BOHR International Journal of Computer Science
2023, Vol. 2, No. 1, pp. 77–90
DOI: 10.54646/bijcs.2023.18
www.bohrpub.com

DESCRIPTIVE

Emergence of cloud computing architecture: The dynamics

Augustine Oghene*

eProcess International, Ecobank Transnational, Accra, Ghana

***Correspondence:**
Augustine Oghene,
augustine.oghene@gmail.com

ORCID:
Augustine Oghene
0009-0003-0882-2623

Received: 16 August 2023; **Accepted:** 21 September 2023; **Published:** 13 December 2023

The conceptualization of cloud computing is the paradigm that has revolutionized software and hardware architecture across varied technological domains. However, governments and multiple sectors' rapid adoption of cloud computing is a significant source of cost-saving, scalability, and collaboration mechanisms. Research in cloud computing technology and advancement is yet to fully embrace the complete spectrum of potential issues confronting cloud technology. It is the fastest-growing field that has gained global adoption in the IT space since 2007. Companies like Amazon, Google, Oracle, and Microsoft provide various products via cloud computing regardless of the many challenges they face in delivering their services to establish assurance to customers demanding continuity of services, speed to market, and guaranteed security. While there are multiple discussions around cloud and data safety, only a few have a grip on the dynamism of cloud technology and the background operation. Three major conventional institutions are at the forefront of providing a clear definition of cloud computing architecture, the technology innovation and advancement driving its operation. They are Gartner, Forrester, and the National Institute of Standards and Technology (NIST). The definition of cloud computing is presented differently by Gartner and Forrester, while the NIST explanation is based on industry-standard terms. This research is an in-depth look at cloud computing architecture from the three institutions' perspectives. It provides researcher insight to uncover the background of cloud technology, tailored toward an extensive focus area for researchers and exposing a new stream of challenges that require a quick resolution.

Keywords: cloud computing, enterprise, architecture, infrastructure, benefits, challenges.

1. Introduction

Regardless of the global misgivings about cloud computing, Vacca (1) states that cloud computing is being acclaimed as the penultimate solution to the problems of uncertain traffic spikes, computing overload, and potentially expensive investments in hardware for data-processing backups. The National Institute of Technology and Standard defined cloud computing as a model that facilitates business enablement and on-demand network access to a pool of computing resources quickly provisioned and released with minimum management involvement (2) state that Cloud computing represents a departure from the norm of developing, operating, and managing I.T. systems. Economically, not only does the adoption of cloud computing have the potential to provide enormous financial benefits, but it also provides much greater flexibility and agility. Cloud computing started in 1960 with the mainframe era, followed by distributed computing in the 1970s; next is the desktop, laptop and PC eras of the 1980s—the client-server era of the 1990s, and finally, the internet era of the 2000s.

Cloud computing manifests through years of technological evolution from the first computers and progressed from the inception of the centralized mainframe technology. The growth underwent a series of phases until technology-enabled access to multiple computers globally. Each aspect of evolution passed through challenges based on one thing or the other (3). There were the mainframe administrators,

the powerful gatekeepers of data and systems. They were also often the most significant bottlenecks because nothing could get done without going through them.

However, when the P.C. was born, I.T. professionals were empowered and could distribute workloads across many work nodes without going through the once-powerful mainframe gatekeepers. Even though the system is built to deploy faster, less expensive, and has more features, in return for gains in agility and flexibility, these result in a massive decrease in actual governance effectiveness and security.

Internet technology allows customers to purchase online for various needs and services (3). The internet created a global revolution where any company or individual with an internet connection could now do business from anywhere in the world, regardless of the time difference and businesses exploitation of internet connectivity technology as the traditional local area networks are extended globally and forming interconnected vast area network. This introduced another level of complexity: As the number of systems increased dramatically, there was decrease in control and governance.

Additionally, the applications' security posture suddenly reduced, making the environment vulnerable to attacks. This triggered debate among business owners and technology experts on the security of their assets (3). Early adopters and risk-takers embrace the new technologies and become the guinea pigs for an enterprise that typically prefers to wait until the technology becomes mature. Only a few individuals and enterprises were breaking ground with new technologies.

Furthermore, the surge in technological innovations and the combination of multiple technology innovations led to cloud computing. It was, in turn, universally adopted and patronized by various organizations. This resulted in a high demand for standards and security as it was viewed as less secure (3). Rules emerged, best practices were published, and vendor and open-source products became widely available to fill the gaps (2). Amazon's first public cloud offering attracted over 5,00,000 customers in its first 18 months. As more enterprises adopted cloud technology, confidence moved from hype and agitation during its emergence. It upgraded to full acceptance as standards and practices became fully operational, although the adoption currently stands between the peak of magnified expectations and setbacks.

Enterprise cloud is tailored to meet the security and service level agreements (SLA), resulting in organizations embracing cloud technology frequently, as many cloud service providers have aligned their strategy to deliver various products and services that meet enterprise-wide cloud expectations. It is, however, expensive and more complex than other models of cloud. However, the different model is not designed to meet security, regulatory, and SLA requirements (4). Cloud computing is changing our conduct and how we work with information. Previously, data, infrastructure, and applications were not accessible from any location. New solutions are now built faster by collaborating to produce new products.

Furthermore, a new engine for the future is built with cloud computing (5). The capabilities of the Cloud as a centralized resource can match industrial scales. This signifies that multiple computer machines' processing power cascades as a single machine connected to the network provides high processing capabilities (6). The capacity contributed to the consumer is to make available the following processing, storage, networks, and other relevant computing resources where the consumer can deploy and run arbitrary software, which can include operating systems and applications (3). Cloud environments are ideal for horizontally scaling architectures. That is, from the inception of the implementation of the design, it is considered that infrastructures like hardware, storage, and networking are assured against challenges.

2. Essential characteristics of cloud

According to Mell (7), Cloud computing enables universal, convenient, on-demand access to configurable computing resources such as networks, servers, applications, and services that can be rapidly provisioned and released with essential management involvement. The services provided by the cloud service provider must conform to the typical characteristics of the Cloud. Although multiple organizations are in the cloud service business, merely having a web-based application running from a remote location does not make it a cloud application (8). Users are not tied to a specific device; the internet allows for location independence. The Cloud enables Cloud computing service providers and customers to access cloud-enabled systems regardless of where they may be located or what device they choose. The cloud model comprises five major characteristics, three services-delivery models, and four deployment models.

2.1. On-demand self-service

This capability allows customers to help on-board themselves to the Cloud regardless of location. The possibility is through automated technology embedded in the cloud infrastructure. Once the cloud service provider portal is accessible to customers.

2.2. Broad network access

These capabilities allow any endpoint device to access the cloud network. There are no restrictions on a group of vendor products. So, the facility is available over network access via standard systems that allow the use of heterogeneous devices.

2.3. Resource pooling

The provider resources share must follow multitenancy approaches such as having a centralized infrastructure with a shared pool, where CPU, storage, and network bandwidth are dynamically allocated without human intervention based on consumer consumption, and the service provider monitors the performance of the infrastructure. The customers also do not have control over the correct location of the resources provided by the provider.

2.4. Rapid elasticity

The deployed facility has elasticity capabilities and functions operationally. They are making it possible to scale up and down as the infrastructure demand changes upward or downward to sustain service stability regardless of the consumption frequency.

2.5. Measured service

Cloud infrastructure automates control and resource optimization without human intervention by depending on the capability embedded in the metering device. The metering capability is applicable during the orchestration of service. In addition, it allows monitoring of resource utilization and provides visibility to the cloud provider and consumer of its usage history.

3. Service model

3.1. Software as a service (SaaS)

This facility allows the consumer to utilize the cloud provider application infrastructure running on the cloud platform. This software is accessible from the client's components, such as a laptop and PC, through the web interface. The customers have no direct control over the underlying infrastructure, such as the network, servers, operating systems, storage, and the application's capabilities.

3.2. Platform as a service (PaaS)

This facility only provides the consumer access to deploy onto the cloud infrastructure. The consumer can purchase applications to implement already using programming languages, libraries, services, and supporting technology tools approved by the cloud provider. This model allows the consumer direct access and controls to manage the underlying cloud infrastructure encompassing network, servers, operating systems, and storage. It is permitted to control the deployed application and configure the environment.

3.3. Infrastructure as a service (IaaS)

This model provides the consumer with the capability to provision computing power, storage, networks, and other fundamental computing resources needed to facilitate deployment by the consumer. The consumer can run arbitrary software, including operating systems and applications. This model, however, does not allow consumer control over the underlying cloud infrastructure, the operating systems, storage, and applications deployment and limited monitoring of selected network components.

4. Cloud computing architecture

Cloud computer architecture refers to the multiple components in terms of databases, software capabilities, and applications re-engineered to take advantage of the power of cloud resources to address enterprise business challenges. They also define the relationship between components and sub-components highly needed in cloud computing. On the other hand, the components generally consist of front-end and back-end platforms, a cloud delivery, and a network device (3). Whether a company has an official enterprise architecture practice in place or not, success in the Cloud depends on applying sound architectural principles and asking these six (6) questions: Why, Who, What, Where, When, and How. Numerous architecture frameworks have different methodologies, such as the Open Group Architecture Framework (TOGAF) and the Zachman Framework. In building a design, an architect must carry out the procedure this framework recommends before building a Cloud architecture. Companies downplay this part, thereby creating multiple errors once in operating mode. Architects must follow this trend to develop a cloud architecture addressing business challenges. The questions the architect must answer are outlined below, describing what each means:

- **WHY:** Identify the problem to resolve, including business goals and drivers.
- **WHO:** Who are the end-users that this problem is impacting?
- **WHAT:** The business and technical requirements, Legal and regulatory challenges, and Associated Risks.
- **WHERE:** Location where this service is consumed. Or any specific requirements concerning the location.
- **WHEN:** At what time is this service needed? What is the financial budget prepared for this period? Any dependencies on other projects?

- **HOW:** This shows how prepared the organization is to deliver these services from architectural and customer perspectives.

Once the response to the questions is collated and analyzed to develop an acceptable outcome that gives insight, the architect will use it to decide on the service model and deployment methodology. The user and data types strongly influence the decision of the cloud architecture (3). The business architecture provides insightful information concerning the numerous touch points and business functions across the enterprise in the initiative's scope.

4.1. Defining the problem statement (Why)

Establishing the problem helps narrow the need for an architect to address what to solve. Problem statement: What are the drivers for ridding on cloud computing services within the enterprise? Responses from organizations differ from one another, also from an architectural perspective.

4.2. Assessment of user attribute (WHO)

The WHO signify the users utilizing the systems. It could be internal and external users and knowing their identity to ascertain the attribute of the enterprise interacting with the entire networks. All users may not have similar profiles and their needs. And the possibility of a single cloud service provider meeting all the differences is likely but not particular. In other words, each user's demographics (age, group, country, and how tech-savvy the person is) are essential to identify them and the type of business, government, etc.

4.3. What questions (Business and technical requirements)

What questions address the business and technical requirements? The business requirements put in the proper perspective the needs of the business, such as data in the systems, screenshot banner display on the systems, the operation workflow, what the system's performance is, identifying users access on the system and conformity of regulatory requirements—the technical specifications and elaborate on architectural design capability. The technical requirements are evaluated to aid in selecting the appropriate cloud services and deployment models. Outlined below are the requirements.

Adoption requirements: End-user requirements and applications running on the platform.

Performance: Systems respond to users and application requests.

Flexibility: The ability to make seamless changes that will impact the business positively without a service outage.

Capability: Effectiveness of executing impromptu business processes to enhance customers' values.

Security: Fulfilling security requirements to meet users' and data privacy and compliance with external regulatory requirements.

Traceability: Systems logging, auditing, notifications matrix, and event processing requirements must be met as a way of monitoring underlying activities in the systems.

Adaptability: Meeting both internal and external reuse levels.

Integrability: Seamless method of integrating multiple systems and other vendor technologies.

Standardization: Conforming to specific industry standards is a crucial requirement.

Scalability: Automating scalability is a significant capability to meet impromptu business requirements.

Portability: Capability to logically deploy into hardware and software various changes to enhance performance.

Reliability: Ascertain the platform's reliability concerning uptime, meeting service level agreement (SLA), availability, and conforming to recovery mechanisms.

4.4. Envision the consumer experience (WHERE)

Architecting cloud computing requires figuring out all constraints consumers of the services are likely to encounter before benefiting from the consumption of the service. Some of these constraints cut across countries. Restrictive policies in some countries slow down Cloud computing innovation and technology (3). China has complex laws that discriminate against foreign technology firms and restrict data types that can flow into and out of the country. A country with restrictive laws like France does not allow financial data outside their shore. At the same time, Japan and countries in Africa have modified their legislation around privacy law, criminal law, and I.P. security to expedite the digital economy and Cloud computing innovation. Also, one primary rule impacting the growth of cloud computing is the USA Patriot Act of 2001. The Act was signed into law immediately after the terrorist attacks on the World Trade Center in New York City. This law empowers United States' enforcement and intelligence agencies to inspect data sources of companies conducting business in the State.

4.5. Identification of project restraints (When and with What)

Budget and expected delivery time profoundly impact cloud providers' delivery of their services. In the event of any decision to onboard a solution from an existing

consumer and a new one, this requires having all the various deployment models available. Once a consumer sends out their request, there is a platform to accommodate it. Since time is critical, all anticipated constraints must be considered when making architectural design changes and decisions. In addition, the architecture decisions must give priority to business goals. Besides, significant critical constraints concerning providing cloud service models are considered before making them available to the consumer.

4.6. Awareness of current constraints (HOW)

Enterprise preparedness is essential when handling "how" concerns. These include the internal resources' skills level and the organization's willingness to move from the CAPEX to the OPEX model. The organization's culture plays a significant role in addressing the current constraints. Corporate change management is responsible for ensuring the organization's new initiative is given the required awareness because behavioral change faces more challenges than implementing the latest technology. Employees need more clarity about a change and how the change will bring a new paradigm within the enterprise. According to Kavis (3), companies with a long legacy of building and deploying on-premises systems will likely experience resistance within the ranks. All hands must be on deck for a cloud infrastructure.

5. Cloud services and technologies

Cloud service is internet-based services made available to the consumer on-demand, accessible from a cloud provider's infrastructure instead of on-premises systems. The cloud services are tailored to provide seamless, scalable access to applications, resources, and services managed by the provider. The design of cloud service is to automatically scale to meet the need of its consumer as the utilization demand more for it. Cloud computing is traditionally classified into three primary functions: Software-as-a-Software (SaaS), Infrastructure-as-a-Service (IaaS), and Platform-as-a-Service (PaaS). These three services are referred to as the Cloud computing stack.

5.1. Infrastructure-AS-A-service (IaaS)

The infrastructure-as-a-service model allows for delivering computing and storage resources to different consumers. Some vendors provide a similar model with different label names, for instance, Amazon EC2, Amazon S3, and Cloud System Matrix. This model allows consumers adequate flexibility to work with the infrastructure without restrictions. Routine maintenance of the operating systems and any middleware is the responsibility of the service's subscriber. This also applies to the application's uptime. The capability to automate demand and make it available accommodates a logical request for additional capacity to support the workload and enhance the platform's performance. Beyond virtual hardware, the model also provides storage services as organizations have varied data requirements for structure and unstructured data in their operating environment. Some data is highly confidential and needs to be safeguarded against cyber-attacks. Enterprise business-critical data should be protected and permit access on-demand in case of failure arising from hardware, software, and unavoidable user errors (9). Infrastructure as a service has gained tremendous traction in recent years, most notably with start-ups and fast-growing independent divisions of larger companies seeking to build their business-critical applications but avoiding the investment and maintenance that infrastructure requires.

5.2. Platform-AS-A-service (SaaS)

This cloud service model serves to develop and deploy cloud applications over abstracted hardware. Similarly, it allows service subscribers to directly develop an app without concern with the infrastructure and systems patches, firmware, and software setup. Microsoft Azure, Apache Hadoop, IBM Pure XML, AWS Elastic Beanstalk, Heroku, Force.com, Google App Engine, OpenShift, and Apache Stratos are examples of a platform-as-a-service model in the industry. The model is designed to support the complete life cycle of an application, from design and development to supporting the built and testing phase and hosting the application deployment infrastructure on the Cloud. According to Sitaram (6), to facilitate automated application management, Platform-as-a-Service solutions provide a more restricted environment than infrastructure-as-a-service for its customers, with fewer choices for operating systems and programming environments. This reduces the management burden on the consumers.

Marinescu (10) platform-as-a-service is not particularly useful when the underlying hardware and software must be customized to improve the application's performance, and its primary application areas are in software development when multiple developers and users collaborate. In a platform-as-a-service model, the provider has no control over the approach adopted to deploy the application as well as the quality of the deployment. However, the consumers have the power to customize their applications or services to meet their desires (11). In a platform-as-a-service environment, the consumer has visibility into the platform's use and determines when new systems need to be added to handle the load. Outlined below are the duties/responsibilities of the platform-as-a-service model clients and customers:

5.2.1. Cloud provider responsibilities

- The provider is responsible for managing the development platform and the back-end components.
- The provider is responsible for patching and updating the operating systems when delivered to the consumer, and should periodically update the operating system when in production and when operationalized as well.

5.2.2. Customer responsibility

- The consumers are solely responsible for activities beyond the operating systems and development platform.
- Responsible for the application and database installation and maintenance.
- Responsible for data deployment onto the platform.

5.3. Software-AS-A-service (SaaS)

This model is designed to provide individual and enterprise software, specifically, application software running on and accessible in the Cloud. It addresses the lack of skills in many organizations. Software providers are looking for ways to offer online cloud-based solutions at a reasonable cost and universally accessible. The provider builds this model to take responsibility for the single or multiple-user access license and the service level agreement (SLA) (11) with software-as-a-service implementations. The service provider usually controls virtually everything about the application. This will limit any form of customization on the platform, and the cost is exceptionally high for the provider and customer.

6. Cloud technologies

The cloud provider is leveraging dynamic technologies to make available cloud services to meet the needs of individuals and small, medium, and large enterprises. High-performance computing (HPC) and network are two significant infrastructures cloud provider business requires. In other words, detailed reviews of how significant technology is an enabler of cloud computing are put in perspective to understand each technology. That is grid computing, utility computing, distributed computing, and Virtualization.

6.1. Virtualization

Virtualization is a critical technology in cloud computing. It creates a virtual machine from physical hardware, storage devices, and network resources. The technology is classified into three (3), and the first classification is the internal process model. The second classification encompasses the Virtualization techniques at different levels of the implementation within the hardware. The third classification is about the hypervisor. There are two main software Virtualization categories: system Virtualization and process Virtualization (6). In process Virtualization, the software runs above the O.S. and hardware combination and only makes user-level instructions available. In system Virtualization, the Virtualization software is between the host hardware machine and the guest software; its primary role is to provide virtualized hardware resources based on the definition of Virtualization by Huang and Wu (12). Virtualization is a technology that combines or divides computing, storage, or networking resources to present one or many operating environments using the methodologies like hardware and software partitioning or aggregation, partial or complete machine simulation, emulation, time-sharing, and others.

The second classification encompasses the entire virtualization techniques at various levels of implementation within the computer. The multiple levels are the instruction set level, hardware abstraction layer (HAL), Operating System level, User level interface or application-level interface. Regardless of the abstraction mechanism, its approaches never change (12). It partitions the lower-level resources using novel techniques to map to multiple higher-level virtual machines. The ISA-based Virtualization is executed in software, emulating the ISA in software where it interprets and translates guest ISA into native ISA and emulates hardware-specific IN/OUT instructions to imitate a device at a level of the provided device abstractions. The ISA virtualization technology supports multiple operating systems running on top of it, and it is mainly applied for software debugging and the purpose of teaching. Besides, the hardware abstraction layer (HAL) is where the computer operating system communicates with the hardware device. This layer is possibly called in two ways: the operating system kernel and the device driver.

The third classification passes through two hypervisors. The hypervisor is a software layer residing on the physical hardware machine, allowing multiple virtual machines to run on the physical hardware. It is the technology behind cloud computing, allowing various virtual machines to be created quickly to make an available platform for the cloud service model. All the vendors like Red Hat, Microsoft Hyper-V, Oracle VirtualBox, and IBM have hypervisor driving their virtualization concept.

The virtualization activities produce multiple virtual machines from physical hardware; each virtual machine is independently separated, but the cloud provider decides the resources allocated to each virtual machine (12) The relationship between Virtualization and the Cloud is that Virtualization could exist regardless of the Cloud, but Cloud computing cannot exist without Virtualization. Virtualization is not vital for the cloud environment; it only facilitates scaling of the resources, which is impossible with a non-virtualized climate.

6.2. Docker technology

The technology docker leverages to function on the operating system's Virtualization, and the operating system and the kernel of the operating systems allow for multiple separated user-space instances to be created. This instance appears like a real server from the viewpoint of the users. The kernel serves as a resource feature to manage the activity of each container. Operating system virtualization is popularly adopted in a virtual hosting working environment, where it is vital to securely allocate finite hardware resources to various mutually distrusting consumers. Also, it reduces the extent of consolidating server hardware by migrating services onto a separate host into the containers on a server. Applications management allows it to separate various applications into containers to enhance security, hardware separation, and resource allocation management features.

Moreover, Docker is an open-source engine that facilitates the automation of applications into containers. It allowed an application deployment engine to be added to a virtualized container operating environment. The designed provision a lightweight and fast operating environment for running and maintaining an efficient workflow to migrate the code from the user's device to a test environment and finally into production. Docker is highly simplified, which can start a few hosts running a compatible Red Hat Linus kernel version with a docker binary.

Docker architecture is a client-server model. The client communicates to the server, and the server, in turn, activates the client's request (12). The docker command is executed in a daemon mode, a Linux operating system docker server with a container deployed, launched, and via a remote client.

6.3. Network-based virtualization

Virtualization capability is extended to network appliances connecting hosts and storage, such as the SAN switch. The virtualization technology is applied in two broad areas: switch-based network virtualization and appliance-based approach. In the former one, the Virtualization takes place in an intelligent switch in the fabric, and the functionality is revealed when it works with a metadata manager within the network. While the latter one, the I/O, flows through an appliance that controls the virtualization layer. Both switch-based and appliance-based have a similar capability to aid disk management, metadata lookup, data migration, and replication.

6.4. Grid computing

Grid computing is a cluster of computers physically connected to actualized dedicated tasks collectively. It harnesses all the computer resources and power to perform a complicated task. It can be thought of as a distributed system with non-attractive workloads that involve multiple files. It is a large-scale, distributed computing endeavor. The technology can be leveraged at a local level. The unique primary difference between grid computing and cloud computing is that the Virtualization of computing resources in grid computing makes storing a large quantity of data possible.

In contrast, cloud computing application doesn't access resources directly; instead, they access them via a service through the internet.

6.5. Distributed computing

The technology of distributed computing has existed for more than three decades (6). Distributed computing is computing distributed over autonomous computers that communicate only over a network. Distributed computing is compared to other forms of cluster computing technology. It can encompass different computations where some nodes perform more than others while few perform specialized functionality (6). The main advantages of distributed computing are that efficient, scalable programs can be designed so that independent processes are scheduled on different nodes, and they communicate only occasionally to exchange results instead of working out of shared memory with multiple simultaneous accesses to a collective mind.

6.6. Hybrid cloud

Hybrid cloud adoption represents a different concept to many individuals and enterprises. It resulted in the varied definition of a hybrid cloud. According to Trautman (13), Hybrid Cloud combines on-premises I.T. (traditional infrastructure and private Cloud) with off-premises resources or services from public clouds such as Google Cloud Platform, Amazon Web Service (AWS) and Microsoft Azure (1). Hybrid cloud infrastructure is forming more than one cloud model (private, community, or public) with a unique entity bound together by standardized or propriety technology that enables data and application portability. In other words, Klaffenbach et al., (4) defined a hybrid cloud as a private cloud environment at the consumer's premises and a public cloud infrastructure that the consumers use.

6.6.1. Flexibility and agility

Agility is the key benefit of an accurately architected hybrid cloud for business growth—faster allocation of resources and deployment of both legacy and new applications. It is also extended to development and testing before production. The model's readiness to accept and host services on the run between on-premises and cloud locations and leverage

resources across other areas aligns with the architectural design. There is flexibility with the task of getting things done faster than on-premises.

6.6.2. Elasticity

The hybrid cloud model introduces flexibility in the design to address impromptu requests for resources. Depending on the enterprise type of business resources, the spike is always a common trend, and the rate fluctuates periodically and goes extremely high, mostly during peak business periods. Applications belonging to individuals demand resources often, and the resources to them are then reclaimed back to the resource pool when they are not in use.

6.6.3. Self-service

Self-service is an added value benefit of a hybrid Cloud. This is accessible through the cloud provider portal. Therefore, it is not limited to access to the services but reduces the pains of I.T. since it no longer must play an intermediary role.

6.6.4. Faster delivery of new products and services

A meticulously designed hybrid cloud promptly makes products and services available faster, subduing and eliminating known and unknown barriers that may likely impact business progress. The advent of digital service that requires quick-to-market leveraging hybrid cloud service model will deliver its values quicker because it becomes easier to create and deploy, and developers and test engineers have complete access to the platform and resources they need to meet their deadlines.

6.6.5. Cost control

The hybrid cloud model introduces a pay-as-you-go model to make the services affordable to all enterprises regardless of size, ultimately reducing their capital investments in infrastructure and data centers (13). Designing data centers to accommodate peak loads only to have infrastructure sitting idle often is a poor choice versus adding cloud resources when needed to provide peak periods.

6.6.6. Avoidance of lock-in

Adopting a hybrid cloud model makes it possible to lock in one cloud provider. Sometimes, it is challenging for an enterprise to move its data from a lock-in cloud provider. In a nutshell, caution should apply when exposed to this risk.

6.6.7. Proximity to new technology

Technology as a business enabler. The enterprise must have access to recent technology to bring a paradigm shift into its operation for competitive advantage. With this, the cloud provider innovates rapidly and offers highly competitive services. So, the hybrid cloud model provides the flexibility to use modern technologies to take advantage of business opportunities.

7. Cloud operations management

Cloud operations management involves designing, overseeing, controlling, and re-architecting cloud operational processes. It is targeted to ensure cloud operations are efficient in making resources available as demand and meeting QoS requirements, compliance requirements, and, most importantly, positively impacting customers' experience. This is possible by managing hardware, software, and network infrastructures to promote an efficient and lean cloud operating environment. Also, operations management is a routine task carried out daily using cloud processes for the service provider and the consumers. The approach differs from provider to provider, but the concept and the applicable practices has never changed (14). The actual operations of the Cloud are the subject of the provisioning and configuration category, whose tasks include provisioning, resource change, monitoring and reporting, metering, and SLA management. Finally, data transfer, V.M. image migration, and the all-encompassing application and service migration are the tasks of portability and interoperability accomplished through the unified management interface.

8. Cloud infrastructure planning, design, and configurations

Developing a plan for Cloud infrastructure planning, Designing, and configuration require first understanding the fundamentals and the technologies. The Cloud computing business is the fastest evolving sector globally as computing power multiplies yearly due to technological advancement. Demand for Cloud services lies heavily on how prepared the Cloud provider is to meet consumers' needs. The technology computes cycles and software application enablers to make the services available faster. In the past, many organizations and different institutions could afford information technology infrastructure composed mainly of a centralized mainframe computer with remote terminals for accessing information computing resources.

9. Planning infrastructure best practices

Planning the transition to the Cloud is one of the significant considerations for transition success. At this stage, the enterprise needs to look inward into their operating environment infrastructure to identify legacy infrastructure to transition and otherwise drop them from the movement to the Cloud to fit with the Cloud provider flexibility and co-exist swiftly. Organizations can modernize existing information technology systems with Cloud-like features such as Virtualization and automation or plan to completely

transition some or all information technology applications and infrastructure to the public, private, or hybrid Cloud.

9.1. Designing cloud configuration and architecting for scale

Still (15) Designing systems to be cloud-ready ensures that they are automated and programmatically driven in their configuration and management. This should consider reliability, recoverability, timely error detection, and continuous operations to provide continuous service without disruption. Since cloud service delivery is primarily based on API, the architectural design of provisioning infrastructure aids the deployment and recovery from failures. According to Francis (16), losing an entire cloud region requires recreating the application but not through a manual process; instead, it should be an automated approach such as Terraform, Chef, Puppet, Ansible, Cloud Formation, and so on. This can re-create environments programmatically to avoid failures, and the infrastructure must be designed to handle failures and the challenges with systems dealing with the State. In other words, designing and architecting applications, specifically for the Cloud, must consider the application scalability to accommodate large numbers of multiple users (2). One of the primary reasons for utilizing the Cloud is to be prepared for and to have an affordable economic model for the unusual problem of suddenly having too many users. The following are design patterns that are attributes of a Cloud.

9.2. Scalable application patterns that match the cloud

Applications of high scalability that match nicely into the model of cloud computing are classified into the following: transference, internet-scale, burst to compute, and elastic storage. These application patterns attract and facilitate the decisions to move to the Cloud since scalability issues are well addressed. Outlined are the different application patterns.

9.3. Transference

This refers to when an application is already in the on-premises environment and it's migrated to the Cloud without any modification in the application. Economic reasons drive this methodology, and it is less expensive to utilize Cloud resources instead of running the application on-premises except if the in-house infrastructure is highly virtualized to better resource utilization. Before adopting this pattern, an application assessment should be performed to identify and customize an application that works appropriately on-premises against the cloud environment.

9.4. Internet scalability

This refers to designing an application for cloud purposes with the attribute to handle concurrently multiple users' requests without attracting substantial financial investment from inception. This is the entry point for prototyping newly introduced applications since it will not incur an additional cost. Rosenberg (2), For example, when Facebook started, it ran off a single server and serviced only Harvard University students. Later, Facebook built its own data center to support 400 million users.

9.5. Burst compute

The pattern is related to the application's ability to handle additional compute requests without idle, over-provisioned resources. Applications of this type have what it takes when there are spikes. This is driven by economic reasons, making it impossible to acquire additional hardware capacity to support this internally.

9.6. Elastic storage

This pattern allows the application to grow exponentially from a storage viewpoint. Although on-premises storage is less expensive, maintenance costs are incurred annually. While adopting a cloud storage platform is far less expensive than local storage, including annual maintenance, this design pattern must be well thought out before deciding. Other areas, like planning for ease of data accessibility, are significant.

10. Cloud implementation deployment model

According to (7), four (4) deployment models are defined for Cloud computing. Each of the models has its merits and demerits with a value proposition. There is a unique attribute with each model that makes it different. The model is Private, Public, Hybrid, and Community Cloud (11). A cloud deployment model is defined according to where the infrastructure for the deployment resides and who has control over that infrastructure.

11. Public clouds

This model is provisioned for public consumption (7). The model may be owned, managed, and operated by a business, academic, government organization, or some combination. This is the most popular and deployed cloud

operating environment providers continuously implement. The availability that comes with this model is extremely high. However, it attracts high financial implications due to the cost of all the infrastructure assets, such as hardware, software, and training. Some enterprises find this model difficult to afford and seek alternative options to satisfy their needs. The Cloud providers already provisioned the infrastructure assets such as hardware, software, and employer to make their offering highly available. This may come with additional availability costs but may be less expensive than owning the asset and operating the model internally. In other words, not all cloud providers have higher availability, cutting across their cloud ecosystem assets. Those who have it classified it as added value with a cost. Otherwise, one may accept the default platform, which likely has limited high availability. However, there is an SLA as part of the contract to provide some assurance concerning higher availability.

Scalability is vital to public cloud architectural design, and this is unique in the public Cloud compared to private clouds. Most private clouds find it difficult to scale their infrastructure capacity continuously, both physically and logically. Depending on the enterprise size, this model can offer different offerings to meet various customers' needs. Also, providers of the public clouds model emphasize accessibility to expand their coverage to allow all their customer base access through multiple devices on the internet with fewer restrictions (11). It is expensive to support various operating systems and web browsers; the development and quality assurance costs can be extremely high.

11.1. Integration restrictions

Software as a Service (SaaS) cloud service systems in public models host subscriber data and become challenging when the data must be exported to on-premises for reporting. Other setbacks are related to performing analytics on data for business intelligence activities; this Cloud leads to additional overhead on the platform and transmitting the data through the internet. Therefore, a security cloud is raised for transmitting across the internet. Besides, application integration as part of the SaaS public cloud service comes with challenges because multiple applications can adapt and work with shared functionality.

11.2. Scale down flexibility

Adopting a specific cloud provider public service makes one subject to schedule-related infrastructure maintenance and upgrade. However, the schedule is strictly adhered to, and customers are not influenced to change the program plan, unlike the private Cloud. For instance, the provider of the public model finds it challenging to permit deploying various versions of applications online because it attracts new systems overhead.

11.3. Compelled downtime

The public cloud provider has total control over their infrastructure maintenance window, and the customers don't influence or force the provider to change the already agreed date for the task. Depending on the infrastructure ecosystem, design maintenance can be structured to allow customers to access their platform regardless, and the support is carried out alongside. But, in most cases, the entire maintenance window is unlikely to be adjourned for a prolonged period.

12. Responsibilities of a cloud provider

The public cloud provider is solely responsible for the services they provide. The provider's responsibilities include sustaining the healthy State of the overall infrastructure. The enhancement of the employee's skill set is faciliated by the cloud provider. The staff should be adequate to respond to consumers' complaints. Depending on the cloud service model, the customer is purchasing, there is a separation of duties. The customers are responsible for installing the client-side application to ensure it meets their expectations. At the same time, the provider takes care of developing the client-side application and simultaneously provides support for it.

13. Security concerns

Security is imperative in the public cloud operating model. The provider controls their customers' complete access and identity as a countermeasure to secure data and the environment from cyberattacks. However, there are various debates around data ownership in the Cloud and access to the data. What level of security controls protect the data and information belonging to customers from being accessed by the provider employees? This question is raised repeatedly by many enterprises because they need assurance before planning.

14. Private clouds

Private clouds are owned and maintained by the enterprise. The complete infrastructure is operated and housed by a local data center within the organization's premises. The enterprise is entirely responsible for purchase, maintenance, and financial support. The private model has numerous benefits, focusing on monitoring and controlling the operating environment. Outlined below are the advantages of private clouds.

14.1. Maintenance and troubleshooting

The operating environment of the private Cloud is more comfortable to troubleshoot than the public Cloud. There is direct access to systems in the private Cloud. System logs, accessing network traces, ability to debug traces, and the access allow advanced troubleshooting somewhat, depending on the cloud provider.

14.2. Maintenance

Organizations handle maintenance tasks across the entire infrastructure ecosystem, and most of the jobs underneath the maintenance routine are not forcefully carried out. Tasks like upgrading hardware resources, firmware upgrades, and operating systems upgrades are done when they become mandatory. It is absolutely under control. This approach takes into consideration the overall impact of infrastructure outages. It allows running with different versions of an application for compatibility benefits.

14.3. Monitoring

With private clouds, access is provided for all systems to allow monitoring of the systems to make visible any potential bottleneck. The monitoring extends to the application running on the systems, including the database.

15. Drawbacks with private clouds

Private Cloud allows a certain degree of access to the operating environment and provides transparency over all the anticipated issues that may arise. Outlined is the shortcoming with the private clouds.

15.1. Cost

Implementing a private cloud requires a substantial financial budget. The infrastructure sizing should be adequately scalable to ensure future growth for all business units. At the same time, the infrastructure must sustain the business at peak times.

15.2. Hardware and software compatibility

Compatibility needs to be professionally managed as it results in multiple issues leading to the outage. So, hardware and software compatibility require reviews before deploying into production, and most importantly, the software implemented must be compatible with clients.

15.3. Highly competent skill resources

Private Cloud requires expertise in the deployment and implementation phase. The internal resources skills need to be upgraded by providing training. An additional drawback is that the resources must have sufficient skills for the hardware, storage, networking, security, and Virtualization.

In a private cloud operating model, shared responsibility is a good layout for all employees to know precisely what they should do. The enterprise is responsible for the end-to-end deployment of integration of new solutions. Including the systems providing the service, the client applications, and the maintenance of the client's systems. The enterprise will oversee the implementation of security controls, both physical and logical. The private cloud model manages access to data and identity of both its employees and customers. Security controls and compliance audit is a straightforward action in the private Cloud.

16. Community clouds

The community cloud model is less famous than private and public clouds. It is mainly used and shared by organizations with a common goal, such as security, compliance, and jurisdiction considerations. It suits ventures, business organizations, research organizations, and tenders. An example of a community cloud is Open Cirrus, a computing research testbed intended to be used by universities and research institutions. There are benefits to this model, mainly around the infrastructure they are shared, as well as the financial implications. Outlined below are the benefits:

16.1. Cost

In this model, the cost is shared by all the members leveraging the Cloud jointly to achieve a common goal. The acquisition of infrastructure by a single entity is instead acquired through multiple organizations. In other words, organizations can now achieve more significant economies of scale. This is appropriately planned for each organization's financial position to avoid any issues around ownership.

16.2. Multitenancy

The community cloud model allows all member organizations to take advantage of multitenancy for the benefit of economies of scale. A single enterprise may find it challenging to handle the financial implications alone; instead, multiple organizations with joint commonalities can come together to finance the acquisition. Multitenancy also allows members to share the support and maintenance

tasks with all the organizations, providing skill resources to support and maintain the operating environment.

17. The drawback with the community cloud model

All cloud deployment models have drawbacks associated with them, and this model is no exception. The disadvantage is mostly conflict among the member organizations. And this must be addressed quickly. If the community cloud model's orchestration commences, terms must be clearly defined before the completion of the deployment. When more than one enterprise jointly agrees to acquire and assemble the infrastructure, a written agreement must spell out what percentage of ownership lies with a member organization. There could be other methods of allowing all enterprise members to know their position in terms of ownership.

18. Hybrid cloud model

The hybrid cloud model is the popular cloud model patronized currently by organizations. The model is the combination of private and public cloud services with multiple touchpoints existing across the environment. In a nutshell, it is comprised of numerous separate cloud environments interconnected. This model offers the freedom to implement whatever is essential to meet organizational expectations. In addition to multiple benefits associated with cloud deployment, the hybrid cloud model offers flexibility to migrate to the Cloud without moving the enterprise service platform to the Cloud. Apart from that, services that can function adequately are migrated, whereas legacy systems can remain on-premises pending when the cloud provider has a suitable platform to host them. This applies to the application, database, and web services (11). Many organizations use a hybrid cloud model for fault tolerance and high availability. This is done when, for instance, specific applications are hosted in two environments; if one environment goes down, the other can still access the application.

18.1. Shortcomings with the hybrid cloud model

Since this model combines private and public clouds, the implementation is complex. Several considerations are brought into the plan before the execution. Exceptions apply to all environments as all the customers operate different private cloud models. Outlined below are the various drawbacks of the hybrid cloud service.

18.1.1. Integration

The integration is cumbersome due to where they reside and the need to access the same data possibly hosted in the Cloud. In some circumstances, copies of the data are created and can only be consistent if there is a replication intelligence technology application on the data. In addition, data movement within the hybrid cloud model is incredibly challenging and comes with bandwidth constraints.

18.1.2. Cybersecurity considerations for hybrid cloud model

The security challenges transparent in the hybrid cloud model lie in the connectivity across the private and public clouds in different geographical regions. Data movement across the cloud environments results in a high-risk posture for the organization. The data must be encrypted from the sources to the destination and applied to all data states.

19. Cloud migrations: benefits and dynamics

Cloud migration is heating up globally. The movement to the Cloud is attracting thousands of companies globally (16). The cloud migration market size is estimated at $232.51 billion in 2024, and is expected to reach $806.41 billion by 2029, growing at a CAGR of 28.24% during the forecast period (2024–2029). The movement to a public cloud is increasing faster; at most, 80% of enterprises' annual strategic plan is to move almost 20% of their workload into the Cloud within the next 4 years.

Moreover, Still (15), Cloud services redefine how many businesses build and host their applications. Flexibility, scalability, cost reduction, and reduced overheads are just some of the reasons for moving too many businesses. This is a genuine trend, with a 2015 survey reporting that 72% of executives stated that the Cloud was essential to their strategy, and 90% of businesses reported using it in some capacity. The enormous driver for this movement to the Cloud is firmly for business reasons. According to Francis (16), a recent study by 451 Research discovered that cost savings are the top motivating factor for CIOs moving to the cloud model, with 38.8% naming that as a critical driver.

Meanwhile, migration is considered a low-risk investment at the early stage of cloud innovation and attracts a moderate cost (16). According to one recent study, 50% of the companies surveyed estimate the migration cost to be between $100 and 500 per machine, with just 17% estimating the cost of more than $500 per device. However, a detailed guide for creating an end-to-end transition plan to prepare organizations for the cloud journey is absent. In other words, migration to the Cloud is a complex proposition (16). It is worth it for enterprise business in terms of increased agility

and additional benefits, but there are a lot of pitfalls that you might run into, and that can be avoided.

Transitioning to the Cloud offers enormous benefits (15). The real benefits of the Cloud are its dynamic nature, the ability to create and destroy infrastructure on demand, the ability to use scalable services, and the ability to create geographically distributed systems.

19.1. Facilitate operational agility

Operational agility is the peak of the values with transitioning to the Cloud. It facilitates and creates opportunities for trying emerging technologies much faster than traditional data centers. In an on-premises environment, one waits long before the server and storage network connections are provided. However, the cloud operating model allows the new instance to be quickly spun up for whatever workloads are required to execute the task (16). The product teams and developers leverage this capability to release new products, get feedback, and quickly iterate and improve them to meet customers' needs. These models are known as operational agility. For example, Amazon, Google, IBM, Microsoft, and other cloud providers deployed new cloud-based services that meet one's needs appropriately with a competitive advantage. This is opposite to the on-premises model; the cloud operating model comes with emerging technology.

Furthermore Francis (16), Capital One demonstrated the value of migrating to the Cloud by moving one of its largest customer-facing apps to the Cloud. That is its mobile app to Amazon Web Services (AWS) in 2016. The movement to AWS was a way of removing the constraints preventing them from developing their ideal applications. The transition was neither a mandate nor a product goal, but it was to build the best application using the best skills and tools.

19.2. Sustain strategic focus

Movement to the Cloud makes the enterprise strategically focused. They sustain the strategic focus to build agility simply because the enterprise does not need to be disturbed about managing their data center since achieving their data center is challenging and complex. Besides, intelligent resources are required to handle provisioning and address data management, security, and critical tasks (16). Power management, space planning, cooling, and contracts with ISPs are complex tasks that require significant resources allocated to them. A skill set is essential for the transition to the Cloud to be successful. Managing the infrastructure requires specialized skills, so the enterprise should re-purpose their technical employees to handle more strategic initiatives for the business, such as re-engineering customer-facing applications instead of maintaining already running infrastructure. Also, if the enterprise wants to turn its capital expenditure investment cycle into a useful operational expenditure financial model, with this approach, it can reap cash back into its core businesses. This strategic approach is the primary driver to moving into the Cloud, and it will help end the annual infrastructure refresh of systems hosted in their data center. It will also leverage the cost-saving benefits of the movement to Cloud, scalability, stand-up times, and moving away from managing their infrastructure to sustaining their core business.

19.3. Financial reduction

Transitioning to the Cloud attracts cost-cutting, and organizations should leverage this attribute to rethink their annual spending. And this attribute is a fundamental driver for moving to the Cloud. However, according to Francis (16), the cost sometimes rises. 451 Research found that the main reason for this was that companies consume more computing, storage, and networking resources after moving to the Cloud. There is an absence of control to supervise how the infrastructure is used. They result in the waste of cloud resources, leading to increased costs. So, many enterprise businesses realized that cost-cutting never met their expectations. Although cost-saving was the driver for cloud adoption, it turned out to be a pain point after the migration. An assessment is advisable to ascertain which workload should move to the Cloud, and the workload's criticality to the business needs to be confirmed. Running a 24/7 workload in the Cloud will be more expensive than maintaining it on-premises. But for infrastructure with multiple variable components, the Cloud is the best option from a financial saving perspective.

Going to the Cloud for these reasons is acceptable and will be less expensive (16). However, Costs may rise through the Cloud. These cloud instances are spun up and then forgotten, which is incredibly challenging. For example, developers might sign up a new instance when they release a new system. Meanwhile, it makes sense if an enterprise searches for cost savings in the Cloud as this is the most apparent benefit of transitioning into the Cloud. Most organizations struggle to budget while looking for every means for cost optimization across their annual infrastructure spending. Sometimes, they reduce the project for the year, thinking the Cloud will bring relief. However, certain potential cost benefits can be had from transitioning to the Cloud. Consuming the appropriate cloud services can scale down operational overhead and infrastructure headcount. In other words, organizations accept their faith that cloud costs will rise. They realize that the operational agility they seek from it makes sense. And finally, accept that it will attract an additional percentage in their annual information technology budget for infrastructure. Organizations set different expectations when migrating to the Cloud. Regardless of the high bills provided, they can develop apps faster and quickly, go to the market

and leverage the platform to learn faster and attract more return on investment they are comfortable with, instead of holding up the business through infrastructure needs.

Occasionally, many enterprises go deep into the migration journey to the Cloud before realizing how the cloud journey will benefit them. The mistake by many organizations in their cloud transformation journey is that they start with infrastructure instead of applications. One common trend with cloud migration is that it is difficult to secure access for developers, but this set of resources is considered the last when migrating to the Cloud. That is where the same benefits will start flowing into the business (16). Might an enterprise be looking to cut costs by simply movement of infrastructure, in this case, that's a difficulty, so they need to start digging into the application state and architecture, which tend to take time to understand.

20. Conclusion

Cloud computing is designed to facilitate on-demand network access for a shared pool of configurable computing resources that are quickly made available and released by the provider of cloud services. According to NIST, cloud computing has five critical attributes: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Solutions deployed from the cloud architecture must model this attribute to be classified as a cloud solution. Cloud computing has three service delivery models: infrastructure as a service (IaaS), which allows the consumer to provision processing, storage, networks, and other fundamental computing resources that enable the consumer to deploy and run various software, such as operating systems and applications. However, the consumer cannot manage the underlying cloud system infrastructure and control operating systems, storage, and deployed applications with restrictions on selected networking components. The software as a Service (SaaS) model allows the consumer to adopt the cloud provider application running on the cloud system infrastructure. However, the application is accessible from the consumer's endpoint devices. There are limitations imposed on consumers, such as not being permitted to control or manage the Cloud's underlying infrastructure, including the following network, servers, operating systems, storage, or different applications. Platform as a Service: This model allows the consumers to deploy their services onto the cloud infrastructure, but they are not allowed to manage the underlying cloud infrastructure such as network, servers, operating systems, or storage and are permitted to manage only the application deployed with their configuration parameters.

Cloud deployment includes the following: private Cloud, Community Cloud, Public Cloud, and hybrid Cloud. Each has a unique attribute. The private cloud model is exclusively owned by one entity with multiple consumers. All the consumers are from different departments within the same organization. So, the single organization owns, manages, and operates the entity. As the name implies, the community cloud model is meant entirely for the community of consumers from organizations with multiple shared services. All the organizations in the community, both on and off-premises, own, manage, and operate this model. The public cloud model is for the entire public. This may be a business, academic, or government agency. The model exists within the cloud provider's operating environment. A hybrid cloud model is a composition of two or more cloud models. The multiple models are private, public and community cloud. But they are bound together by standardized technology, allowing data and application portability.

References

1. Vacca JR. *Cloud Computing Security*. Boca Raton, FL: CRC Press (2016).
2. Rosenberg J, Mateos A. *The Cloud at Your Service: The When, How, and Why of Enterprise Cloud Computing*. New York, NY: Manning Publications (2010).
3. Kavis M. *Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)*. Hoboken, NJ: Wiley (2014).
4. Klaffenbach F, Klein M, Sundaresan S. *Multi-Cloud for Architects*. Birmingham: Packt Publishing (2019).
5. Wang L, Ranjan R, Chen J, Benatallah B. *Cloud Computing*. Boca Raton, FL: CRC Press (2017).
6. Sitaram D, Manjunath G. *Moving To The Cloud: Developing Apps in the New World of Cloud Computing*. Burlington, MA: Syngress (2011).
7. Mell P, Grance T. The NIST definition of cloud computing. *Natl Inst Stand Technol.* (2011) 53:1–7.
8. Rittinghouse JW, Ransome JF. *Cloud Computing*. Boca Raton, FL: CRC Press (2017).
9. Laberis B. *What Is the Cloud?* Sebastopol, CA: O'Reilly Media, Inc (2019).
10. Marinescu DC. *Cloud Computing: Theory and Practice*. Amsterdam: Elsevier Science (2013).
11. Rountree D, Castrillo I. *The Basic of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice*. Amsterdam: Elsevier Science (2013).
12. Huang D, Wu H. *Mobile Cloud Computing*. Burlington, MA: Morgan Kaufmann (2017).
13. Trautman P. *Designing and Building a Hybrid Cloud*. Sebastopol, CA: O'Reilly Media, Inc (2018).
14. Faynberg I, Lu H-LS. *Cloud Computing*. Hoboken, NJ: Wiley (2016).
15. Still A. *Optimizing Cloud Migration*. Sebastopol, CA: O'Reilly Media, Inc (2016).
16. Francis S. *Preparing for Your Migration to the Cloud*. Sebastopol, CA: O'Reilly Media, Inc (2018).