have a secure channel of communication among tenants; vendors must provide automatic security notification; consumers should request third parties to broker the SLA negotiation and audit the services; among others.

5. ENISA Security Guideline

The ENISA (European Network and Information Security Agency) is an organization that aims to enhance the capacity of the European Union, the member states of the European Union and the business community to prevent, address and respond to information security issues and networks. The guide starts with a specification of the benefits of cloud computing from the perspective of security, listing the benefits of security in cloud computing. Next, a description of risk analysis and assessment process is performed based on three use case scenarios: (i) small and medium-sized cloud computing; (ii) the impact of cloud computing on service resilience; and (iii) eGovernment cloud computing. This analysis is based on the probability of incident scenarios with an estimate of business impact and risk levels (low, medium, high). The list of security issues contains risks that are specific to the cloud computing model, as well as risks related to other technologies. The security issues relevant to cloud computing are presented in the table below.

Key Points	Issues
Political and Organizational Issues	**1** - *Lock-in*;
	2 - Governance;
	3 - Compliance;
	4 - Loss of Business Reputation Due to Tenants;
	5 - Termination or Failure of the Cloud Service;
	6 - Cloud Provider Acquisition;
	7 - Supply Chain Failure.

Key Points	Issues
Technical Issues	**8** - Exhaustion of Resources;
	9 - Fault Isolation;
	10 - Internal Threats;
	11 - Interface Management;
	12 - Interception of Data in Transit;
	13 - Data Leak in Upload and Download;
	14 - Deletion Without Effect or Unsafe Data;
	15 – Distributed Denial-of-Service
	16 – Economic Denial-of-Service;
	17 - Cryptographic Key Loss;
	18 - Capture of Probes or Malicious Scans;
	19 - Service Engine Commitment;
	20 - Conflicts between Customer Procedure Hardening and the Cloud Environment.
Legal Aspects	**21** - Electronic Discovery and Judicial Intimations;
	22 - Risks of Jurisdictional Changes;
	23 - Risk of Data Protection;
	24 - Licensing Risks.

The list of political and organizational issues begins with the discussion of the lock-in issue (item 1), which reports the portability status among cloud providers in each service category in the cloud (IaaS, PaaS, and SaaS). After this, Governance (item 2), Conformities (item 3) and indirect threats of users who are using the same vendor (item 4 - loss of reputation due to tenants) are discussed. It is highlighted that availability challenges can be the result of issues of the cloud vendor itself (items 5 and 6) or third parties that the vendor trusts (item 7).

The list of technical issues begins with threats resulting from Exhaustion of Resources (item 8) such as the inability to provide resources (agreed upon in SLA or additional) to customers, unavailability of services, among others. Item 9 addresses failures in mechanisms that isolate shared resources between users (hypervisor failures). Following are the vulnerabilities they because that may lead to internal threats, such as malformed roles and responsibilities, operating system vulnerabilities, inadequate physical security procedures, and so on.

Some of the risks presented can be more broadly grouped, such as interface management (item 11) and service engine commitment (item 19) that address the security of applications listing vulnerabilities in the cloud provider's software. Network traffic interception (item 12) is also analogous to upload and download data leakage, discussing the interception of data by vulnerabilities in the cloud provider infrastructure or the user link.

Denial-of-Service (DoS) threats are presented as two risks in the document: distributed denial of service (item 15 - Distributed DoS), when an attack causes problems of availability, and denial of service (item 16), when malicious service requests increase traffic on the network causing an increase in the cost of services for the cloud user. Other technical issues such as detection of malicious probes and malicious scanners (item 19) to the cloud infrastructure, and insufficient consumer efforts to ensure cloud security (item 20) complete the list of technical issues addressed by ENISA. The list of legal issues begins with procedures for responding to electronic discovery and court subpoenas (e.g., the government may have to request some data stored in the cloud for some reason - item 21). The other three questions (items 22, 23 and 24) describe concerns about data manipulation, such as Location Conformance (item 22), Protection (item 23), and risks from loss of intellectual property of data stored in the cloud (item 24).

6. Classification of Selected Cloud Provider Offerings

The classification of eight Cloud Providers had been performed with respect to the following criteria:

1 Governance
2 Compliance
3 Trust
4 Architecture
5 Identity and Access Control
6 Software Isolation
7 Data Protection
8 Availability
9 Accident Liability

and is shown in the following table, indicating as far as available all relevant details such that an evaluation of these services can be reached.

	Key Points								
Cloud Provider	Governance	Compliance	Trust	Architecture	Identity and Access Control	Software Isolation	Data Protection	Availability	Accident Liability
DSwiss AG (securesafe)		1) 2 data centers in Switzerland which comply with FINMA 2) built in accordance with the NIST and BSI security guidelines		Security architecture has been made openly available with multiple testing by third parties	1) Secure logging from anywhere with Two-step login procedure (mobile TAN) 2) EV SSL certificates		1) HTTPS 2) AES-256 and RSA-2048 encryption standards 3) Secure remote password protocol of RFC 2945 4) Zero Knowledge	Location indepentent	data stored in 3 copies in two defferent places
Tresorit AG			1)The non-convergent cryptography used by Tresorit makes it impossible to determine when your content matches others' content in the cloud, which could leak valuable data about you to outside observers. 2) Transparent data provisioning ellabotated in the following report: https://web.tresorit.com/l#ZhG0I68mgTUb4II9L0R8HA		1) With the admin pannel, users can be grouped and their activites are monitorable. 2) 2 factor authentication		1) The encryption algorithm used by Tresorit is AES256 in CFB mode. 2) Each file version gets a new, randomly generated 128-bit IV to semantic security guarantee. The encryption keys of files and folders are modified from time to time using a so-called "lazy re-encryption" scheme. This means that after changes in the membership composition of a team, the encryption key is recreated the next time contents of a file are edited (see patent WO 2012/131407 A1)	Location indepentent	
Econis AG		1)Geo-redundant data management guaranteed in Switzerland 2) Process framework that meets the FINMA requirements						Guaranteed availability	1) Central backup solution 2) SLA-based response times and on-site support
Abraxas Informatik AG		Depending on personal data processing, in addition to the applicable Swiss law (Federal Data Protection Act (DSG) of 19 June 1992, SR 235.1), European data							
FileSync GmbH		Server located in EU and Switzerland		Not Provided		Not Provided	Communication to server with SSL 128bit. Cloud encryption with AES 256bit (Zero Knowledge). Local cache encrypted as well (128bit)	Deleted Data Mantained for 30 days	
green.ch AG (Nextcloud)		Server located in Switerzland		NextCloud on Dedicated VM		Virtualization	Encrypted data transfer with 256-bit SSL encryption. Encryption of data on the cloud server	Data backup in multiple data centers	
ProCloud AG		Server located in Switerzland		Not Provided		Not Provided	Encryption your data is encrypted on the system 2048bit. Zero Knowledge	We guarantee an uptime of 99% in our business drive	
MTF Swiss Cloud AG		Server located in Switerzland		Not Provided		Virtualization	Data are transferred encrypted and stored encrypted. Neither third parties nor MTF can access this data, (alone controlled key). No Information on technology	Redundant Datacenter,	