THE SKY IS FULL OF DATA

That is why Cloud Computing is the storage of the future

COLLENDA

Cloud computing through the years

When the idea of cloud computing was born, IT departments still looked like the set from a James Bond classic. Clunky mainframe machines with the power of today's pocket calculators filled the rooms. Scientists in white coats and tailored suits programmed the first applications on them. IBM employee Dr. Herbert R. J. Grosch was one of these pioneers. The Canadian, born in 1910, was already working in the 1950s on the so-called time-sharing method, which was to allow access to the mainframe computer from several terminals. The original idea of cloud computing had been conceived.

And today, over 60 years later? Storage in the cloud has long been established in both the private and corporate sectors. This is also reflected by the figures: 35 percent of the German population aged between 16 and 74 use cloud services to store files, according to the latest figures from the European statistics authority Eurostat - and the trend is rising. This puts the Germans exactly in line with the European average. Pictures are moved to the cloud, programs such as Google Docs or Microsoft 365 are used in the cloud, backups from smartphones or PCs are stored in the cloud. Access is possible from any location.

In the business world, the use of the cloud has so far been particularly popular among large companies. According to the Federal Statistical Office (Statistisches Bundesamt), 62% of all companies in Germany with 250 or more employees use cloud services (as of January 2021). Services for storing data (60%), e-mail services (56%) and office applications such as word processing or spreadsheets (47%) are used particularly frequently. These figures will increase significantly in the coming years. Because one thing has been revealed by Corona at the latest: Companies that have pushed ahead with digitization before the pandemic have a decisive advantage in these difficult times.

Companies with subscription to fee-based IT services in the cloud	Employees		
	10 - 49	50 - 249	> 250
	Share in % of all companies		
Total	31	41	62
E-Mail	57	54	50
Office-Applications	45	52	55
Databases	36	39	39
Storage	65	68	67
Finance Applications	40	36	27
CRM-Software	18	23	30
Computing capacity own software	20	24	36

Table 1: Usage of Cloud Computing (Source: Statistisches Bundesamt)

Advantages of cloud services

The advantages of cloud computing are obvious: data and applications can be accessed online from any location. Standardized services are less prone to errors and can be offered faster and at a lower price than many companies could implement with their internal IT. Cloud computing also has a decisive advantage over on-premises solutions when it comes to implementation: speed. Computing power and storage space can be booked at the touch of a button and used immediately, without the company's own IT department having to purchase and set up hardware. The fact that capacities in the cloud can be adjusted at lightning speed also leads to

greater cost efficiency. Larger companies in particular usually operate from multiple locations. Data and applications are available in the cloud for all employees, regardless of where they are located. This factor is even more decisive when expanding abroad. Here, too, “data in the sky” offers advantages, as companies can start operations without major start-up investments and respond flexibly to market developments. Delays due to time differences no longer exist.

Cloud or on-premises? A question of requirements.

So is a cloud solution always preferable to on-premises infrastructure? It is difficult to give a blanket answer to this and depends on various factors. One argument in favor of the on-premises solution may be that older software does not run smoothly in the cloud. Also, the lack of Internet bandwidth has been an issue in the past. On-premises solutions had the edge here due to lower latencies. That is completely different today. Most private households have very fast Internet connections by now. In addition, there are special solutions that can reference and transport mass data via special interfaces.

Since the customer in the cloud usually shares the resources with other customers - whether virtually or physically - the topic of the General Data Protection Regulation (GDPR) must of course be a particular focus. It is imperative that every cloud solution complies with all GDPR requirements!

The security of trade secrets - i.e. "intellectual property" - is also the reason for many a company to choose an on-premises solution. However, many experts now believe the risk in cloud environments is similar, if not lower. Security departments can react more quickly to cyber attacks in the cloud and do not first have to search for errors in their own infrastructure. In its "Cloud Monitor 2020", the auditing firm KPMG states that while suspicious cases are increasing, security incidents are decreasing. This is a clear indication that many cloud providers have done their homework when it comes to security. As a rule, cloud providers have greater security expertise than the internal IT departments of many companies and offer up-to-date and specialized tools for access and vulnerability control.

Last but not least, in the rare event of a natural disaster such as a fire or flood, the cloud can become a data savior for a company.

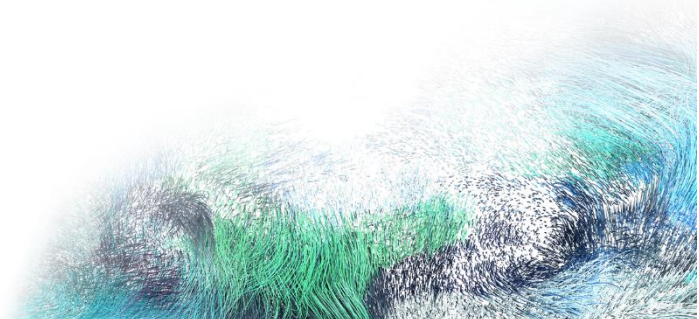
Types of cloud services

- **Private cloud:** The IT infrastructure is provided dedicatedly for one user, for example a company.
- **Public cloud:** Here, the provision of a large infrastructure for various users takes place via the Internet. There is a virtual separation of customer environments.
- **Community cloud:** Similar institutions are interconnected in an IT infrastructure.
- **Hybrid cloud:** A combination of different cloud structures, for example a private cloud with parts of a public cloud. Virtual hardware is provided to the customer on a dedicated basis.

Measures for optimum protection of data in the cloud

Nevertheless, an intelligent security architecture by the cloud provider is of course indispensable to ensure optimum protection of data. This applies in particular to areas where sensitive information flows through the data cables. For this, it is important to pay attention to different security features.

- **Configuring the cloud**: Secure configuration of infrastructure and services is the first important step in setting up the cloud. Even during deployment, the services of cloud providers must comply with certain controls and regulations. An indication that cloud providers take security seriously are corresponding certifications.
- **Certification**: Audits such as ISAE3402 or ISO 27001 provide proof that companies meet certain process and security standards in segments such as reporting, incident and change management, logical access management (role authorizations and internal processes) and general IT controls. It is important to note that both cloud providers and cooperating provider solutions, for example, must meet the relevant certification.
- **Data backup and encryption**: A no-brainer for any serious IT professional: regular data backups are essential. They should be performed by both the cloud operator and the user. In the event of data loss or prevented access to the data, this always ensures an emergency solution. In addition, data on hard disks, backup media and in databases should always be stored in encrypted form. Even in transit, this data must be encrypted end-to-end by using HTTPS and SFTP.
- **Access restriction**: Access to the cloud from outside can be restricted to a specific IP range or via site-to-site VPN: the IP range grants access in advance only to certain IP addresses; VPN means Virtual Private Network, in which only partners belonging to the network are in encrypted connection with each other. Site-to-site VPN usually describes a connection of branch office networks with the network of the company headquarters.



Both options simply lock out unauthorized user groups.

- **Separation of duties and responsibilities**: Access rights management must deny data access to unauthorized parties. Access should be permitted according to the principle of "knowledge only when necessary". To this end, the management of user rights must be organized, regularly reviewed and logged. Classified information is separated from public information and access rights are assigned according to the least-privilege principle.
- **GDRP compliance**: On the subject of the General Data Protection Regulation (GDPR), both cloud operators and cloud users have a duty. For example, a server location in Germany or Europe is a relevant factor for GDPR compliance. For error-free implementation, the help of a data protection officer should be sought in case of doubt.
- **Pentests**: Vulnerabilities in the security umbrella should be tested regularly. Cloud users can put security to the test with so-called pentests (penetration tests). This is usually done by hiring an external service provider who floods the servers with spam or tries to hack into the systems as a test. In addition, of course, there should be continuous protection of the infrastructure, through physical, operational and software-based measures. Regular Docker image scans help identify vulnerabilities early on.
- **Industry specifics when outsourcing data**: Different regulations must be considered in different industries. In banking, for example, the German Federal Financial Supervisory Authority (BaFin) requires certain certifications and measures in accordance with BAIT (Bank Supervisory Requirements for IT) or MaRisk (Minimum Requirements for Risk Management in Banks). These requirements must be carefully checked before data is outsourced to the cloud.

More Information

About Collenda

Collenda is a leading supplier of credit management and collections software to banks, corporations and collections agencies across Europe. Backed by deep industry experience, Collenda offers a cloud-ready suite of applications for managing consumer and commercial credits which help automate the complete credit lifecycle from first application to final payment. Collenda's comprehensive product suite utilizes smart workflows, artificial intelligence and user-friendly self-service apps, which help to ensure efficiency and accuracy in the handling of credits for creditors and their customers.