MFSA FinSights | Enabling Technologies

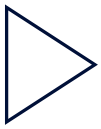
Cloud Computing

The financial sector is continuously evolving through the rapid development and adoption of new technologies. The term 'FinTech' generally refers to financial innovation that seek to provide enhanced financial service offerings through the utilisation of enabling technologies. These generally include Distributed Ledger Technology & Smart Contracts; Artificial Intelligence, Machine Learning & Big Data, Cloud Computing, Web 3.0, Application Programme Interfaces and Micro-Services; Robotic Process Automation and the Internet of Things.

As part of the MFSA's initiatives to generate awareness, drive culture and deliver a cross-sectoral knowledge platform which can support the MFSA's functions in preparing for the financial services of tomorrow, these insights will delve into enabling technologies, enabling innovations and their sectoral applications.

1 What is Cloud Computing?

While Cloud computing traces its origins back to the 1960s during the early stages of the Internet, it was in the early 2000s that the modern-day version of this technology gained popularity. While innovations within this space are ongoing, the most pertinent definition of Cloud Computing is that provided by the National Institute of Standards and Technology (NIST) which defines it as, *"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"*. This definition identifies five characteristics which are central towards this technology:



On-demand self-service: no human interaction is needed to access the cloud resources.

Broad network access: the user can access the cloud via the internet from different devices.

Resource Pooling: the provider pools its computing resources and allocates them to the user as needed.

Rapid Elasticity: the capacities can be provisioned flexibly, so that the storage and performance seem unlimited.

Measured service: the cloud system automatically monitors the use of the service and optimizes it.

1.1 Service models

As illustrated in Figure 1 below, there are four possibilities how Information Technology (IT) can be managed. While the first model, **On-premises** is fully managed internally, the remaining models utilise cloud-computing through reliance on cloud service providers through service models, as follows:

1. **Infrastructure-as-a-Service (IaaS)** – In an IaaS model, consumers are in control of storage, deployed applications, and operating systems; but does not exercise control over the Cloud Infrastructure and may have limited control over certain networking components like host firewalls. Consumer resources are then connected to the Service Provider's servers via Application Programming Interfaces ('APIs').

2. **Platform-as-a-Service (PaaS)** – Under a PaaS model, consumers exercise control over deployed applications and configuration settings but do not manage operating systems, storage, or servers. This model also allows consumers to deploy applications onto their Cloud Infrastructure using the tools provided by the Cloud Service Provider. Thus, such models may also provide the user with access to

emerging technology and solutions utilising, amongst others, Quantum Computing, Artificial Intelligence, and Internet of Things.

3. **Software-as-a-Service (SaaS)** – Under this service model, consumers do not exercise control over the Cloud Infrastructure but are granted the capability to use the Cloud Service Provider's Application Software and may at times have limited access to application configuration. Nevertheless, this model makes it possible to test applications easily and quickly, without investing lots of time or money.

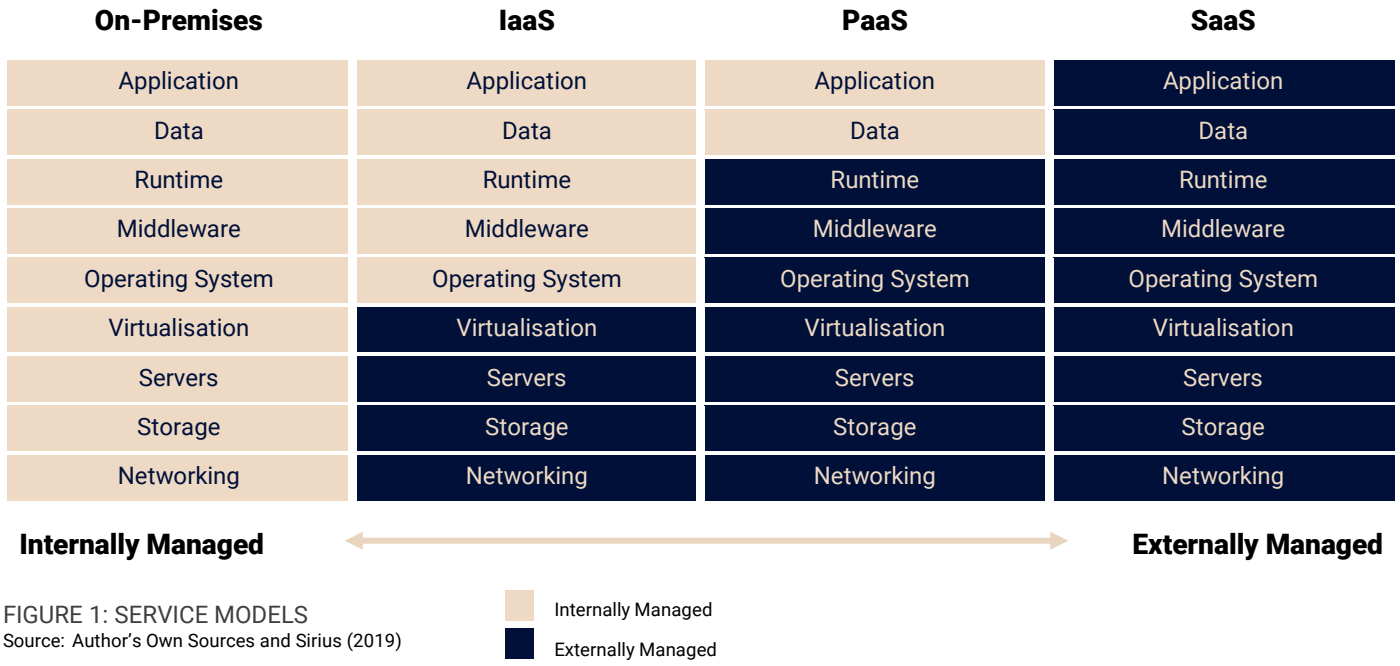


FIGURE 1: SERVICE MODELS
Source: Author's Own Sources and Sirius (2019)

1.2 Deployment models

Beside the different service models, there are also various cloud deployment models as illustrated in Figure 2 below. In many instances, reference to cloud services is synonymous with public cloud service providers namely, Google, Microsoft and Amazon. However, many different types of cloud services are available on the market, some of which include:

1. **Private Cloud**
   The Cloud Infrastructure is set up for one organisation and managed by the organisation itself or externally via a third-party service provider. An example of a private cloud deployment model is colocation[1].

2. **Public Cloud**
   This type of cloud environment offers IT infrastructure to the public, via the provider's resource availability. This deployment model may be managed by a government, business, or academic organisation.

3. **Hybrid Cloud**
   This deployment model combines different cloud infrastructures, such as the private and public cloud. The cloud's environments are independent but remain interconnected to exchange information.

[1] 'Colocation is a private cloud deployment model where the organisation purchases or leases servers, networking equipment, software and rack space, all of which reside in a data centre managed by the colocation services provider'. (MFSA 2020, p.25)

4. **Community Cloud**
   Such cloud solutions are accessible limitedly to members of a community of organisations, such as universities, which share a common purpose, concerns, and needs.

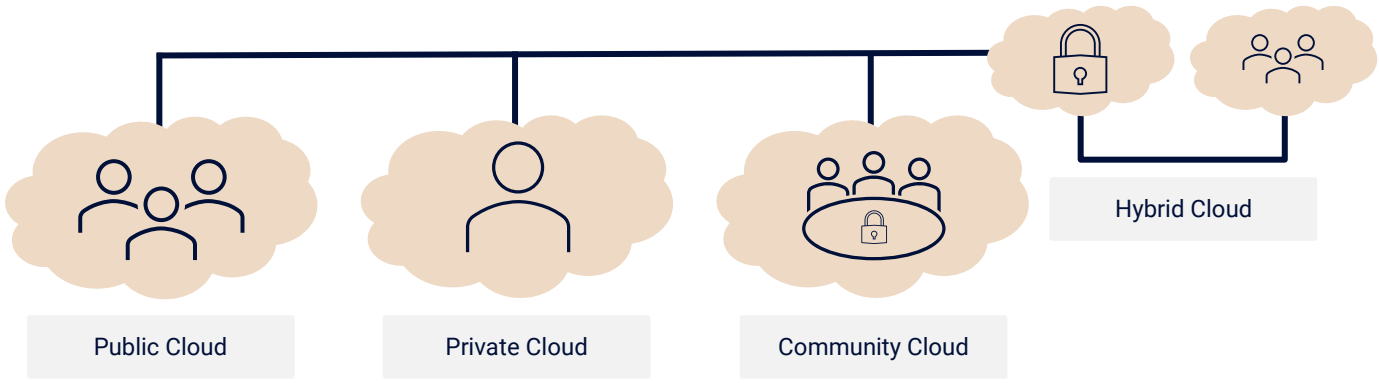


FIGURE 2: DEPLOYMENT MODELS
Source: QSS Technosoft (2019)

2 Benefits and Risks

Cloud Computing has several benefits and risks. Moving the whole IT-infrastructure to the cloud opens several advantages but also introduces new risks concerning outsourcing.

BENEFITS

Costs and Economies of Scale – With cloud migration, an organisation can save substantial resources on hardware. In addition, amongst others, the expenses for energy, premises, security and equipment will decrease, as well as the support costs for help desk or maintenance. The cloud service provider will take over these expenses along with the services and can provide them at a lower price as the cost is spread over a large number of users. The pay-per-use model also provides users with the ability to easily and efficiently scale up or down their IT resources and only pay for such resources when required.

Innovation – such solutions have lower market entry costs and other barriers to entry into new or existing markets as well as enhanced efficiencies, thereby fostering greater competition and innovation. This allows organisations to focus completely on their objectives and potential innovations.

Agility, Mobility and Scalability – Cloud computing makes an organisation more agile as it enables a faster and more cost-effective response to change. This increases the likelihood of achieving the user's objectives, such as sales, customer onboarding, and makes it possible to have a higher and long-term cost reduction, along with a more effective risk and reputation management. Cloud computing improves the way of working for the whole organisation. It enables an open technology and business environment, which creates a new approach for the provision of services. Persons having access to such cloud infrastructure can access the system at any time, thereby creating a better connected and more responsive environment. Moreover, given that not every organisation has the same IT needs, cloud computing enables the user the possibility to increase the capacity they need in an efficient manner without requiring investment in physical infrastructure.

Remote working – Another advantage is associated with the opportunity to work remotely. During Covid-19, organisations with a cloud infrastructure had access the organisation's data and information from everywhere and anywhere in the world. Collaborative tools and video conferencing software, which is

nowadays usually built on such environments have also reshaped how organisations function in their day-to-day business as usual.

RISKS

Data Security – Losing control over data that has been transmitted to the cloud is one of the biggest risks a user faces even more so when various parties are involved. Therefore, it is imperative that the handling of data is carried out in accordance with best practices and international standards. Agreements concerning this topic can be made through special clauses in the contract, service level agreements and conditions of a contract, which also typically include additional security practices such as systems and IT audits.

Vendor Lock-In – This occurs when a user of a particular cloud service provider finds it hard to switch providers. In this respect, users should, among other things, make use of best practices and international standards, have the necessary guarantees in places that migration to another service provider is possible and have clear exit strategies in the event of migration and/or issues arising from the provider such as Interruption of Service and closure.

Interruption of Service – Cloud systems are not infallible and an interruption or a failure of service beyond what is stipulated in the service level agreement may still occur. A backup plan and data backups are mandatory when critical data and applications are being transmitted over the cloud. A stable internet connection between the user and the cloud provider is also required, otherwise business continuity is not guaranteed.

Laws and Requirements – Many countries have mandatory regulatory frameworks and/or best practises covering various aspects of cloud computing. Additionally, most countries nowadays have data privacy requirements such as the European Union's General Data Protection Regulation (GDPR) which only permit users to host data in specific locations. Therefore, users may need to take into consideration the various frameworks across multiple jurisdictions, which may not always be fully aligned.

In conclusion, cloud computing is a great technology to enhance the operations of a business. Nowadays, remote working and flexibility are very important. However, one should not underestimate the risks these may introduce. An elaborated IT-strategy concerning the exit and backup plan is essential to mitigate the risks that may occur.

Supplementary Reads…

Peter Mell and Timothy Grace, 2011. The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology. Available online.

Bernardo Nicoletti, 2013. Cloud Computing in Financial Services, *Palgrave Macmillan Studies in Banking and Financial Institutions*. Available online.

EBA, 2019. EBA Guidelines on Outsourcing Arrangements. Available online.

The Malta Financial Services Authority, 2020. Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements. Available online.