

Cloud Computing Security

Case Study

Saumya Gupta
Michel Müller
Liu Qian
Ajita Gupta

December 13, 2011

Advisor: Dr. Christian Slamka, Detecon Consulting
Supervisor: PD Dr. Hannes Lubich

Computer Engineering and Networks Laboratory, ETH Zurich

Abstract

Cloud Computing has become a trend in IT and is being adopted by an increasing number of companies. In this case study, we have identified the key characteristics, models and security issues of cloud computing and contrasted these to a traditional setting. We have analyzed the application portfolio of SwissTec, the leading manufacturer of packaging equipment, and recommended a deployment model for each element. Finally, we have suggested a four-step implementation procedure for SwissTec to migrate its resources to the cloud.

Contents

1 Cloud Computing - An Overview	4
1.1 Definition	4
1.2 Characteristics	5
1.3 Service Models	6
1.4 Comparison of Computing Approaches	6
1.5 Security Implications	8
2 Cloud Deployment Models	9
2.1 Overview	9
2.2 Infrastructure	9
2.3 Advantages and Disadvantages	10
2.4 Costs	11
3 Security Challenges and Risks	12
3.1 Common Challenges	12
3.2 Common Countermeasures	12
3.3 Model-specific Analysis	14
4 Application Portfolio Analysis	15
4.1 E-Mail	15
4.2 Website	16
4.3 Intranet	16
4.4 File Server (Network Share)	16
4.5 Computer-Aided Design (R&D)	17
4.6 Customer-Relationship-Management	18
4.7 Financial Accounting and Payroll	18
5 Migration to the Cloud	20
5.1 Planning	21
5.2 Negotiation	22
5.3 Migration	22
5.4 Operation	23
6 Conclusion	24
Bibliography	25

List of Figures

1.1	Cloud Computing Architecture	5
5.1	The 4-Step Migration Approach	20

List of Tables

1.1	Traditional Computing versus Cloud Computing	7
1.2	Pros and Cons of Computing Approaches	7
1.3	Security Implications of Cloud Computing	8
2.1	Realization comparison of Cloud Models	10
2.2	Advantages and Disadvantages of Cloud Models	10
2.3	Costs for Cloud Deployment Models	11
3.1	Cloud-specific Security Challenges and Countermeasures	14

Chapter 1

Cloud Computing - An Overview

In this chapter, we provide a comprehensive introduction to Cloud Computing, the paramount focus of our project, and the various security issues related to it.

1.1 Definition

Cloud Computing is the current trend. "*It has become the phrase du jour*", says a senior analyst at **Gartner**¹, the world's leading Information Technology research and advisory company.

Cloud Computing is an evolving term that describes the development of many existing technologies and approaches to computing. A cloud separates application and information resources from the underlying infrastructure and the mechanisms used to deliver them.

More precisely, a cloud describes the use of a collection of services, applications, information and infrastructure (comprising computation, network, information and storage resources). These components can be rapidly orchestrated and provisioned; offering an on-demand utility model of allocation and consumption.

There are many definitions today which attempt to address Cloud Computing from the perspective of academics, engineers, managers and consumers. We focus on a definition that is most suitable to IT network and security professionals (as given in [1]).

The U.S. National Institute of Standards and Technology (NIST) defines Cloud Computing by describing five essential characteristics, three cloud service models and four cloud deployment models. These are summarized visually in Figure 1.1 and explained in the next few chapters.

¹<http://www.gartner.com/technology/home.jsp>

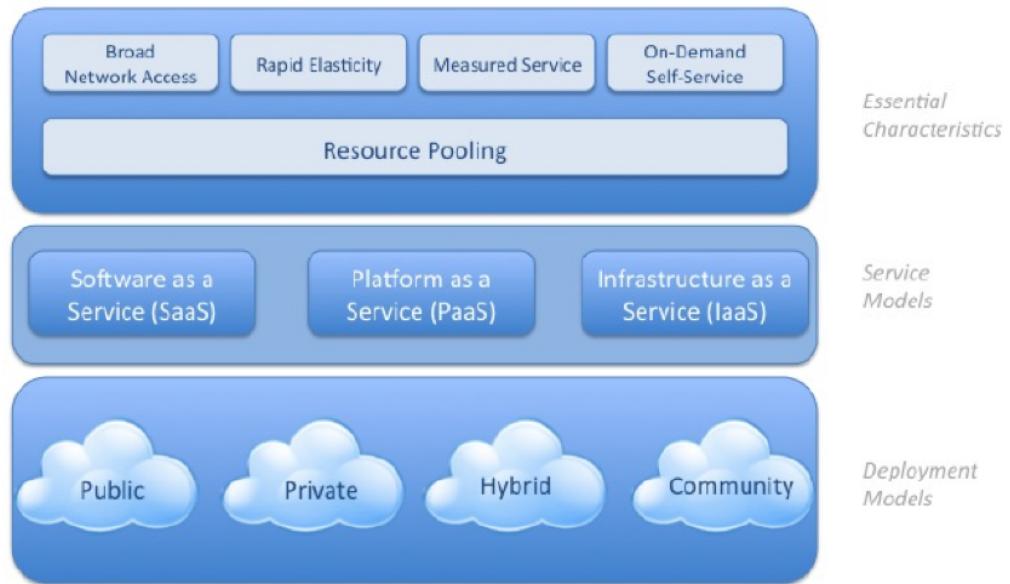


Figure 1.1: **Cloud Computing Architecture.** This figure (adopted from [2]) shows the complete model of Cloud Computing as described by NIST.

1.2 Characteristics

Below is a list of the five key features of this phenomena along with a brief description.

1. On-Demand Self Service

A client can unilaterally provision computing resources as needed ‘on-the-fly’ without explicit interaction with the cloud provider.

2. Broad Network Access

Infrastructure is available over the network and can be accessed over conventional devices and platforms (e.g. laptops, PDAs, mobile phones) and software services.

3. Resource Pooling

The provider’s computing resources are collected to serve multiple customers using a multi-tenant model. Concrete examples of resources include storage, processing, memory, network bandwidth and virtual machines. Users can connect to systems using a conventional platform, irrespective of their current location, since the infrastructure is located off-site (typically provided by a third-party service provider).

4. Scalability

Resources and infrastructure can be provided elastically to an unlimited extent (from a practical point of view).

5. Measured Service

Cloud systems control and optimize resource usage by leveraging a metering capability appropriate to the type of service (e.g. storage, processing, bandwidth).

1.3 Service Models

Cloud services can be classified into three fundamental categories, often referred to as the ‘SPI Model’.

1. Software as a Service (SaaS)

The client is given the capability to run applications on a cloud infrastructure offered by the provider. He is free from management and control issues of the underlying architecture (network, servers, operating systems, storage), but has the option of adapting application configurations to his needs.

2. Platform as a Service (PaaS)

PaaS is defined by the capability of deploying tailored applications that were created using tools and languages supported by the provider. The client does not manage the underlying infrastructure, but is in command over the deployed applications, as well as certain hosting environment settings.

3. Infrastructure as a Service (IaaS)

This service provisions the client with fundamental resource pools using virtual machines. The client is then able to run arbitrary software (e.g. operating systems, web applications, etc.) on top of these VMs. The client is given the highest amount of control in this case. However, the control over networking components (e.g. host firewalls) is still restricted by the provider.

1.4 Comparison of Computing Approaches

In this section we compare the two primary computing approaches based on defining criteria (see Table 1.1) and outline their major advantages and drawbacks, as shown in Table 1.2.

Criteria	Traditional Computing	Cloud Computing
Tangibility	physical servers, data centers, networks and specifications in near proximity	virtual pool of computing resources deliverable over the network
Flexibility	fixed set of resources	IT services are available on demand and an as-needed basis
Scalability	new requirements are met by acquiring new infrastructure.	real time (partially automated) scaling of resources according to current load
Pricing	"Plans" (allocate a set of resources to each user)	measured service ("Pay for what you use")

Table 1.1: Traditional Computing versus Cloud Computing

	Traditional Computing	Cloud Computing
Advantages	<ul style="list-style-type: none"> ⊕ dedicated system → no competition/resource sharing ⊕ with skilled IT personnel → support and control 	<ul style="list-style-type: none"> ⊕ unlimited resources → allow traffic spikes, high scalability, load balancing ⊕ multiple points of failure → high availability ⊕ maintenance included → easy/regular updates ⊕ convenient collaboration for geographically dispersed or mobile workforce
Disadvantages	<ul style="list-style-type: none"> ⊖ single point of failure → low availability ⊖ without skilled IT personnel → no support and control 	<ul style="list-style-type: none"> ⊖ huge workload, short downtime → high maintenance/operational costs ⊖ server-intensive applications → slower loading times ⊖ no bandwidth guarantees

Table 1.2: Pros and Cons of Computing Approaches

1.5 Security Implications

As cloud computing is achieving increased popularity, concerns are being raised about security issues introduced through the adoption of this new model. The effectiveness and efficiency of protection measures are being reevaluated, since the elements of this innovative deployment scheme differ widely from well-known traditional architectures.

This section provides a collection of potential threats and cures as recommended by the *Cloud Security Alliance* (see [3] for more details) with regard to the traditional security triad - **Confidentiality**, **Integrity** and **Availability** (as shown in Table 1.3).

	Attack Vector	Sanitation
Confidentiality	<ul style="list-style-type: none">- malicious insiders- gain inappropriate level of control on the underlying platform- anonymous data access<ul style="list-style-type: none">- data leakage- account / service hijacking	<ul style="list-style-type: none">- transparency through compliance reporting- strong isolation of individual architectures- access control, logging<ul style="list-style-type: none">- encryption- prohibition of user ↔ service credential sharing
Integrity	<ul style="list-style-type: none">- improper authorization- data loss (on unreliable media)	<ul style="list-style-type: none">- strong authentication, monitoring- specify backup strategies
Availability	<ul style="list-style-type: none">- Denial of Service attacks	<ul style="list-style-type: none">- resource redundancy

Table 1.3: Security Implications of Cloud Computing

Chapter 2

Cloud Deployment Models

In this chapter we examine and evaluate different cloud deployment models with respect to various criteria: infrastructure, advantages, disadvantages and costs.

2.1 Overview

1. Public clouds

Cloud computing services offered by a service provider over the internet to the general public are called public clouds.

2. Private clouds

When the cloud computing infrastructure is used by a single organization it is considered to be a private cloud.

3. Community clouds

Cloud infrastructure that is being shared by member organizations of a specific community (e.g. organizations with a common interest) are called community clouds.

4. Hybrid clouds

Hybrid clouds represent a combination of multiple clouds (private, community or public). They can also be seen as a chain of cloud systems that facilitate the migration of from one deployment system to another.

2.2 Infrastructure

Table 2.1 gives an overview over the managing party, the ownership characteristics and the location of the infrastructure given in different cloud models.

	Managing Party	Ownership	Location
Public	third party	third party	off-premise
Private	self or third party	self or third party	on-premise or off-premise
Community	self or third party	self or third party	on-premise or off-premise
Hybrid	self and third party	self and third party	on-premise and off-premise

Table 2.1: Realization comparison of Cloud Models

2.3 Advantages and Disadvantages

Table 2.2 lists the advantages and disadvantages for all cloud deployment models. The financial aspect is excluded as of now and will be discussed in more detail in Section 2.4.

	Advantages	Disadvantages
SaaS (Public cloud)	<ul style="list-style-type: none"> ⊕ highest efficiency in resource sharing ⊕⊕ fastest time to market ⊕⊕ easiest deployment of new software releases ⊕⊕ easiest enablement of home- and mobile access 	<ul style="list-style-type: none"> ⊖⊖ lowest level of control ⊖⊖ company-specific functionality might be lost ⊖ only internet bandwidth available
IaaS (Public cloud)	<ul style="list-style-type: none"> ⊕ full control over software 	<ul style="list-style-type: none"> ⊖ no software support included ⊖ only internet bandwidth available
Private	<ul style="list-style-type: none"> ⊕⊕ highest level of control ⊕ high bandwidth ⊕ high accountability 	<ul style="list-style-type: none"> ⊖ no software support
Community	<ul style="list-style-type: none"> ⊕ easy enablement of home- and mobile access ⊕ software can be influenced 	<ul style="list-style-type: none"> ⊖ no direct control over software
Hybrid	<ul style="list-style-type: none"> ⊕ high bandwidth available ⊕⊕ highest availability 	<ul style="list-style-type: none"> ⊖ no direct control over software

Table 2.2: Advantages and Disadvantages of Cloud Models

2.4 Costs

IT-related costs can be segregated into four components: investment, migration, operation and hidden costs. Hidden costs mainly consist of deferred liabilities to cover the risks. They cannot be quantified for a general case, since they highly depend on how well the security aspects are handled. This will be discussed at in the next chapter.

Public clouds usually have the lowest investment costs, since the cloud providers offer a subscription fee model. Migrating to a SaaS model usually inflicts the highest migration costs, since company-specific data structures and workflows need to be modeled onto standardized software. IaaS clouds and private clouds on the other hand, allow for full control over the software. Thus, the migration vectors often contains low costs.

IaaS providers often have relatively high service fees, since they need to cover significant hardware investments. The software running on top of the virtual infrastructure needs to be installed and managed by the client. Therefore, the investment costs are higher compared to a SaaS model.

The costs of community clouds are spread over a smaller number of users than in a public, but more than in a private cloud. Hence, the investment and operational costs lie somewhere in between.

The expenditure in hybrid clouds depends heavily on multiple factors: service fees (in case of public clouds), implementation, usability and maintenance.

Table 2.3 summarizes the measurable cost components for the four elementary cloud models.

	Investment	Migration	Operation
SaaS (Public cloud)	low	high	low - medium
IaaS (Public cloud)	medium	low	medium - high
Private	high	low	medium - high
Community	medium	medium	low - medium
Hybrid	medium - high	medium - high	medium - high

Table 2.3: Costs for Cloud Deployment Models

Chapter 3

Security Challenges and Risks

Despite the many benefits of cloud computing, it is important to be aware of the security issues involved in a cloud migration procedure. In this chapter we identify general security challenges and risks, analyze them separately for each deployment model and finally suggest technical and non-technical mitigation solutions.

3.1 Common Challenges

The relationship between a cloud service operator and a migrating company is essentially a customer-contractor relationship. While migrating vital IT infrastructure to an external contractor it is important to consider the implications on the amount of confidential information accessible to the contractor. In addition to access provision, migrating IT to the cloud often implies shifting company data to a foreign country with a different legal system (i.e. laws concerning data privacy and protection).

3.2 Common Countermeasures

This section describes technical and non-technical measures to address risks that are introduced or even increased by cloud computing. Since encryption is a widely deployed technical measure, it will be elaborated on to a significant extent.

Selection of Data Location

As described in Section 3.1, it is important to evaluate the legal implications while migrating to a foreign provider. Both the hosting company's origin and the physical data location should be taken into account. Some of the large cloud services such as Amazon EC2¹, IBM Lotus Live and "SAP in the cloud"² offer the ability to choose the location of the hosting data centers.

¹<http://aws.amazon.com/ec2/>

²<http://www.sap.com/swiss/press.epx?pressid=15023>

Secret-Key Encryption

Secret-key encryption is the most fundamental encryption scheme. The plain-text is encrypted using a secret key shared between two trusted parties. Today's most common example is the encryption of local hard-disks. The key is stored in a local file and encrypted with the user's password. Without both the assets, the data cannot be read by anyone, including the owner. However, one must note that passwords are generally not cryptographically strong enough to encrypt large amounts of data.

Public-Key Encryption

The major difficulty when using secret-key encryption for sharing content over an insecure channel (like the internet) is the key management. In order to share the secret key one would always have to establish a secure channel first. For this reason, (asymmetric) public-key encryption was introduced. The basic idea is to use two keys: The first key called the public key, is used to encrypt the data and is available to all users of the system. However, only the holders of the second key, the private key, are able to decrypt data. By assigning each user a public key using a trusted public key infrastructure ("PKI") it becomes possible to share encrypted data over insecure (non-authenticated and non-confidential) channels without first establishing secret keys.

This encryption scheme lays the foundation for secure communication and content sharing over the internet. Many common internet security protocols (i.e. https, ssh) use PKIs. Since migrating company infrastructure to the cloud mandates a secure communication over the internet as an inherently insecure channel, a PKI becomes a necessity.

Client-side Encryption

Another way to address the outsourcing problem is to simply consider the cloud provider to be the insecure element or the untrusted entity. Client-side encryption uses an encryption scheme that allows the key to stay within the company premises and is handled by the client himself. The cloud provider only deals with encrypted data, information, which has no value for an attacker, as long as the encryption is strong enough.

If the content needs to be accessed by a limited number of users (e.g. over e-Mails or chat messages), it can simply be encrypted with the public keys of every single user. However, if data is shared between a large number of users, the scheme can be scaled using a PKI: Each document must be encrypted with a secret key. This key is uploaded to the cloud provider after being encrypted with the public keys of each participant.

The Client-side encryption service is being offered by a various providers. The most popular one is *Amazon S3* cloud storage³. For a simple file storage, *Wuala*⁴

³<http://aws.typepad.com/aws/2011/04/client-side-data-encryption-using-the-aws-sdk-forjava.html>

⁴<http://www.wuala.com>

and *SpiderOak*⁵ are convenient providers.

Building an In-house Public Key Infrastructure

To build a secure client-side encrypted system where the organization itself possesses the master key, it is vital to build and keep a public key infrastructure in-house.

3.3 Model-specific Analysis

We now analyze security issues and countermeasures for each cloud model individually. Table 3.1 lists challenges and possible countermeasures, along with concrete scenarios where these problems are encountered.

Security Risk	Countermeasure	Scenario
leaked data traffic	network layer data encryption	all off-site cloud infrastructure
data leak in cloud storage through exposed master keys	client-side encryption; ensuring provider liability through compliance and eDiscovery	external cloud storage
data leaks in the cloud storage through software vulnerabilities	choose a smaller provider (smaller target surface); strong storage encryption; vulnerability management	off-site cloud storage
availability issues (dependency on ISP and cloud provider)	high availability guarantees in SLA	public and community cloud
vendor lock-in	evaluate data export capabilities	SaaS cloud services
security issues amplified through increased system complexity	define best practices before and during system design outsourcing	IaaS cloud services, hybrid clouds

Table 3.1: Cloud-specific Security Challenges and Countermeasures

⁵<https://spideroak.com/>

Chapter 4

Application Portfolio Analysis

In this chapter we analyze the application portfolio of **SwissTec**, the leading manufacturer of packaging equipment, and suggest reasonable deployment scenarios with regard to previously discussed criteria (see *Chapter 2: Cloud Deployment Models*).

4.1 E-Mail

The E-Mail service has the following characteristics relevant for security:

1. Attached documents contain a high amount of confidential information like internal meeting protocols, client data and notes about internal processes. Making such information readable to a contractor should be avoided.
2. High general availability of the service is crucial. However, rare occurrences of downtimes (of up to half a day) can be tolerated.
3. If the provider does not properly sanitize the traffic, using a public mailhub for outgoing mail comes with the risk of being blacklisted. One prominent example is the blacklisting of T-Online mailhubs in September 2011¹. A large number of outgoing E-Mails from T-Online customers were blocked for more than a week.

Benefits for a medium-sized company like SwissTec for migrating E-Mail to a cloud provider include:

1. A shift of the financial burden from upfront capital expense to ongoing operating expense.
2. The flexibility of dynamically adapting resources to the company's needs.
3. Being able to use cloud-based virus protection.

Based on these characteristics we conclude that this application is suited for migration to a public cloud. The benefits of a higher availability in hybrid and private clouds are outweighed by the total costs of these solutions. We

¹<http://www.heise.de/ix/meldung/T-Online-Mailserver-von-Blacklistings-betroffen-1341226.html>

recommend the following measures to address the security concerns outlined above:

1. Using a client-side encryption system for internal E-Mails as discussed in section [3.2 Client-side Encryption](#). An internally controlled PKI is a prerequisite.
2. Having availability guarantees of at least 99.9% defined in the SLA.
3. Usage of a smaller local E-Mail provider in order to reduce blacklisting risks. Evaluating their policies about outbound spam filtering for **all** the customers of the mailhub is important.

4.2 Website

The following security characteristics apply to hosting of company websites:

1. Public websites usually only contain publicly disclosable information. Confidentiality is therefore not the highest priority for this application.
2. Websites are important for the company's reputation. A high availability and avoidance of security breaches is crucial for this service.

We recommend a public webhosting service. An availability of 99.9% should be guaranteed as part of the SLA. Regular security audits (for example on an annual basis) should be conducted to reduce potential security vulnerabilities (i.e. SQL injection, cross-site scripting) to a minimum.

4.3 Intranet

The following characteristics typically apply to intranet solutions:

1. The maintenance cost is rather low.
2. The availability of the service is not mission critical.
3. The confidentiality level is usually medium (depending on the offered content).

Because the expected cost savings are rather low, migrating this service to the cloud is not considered the highest priority among the other applications. However due to the similarities in the technical requirements, combining this service with a publicly hosted website may result in collective cost efforts, assuming that previous recommendations about security issues are being followed.

4.4 File Server (Network Share)

The following characteristics typically apply to file servers:

1. The availability of the service is critical to the internal operations.
2. In some departments (i.e. R&D) there are high requirements for the available bandwidth.

3. The level of data confidentiality is high.

Because of over-average bandwidth requirements we recommend a hybrid cloud model for this service. A hybrid architecture creates an on-premise appliance that caches data locally and replicates it to a cloud storage provider over time. The benefits of this solution are the following:

1. Cache, i.e. the quantity of local storage, remains relatively small compared to a private solution.
2. The system is able to easily adapt the available resources to the current needs.
3. Costs for managing the local storage can be reduced since tasks like capacity expansion and system upgrades are now the responsibility of the cloud provider.

To address confidentiality concerns we recommend encrypting the data that is being stored in the external cloud. The decryption task could be performed by the local servers or by the clients. One system offering such a solution is *Wuala*². It offers client-side encrypted cloud storage with local caches.

4.5 Computer-Aided Design (R&D)

The following characteristics typically apply to computer-aided design:

1. The software is often tailored to the needs of a certain industry. These tools are usually not mass market products.
2. The requirements for storage and bandwidth are high.
3. The number of users is low. In case of *SwissTec*, we expect the size of the R&D department to be below 10% of the overall staff.
4. Data confidentiality is very important since a leak of blue prints for new developments could hinder the competitive advantage the company is hoping to gain from R&D.
5. Availability of services is important since employees might need to delay their work due to downtime. However it is usually not essential for business continuity.

Given those characteristics we cannot recommend a cloud solutions for CAD for the following reasons:

1. The cloud solutions market does not seem to be ready for this application.
2. The available internet bandwidths are often too small for outsourcing CAD to the cloud.

Depending on the CAD software used, there might be private cloud solutions available. Sharing the computing resources of the involved workstations could possibly save costs in hardware. The feasibility and the effects on productivity of such a solution could be evaluated within a subgroup of the R&D department.

²<http://wuala.com/>

4.6 Customer-Relationship-Management

The market for CRM solutions has massively changed with the advent of SaaS cloud solutions. The required bandwidth for such solutions is typically low while license costs for private CRM systems is high. This renders CRM to be a good candidate for a cloud sourcing. The following list gives an overview over today's most common cloud CRM providers:

- Salesforce¹
- SugarCRM²
- Microsoft Dynamics CRM³
- Oracle On Demand⁴

From a security perspective, CRM has the following characteristics:

- High availability of the service is crucial for business continuity.
- Confidentiality is very important as a leak of CRM data could be most beneficial to competitors.

While the cost saving potential is obvious when considering one of the cloud CRM services mentioned above, the privacy remains questionable:

- All of the large cloud CRM providers typically host their services in USA. The data is therefore subject to US law, including the Patriot Act that obligates US companies to give the US law enforcement access to all data when asked.
- High profile web services are more likely to become a target for security attacks. Salesforce.com was successfully attacked⁵ in the past with a decent amount of critical customer data leakage.

For the reasons discussed above, we recommend SwissTec to only consider cloud sourcing when the data is guaranteed to stay within Swiss borders. Swisscom, who has not (yet) openly advertised this, appears to be offering such a solution in collaboration with Oracle On Demand⁶.

4.7 Financial Accounting and Payroll

Both financial accounting and payroll applications share the following characteristics:

1. There are many requirements specific to local laws and practices.
2. The bandwidth requirements are low.

¹<http://www.salesforce.com>

²<http://www.sugarcrm.com/crm/>

³<http://www.microsoft.com/germany/dynamics/produkte/crm/ueberblick/>

⁴<http://www.oracle.com/de/products/ondemand/index.html>

⁵<http://www.infoworld.com/d/security-central/update-salesforce-com-falls-phishing-scam-warns-customers-980>

⁶http://finance.swisscom.ch/download/crm-software_aus_der_steckdose.pdf

3. The required computing resources are low.
4. The privacy requirements are high.
5. The number of users is small.

The two applications differ in terms of availability requirements: While the financial accounting system needs to have a high availability (in order to keep the daily operations going), payroll software is typically only needed for a short period once a month. Because the two applications need to share a lot of common data, having a packaged solution for both is usually advisable.

When considering a cloud migration of those two applications we arrive to the following conclusions:

- A Swiss provider is required because of the local specifics as well as the security concerns discussed in section *4.6 Customer-Relationship-Management*.
- The low bandwidth and computing power requirements make these applications a candidate for the public cloud.
- Whether substantial cost savings are possible mainly depends on the current solution and the involved license fees.
- Besides possible cost savings, cloud solutions could offer the additional benefit of more flexibility for employees (e.g. home office work).

The leading provider of such a cloud solution in Switzerland is Abacus¹.

¹<http://www.inside-it.ch/articles/20218>

Chapter 5

Migration to the Cloud

The most important prerequisite for the design and the proper implementation of a cloud strategy is to understand the basics of cloud computing and being able to assess issues like security, identification of applications and find the right cloud deployment model (see [4] for details).

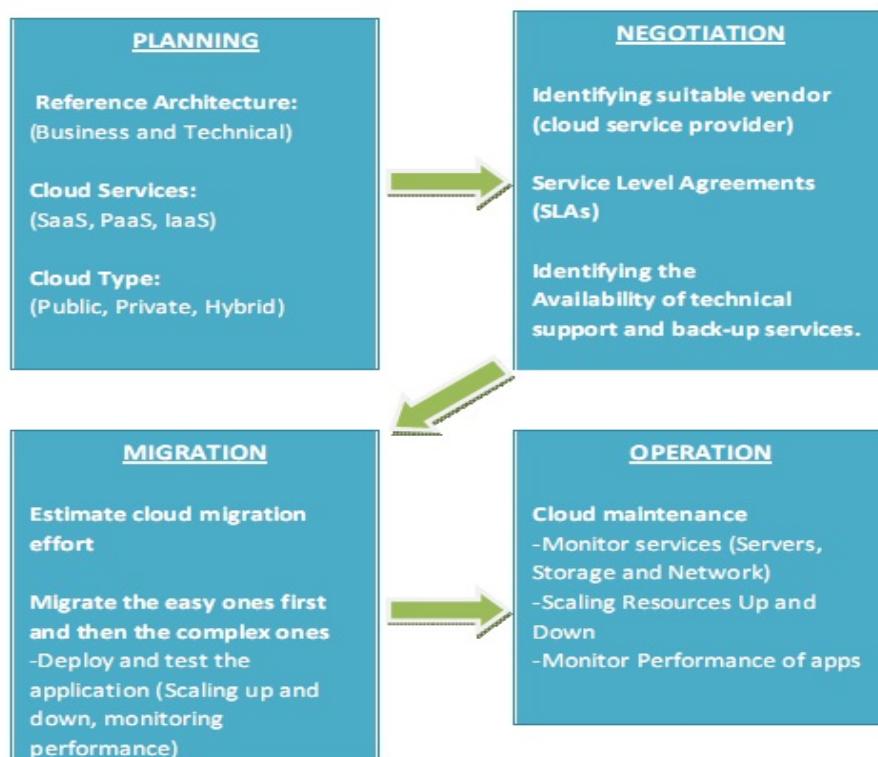


Figure 5.1: **The 4-Step Migration Approach.** This figure summarizes the 4-step approach recommended for SwissTec.

The cloud does not introduce any new security threats or issues, but it does increase the number of people who have access to the company's resources. This results in the transfer of control to a third party. Some of the most common security controls include securing data, storage, networks and endpoints, defining identities and the access control policies, as well as key and certificate management.

Application migration is the process of redeploying an application, typically on newer platforms and infrastructure. There are many different aspects to consider while migrating an application to the cloud. The process begins with the analysis of factors for the application and a comparison of these factors to different types of cloud computing environments and models. Although, no single approach will work for all applications, the most important security issues that should be taken care of during migration can be based on the chosen cloud deployment model. In SwissTec's four step approach (see Figure 5.1), we suggest the following security issues to look into:

5.1 Planning

1. To classify applications for migration to a cloud, it is necessary to first identify and understand the business and technical factors for the migration.

Information assets such as intellectual property, trade secrets, research, financial data and personal information are most valuable to the company (see [5] for an overview).

This process can be securely done in 3 steps:

- Identification with the policies and regulations for storing, accessing, and deleting the information. In the absence of these regulations, there might be huge data loss and corruption.
 - Classification on the basis of information value and the potential damages if it is lost or has unauthorized access.
 - Protection by creating a security chain for each class of information which will protect the information at all levels of security, including physical security, technical security, procedural and legal steps. These chains can be modified anytime to change access rights.
2. Identifying the suitable deployment model is important as sometimes moving extremely valuable information to the public cloud can pose risks that outweigh any benefits of using cloud computing. Every model introduces a specific set of risks as discussed in section 3.3 *Model-specific Analysis*. There is always a trade-off between the benefits of various cloud deployment models and the security issues related to them. It is therefore necessary to assign the most suitable model to the application in question in order to minimize the security risks.
 3. It is very important that the company knows its objectives as it considers different vendors. Different vendors have different information security

policies and regulations which turn out to be most beneficial if matched to the correct application and its specific security requirements while minimizing cost at the same time. Thus, in order to ensure maximum information security, it is advised to consider different vendors for different applications.

4. Certain legal environments like the *U.S. PATRIOT Act* may prevent the placement of data in certain locations to be in compliance with company policies. It is also important to establish which jurisdictional laws will apply in case of a dispute with the application owner. These considerations essential for choosing the right cloud provider for an application.

5.2 Negotiation

1. Depending on the type of cloud service, a vendor might need to be certified for certain standards (ISO 27001). Privacy is a concern for any application that deals with sensitive data and establishing a contract with the reputed vendor will be one of the safeguards against data theft.
2. A Robust and clearly defined Service Level Agreement must include:
 - Complete specifications of the services provided.
 - Responsibilities of both vendor and the company.
 - A set of metrics to determine whether the vendor is delivering the service as promised.
 - The availability of the vendor as well as the recovery procedures in the event of any failures.

This helps to ensure information security and existence of robust recovery procedures in case of failures.

3. It is essential to monitor that the vendor keeps being in compliance with the company's security policy. The vendor must provide transparency, notifying the company of any outages or problems that occur.
4. It is crucial for the company to know what architecture and technology the vendor has provided to deal with system failures that might potentially lead to data loss or data exposure, including redundant systems and self-healing infrastructures.

5.3 Migration

1. It must be possible to migrate data in an encrypted format. In addition, some consumers will need their data to be stored separately from other consumers.
2. It must be possible to ensure that migration happens through a medium which is trusted and secure to prevent any leaks.

3. The vendor's security policies for virtual and physical isolation, as well as compliance should be examined. Hiring an ethical hacker to attempt to break into them might help developers to close any loopholes in time (refer to [6] for an elaborative discussion).
4. Use firewalls liberally to ensure no accidental backdoors are opened through routes other than the application itself. Encrypt all communications with the external application and lock it away behind a proven authentication system that will guarantee that the only people who can access it are those who are permitted to.

5.4 Operation

The operational flexibility to the company is provided by rapid provisioning and deprovisioning of cloud computing. Many security issues can arise during the execution of applications via cloud.

1. **Federated Identity / Single Sign-On:** An authentication service should be applied to control that a user with a particular role should be allowed access to a given resource without any prior knowledge of the user to limit the access of particular users to some specific and sensitive data sources. Otherwise, there will be no control on the number of users accessing the data - some of which may not even be part of the organisation.
2. **Portability:** Ensuring portability provides freedom to the company to work with multiple vendors and not restrict to the terms and conditions of a sole vendor. It also provides the ability to run components in different environments.
3. **Privacy Compliance:** It should be monitored that the vendor does not expose data during operation and maintains compliance with the organisation at all times. In case of any new installations or upgrades, the vendor provides a complete technical description of the same and ensures that security requirements are met.
4. **Load Testing:** Stress-testing multiple instances of an application under massive loads can be done by starting the application on many virtual machines and running simultaneous tests.

Chapter 6

Conclusion

Cloud computing helps service providers to offer services in the form of an on-demand self-service, broad network access and resource pooling. It also extends scope in scalability and measured service for the use of applications. Cloud computing can help in providing Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), as well as a combination of all (hybrid model). There are striking advantages of implementing a cloud solution instead of the traditional computing interface. It helps companies save costs as it requires no dedicated system and no skilled IT personnel. It provides unlimited resources and availability. However, it also offers serious security consequences, if not addressed appropriately.

In this study, we have analyzed the various applications of **SwissTec**, the leading manufacturer of packaging equipment, and presented a cloud deployment solution best fitted to the needs of its portfolio. We suggest the migration to a public cloud for the E-Mail service, the official website and the Intranet. Human resources and management duties can also be delegated, but only to an inland provider. A hybrid cloud is the most pertinent solution for a File Server used for network sharing, since data is cached locally and replicated to the provider if accessed infrequently. Some Computer-Aided Design tools used in the R&D department may be migrated to a private cloud, depending on requirements of the software.

As a result of this analysis, we have proposed a four-step approach and pointed out relevant security issues in order to ensure safe migration and stable operation of the applications in the cloud. Our strategy comprises a planning and a negotiation phase, which lay the foundation for the implementation. In the subsequent migration stage the applications are deployed to various cloud models and, in a final step, tested with respect to their functionality to guarantee privacy, security, stability and robustness of the portfolio as a whole. We conclude that, in order to cut down costs, SwissTec would benefit to a reasonable extent by adopting a cloud computing approach as per the security guidelines and suggestions provided in this study.

Bibliography

- [1] Jerry Archer, Alan Boehme, Dave Cullinane, Paul Kurtz, Nils Puhlmann, and Jim Reavis. Security guidance for critical areas of focus in cloud computing. Technical report, Cloud Security Alliance, December 2009.
- [2] Peter Mell and Timothy Grance. The nist definition of cloud computing. Technical report, National Institute of Standards and Technology, September 2011.
- [3] Jerry Archer, Alan Boehme, Dave Cullinane, Paul Kurtz, Nils Puhlmann, and Jim Reavis. Top threats to cloud computing. Technical report, Cloud Security Alliance, March 2010.
- [4] Cisco Systems. Planning the migration of enterprise applications to the cloud, March 2010.
- [5] Cloud Computing Use Cases Discussion Group. Moving to the cloud, February 2011.
- [6] Richard Holland. Ten steps to successful cloud migration, March 2011.