Cloud computing: greater efficiency but at the expense of greater risk?

# SECURITY IN THE CLOUDS

**The Internet is increasingly turning into a virtual service provider. With cloud computing, all the data organisations want is available to them on multiple smart terminals. Organisations can plan their daily work much more efficiently with cloud-based services. However, it is important not to overlook the enormous information risks associated with global networking in the process.**

*by Urs Kürzi, Customer Segment Manager, and Markus Artho, Product Manager*

The main idea behind cloud computing is for an organisation to outsource its own IT infrastructure to a cloud. The term "cloud" comes from the IT industry because networks were often depicted there as clouds. The cloud ensures that the user's data can be stored on the Internet and processed there with applications leased on an ad hoc basis. The cloud even makes available virtual servers and desktops. This type of outsourced data processing and data keeping has an advantage for users. They can always open the latest version of a document regardless of where they are and what terminals they have and need only pay for the services they actually use.

With more and more people concurrently using computers, notebooks, tablet PCs and smart phones, cloud services are becoming the obvious choice. As mainframes of a sort, clouds remind us of the early days of computer technology but they are actually more akin to a smart set of functions implemented on the Internet. The on-site devices serve as the points of access to the cloud. Thanks to networking, the devices receive their users' e-mails, appointments, addresses and documents "as if by magic". For example, if a user enters an appointment in his smart phone on his way to the ministry, it will already be in his computer calendar on his arrival at the office. Certain cloud computing applications such as appointment entry are changing our work methods in positive ways. We do not even talk about them any more, we simply utilise them as a matter of course.

### Potential cloud

With clouds, users' needs become the focal point of attention. On the one hand, the focus is on communication and collaboration; on the other, the users no longer worry about the "how" and the "where" of IT infrastructure. There are virtually unlimited IT resources available in the cloud and they can be switched on and off as needed. Users can purchase need-based server time and storage capacity from the cloud. And they can do so without the involvement of skilled workers (on-demand self-service), furnished in the background by the provider. Points of access to the cloud are ensured with mobile phones, notebooks, etc. using standard


In the IT industry, a cloud drawing is used as a metaphor for a network such as the Internet, for example.

A private cloud is suitable for organisations requiring a high level of security.

A community cloud is suitable for administrative data processing because the providers are trusted by the ministries involved.

A public cloud is the choice for private and business users in particular.

mechanisms (Broad Network Access). The users of computing resources are naturally heterogeneous. Resource providers apply different leasing models to pool these users according to physical and virtual criteria so resources can be allocated dynamically. This approach improves the utilisation rate of infrastructures and services in the cloud many times over (far above 50 %), to a greater extent than would be possible with one's own network (resource pooling).

### Service models in the clouds

Every provider makes available applications such as e-mail or standard office programs in the cloud. So, aside from internal networking, organisations or companies no longer need to maintain their own IT department, a task that requires enormous investments. Thanks to cloud computing, public authorities lease software and programs in a cloud and convert their IT from strictly a cost centre to a services unit (Cloud Software as a Service – SaaS). A further example: to develop their own advances, governmental organisations can lease the necessary work platforms from a cloud instead of purchasing them at great expense (Cloud Platform as a Service – PaaS) and then make them available to their internal (and also external) developers. Cloud computing also relieves users of having to worry about the underlying infrastructure.

### Cloud-based supply models

There are various models for setting up cloud computing. A cloud used on the Internet is known as a public cloud. In this case, users draw all services from the public network, i.e. generally from the Internet. The data is physically located in the public cloud and thus no longer in the users' own servers or networks. This fact quickly leads the discussion to the subject of data protection. Organisations or users have to decide for themselves which data with which classification level they wish to keep in the cloud outside their own sphere of influence. In addition, users have no way of knowing where their data is being stored. It could be in the users' own country or even overseas! It is therefore difficult for users to assess the legal situation.

### Data availability

Users have a convenient situation when it comes to data availability. The provider generally guarantees a certain level of availability in a Service Level Agreement (SLA). However, users are well advised to define another question more precisely, namely: What happens if the cloud can no longer be accessed? The connection onto the Internet and cloud computing must be viewed jointly but users generally have to enter into separate SLAs to purchase them. A failure in data availability or Internet access means work grinds to a stop as well.

### Cloud models

There are different models for supplying cloud computing. A private cloud is fully and exclusively under the control of the user whereas a public cloud is in the hands of the providers from whom all IT services can be purchased. A community cloud is an alternative to these two models. The provider is known and has the trust of multiple ministries, for example, and renders cloud services for them in shared virtual infrastructures.

### Private cloud – the cloud for authorities requiring top security

The situation with a private cloud is different. In this case, cloud providers and users are in the same organisation. The infrastructure is run by the users' own organisation. This means the data is also stored in the users' own network and remains there. Sensitive data is permitted to leave the data owners' protected, inaccessible area only after being encrypted.

### How does an organisation requiring top security benefit from cloud computing?

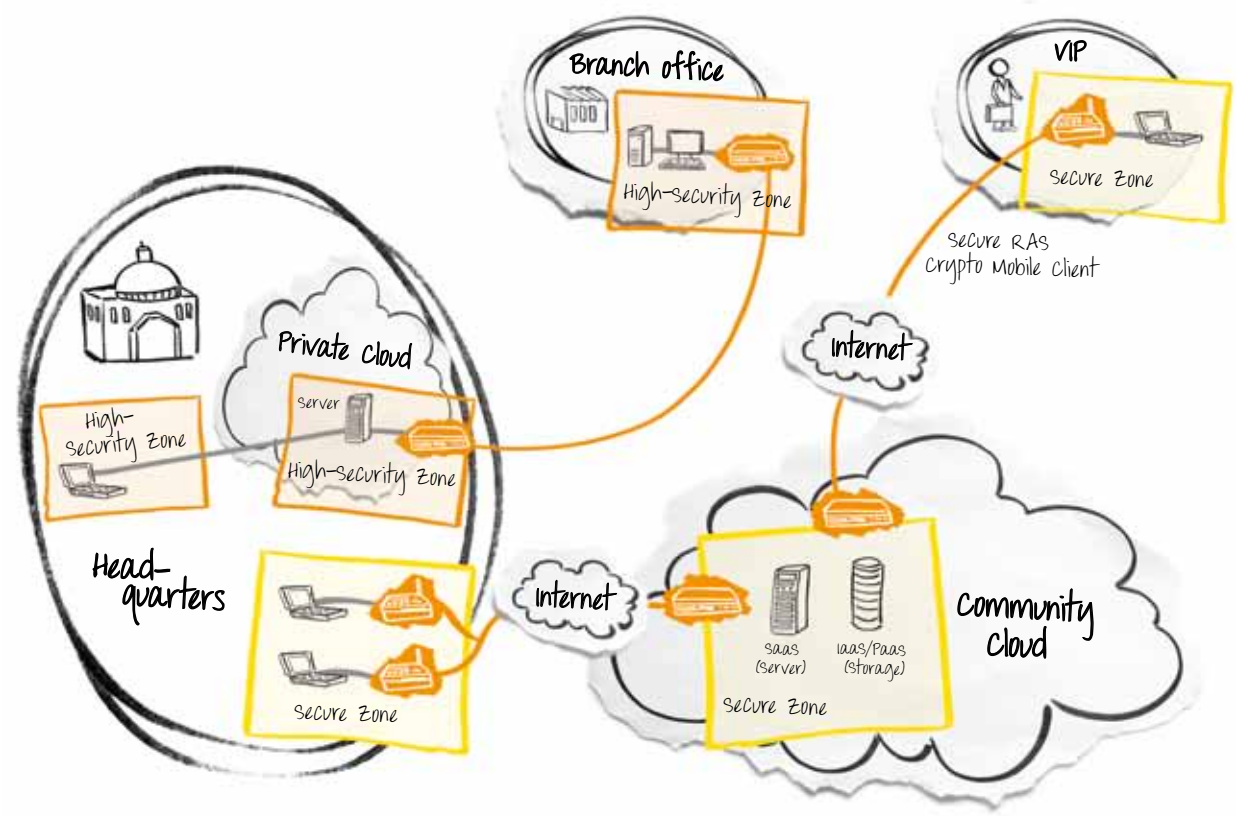
Let us say that a ministry wants to make its own infrastructure increasingly cloud-capable to accommodate the unabated trend towards mobility. This means an infrastructure is to be designed for mobile working despite the need for top security. In this situation, a remote access solution from Crypto AG allows data in a protected zone to be viewed and edited from without. The technology for this function is based on a thin client approach in which only the information on the screen and the keyboard commands are encrypted, not the document itself. Consequently, thin clients cannot download or locally store complete files. They are only able to edit the data from a distance. Their view is similar to when one looks at headquarters through an encryption-protected telescope. In this work approach, users leave no traces on the access unit. Physical and logical precautions taken at the interface continue to provide protection against unauthorised access and examination at zone transitions into the home network.

### How to achieve security in the clouds

It is advisable to take a holistic approach to security and launch a cloud project at the same time. The first step must be to classify sensitive data to render the need for protection visible. The focus is on availability and confidentiality. Both factors have a decisive influence on how data is treated in the cloud. Only data owners can decide whether a set of given data is allowed to enter the community cloud for processing or whether it is forced to stay in the private cloud. Security governance rules have to be set for these situations and users must be duly aware of ICT security topics.

An ICT security architecture defines the security zones for data storage and processing and the zone transitions for admissible data transfer. TOP SECRET is a classification level that generally accounts for about 20 % of an organisation's total data volume.

The other 80 % or so of the data that can be assigned to other classification levels (SECRET, CONFIDENTIAL, etc.) can be transferred without difficulty to field offices and home offices via a community cloud. Community clouds are shown to their best advantage in this context albeit with a reduced level of security.




Sensitive data never leaves the protected private cloud but can be viewed and edited risk-free using our remote access solution. The remaining data volume of about 80 % can be processed in a community cloud.

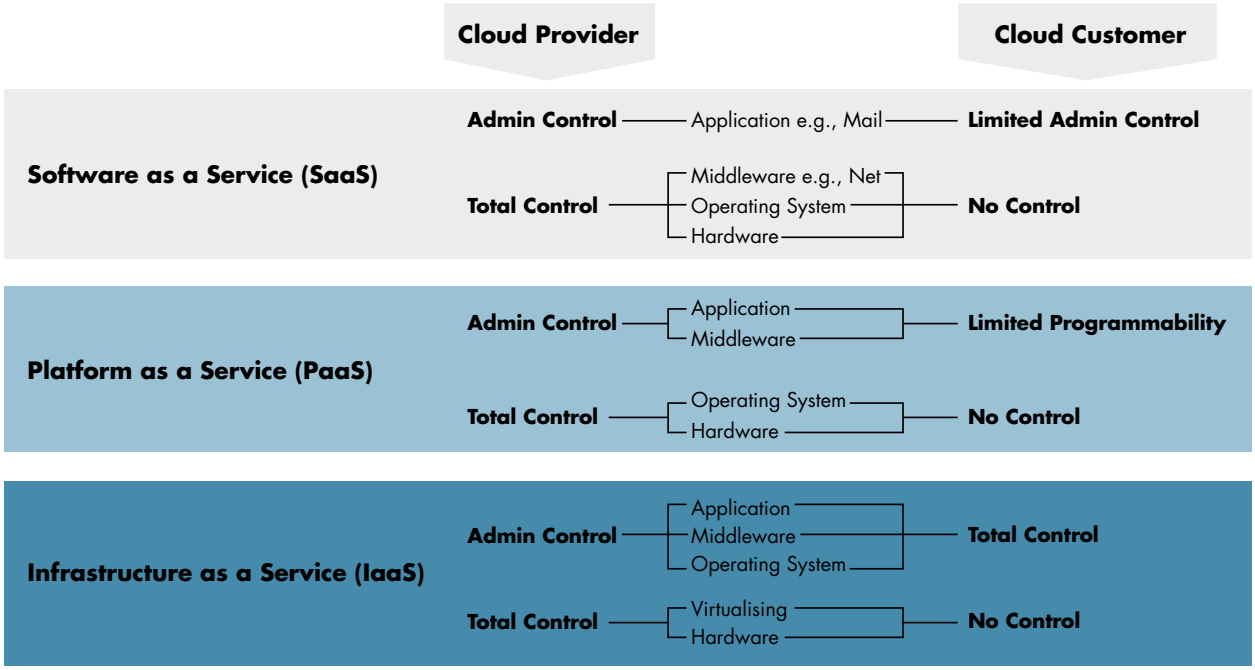
**WHAT IS CLOUD COMPUTING?**

- Computing capacity from the Internet (cloud)
- Is leased in minutes without having to contact the provider
- You only pay for services and applications you actually use
- Computer networking and synchronisation in the background
- Can cover maximum peaks for computing capacity and storage requirements
- Usable with any terminals at any location

### Responsibility and flexibility in the cloud

The flexible purchasing of IT services from the cloud affects the cost structure dramatically and goes a long way towards explaining the success of cloud computing. If an organisation needs additional IT capacity one day for 200 employees but the next day for just 20 employees, it only pays for the services it actually uses. This flexibility in computing capacity is optimised by the elimination of step-fixed costs.

On the other hand, responsibilities change when IT services are outsourced. The cloud provider assumes the role of IT administrator and, as such, has access to the users' stored and processed data. The cloud provider must be able to guarantee that users can utilise its services as needed. The cloud users themselves retain only limited influence on office applications and platforms.




The cloud provider has extensive access to customer information because it has to guarantee the customers the service in its capacity as administrator.

**Sources:**
2011 ISSS Conference in Bern 2011, 1 September 2011, Willy Müller
Professional Computing, Issue 4, December 2011, Cloud Computing Trends 2012
"Multimedia und Unterhaltung" No. 44, 1 November 2011