NEWSLETTER
INSURANCE AND FINANCE

THE GENEVA ASSOCIATION

No. 14, August 2014

Cloud Computing: a Fundamental Shift in IT

By Farhad Khalilnia[+]

Synopsis

This article presents a broad overview of cloud computing, addresses common questions and some of the relevant issues that face sensitive and regulated industries such as finance and insurance.

Cloud coming-of-age

Cloud computing today refers to the process of leasing computing assets and the set of added services and assurances that accompany these assets, like provisioning services, backup systems, applications or service level agreements.

The recent surge in cloud computing is due the convergence of a number of technologies making it more secure, user-friendly and cost-effective, as well as a mindset shift as people have been exposed to the likes of Hotmail, Dropbox, Facebook and numerous other cloud-based services.

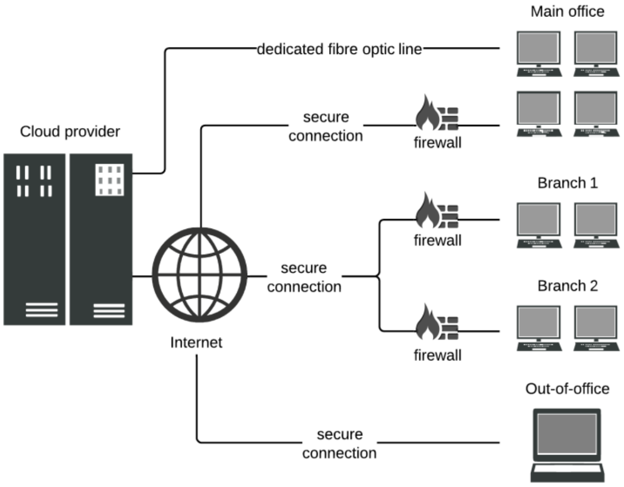
Developments in Internet networking now allow encrypted and secure connections across shared lines, virtual private networks (VPNs) and access to dedicated high-speed point-to-point connections across continents. Storage technologies have evolved to allow shared physical storage space—hard disks—with software separation without compromising confidentiality. Equally, the computing power—the CPUs and RAM—that runs the applications can be effectively shared and separated.

The above combination unlocks the potential for economies of scale in businesses that have traditionally thought it necessary to run their own IT infrastructures— similar to the advent of electrical power stations in the late 19th century, before which factories and wealthy households ran their own generators, including raw material sourcing, stokers and engineers.

It is now possible to plug into the net, use all of your computing resources as necessary, without concerning yourself with how it is provided, and pay one transparent flat fee.

[+] Farhad Khalilnia is founder and CEO of the Swiss private cloud provider Penta Corporate Hosting Ltd.. He was one of the pioneers of server-based IT infrastructures for business in Switzerland in the last 1990s. Penta is based in Geneva and Dubai, and specialises in compliant, audited and secure cloud-based IT for the financial sector and other sensitive industries.

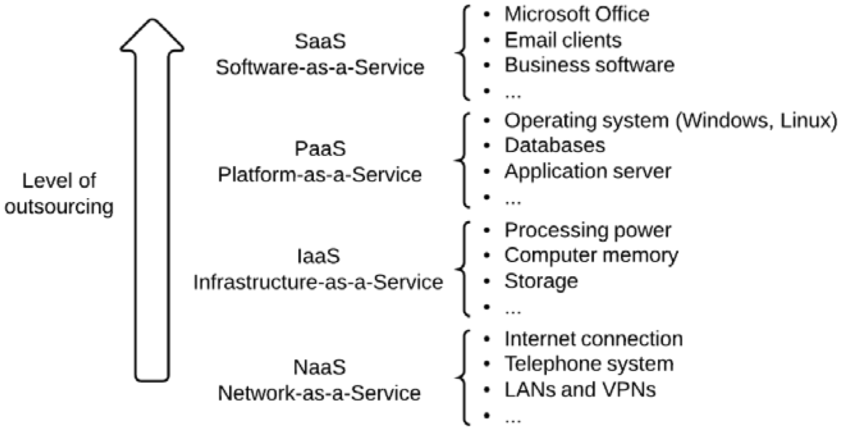
Figure 1. A basic cloud set-up



How it works

There are different levels of IT cloud outsourcing, illustrated in figure 2 below:

Figure 2. Levels of IT outsourcing



Having an outside company manage your network or network-as-a-service, such as telephones, Internet connections and routers, is already widely adopted.

Outsourced infrastructure-as-a-service is also a familiar, typically local IT company that will install computers and servers in your office and dispatch technicians for maintenance. In a cloud set-up, there is still a need for basic desktop computers. However, these serve merely to connect to the off-premise hosted data centre, sending keyboard strokes and mouse clicks one way and receiving the monitor image on the other. Today's high-speed connections make the interaction seamless and office computers only need basic specifications as the real work takes place in the cloud.

Platform-as-a-service dispenses with the need to buy and maintain your own operating systems and databases. The necessary platforms are run from a data centre and delivered on a continuous basis—including updates, security patches, new versions and so on.

Software-as-a-service takes the concept a step further and delivers the end-user applications—the actual software used to work such as Microsoft Office and custom or off-the-shelf programmes.

Opportunities for risk mitigation

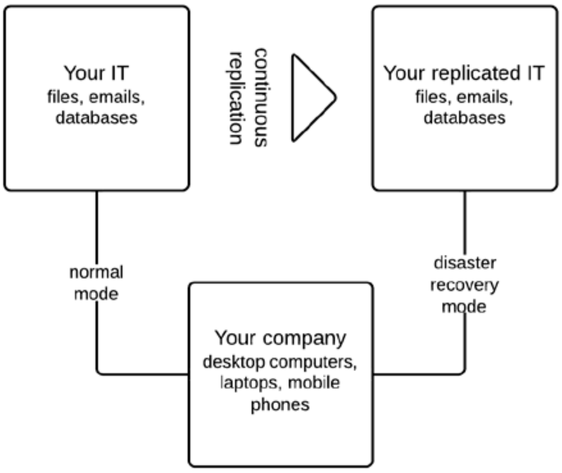
With IT so central to modern business, the cost of downtime or data loss can be high, even existence threatening. A properly run IT department will devote substantial resources to manage these risks.

Geographically separated and physically isolated data centres allows for easier and more cost-effective risk mitigation than an in-office server. For example, multiple electricity and internet suppliers, generators, fire suppression systems and biometric access controls among other safeguards can be designed for and brought in for several providers.

Virtual threats are managed centrally and for multiple clients simultaneously, meaning more and better equipment and expertise can be dedicated to implementing and monitoring processes, ensure quick reaction, and keep systems and knowledge up to date.

Business continuity and disaster recovery are well-developed disciplines that have evolved beyond the traditional backup copy. Deduplication ensures that multiple copies of files are only backed up once, while the parallel copying of multi-threaded restores drastically reduces the time to get back up and running again. Continuous active-active backup between data centres means minimal data loss at any given moment and the ability to automatically fail-over without the end-users even noticing that there is a problem.

Figure 3. Business continuity and disaster recovery set-up



Installing and maintaining a state-of-the-art business continuity and disaster recovery infrastructure is expensive and resource intensive. A cloud provider is able to use the same sophisticated infrastructure for many companies and spread the cost.

Is it secure?

Cloud is a very broad term that refers to innumerable different infrastructure set-ups. It is possible, for example, to have your own hardware and network connections set up in a completely “private” cloud with no physical sharing whatsoever. On the other end of the scale are “public” clouds where there is little or no control over where, how and with whom your data is stored.

One way to conceptualise it is to consider that the risk of intrusion or data loss is exactly the same in-house as in the cloud, given the exact same security measures. The question then becomes, can your in-house set-up match what a dedicated cloud provider can bring to bear? Does your server get knocked every time the vacuum cleaner goes by? Is all the hardware replaced every three years? Is access to the server room logged? Are the USB ports isolated from company data? How long will it take to restore the company network in case of a fire?

The technology today can completely separate data on shared hardware with zero leakage. You can also choose to have all your data encrypted so that not even the cloud provider can read it or have a physical key to access your own hardware within the external data centre.

Regulatory compliance

Regulated industries such as finance and healthcare are mostly required to meet certain standards in IT and data handling. Certification schemes and legislation vary, but generally involve meeting certain best practices with regards to hardware set-ups, operational processes, and keeping the data in certain jurisdictions. Previously, this translated into tight in-house control of IT that could be audited for regulatory compliance.

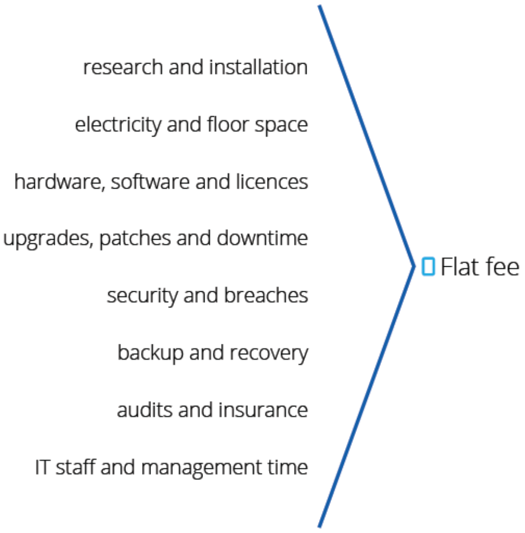
Cloud technology these days can meet and exceed the most stringent regulatory compliance standards, which means an interesting advantage over in-house IT—a single audit or certification ensures all the hosted companies meet the required compliance standards. Again, the costs can be spread across multiple clients.

Changing cost structure

The true cost of in-house IT can be elusive—like when owning a car. The transparent costs include hardware, software licences and IT staff. However, the financial impact during the whole life cycle includes lost productivity while employees troubleshoot their own or colleagues' problems, purchasing research, migration expenses, electricity and floor space, downtime and recovery, training, insurance, decommissioning and auditing, among dozens of other items. In a cloud set-up, most of these costs are managed by the provider while the business pays one flat predictable fee (see figure 4).

Capital expenditure on IT is reduced to barebones desktops or laptops while the outlay for heavy duty machines, servers, and allowance for future capacity is moved to scalable and predictable operational expenditure.

Figure 4. Total cost of ownership


research and installation
electricity and floor space
hardware, software and licences
upgrades, patches and downtime
security and breaches
backup and recovery
audits and insurance
IT staff and management time
Flat fee

Trust, but verify

The one disadvantage of outsourced cloud computing is a loss of control—at the end of the day, your data is being handled by an external supplier.

For that reason, it becomes critical that the custodian of your data plays it straight and transparent, and does not gloss over difficulties. Ensure they can deliver what is promised, that they are financially secure, and that you can take your data elsewhere if relations deteriorate.

The key to a successful outsourced cloud implementation is trust—backed by checks, certifications and auditing.