IT Infrastructure

Security and Resilience Solutions

Ralf Süß
Yannik Süß

Apress®

IT Infrastructure

Security and Resilience Solutions

Ralf Süß
Yannik Süß

Apress®

IT Infrastructure: Security and Resilience Solutions

Ralf Süß
Singapore, Singapur, Singapore

Yannik Süß
Unterhaching, Bayern, Germany

ISBN-13 (pbk): 979-8-8688-0076-4
ISBN-13 (electronic): 979-8-8688-0077-1
https://doi.org/10.1007/979-8-8688-0077-1

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Coordinating Editor: Shaul Elson

Cover designed by eStudioCalamar

Cover image from www.pixabay.com

Distributed to the book trade worldwide by Apress Media, LLC, 1 New York Plaza, New York, NY 10004, U.S.A. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub (https://github.com/Apress). For more detailed information, please visit https://www.apress.com/gp/services/source-code.

Paper in this product is recyclable

In gratitude for that initial laptop from father to son, laying the foundation for our deeply cherished and shared path in technology.

Table of Contents

About the Authors

Ralf Süß has dedicated over 40 years to the IT industry, deepening his expertise in all aspects of computing, data center design, and management. His experience is underscored by a significant role with Hewlett Packard's Pacific Asia Technical Sales. Ralf's professional journey has led him to collaborate with global giants in the realm of cloud services, including Amazon, Apple, and Microsoft. In tandem, he has catered to the needs of renowned network equipment providers, including Ericsson, Nokia, and Cisco. Melding theoretical acumen with practical experiences, Ralf has seamlessly adapted, ensuring his skills remain both relevant and innovative. This adaptability, combined with his rich experience, positions him as a knowledgeable figure who consistently offers insights and reflections from his vast tenure in IT infrastructure.

Yannik Süß has an extensive two-decade background in the Web and e-commerce. Driven by a deep passion for technology, he has managed critical web projects, spanning from site development to intricate e-commerce platforms. Proficient in data-driven decision making, he has implemented and overseen the development of robust data warehouses to optimize business intelligence and analytics. With a master's degree in

Strategic IT Management and an ongoing doctorate, Yannik expertly bridges theoretical frameworks with practical challenges. He has also authored the second edition of *E-commerce for Small and Medium-sized Enterprises*, published by Springer, showcasing his comprehensive grasp of the digital commerce landscape.

Introduction

This book describes how IT systems have evolved from a relatively marginal role to perhaps the most essential pillar of modern infrastructure. Even in the 1950s, infrastructure was an element of roads, bridges, electricity, water supply, wastewater collection, and voice telecommunications. Today, we can hardly imagine living in a world without ubiquitous telecommunication and IT services. In this book, we explain how critical building blocks such as data centers, computer systems, storage systems, and IT security systems have evolved and how they provide the foundation to build a state-of-the-art resilient IT infrastructure.

How Did It All Begin?

Computing started in the fields of science and military applications. However, at the beginning of the computer era, the most famous historical event is probably the system that Alan Turing, an English mathematician, created during World War II. His machine was able to break the secret Nazi communication code. The Nazis had used the Enigma, a mechanical encoding machine, which created a changing encoding pattern every 24 hours. It was considered unbreakable. With Turing's "computer system," the British intelligence service was able to decode Nazi internal communication. This proved to be one of the contributing factors that eventually led to the end of World War II.

Until the 1950s, the word "computer" was mainly used to describe the actual people who did calculations for an organization, such as people calculating data in a research institute. The emergence of the

word “computer” with a broader audience, as depicted in Figure 1, began to occur only in the 1960s, shaping our modern understanding of it. IT systems have come a long way during the last 60 years.

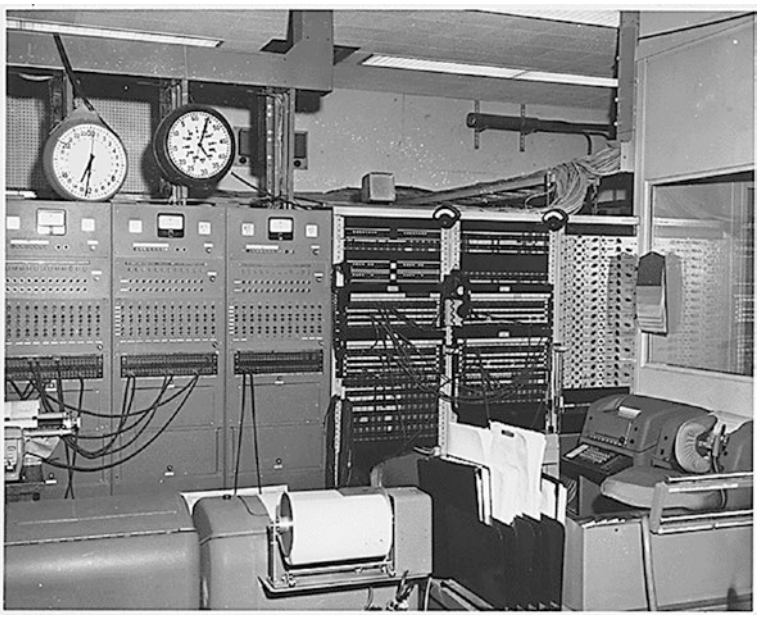

Figure 1. *Computers at NASA (NationalArchivesCatalog, 1952–1968)*

At the beginning of the 1960s, IT systems were just emerging and had a limited list of applications:

- **Military systems:** Military systems were important applications for computers at this time, mainly in the fields of surveillance, cryptography, missile defense systems, and logistic systems.
- **Scientific research:** The second leading application for computer systems, mainly used for modeling and simulations, was scientific research.

- **Government applications:** Governments used computers in several fields, such as tax collection and census analysis.
- **Business applications:** Business applications were limited to the accounting and payroll processing of larger organizations.
- **Education:** Computers were primarily used for research and teaching purposes for education.

Today's IT Infrastructures

Leaping forward 60 years to today, IT systems have become an integral part of modern-day society, and their importance cannot be overemphasized. There were two main phases. First, from the 1960s to the late 1990s, computer systems played an ever-increasing role in supporting a company's business. Computer systems were used for everything from hiring people, accounting purposes, sourcing materials, managing supply chains, providing marketing, driving sales, internal training, and so forth. In the second wave of computing, IT systems were not just supporting companies' business, they became an essential part of a new type of company. Google, Facebook, Amazon, Airbnb, Netflix, and Uber are companies that have built their core business with applications running on computer systems.

Today's world of social media is entirely built on computer systems and modern telecommunication infrastructure. At the core of the second wave of computerization is the evolution of the Internet, which enables people to connect to almost anybody in the world in real time from anywhere. In addition, the ubiquitous presence of the Internet made it possible to automate most business processes.

In summary, IT systems have become an essential part of our daily lives. How we live, work, and communicate has drastically changed over the last 60 years. As technology continues to evolve, IT systems will continue to play an increasing role in our societies for the foreseeable future.

In the next chapter…

- IT evolution
- CSP
- Cloud services

CHAPTER 1

The Architecture of IT Cloud Services

From mainframes to cloud computing, cloud services have evolved over the years and were mainly driven by the advancements of three hardware pillars, namely: computer systems, storage systems, and data networks. We will look closer into the evolution of these three components in Chapters 3, 4, and 5. However, in retrospect, the eras in this technological evolution span in this way:

Mainframe computing (1960s to 1980s): Large, expensive, and complex machines were called mainframes, primarily used by large organizations for business applications like payroll and accounting. Mainframes are centralized computer systems where all processing and data storage occur on a single machine. During this period, IBM was the dominant computer company to the degree that the words "computer" and "IBM" were used synonymously.

Client-server computing (1980s to 1990s): Although the mainframe era was based on a fully centralized concept, the emergence of technical workstations for engineering and PCs for general

R. Süß and Y. Süß, *IT Infrastructure*, https://doi.org/10.1007/979-8-8688-0077-1_1

office purposes changed the landscape drastically. During this time, computing became more decentralized as data processing and storage were distributed across multiple machines. In addition, servers handle requests from numerous clients, such as a database server. An essential enabler for this era was the development of the Ethernet and the TCP/IP, which allowed for the first-time communication between computer systems manufactured by different vendors and running other operating systems.

Internet computing and utility computing (late 1990s to mid-2000s): The client-server era changed the architecture of applications. Until the 1990s, applications were running on a vertical stack from a vendor that included micro processes, operating systems, middleware, and application. Everything was proprietary, and moving an application from one vendor to another was a massive effort. During this era, the application architecture started to become horizontal, and many vendors used the same microprocessors from Intel and Motorola, standard operating systems such as Unix and Windows, and standard database software from vendors like Oracle and Informix. This made it possible to move an application from one vendor to another. In addition, the wide adoption of the Ethernet and TCP/IP enabled general connectivity between all computer systems that allowed such access.

The Internet emerged with even more enhancements and standardization of crucial protocols, including network protocols, and the development of browsers. The application became web based with early adoptions such as email, search engines, and e-commerce. These services were delivered over the Internet and were accessible from anywhere as long as there was a stable Internet connection.

These developments lead to the next step: utility computing. Amazon was the first starting to build large data centers and offered IT services like a utility under the AWS (Amazon Web Services) brand. Microsoft followed Amazon under the brand Azure. Later, Google entered the market with its Google Cloud Platform.

Cloud computing (late 2000s to present): Cloud computing evolved from utility computing. Cloud services are delivered on a pay-per-use basis, allowing organizations to scale up and down the IT resources they need. The data cloud center depicted in Figure 1-1 showcases a large facility comprising multiple server racks arranged in a highly organized manner.

Over time, cloud service providers (CSP) have built massive IT infrastructure resources that power a fair share of global IT applications. As a result, IT has become for modern societies what electricity was at the beginning of the industrial revolution.

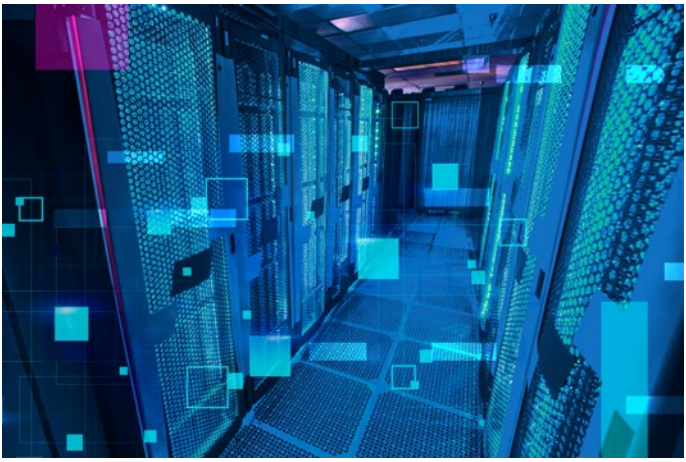

Figure 1-1. *Cloud Data Center Example (rawpixel.com, 2023)*

1.1 Cloud Services

The main characteristic of Cloud Services (CSPs [is this correct?]) is its distributed computing model. A vast number of servers are installed in racks and connected through a highly reliable and fast DC network infrastructure. This allows CSPs to provide services to organizations over the Internet. Although the cloud data center infrastructure varies depending on the benefits offered, several features appeared in most systems:

- **Virtualization:** Virtualization technology allows for the creation of virtual machines or containers that will enable multiple users to share the same physical hardware that will ensure efficient resource utilization by scaling their services to meet demand.
- **Data storage:** User data is stored in distributed storage systems that are designed to scale and provide high data security, such as file systems or object stores.

- **Load balancing:** In cloud environments, applications are distributed through a load balancer. This has two main advantages:
    - First, workloads can be distributed to resources that are not used.
    - Hardware problems become minor issues, as the load balancer can quickly move a workload from one defective system to another system.
- **Security:** Cloud services use various security measures to protect user data, including encryption, access controls, and monitoring. Processes to run and monitor a data center will generally be more advanced with larger CSP organizations than with smaller IT organizations.
    - **Front end:** Cloud services can be provisioned through several front ends, including a web browser, a mobile app, or a command-line interface.
    - **Back end:** The server infrastructure, storage systems, and the software that provides the service are called the back end of a CSP.

The CSPs have built their infrastructure based on an advanced cloud services architecture designed to provide users with scalable, reliable, and secure services over the Internet.

1.2 IT Services Provided by CSP

With CSPs' introduction of cloud data centers, a growing share of IT workloads was moved from private data centers, also called private clouds. At first glance, this looks like an either/or approach. An organization

operates its private cloud or uses a CSP. But organizations use private and public clouds at the same time. The CSPs offer several options to use their IT services, most commonly

1. Data as a Service
2. Communications as a Service
3. Infrastructure as a Service
4. Platform as a Service
5. Software as a Service
6. Business as a Service
7. X as a Service

Here is a description of each of them.

1.2.1. Data as a Service (DaaS)

Data as a Service is a model for distribution and information provision, which allows customers to access various data files via a network like the Internet. Data files include text, images, sounds, and videos. This model offers customers and client-oriented enterprises convenient and cost-effective solutions. Data as a Service enables decoupling data cost and utilization from platform or software cost. The prices DaaS providers offer can be volume or format-based.

Volume-based pricing contains a fixed price per megabyte of data in the whole repository. In format-based pricing, the charge is set based on the data format. Data as a Service can easily move data between platforms. This avoids the conflict and confusion arising from multiple copies of the same data or file. In addition, DaaS implements access control measures like strong encryption and passwords, avoiding "vendor lock-in," ease of administration and collaboration, diverse platform compatibility, automatic updates, and global accessibility. These measures preserve data integrity.

1.2.2. Communications as a Service (CaaS)

Communications as a Service can contain Voice over IP (VoIP), collaboration, mobile and fixed device applications for videoconferencing, and instant messaging (IM). A Communications as a Service vendor assures guaranteed Quality of Service (QoS) and oversees all hardware and software management. Businesses operating on Communications as a Service can deploy communications and modes on a pay-per-use basis as and when they need it. The advantage of Communications as a Service is that it does not require significant capital investment and doesn't incur any ongoing overheads.

With CaaS, small and medium-sized businesses can be more flexible and expandable, which allows advantages like on-demand coverage and the addition of devices or modes. The network capacity and features are changed daily if necessary to avoid resource wastage and to ensure the functionalities are at par with the demand. This guarantees that the system is not outdated and would not require significant replacements or upgrades.

1.2.3. Infrastructure as a Service (IaaS)

Infrastructure as a Service is generally used by IT administrators, architects, and operators. IaaS provides virtual hardware resources on demand. It offers multiple on-demand features like individual email, domain name servers, messaging systems, and private networks. IaaS applications may incur OS license fees and require the installation of compatible software on the servers. Here, the customer has the flexibility to provision and de-provision the resources as per their business demand. An entire computing infrastructure can be built by an organization using an application. This type of service is beneficial for startup companies. It will help the company focus on its business process as IT infrastructure management and uptime are maintained by the IaaS cloud service provider.

1.2.4. Platform as a Service (PaaS)

Platform as a Service was mainly created for developers because it is required to run the software products, which need physical servers, web servers, and database software. The application is active on the software stack along with compilers, dependency files, etc. The disadvantage of Platform as a Service is that it can take very long and is rather complex to build the application's platform. PaaS must be updated and monitored regularly.

PaaS is directed at (because the definition of PaaS is Platform as a Service, it was repeating...) developers as it provides them with all the tools and dependency files required to develop new software (there was too much "developer"). The deployment platform, however, includes all controls to maintain the developer's customers for whom the product will be deployed. Platform as a Service provides an external platform to execute software applications without any administrative requirements of the lower-level components.

1.2.5. Software as a Service (SaaS)

Software as a Service is an application generally used by the end user. The advantage of this model is its lack of installation requirements. A network connection and a browser complete the Software as a Service requirements. The software is installed in the service provider's application server, and the customer gets the software service offshore (i.e., software delivered from the server), which is an outside organization. The service provider also achieves multi-instances, and although it has only one copy of the installation, multiple users can be handled with their dedicated storage space. Software as a Service is generally leased from a single vendor. It is an outsourced enterprise communication solution, which refers to the services hosted outside an organization.

1.2.6. Business Process as a Service (BaaS)

Any horizontal or vertical business process delivered based on the cloud service model is known as a Business Process as a Service. Software as a Service, Platform as a Service, and Infrastructure as a Service rely on this service. With the advent of cloud computing, companies prefer a more service-oriented approach. Instead of assuming that a packaged application is needed that includes business logic, data, and processes, selecting a process application not tied to a single application is possible.

A business is unable to forecast the future leverage of a business process. Hence, a Business Process as a Service must support multiple languages and deployment environments. In addition, a Business Process as a Service environment must be able to handle massive scaling. It must be able to progress from running a few to an increasing number of processes and customers. The service accomplishes that objective by optimizing the underlying cloud services to support this elasticity and scaling.

1.2.7. X as a Service (XaaS)

XaaS denotes the growing number of services distributed over the Internet instead of local or on-site provision. It is at the core of cloud computing. X as a Service uses hybrid cloud computing to deliver IT as a service. It refers to either a single or a blend of Software as a Service, Infrastructure as a Service, Platform as a Service, Communications as a Service, and Business Process as a Service. X as a Service is frequently used for the previously detached services on private or public clouds that are now integrating and becoming transparent. Table 1-1 provides a comprehensive overview of the service options.

Table 1-1. *Comprehensive Overview of the Service Options*

Function managed by	Onsite	DaaS	CaaS	IaaS	PaaS	SaaS
Application	Client	Client	Client	Client	Client	CSP
Data	Client	Client	Client	Client	Client	CSP
Runtime	Client	Client	Client	Client	CSP	CSP
Middleware	Client	Client	Client	Client	CSP	CSP
Operating system	Client	Client	Client	Client	CSP	CSP
Virtualization	Client	Client	Client	CSP	CSP	CSP
Server	Client	Client	Client	CSP	CSP	CSP
Storage	Client	CSP	Client	CSP	CSP	CSP
Networking	Client	Client	CSP	CSP	CSP	CSP

1.3 Deployment Models of Cloud Services

Cloud computing offers various deployment models for organizations: public, private, community, and hybrid. While these models save money, they can also pose security and management challenges. Businesses must therefore assess their needs before selecting a deployment model. For example, the public model allows public and organizational access, the private model ensures data security but is more expensive, and the community model involves shared resources. Finally, the hybrid model combines the benefits of both private and public models while maintaining data security.

1.3.1. Deployment Models

There are four main deployment models:

1. Public model
2. Private model
3. Community model
4. Hybrid model

Here is a comprehensive description of each deployment model. Considering these factors reduces the risk and assists in choosing the best option for each specific business.

1.3.2. Public Model

The public model is a cloud deployment model that allows both the public and organizations to access the IT infrastructure. It provides a shared environment where multiple users can access resources and services. The public model is typically cost-effective as the infrastructure and maintenance costs are spread across various users. However, since the infrastructure is shared among multiple entities, it may raise data security and privacy concerns.

1.3.3. Private Model

In this model, hosting is built and maintained specifically for each client, which ensures data security. The necessary infrastructure can be on-site or at a third-party location. Private models can be networks residing within an organization or hosted in another data center.

For instance, if it is hosted in another data-center leasing organization or by a network provider, it is termed a virtual private network. The private model is not cost-efficient, but the advantage of this model is

the level of security it offers. As data security has become a concern for many organizations, the private model ensures a secure-access VPN on the physical location within a client's firewall system. The significant advantage of the private model is the total cost of ownership for hardware and other components remaining with the organization.

1.3.4. Community Model

The community model involves multiple organizations sharing a common infrastructure, leading to cost reduction and resource optimization. It requires cooperation and standardized policies for data and application management. This collaborative approach saves money, is scalable, and fosters efficient resource utilization. However, successful implementation relies on coordination and adherence to shared governance frameworks and compliance standards. The community model offers organizations a cost-effective, streamlined resource-sharing data management approach.

1.3.5. Hybrid Model

This model enables different businesses to utilize secured applications and data hosting on a private model. However, companies continue to get cost benefits as the shared applications and data are kept on a public model, which has advantages over both private and public models. Migration of workloads between private and public clouds is assisted without inconveniencing the user. Several PaaS deployments expose application programming interfaces (API). This can be combined with internal or private cloud-hosted applications without compromising on security features. Hybrid models are more secure since customers can maintain highly sensitive data with their servers and less sensitive data with the network service provider's server.

Table 1-2 shows a comprehensive overview of all deployment models. CSP stands for Cloud Service Providers and DCH stands for Data Center Hub.