Hybrid cloud computing: Security Aspects and Challenges

Conference Paper · May 2015

CITATION
1

READS
6,516

1 author:

Roman Nedzelský
Prague University of Economics and Business
6 PUBLICATIONS **6** CITATIONS

SEE PROFILE

Hybrid cloud computing: Security Aspects and Challenges

Ing. Roman Nedzelský

roman.nedzelsky@outlook.com

The Faculty of Informatics and Statistics
University of Economics
Prague, Czech Republic

Abstract

Nowadays, the concept of hybrid clouds is constantly being discussed, private as well as public clouds. For large companies and state institutions the hybrid solution is the only way to get involved in innovation in cloud computing, because most of the data must be placed on on-premise hardware and cannot be moved to any public cloud. Even if there is no legal restriction within the hybrid scenarios, companies are afraid of information leakage or other constraints that may arise when they do not have their data under their control. On the other hand it is very tempting to take advantage of outplacement infrastructure which the user does no need to worry about, or to use the services in the field of machine learning, business intelligence, stream analytics and other SaaS features. This migration to cloud solutions (or using cloud features) is mainly from the cost savings point of view a very desirable solution. However, public cloud solutions face the problem with functionalities of some cloud services which cannot be used in combination with local, on-premise servers.

Many researches that have been carried out recently, focus only on the area of private or public clouds. This paper focuses on security within hybrid clouds for large companies and governments. It deals with the exploration of various kinds of security within the concept of IaaS and SaaS, various principles of authentication and security and also challenges in terms of security in this area. Motivation for this work were also forecasts provided by Gartner, who estimated that in 2017 most of the large companies will be using hybrid cloud scenarios. This paper compares several suppliers that are specialized in hybrid cloud solutions for government agencies. Some of them are already providing cloud services with a focus on the public sector and it is therefore appropriate to summarize these offers and compare them with emphasis on safety.

Keywords: Hybrid cloud, security, IaaS, SaaS, governance, authentication.

1 Overview

According to KPMG surveys [1] 25% of governments around the world are interested in cloud computing. They are interested in the benefits of different options, and about more than half of them realize that for cost savings these IT cloud technologies are necessary. These views are shared by large corporations [1], [2]. Governments recognize the possibility of quite large cost savings by using outsourced IT. Another factor that plays a role from the cost saving point of view is the fact that governments and large corporations often have very beneficial agreements with potential vendors (with whom they often collaborate even outside cloud solutions). Moreover, for such a transfer to cloud solutions or partial use of cloud services there are many donation programs within the European Union.

The problem that large companies and public sector are trying to solve is, among other things, data security. Each solution provides different forms of security, there are a lot of options. The trust, according to KPMG [1], increased towards cloud solutions provided by certified suppliers, just slightly or rather his certified services by the government authority. In case of governments, there are other necessary requirements - especially for certification standards (ISO) of storage and handling with (sensitive) data. Such storage concerns many regulations regarding the legislative, even some kind of data it is not possible to transfer out of the building at all (and therefore outside servers). Another problem could be the country where the data is stored – again, some confidential data cannot be stored outside of the country, because of legislation.

Cloud computing services were recently broadened by a new specialization for multinationals and government organizations. Their hands are usually tied because of the requirement for them to handle classified and sensitive information with extreme care. Here it is worth mentioning that some of the providers came up with the idea of creating a special cloud space for such organizations - Amazon AWS GovCloud, Microsoft Azure Government, IBM SmartCloud for Government and VMWare [3]–[6].

2 Literature overview

2.1 Service Models

At the moment there are more service models than the four basic ones, which were pioneers of cloud computing. Companies are still inventing new models that can be provided as a service. However the basic four, according to NIST [7] are the following (without SECaaS):

- **Saas** - Software as a Service - Application Layer
- **IaaS** - Infratructure as a Service - Hardware Layer
- **Paas** - Platform as a Service - Middleware Layer
- **Daas** - Data as a Service, or Database as a Service
- **SECaaS** - Security as a Service

The latest service is certainly worth mentioning. Using SECaaS the customer gets access to a number of tools that help to improve security. This, however, brings with it both advantages and disadvantages. Generally, the cloud is one big black box for the customer. He does not know how security is exactly ensured there and which metrics should be used for monitoring [8], [9]. Based on Carvalho [8] as an advantage may be also included the quantity of SECaaS services, which means the potential combination of multiple vendors. Another advantage is represented by the cost model of cloud services (on-demand model). Others include bigger focus on security including the possibility of security outsourcing. It is a huge time saver, which allows the customer to spend more time to focus on core business and organizational processes. A supplier of such extra services has generally much bigger knowledge of possible issues and is able to ensure the management of security and monitoring within the pre-defined SLA.

Such outsourcing of security also brings risks such as the domino effect, thus affecting all services when attacking or breaking one of them. Other risks should be mentioned concerning sharing services security and limiting the possibility of adjustments towards the customer's needs. SECaaS is still considered a solution which is provided as a service to more than one customer [8].

2.2 Deployment Models

At the beginning, it is appropriate to mention the basic deployment capabilities of individual models of cloud services. NIST [7] defines four basic models of cloud computing:

- **Public** - Cloud infrastructure is owned by a service provider and its entire administration.
- **Private** - Infrastructure is owned by a company or hosted by a provider, but it is always developed and managed by the customer or third parties.
- **Community** - Cloud infrastructure is shared by several companies / organizations and it is managed by one of the companies or a third party.
- **Hybrid** - This model is the interconnection of previous models, combines them, but also creates a custom entity (see Figure 1).

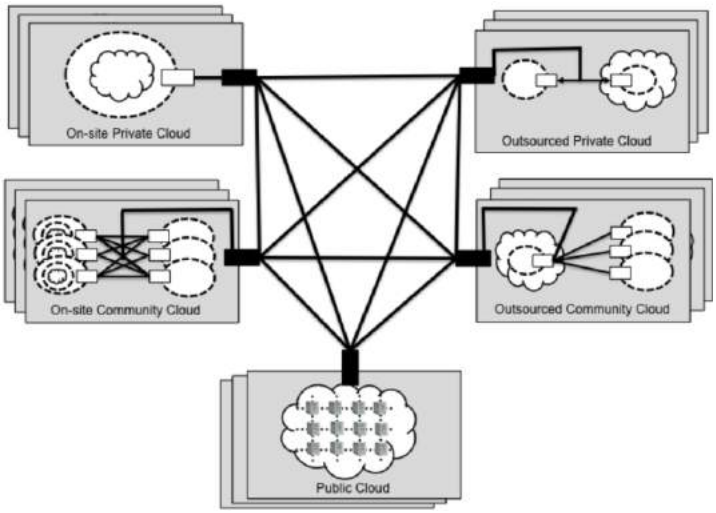

Figure 1: Hybrid cloud, source [10]

2.3 Cloud Security Challenges

Generally speaking, certain aspects of cloud security are very similar to physical local networks and systems. Both are potential subjects of attack, information theft, including espionage and human error. Cloud services have, as opposed to physical servers owned by companies, the advantage of distribution. (Distributed vs Concentrated servers). As a result of this Cloud service providers have to invest in security far more resources than the company that uses the services. On the other hand, providers do not have a single customer, but usually many customers and can thus become a popular destination for all attacks or cyber-attacks with the objective to steal data. Here can be seen the difference between individual users who may become victims through separate attack on private servers. For a provider is an individual user who is excluded, a whole company is becoming as a subject of the cyber crime. It may not always be true, but attacks targeting to a specific person are much easier in the case of on-premise solutions [11].

From the cloud service providing point of view, there is also the security challenge when hosting more than one customer, the so-called multi-tenancy, or the sharing of computing resources between more customers. Security also has to be designed in terms of splitting of responsibilities between the solution provider and the customer itself, or among multiple providers (provider mediates end service, but a repository for this service is provided by an additional, third party company) [11].

Based on Sharma, Date and Chavda [12], it is possible to divide the different aspects of security into four basic areas - infrastructure, platform & application layer, administration and adherence / compliance. Infrastructure covers the area where it is possible to meet threats in the physical layer. It can be further divided into layers such as Network, Host, Virtualization, or Physical. All these components are hosted in the cloud and the customer does not have an access to them. The customer has access to the parts in the on-premise solution, but in the cloud this is managed by the provider. Application layer represents all applications that are provided within the cloud, i.e. towards the customer. The area of compliance is related to laws and regulations that may apply in a given area - often associated with cloud computing, data storage, risk management, certifications and standards in the case of state institutions.

3 Proposed Hybrid Cloud Solutions

Hybrid cloud is based on previous explanation combination of public and private (or even community) cloud.

The main issues from personal experience with Customers

- **Transfer of domain controllers to the cloud** - recommendation of a majority of vendors is (for example, when a larger number of DCs) that at least one domain controller is being left as an in-house server (ideally physical, functioning as a replica server). Security should be done through an IPsec VPN tunnel with unidirectional Trust. Often the authentication is being solved with the federated access (or cross domain single sign-on - CD SSO) within the trustworthiness of the individual domains [13], [14].

- **Integration with corporate IS** is another concern that customers have when they consider transfer to the cloud (or transfer of some services, or transfer of infrastructure into the cloud). Usually it is necessary to maintain the integration of enterprise systems. Concerns are raised mainly with the security of the connection between the public and private cloud Servers (private cloud). Services can authenticate to the domain controller based on its location. However, it is necessary to take into account that the systems, which remain in-house infrastructure contain more confidential data.
- **Government wants to solve the need of private cloud, but outsourced at a company**. The term "outsourced private cloud" is a little bit misleading, now ever this scenario is feasible. Distinct space is given by cloud providers for the entire private cloud, which is implemented in the context of an isolated security perimeter as shown in Figure 2 [10].

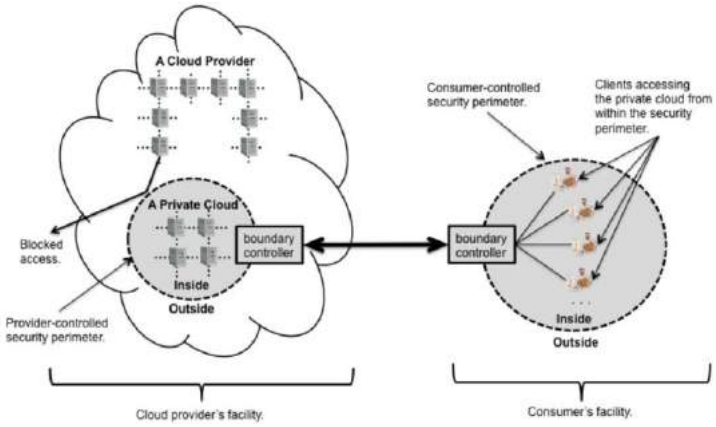

Figure 2: Outsourced Private Cloud, source [10]

3.1 Solution Possibilities

The first option is a situation, where a company has its own infrastructure with information systems or virtualization and possibly private clouds - thus providing its employees virtualized applications (e.g., App-V) or a full-featured model of an IaaS private cloud created on one of hypervisors (Microsoft, VMWare, Citrix or others). The company wants to reduce the usage of its infrastructure however and move it to the cloud. This means that part of the infrastructure will remain at the company which will continue operating its information systems. The second part will be either reallocated or removed. Then in the public cloud will be purchased predefined services (such as mail server, intranet portal, or communication platform), which will be connected to the physical (onsite or virtualized) servers (see Figure 3).

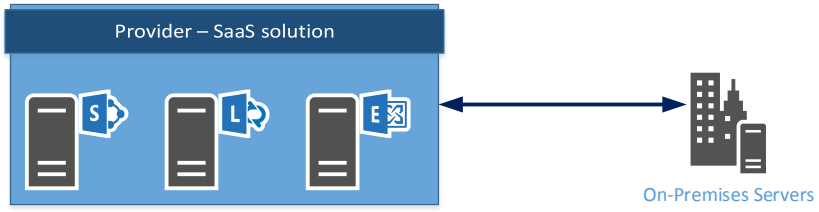

Figure 3 – On-Premise Infrastructure connected to SaaS

User authentication is being solved either through separate accounts (i.e. a separate login to cloud services), federated authentication (i.e. connecting domain diluter company with authentication in the cloud) or possibly even through adding a second option in the form of multi-factor authentication (for example, through additional authentication via cellphone).

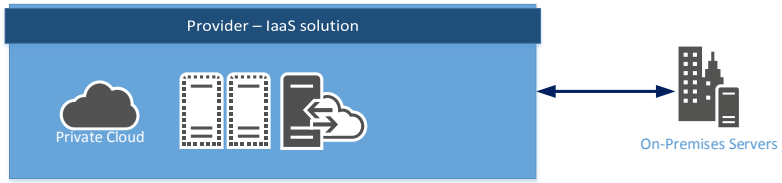

Figure 4 – On-Premise Infrastructure connected to IaaS

The second option is a scenario where a company has the same infrastructure as in the first one, but wants to transfer virtualized servers to the public (or outsourced private) cloud (IaaS). The advantage of such a scenario is primarily a "lightening" of physical servers, reducing the cost for employees (physical server administrators), etc. Here can be observed the biggest security change in channel between private and public IaaS. Companies and government have to solve several key points that discourage selecting certain hybrid cloud solutions. Data that is inside the company cannot be moved to the cloud, either due to data confidentiality or due to requirement to have them in on-premise solution by the law or any of the ISO standards. If the data will be transferred to the public cloud, the question is where it will be physically stored? Companies often do not want their data to leave the country and search for a cloud provider with data centers in the Czech Republic because of this reason.

The overall comparison of the models in terms of safety can be seen in Figure 5.

	PRIVATE	COMMUNITY	PUBLIC	HYBRID
SCALABILITY	Limited	Limited	Very High	Very High
SECURITY	Most Secure Options Available	Very Secure	Meoderately Secure; Depends Greatly on Service Provider	Very Secure
PERFORMANCE	Very Good	Very Good	Low to Medium	Good
RELIABILITY	Very High	Very High	Medium	Medium to High
COST	$$$; Requires More Resources (i.e. Data Center Space, Electricity, Cooling)	$$	$; Pay-as-you-go Model	$$

Figure 5: Overview of parameters regarding to Cloud Deployment Models, source [16]

The biggest problem is the general absence of a schedule, which is generally needed for the migration of part of or the entire infrastructure or services.

3.2 Solution Design

An outsourced private cloud solution seems like a good option. Of course, it is up to the customer, what the final scenario will be. In the event that the company only wants to use a private cloud within the infrastructure, it is enough to incorporate an outsourced private cloud in the in-house private cloud, but if he wants to limit additional services on their own servers and take pressure of their infrastructure, the environment can be moved to a public cloud, which will provide SaaS services. The only risk with this solution is the exposure of sensitive data.

The solution of these scenarios may be a variant of the hybrid cloud, where there is private cloud that is both hosted / outsourced by a provider - a company with a data center in the Czech Republic, and placed in In-house infrastructure on the other side. This is due mainly to the distribution of services and therefore not necessarily need to have complete redundancy of all services in between the private cloud provider and private cloud within the in-house environment. The provider manages entrusted infrastructure within all security requirements. On this administration are written individual agreements (SLA etc.). This company provides, inter alia services like SECaaS and thus solve all the requirements of both the large company, or potentially for state institutions. It is important to solve with a provider the security of the physical servers as well. Thus, the already mentioned multi-tenancy (sharing of hardware among several customers). If there are special requirements for security of physical infrastructure, there is need of properly communication (including biometrics and other options). Subsequently, implemented a hybrid scenario is executed. With the need of authentication by the contracting lets probably be part of the infrastructure on-site / on-premise and uses it to authenticate or to operate critical systems. It is therefore necessary to connect the system authentication secure channel with servers that are located at the provider (site-to-site VPN, encryption, user authentication multi-factor authentication etc.). It also may be required to divide what services will be operated within a private in-house solutions. Within an internal solution that tend to be service on authentication and identity management, part document management and archiving of documents under legislation (if this solution is not specifically agreed to the SaaS provider of some services, or is developed by government itself), or other information systems that it is not possible to move to a private cloud for n different reasons.

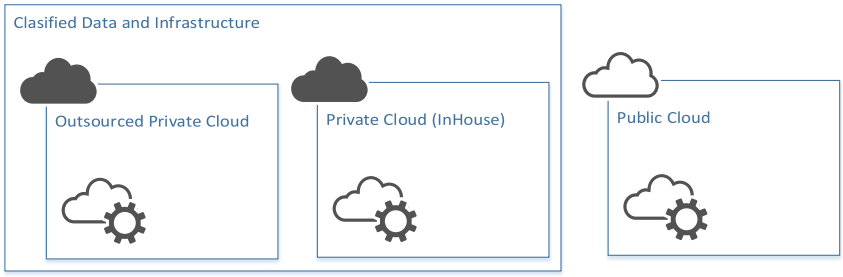

Figure 6: Proposed solution of hybrid cloud (multi-cloud private & public cloud)

4 Conclusions

Cloud solutions certainly solve many problems of our time and bring a lot of value in use, whether in the form of services or in the form of cost savings on infrastructure. Return on finances is certainly considerable. First of all it is necessary to plan the transition with great consistency. Security risks that are most researched topic. These are also reflected in the menu of services many cloud providers and often these risks are similar or less in the cloud environment than in the case of in-house infrastructure. The largest security risk, remains the "path or channel“ between the in-house and the cloud infrastructure of the provider. It is therefore necessary to emphasize the quality and security of the customer’s own infrastructure and the need to secure the internet connection. The second challenge remains centralizing the authentication of individual users, which is constantly under development, and constantly supplemented with new additions to the "simple" authentication - for example multi-factors authentication using mobile phones, additional biometrics (e.g. face recognition using the options on the website etc.).

References

[1] KPMG, "KPMG - Exploring the Cloud - A Global Study of Governments' Adoption of Cloud." KPMG.

[2] KPMG, "Cloud jako cesta k úsporám ve státní správě." [Online]. Available: https://www.kpmg.com/cz/cs/issuesandinsights/articlespublications/press-releases/stranky/cloud-jako-cesta-k-usporam-ve-statni-sprave.aspx. [Accessed: 24-Mar-2015].

[3] Amazon Web Services, "AWS GovCloud (US) Region Overview – Government Cloud Computing," *Amazon Web Services, Inc.*, 2015. [Online]. Available: http://aws.amazon.com/govcloud-us/. [Accessed: 11-Apr-2015].

[4] "Microsoft Azure Government." [Online]. Available: http://azure.microsoft.com/en-us/features/gov/. [Accessed: 24-Mar-2015].

[5] IBM Software and IBM SmartCloud Social Collaboration for Government, "IBM SmartCloud Social Collaboration for Government," *IBM SmartCloud Social Collaboration for Government*, 30-Dec-2014. [Online]. Available: http://www-01.ibm.com/software/lotus/cloud/government/. [Accessed: 11-Apr-2015].

[6] D. Brown, "Now Available: VMware vCloud Government Service | The Journey to Hybrid Cloud," *The Journey to Hybrid Cloud*, 2015. [Online]. Available: http://www.hybridcloudforum.com/646/now-available-vmware-vcloud-government-service. [Accessed: 24-Mar-2015].

[7] P. Mell and T. Grance, "The NIST Definition of Cloud Computing." National Institute of Standards and Technology, Sep-2011.

[8] M. Carvalho, "Secaas-security as a service," *Inf. Syst. Secur. Assoc.*, vol. 9, no. 10, pp. 20–24, 2011.

[9] N. Oza, K. Karppinen, and R. Savola, "User experience and Security in the Cloud an Empirical Study in the Finnish Cloud Consortium.pdf." VTT Technical Research Centre of Finland.

[10] L. Badger, T. Grance, R. Patt-Corner, and J. Voas, "Cloud Computing Synopsis and Recommendations." National Institute of Standards and Technology, May-2012.

[11] E. A. Fischer and P. M. Figliola, "Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management." Congressional Research Service, Library of Congress, 2015.

[12] O. Sharma, P. Das, and R. K. Chawda, "Hybrid Cloud Computing with Security Aspect," *Int. J. Innov. Adv. Comput. Sci.*, vol. 4, no. 1, pp. 76–80, 2015.

[13] B. Hunt, "Windows Azure Hybrid Cloud Authentication and Access Architectures – Discussion (31 Days of Windows Servers (VMs) in the Cloud – Part 31 of 31) - The IT Pro Exchange - Site Home - TechNet Blogs," *Technet blog*, 2013. [Online]. Available: http://blogs.technet.com/b/bobh/archive/2013/01/31/windows-azure-hybrid-cloud-authentication-and-access-architectures-discussion-31-days-of-windows-servers-vms-in-the-cloud-part-31-of-31.aspx. [Accessed: 12-Apr-2015].

[14] Juniper Networks, Inc., "Identity Federation in a Hybrid Cloud Computing Environment Solution Guide." Juniper Networks, Inc., 2009.

[15] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0." Cloud Security Alliance, 2009.

[16] Carpathia, "Hybrid Cloud Solutions for Government Agencies: How to Have the Best of All Worlds | Blog," *Hybrid Cloud Solutions for Government Agencies: How to Have the Best of All Worlds*, 04-May-2015. [Online]. Available: http://carpathia.com/blog/hybrid-cloud-solutions-for-government-agencies-how-to-have-the-best-of-all-worlds/. [Accessed: 24-Mar-2015].