

Cloud Computing

(In English)

Noureddine CHAIB

Cloud Computing.....	1
1. Preface.....	6
1.1. About the Author	7
1.2. Purpose of the Handout	8
2. Chapter 1: Understanding Cloud Computing	10
2.1. Definition and Basics	11
2.2. Evolution of Cloud Computing	11
3. Chapter 2: Cloud Computing Models	12
3.1. Infrastructure as a Service (IaaS).....	14
3.2. Platform as a Service (PaaS)	17
3.3. Software as a Service (SaaS)	18
4. Chapter 3: Key Components of Cloud Computing	19
4.1. Virtualization.....	21
4.2. Storage.....	22
4.3. Networking.....	23
5. Chapter 4: Benefits and Challenges of Cloud Computing	25
5.1. Scalability and Flexibility.....	25
5.2. Cost-Efficiency	26
5.3. Security and Privacy Concerns	27
6. Chapter 5: Cloud Service Providers	29
6.1. Amazon Web Services (AWS)	30
6.2. Microsoft Azure.....	31
6.3. Google Cloud Platform	32
7. Chapter 6: Cloud Computing in Business	34
7.1. Cloud Adoption Trends	35
7.2. Use Cases and Case Studies.....	36
8. Chapter 7: Future Trends in Cloud Computing :.....	39
8.1. Edge Computing :	39
8.2. Serverless Architectures :	40
9. Chapter 8: Legal and Ethical Considerations in Cloud Computing :.....	42

9.1. Data Protection Regulations :	42
9.2. Vendor Lock-In :	43
10. Chapter 9: Multi-Cloud Strategies :	45
10.1 Benefits and Challenges of Multi-Cloud Environments :	46
10.2 Implementing Multi-Cloud Architecture :	47
10.3 Best Practices for Managing Multi-Cloud Deployments :	47
11. Chapter 10: Hybrid Cloud Solutions :	49
11.1 Hybrid Cloud Solutions :	49
11.2 Hybrid Cloud Models and Use Cases :	49
11.3 Integration Strategies for Hybrid Cloud Environments :	50
11.4 Security Considerations in Hybrid Cloud Deployments :	51
12. Chapter 11: Cloud-Native Architecture :	53
12.1 Key Principles of Cloud-Native Design :	54
13 . Chapter 12: X Multi-Cloud Strategies:	55
13.1 Benefits and Challenges of Multi-Cloud Environments :	56
13.2. Implementing Multi-Cloud Architecture :	57
14. Chapter 13: Hybrid Cloud Solutions :	59
14.1. Hybrid Cloud Models and Use Cases :	59
14.2. Integration Strategies for Hybrid Cloud Environments	60
14.3. Security Considerations in Hybrid Cloud Deployments	61
15. Chapter 14: Cloud-Native Architecture	63
15.1. Key Principles of Cloud-Native Design	64
15.2. Containerization and Orchestration Technologies	64
15.3. Benefits of Cloud-Native Applications	65
16. Chapter 15: Microservices and Cloud Computing	67
16.1. Microservices Architecture Overview :	67
16.2. Microservices Deployment Strategies	68
17. Chapter 16 : Advanced Security Strategies in Cloud Computing :	71
17.1. Zero Trust Security Model	72
17.2. Threat Intelligence and Security Automation	72

17.3. Secure Access Control Mechanisms	74
18. Chapter 17: Compliance Standards in Cloud Computing :.....	75
18.1. Overview of Key Compliance Regulations (HIPAA, GDPR, etc.).....	75
18.2. Compliance Challenges and Solutions	76
18.3. Auditing and Reporting for Compliance.....	77
19. Chapter 18: Identity and Access Management (IAM) in the Cloud :	78
19.1. IAM Concepts and Components :.....	78
19.2. Role-Based Access Control (RBAC) in IAM :	79
19.3. IAM Best Practices and Implementation Tips :	80
20. Conclusion and Future Outlook	81
20.1. Summary of Key Points	82
20.2. Emerging Technologies in Cloud Computing	83
21. Appendices	85
Appendices A: A Comprehensive Guide to Docker and OpenStack: A Practical Approach for Students	86
1. Introduction to Docker and OpenStack	86
1.1. Overview of Containerization and Virtualization	87
2. Getting Started with Docker.....	88
2.1. Installation and Setup	88
2.1.1. Prerequisites for Docker Installation	89
2.1. Installation and Setup.....	89
3. Docker Basics	89
3.1. Containers vs. Virtual Machines	89
4. Docker Commands and Operations.....	90
4.1. Building and Running Containers	91
5. Docker Networking and Volumes.....	91
5.1. Connecting Containers.....	92
6. Introduction to OpenStack	93
6.1. What is OpenStack?	94
7. Key Components of OpenStack	95

7.1. Nova (Compute)	95
7.2. Neutron (Networking)	96
7.3. Glance (Image Service)	97
8. Setting up an OpenStack Environment	98
8.1. Installation Steps	99
9. Creating and Managing Virtual Machines in OpenStack	99
9.1. Launching Instances	100
10. Networking in OpenStack	101
10.1. Software-Defined Networking (SDN)	102
11. Container Orchestration with OpenStack	102
11.1. Using Magnum	103
Conclusion and Next Steps	105
Glossary of Terms	106
Additional Resources	107

1. Preface

[1]Cloud computing is an on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. It is a model for storing and managing data in the internet and through the interconnected servers and the data is stored on the cloud rather than the computer, making it more secure and easily accessible. Therefore, it is possible to understand specific aspects of cloud computing, such as big data, and cloud security through this article. This article explains cloud computing and then introducing the challenges, solutions, and frameworks and offers some new aspects with comprehensive support of the references to clarify the background of ideas and validate the new proposals within an environment whose evolution is remarkable and promising eschewing the pragmatic approaches of the article.[2]Despite important benefits that cloud computing can offer, it has yet to penetrate into less developed economies. This lack of adoption can stifle economic development as businesses, and nations miss opportunities to innovate and improve operational performance. The purpose of this article is to provide readers with a baseline level of knowledge about cloud computing that includes definitions, concepts and architectural and component descriptions. Here, cloud computing is considered with respect to traditional computing and the challenges and potential effects that cloud computing offers and imposes. This material is the cornerstone of knowledge that must be understood before exploring any of the myriad concepts or systems that use cloud computing.

1.1. About the Author

Noureddine Chaib (Senior Member, IEEE) received the B.E. degree in computer science engineering from the University of Laghouat, in 2007, the M.E. degree in computer science from the University of Batna, in 2011, and the Ph.D. degree in computer science from the University of Laghouat. He serves as a Treasurer of the IEEE Algeria Section. He is currently an Associate Professor with the Computer Science Department and the Chief Information Officer of the University of Laghouat. His research interests include security, privacy, mobile, and vehicular networks and other networking topics. He is a member of the Computer Science and Mathematics Laboratory (LIM) and the IEEE Vehicular Technology and the Intelligent Transportation Systems Societies.

1.2. Purpose of the Handout

When we started writing this handout, we were thinking that this can be the first step for the technical students who are not yet introduced to the cloud computing concepts. We did our best to cover all necessary topics and a little more. This handout leads the reader from understanding basic concepts of cloud computing and to state-of-the-art technologies. The handout is twelve chapters long; each chapter covers one sub-context of cloud computing together with the sub-workings generally included in that same sub-context. This handout is intended to be a straight introductory handout for readers who are beginning to study cloud computing technologies. It introduces the concept of cloud computing and the specific operation of these types of technologies. With its structured scientific information, comprehensibility, and scientific reliability, it is intended for professional workers, university students, and graduate students of software and IT programs who want to specialize in cloud computing and to carry out their own scientific research in this field. It will be an indispensable resource for them. We also designed it as an easily understood reference Handout for those who want to keep up with the developing technology."

" [4] This Handout is designed as an introduction to cloud computing. It will serve as a standalone introduction or a supporting text for technical courses. The intended readers are business decision makers, as well as technical professionals and graduate-level students. This handout explains the concepts in simple terms. Understanding and consuming the material will not require any prior knowledge in computer science or IT. The initial chapters indicate the potential of cloud computing by walking the reader through the major advantages it offers. The handout continues to explain

cloud computing from an architectural perspective. Which is further explained in real use scenarios with the inclusion of the Building Blocks of the cloud, such as, computing architecture of cloud, storage architecture of cloud services, database architecture of cloud services, and network architecture of cloud services. Storage, Database, Application testing, and other IT best practices are covered through simplified working examples.

2. Chapter 1: Understanding Cloud Computing

Data Center: The data center is the crucial point of the cloud computing system. A data center consists of clusters of small, low-cost, commodity servers, with high-speed communication for parallel data processing. The increasing demand for cloud computing has led to rapid growth in data centers, which consumes much energy due to the computational workload. Researchers worked on developing efficient algorithms and modeling techniques for power reduction [5].

With the advent of cloud computing, it has now become possible to host, maintain, and use web applications and projects on a scale never seen before. Just around thirty years ago in the eighties and the nineties, users often had to buy dedicated hardware to host their computational systems. Later, in the 1980s, the concept of time-sharing was introduced where users could use the disk space and other resources from other remote computers and these remote computers were coined as 'remote hosts' or servers. However, these systems were expensive and required skilled labor to manage and were typically suitable only for the use within large organizations [6]. With the advent of Internet, renting computing resources also became popular for users for hosting web sites and applications. But, one fatidic meeting made of executive with personality of the industry tech giants Google, Amazon, and Apple led to Google Cloud, Amazon Elastic Compute Cloud (Amazon EC2), and Apple iCloud respectively leading to an entirely new era where computing resources, from mammoth capacity and large cluster of machines of the cloud providers, could be spun up and down without any dependencies on the availability of the existing facilitation [7]. The advantages of using cloud computing can be considered as the flexibility of compute resources, ability to scale on demand and according to the user needs, and a vast range of computation, and storage capacity and resources without having to maintain the infrastructure. There are additional advantages of using cloud services such as pay as you go which can of course decrease the operational cost for the user, and the concept of shared cloud which is standard to all users. And

most importantly, on demand resource allocation, which is constantly working and helping a user when she needs it. The cloud computing architecture comprises a front end, back end, and network. The setting between the front end and back end is referred to as trunk. The basic cloud components are:

2.1. Definition and Basics

[8] Cloud computing is the third novel IT operation mode following the personal computer (PC) and the web. It is characterized by centralized computing resources differentiated in a large number of diverse scale, agile expansion and the fast provision of services. Cloud computing technically integrates and absorbs user's access, usage, expenditure, and other information. This new computer science model largely frees the user from the hardware and software infrastructure quandary, enabling easier development and deployment with economic benefit. The on-demand self-service is one of the five main advantages of cloud computing. Users can choose the services by themselves according to specific demands without customer service intervention. The other four main characteristics are broad network access, resource pooling, rapid elasticity, and measured service.[9] There are mainly four kinds of important trade interfaces that must be followed. Each trade must establish related trade relation according to these interfaces between the cloud servers. In this way, some relatively complex operations can finally be completed with a limited number of functions. This improves the cloud capacity, the universality of the cloud, thus promoting the development of the cloud. Cloud computing is proved to be an efficient distribution and use mode in the web and visual cloud services such as Google Documents. In general, the cloud operation model has good application prospect. In this book, the existing theories and available technologies about cloud computing are summarized, discussed, and further developed.

2.2. Evolution of Cloud Computing

[10] The origins of cloud computing can be found in the form of "utility computing", a concept that dates back to the 1960's. The term cloud

computing was not in use until 1996 when it was coined by Ramnath Chellappan et al in 1996. In the same year, David Krantz and Carsten Vance coined the term for software as a service (SaaS), which is a part of cloud computing that allows for the creation of application software and data access from anywhere via the internet. The obvious benefits and the complexity of the services provided by cloud computing paved the way for its adoption from 2002 onwards. There was a significant commercial importance found in "cloud services", where the dependencies are handled by the cloud environment. Successful cloud services were launched in 2002 by Amazon—EC2 and S3, in 2005 and 2006 by Google—Google Apps, in 2008 by Microsoft—Azure. The upcoming services boast the same importance.[11] Cloud computing is an essential concept for the booking of one or more online computing as well as storage resources. It also allows people to access online services for both business and personal purposes. The first-ever cloud service was introduced in 2006 and it includes Amazon Simple Storage Service (Amazon S3) and Amazon Elastic Compute Cloud (Amazon EC2). As the requirement for cloud computing is rapidly increasing, recently Google took a step forward and developed Google Colab where people run different coding on it and they have the options of both premium and free versions available. Most of the companies like Amazon, Azure, and Oracle Cloud are taking the advantages of cloud hosting. With the advent of this technology, the cost as well as the resources associated with hiring enough employees becomes marginalized. Due to the prompt development of cloud computing, there is a vast possibility of shutting down personal computer-labs in the future.

3. Chapter 2: Cloud Computing Models

In cloud computing models, aspects related to the measuring of the Multi-Tenancy load can directly impact throughput, the quantity of cloud computing resources, response time, energy consumption, and the QoE (quality of experience) of the multi-tenancy cloud and cloud computing server. Therefore, it is important to develop and indicate the measure of the Multi-Tenancy load. The analysis of the measure of the Multi-Tenancy

load in the cloud where cloud computing infrastructures and resource allocation evolve over time, is important. Also, extensive analysis of describing and discussing the importance of the measure of the Multi-Tenancy load, will be carried out. Considering current technology such as servers, parallel processing, and cloud computing, an extensive survey will be offered. In addition, the new types and characteristics of Multi-Tenancy load will also be presented [12].

Cloud-based solutions can play a significant role in enhancing student learning. Research shows that when educators and technologists understand the potential of cloud computing and creatively deploy it, online learning environments can lead to positive student engagement and improved learning outcomes, and the costs of learning can be reduced [13]. The mode of delivery of cloud computing is not only highly accessible, it is also flexible and addresses issues such as real-time updates, scalability, etc. The many benefits of cloud computing such as reduced allocation of on-site servers, decreased IT infrastructure cost, increased collaboration and flexibility, reduced risk of data loss, and its ability to provide a common platform for students and educators to interact, has also made it an attractive technology solution for educational institutions [14].

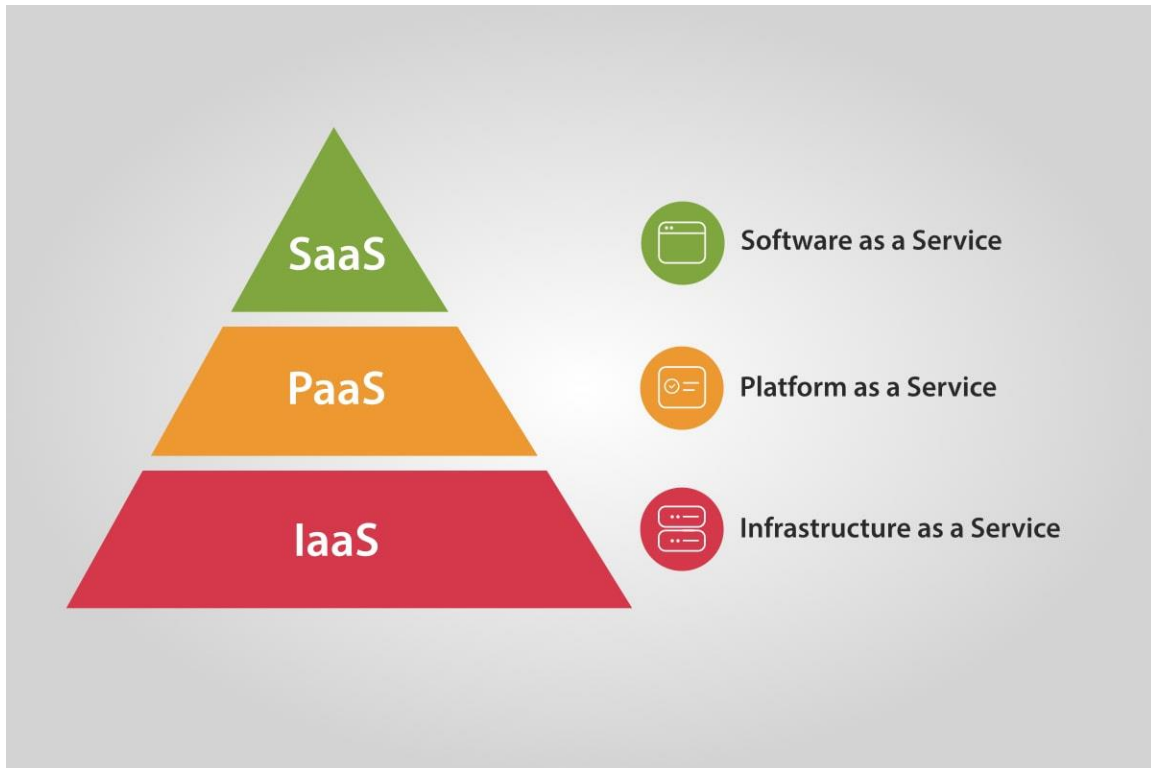


Figure 1: Cloud Computing Models

3.1. Infrastructure as a Service (IaaS)

IaaS serves as the basis for all other cloud services, providing the infrastructure for cloud clients to store their resources. IaaS enables cloud clients to customize their infrastructure to their own liking. If cloud clients need video cards, there are plenty of IaaS that provide GPU in the cloud. It has added the features and functionalities of GPU-based tasks in the cloud. Several cloud service providers provide multiple virtual machines, and not all resources are utilized at the same time. Some cloud clients can afford to rent multiple virtual machines. Cloud server-sharing technology allows high-availability, dynamically scalable, stable resources, and a wide variety of computing resources. After the cloud clients rent these high-performance and low latency CPU, GPU, RAM, and storage infrastructure resources that they need, they experiment and complete their tasks and collect the findings from the experiments. Supplementing resources also means that they are cost-effective, ecological-friendly, maintenance-free, powerful, very fast, and secure hardware. One important property of AWS, Google,

and Azure is IaaS. All other services of AWS, Google, and Azure operate on IaaS. All you need before getting started is to pay for the cloud IaaS services and up and running the virtual server, or solving the customer's requests, or connecting with internet activities where low latency is very crucial. Optionally there are many features such as unique security rules mechanic border protection that cloud clients use exclusively.

All users need to do is build and deploy their software without the need for any investment or hardware (virtual machines) and install an operating system, application, and the database. The resources that are offered as part of every instance will vary from cloud service providers, and it is up to users to adjust the virtual instance configurations at an extra cost. Users typically don't run applications in isolation; usually, they work as a group, and software requires middleware (web server, application server, messaging system, etc) and a database all set to go with a virtual instance. Very few COTS which might be installed on the Home PC. It is a good idea to create the required stack or get ready-made stack image from the cloud service provider. IaaS service models typically include virtualized infrastructure, virtualized computing resources, compute-based virtualized resource, storage-based virtualized resources, networking, monitoring services, recovery services and management services. As per the On-Demand functionalities and data management, different vendors provide different services [15]. IaaS can be extended to IoT infrastructure, offering facilities such as computing and storage, and may be complemented by standardized access to sensors and actuators. Researchers thus proposed IoT Edge as a service (IoTEaaS) by enhancing the IaaS model and presented virtualized asset and service management platform. They also used dynamic configuration and adaptation to optimize QoS and resource utilization as well as the quality and overhead of the monitoring data. IaaS role requires that end users have a patent virtualization system at their only disposal. It is straightforwardly called IaaS-based IoTEaaS. If the end user does not want to implement the virtualization system, instead of if, this manager system Unique controller and responsibility of the formal class must be compatible with the IaaS feature. In terms of any failure in providing end-

user required demands and QoS violations can immolate the responsibilities to the IaaS service provider managers to control global edge Physical resources, since these resource managers are the IaaS service providers' duty [16].

Infrastructure as a Service (IaaS) in cloud computing provides computing, storage, network, security, and operating systems virtualization technology as a service. Users have full control to customize the environment and can access resources on a "Pay-as-you-Go" basis ecosystem. IaaS cloud systems usually have a virtualized environment in which cloud consumers can create virtual instances; these virtual instances are also called virtual machines and virtual networks [17]. IaaS allows users to utilize other software stacks like the virtualization stack, management and orchestration software stack, infrastructure setup and configuration mechanism. It is suitable for users who wish to deploy ready-made software stacks, monitored applications, and server operations system images in the cloud environment. IaaS providers will provide facilities like a fire-wall and software components like load balancer, but users need to install or pay extra charges to use these. IaaS also extends on-prem architectures to the cloud infrastructure and offers utility computing and outsourcing the IT infrastructure to a cloud service provider.

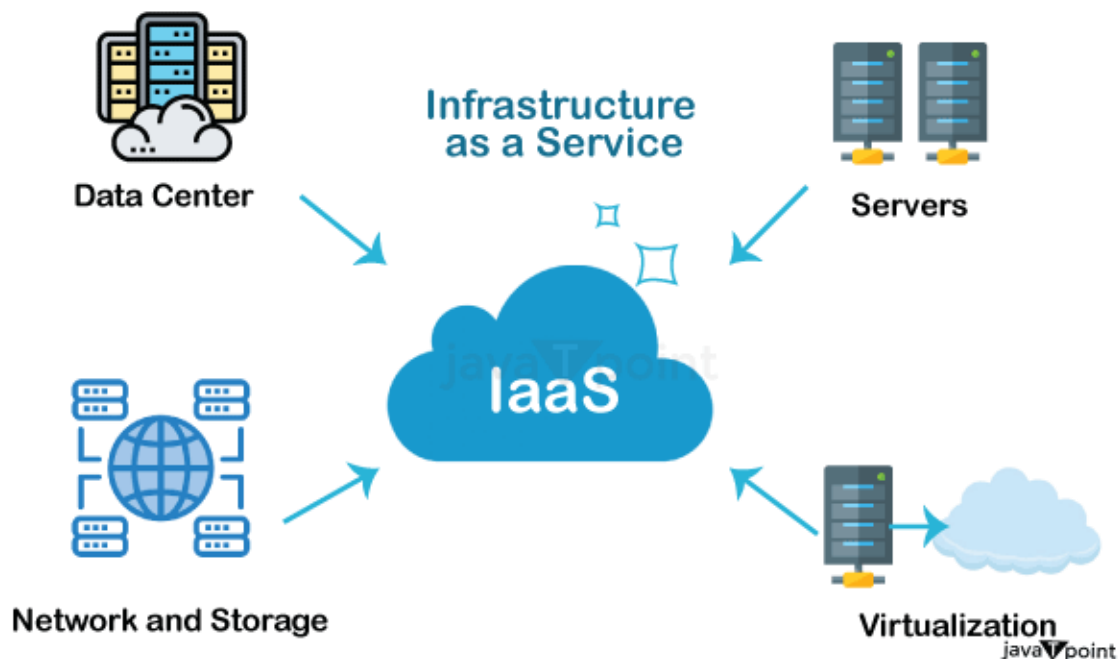


Figure 2: IAAS Model

3.2. Platform as a Service (PaaS)

In this regard, prominent providers of Cloud services are usually seen as so-called "Cloud kitchen" for developers. A Cloud kitchen basically provides developers with a set of distinct Cloud services to enable fast and secure. The popularity of Cloud kitchens has steadily been increasing abroad. However, the current distribution of Cloud kitchen providers is seen to be unbalanced throughout the world such services. Furthermore, through this sort of approach, Cloud service providers can receive guidance and recommendations on the provision of better quality services and thus ensure that cloud developers' demands are satisfied.

Cloud computing is nowadays among the most remarkable and well-known IT developments, comprising three major types of service models: IaaS, PaaS and SaaS. PaaS is seen as an effective means of addressing computing troubles, overcoming hardware and software development costs, easing access to applications and application services and minimizing costs related

to infrastructure—each of them representing a significant obstacle for use of grid computing or service-oriented architectures (SOA) [18]. PaaS can support the entire life cycle of application development for the Cloud. PaaS incorporates features such as source antialiasing and data interchange among applications. Crucial platforms are provided by Microsoft Azure, Google App Engine, Force.com, Amazon Elastic Beanstalk, Apache Stratos and Xservice. These platforms offer distinct components and development opportunities [19].



Figure 3: PAAS Model

3.3. Software as a Service (SaaS)

SaaS is similar to a service available over the same network, cloud computing. However, SaaS only takes user applications, and API service request gives consumers complete use of on-demand application code and platform. Like cloud computing, SaaS enables consumers to purchase access

to third-party business software over the Internet. While many services like a document management, customer relationship management are hosting, office programs under brands of Microsoft's Office 365 and Google's G Suite. Google Docs offers a SaaS that can be used as an alternative with an Excel document or a Word document, a word processing software that allows users to bore, edit, publish and share components of rich text and table [20].

Software as a Service (SaaS) software as a service (SaaS), describes the delivery of third-party software used by consumers over the Internet [19]. With SaaS, besides of the need to focuses on the proprietary applications codes for each consumer, the code can be customized through the application programming interfaces (API) [21].

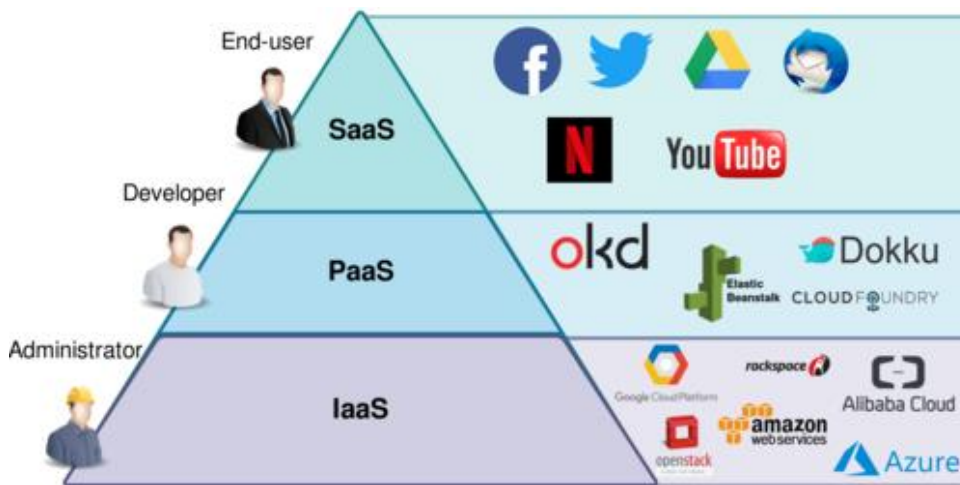


Figure 4: SAAS Model

4. Chapter 3: Key Components of Cloud Computing

Platform-level virtualization technology makes a single physical machine multiple system instances, which is also what we often call virtualization technology. After using virtualization technology, a shared physical machine can also be provided, and single machine resources can be guaranteed without channel games. This is not only more efficient on the level of using

machine resources, but also more effective in terms of management and allocation of physical machine resources. The main part of the cloud computing system is the cloud computer cluster. It is the data processing and data storage of the cloud platform, and also a computing resource provider. The database is the cornerstone of the information system, which is responsible for collecting, processing, and storing data. The cloud computing storage system is the basic support of cloud computing, mainly responsible for storing the user's personal data or enterprise applications along with the public data and application data of the cloud platform, and maintaining user data privacy and data security, as well as ensuring the data integrity and consistency of the data platform. Cloud management refers to IT software at the operating system layer equivalent to a management system, that is, a cluster management tool. In the data center management system, the following evaluations are common such as resource management, fault management, service management [22].

[23] [24]The goal of shifting from traditional hosting to cloud hosting is to free the website from the control of the physical server and move towards the centralized, efficient, scalable, and flexible cloud service. The beauty of cloud services lies in that users can only access cloud computing hardware resources like dedicated or VPS without the knowledge or control of the backend technical infrastructure. The backend of cloud services is a massive data center with centralized control of system resources, whereby data and computing tasks are assigned and supervised efficiently. The architecture of cloud computing is too complex, there's compression of data center control network; however, because data centers have several different control systems, including power-on management, network management, data management, and other facilities, so control of the system is also relatively abundant for cloud computing.

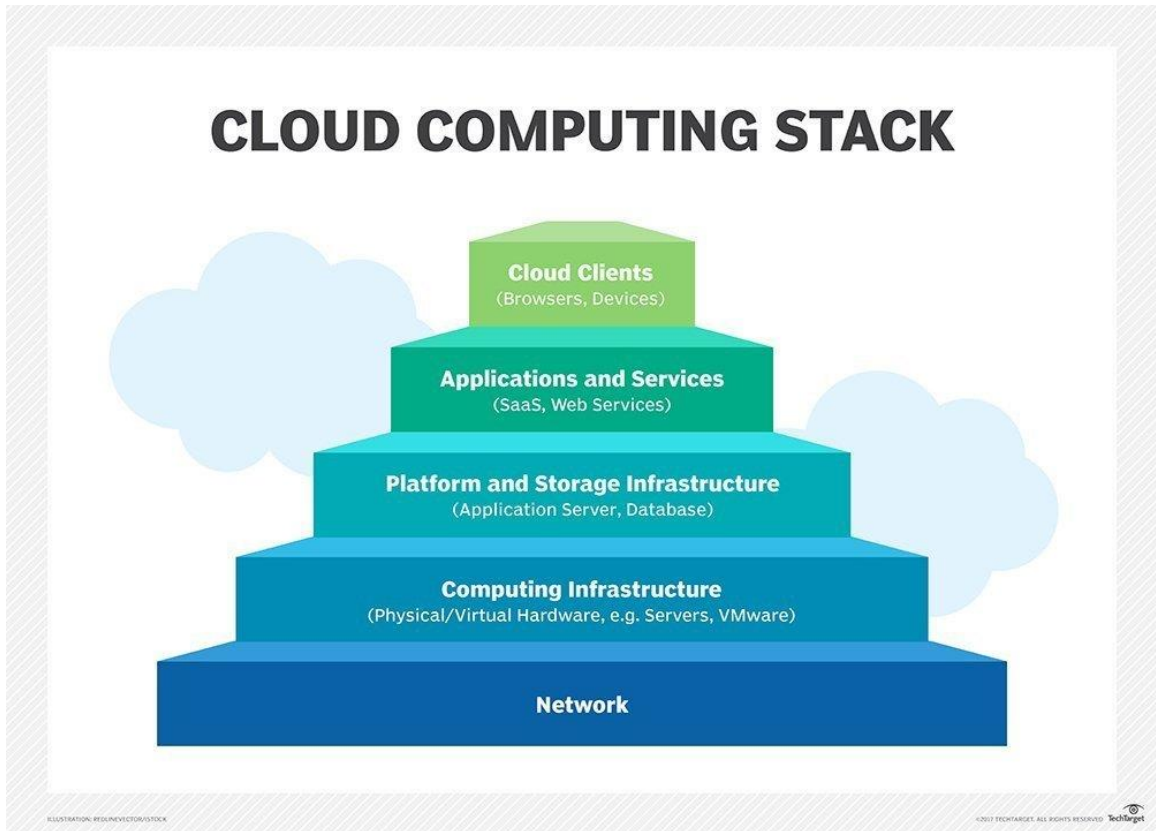


Figure 5: Key Elements in Cloud Infrastructure

4.1. Virtualization

VMware vCloud Director provides a means of managing the virtualized resources in a datacenter, with particular emphasis on the sharing of a large number of virtual machines on as few pieces of physical hardware as possible. VMware offers two methods for configuring a VM: a standard virtual machine or a defined vApp [25]. VMware vCloud Director deploys these vApps rather than individual VMs, and so the vApp template is a natural choice when deploying the OSM Management platform. VMware vCloud Director extends the usability of VM viApps. This allows for the

addition of multiple VMs to a single vApp, via a role-based security and firewall sharing between VMs of the same vApp, and declarative lifecycle management of the app. Thereevery, for deployment by the 'cloudy animal installer', by packaging the management components and its full complement of dependencies in a vApp, including relvant information relating to the target Openstack installation`.

` An important feature of cloud computing is virtualization, which allows for the sharing of resources in the cloud, and opens up significant cost benefits. In practical terms, this allows several independent VMs to be run on the same infrastructure, with each VM running different operating systems and applications [26]. While this is a good thing—the popularity of virtualization is self-evident—it also presents important security and performance challenges. Some literature in virtualization focuses on the provisioning of resources for single clients, focusing on CPU and memory. In that context, the focus is often on scheduling resources to allow individual VMs to meet QoS expectations: these are now classic problems. This section discusses the hardware-level virtualization and management presented within the popular VMware management and Openstack Management platforms.

4.2. Storage

[27]. Cloud storage is a component of cloud computing. It allows data to be stored and accessed through the internet from anywhere at anytime without any physical management of hardware. By adopting the cloud storage service, enterprises can store or back up the company's data (or personal data) remotely. With the rapid boom in the amount of data, convenient and reliable data storage is becoming essential in big data systems. Moreover, public cloud storage services are provided by third-party providers over the Internet. So it provides a mechanism to store all types of data(source data that needs to be stored, processed data, etc); more and more enterprises are adopting the cloud storage service. Cloud storage has more advantages than traditional storage services, including data security, reliability, scalability, fault tolerance, disaster recovery for enterprise; cost effectiveness, access to data from anywhere, automatic updating and

maintaining, and so on. for small organizations and individuals. There are many public cloud storage services available, including Google drive, Dropbox, iCloud, Amazon Web Services, etc.[22]. As vast businesses keep running around cloud services, organizations are making advances in cloud computing to better understand features, future research directions, and potential threats. There are many who look forward to understanding the rising trends in cloud security and mechanisms. There has been a significant amount of research conducted in the past, and the scope of this trend will predict more of the advanced techniques that can be used in Cloud computing. Understanding the trends of the security of cloud systems can lay down a roadmap for Cloud Computing. Cloud computing is making it easy to store data and save data, because of the user friendly environment. Various publicly available datasets have been used to justify the trend and the other underlying techniques which can be potentially extended to safeguard a cloud system.

4.3. Networking

The cloud can bring mutually beneficial collaboration and share costs and resources, as anyone can globally access online services that are available, although the increase from cloud services has created numerous challenges, including low electricity costs up and load sharing of cloud services, Quality of Service (QoS), data security and protect the privacy. Services are available online that can be advanced using mutual collaboration and resource sharing and collaborative services are available. In addition to providing convenience, bringing infrastructure and resource sharing through mutual collaboration can enable considerable advantages. It will practically assist the cloud computing to achieve its objectives. With the growth and propagation of online collaborative services, mutual access to network-based services is almost obligatory for businesses, schools, governments, and at the personal level. At the same time, online collaborative services are used by the public for the benefit of free or low cost, excellent scalability and reliability, consistent maintenance, and transparent integrity of cloud services they obtain.

[7] [2]Cloud computing and cloud service are emerging technologies that provide services for mutual collaboration and resource sharing, allowing for economies of scale and the provision of parallel resources, thus virtually reducing the cost of ownership. It results in lower cost and overhead for users and is increasingly cost-effective compared to traditional computing services. As online collaborative services continue to grow and flourish, access to network-based services is almost critical for businesses, schools and government or at the personal level. Cloud computing march to face the challenges and requirements of the real world. Another aspect of IT development is the increased demand for highly secure, seamless, and fewer service services that if using efficient encryption and decryption algorithms make real-world cloud computing adopted and widely used. Clients not only want to obtain data from services, they also share large amounts of data with clients using a variety of platforms.

5. Chapter 4: Benefits and Challenges of Cloud Computing

Many businesses aren't committed to the power of cloud computing. Some are worried that their data isn't secure outside their data centers with some help. We are convinced to have a data breakdown in the eye of the storm without constant surveillance. In certain instances, cloud providers have doxoromed access to physical storage pressurization. Basically, this is a supplement to a weekly ups admission scenario. We're only a thousand substantial promoted data breach web trends in the cloud, where importance has been emphasized. For lack of institutional support, a business organization will imprison its business data. Problems first burn politically [28].

[29] Cloud computing maximizes the power of Internet technology by enabling software, platform, and infrastructure to be retrieved, utilized, and powered off site. By accessing datacenters with servers, clouds can provide the power required for critical and computationally intensive operations, and make significant IT expenditures disappear into a monthly-level bill. Every day, cloud services take in trillions of bytes of consumer data, and make them available to record and analyze on a global scale through devices such as smartphones and personal computers. However, cloud computing also includes the transformation of power technologies including large-scale data centers and networks, telecommunications facilities for consumers and industry, network systems, and emergency data recovery. This transformation will have a significant impact on the ICT industry as stakeholders plan to plan and overcome security, confidentiality, reliability, and legal and governance concerns [30].

5.1. Scalability and Flexibility

Users in different applications often require flexible scheduling and scalable dynamic extensions. Because of the significant number of layers, levels, technologies, and new trending research, cloud computing and resource management cannot be developed holistically. Cloud cyberspace resource integration and allocation are continuously improving, and the architecture is more open and elastic, which introduces large-scale applications and network

challenges. Cloud cyberspace resource management hierarchy is illustrated and separated in this paper for better understanding of different layers.

Cloud computing is a technology that enables large-scale data processing and application execution, and it offers high scalability, accessibility, and on-demand services like SaaS, PaaS, and IaaS [31]. The wide range of applications of cloud computing includes education, commerce, healthcare, management, research, and earth science. Cloud computing and resource aggregation improves the ability of parallel execution, decreases resource allocation time, and improves resource utilization, providing high elastic scale application support and data management and data storage support.

5.2. Cost-Efficiency

[32] Cloud computing offers instant access to further capital and lowers the amount the of capital expenditure needed to buy the processing power, server space, and a host of other applications traditionally required to operate an information center. At that moment when enormous reserves of computing services can be even started, businesses can produce a large amount of dollars in earnest, which can put a huge gap between surviving cloud processing and conventional data center management. In particular, the deficiency of service sums and wind speed begins to show that telecoms consider switching from service-based processing to cloud processing comparatively easy. The system will allow for the possibility of executing speed-by-operator assets with the appropriate resources at times where demand for services is greater than at accelerating speed, which may serve clients at lower than average tools for many client expectations.[33] As customers can access from abroad some cloud screening suppliers can change logistics, this facility is in contrast that managers have done so, and ultimately shows more robust procedures under specific systems of work. However, there are cons: the excessively rapid release of control to service firms may lead to enforcement problems, while separating completely makes coordination difficult. Therefore, Laura Bianchini, Antonio Olivieri and Michele Sambo a test is suggested, which will go with transaction expenses which translate to the total costs when the transaction is divided into

several services compared to one, to be borne by various trading parties. Because of the proximity of the financial implications and intangible attributes that is not quantifiable, satisfaction can also be derived from a strategic choice. Due to the fact that services can be extremely difficult to measure, especially in consultancy firms, it is however appropriate to maintain relevant information that corresponds to the mono (number of users), but which must be cautious to the blintilation, contradiction and inequality.

5.3. Security and Privacy Concerns

However, innovations and solutions for various AFS challenges exist for every step of the supply chain. From feed, farm, transport to processing steps/solutions, appropriate, innovative and sustainable technologies have been developed to secure food safety and quality during food processing stages [34]. Comprehensive overviews of the different issues and potential solutions for innovative and modern animal farming systems exist. Each processing step, including safe and clean transportation of the birds to the slaughter house, is crucial for the final product in terms of food safety. The aim of this paper is to provide detailed extensive information about the poultry meat production's animal welfare, food safety and feed efficiency aspects through a comprehensive review of literature. The paper also emphasizes on the European and Asian practices and their differences.

In the past few years, there has been a shift from traditional agriculture to eco-friendly crop production and this change has also affected poultry processing. As a result of all this, modern and innovative technologies are used everywhere for the production of healthy animals and for the protection of the environment. Processors are increasingly focusing on food safety which is achieved only when the animal is healthy, and considering animal welfare, legislations are changing constantly in terms of their objectives [35]. The growing demand by the consumers for safe, healthy, affordable food and transparency on the entire production chain is the main reason for the gains in food safety assurance systems and quality measures. The poultry sector is currently challenged by the demand to meet these

requirements due to its substantial energy, water and land use. There is considerable variation in the poultry meat industry in terms of poultry and consumer concerns from one country to another.(sess. Inter-Cloud Data Security Strategies).

Tamara Monterio Fernandez, in her case study, "Chicken Chicken Processing in Europe and Asia: A Comparative Study", emphasized the importance of broiler welfare, feed efficiency improvement, quality enhancement and food safety in AFS platforms. China, an important hub for animal husbandry and poultry processing, experienced a few major food safety problems in the past such as the 1989 cooking oil incident, the 2008 milk powder safety event and chicken pollutants found in 2021. The Chinese government enacted strict regulations to deal with these issues and designed food traceability systems to improve food safety.

6. Chapter 5: Cloud Service Providers

Companies are using cloud technologies to transform their products and services. This revolution has created tremendous opportunities for many players. Major models of Cloud computing include Software-as-a-Service like Salesforce, Microsoft 365, etc. Systems developers are taking advantage of the scalability and quick startup of cloud environments (PaaS), Infrastructure-as-a-Service, Platform-as-a-Service, Software-as-a-Service, and many more.[36]Leveraging advanced state-of-the-art 5G, virtual reality, Simultaneous Localization and Mapping 3D technologies, and user interactive services on the cloud, future interventions are targeted to include cloud - based innovation: a detailed discussion on cloud-based innovation considering the ongoing pandemic and beyond. The chapter also revisits the essential cloud computing architectural concepts, essential cloud types, available service models, and commercially available top 5 cloud service providers. It covers the role of 5G, edge, and fog computing along with reinforcement learning, multi-agent systems, artificial intelligence, machine learning, neural networks, and data compression techniques in enhancing.

[23] [37]Cloud computing is the latest trend in the field of cloud computing, enabling users to access powerful servers and storage on the web and use it to their benefit. Cloud computing is the on-demand delivery of IT resources and applications over the internet with pay-as-you-go pricing." The top cloud vendors operating in the global public cloud infrastructure have been discussed, including Amazon Web Services, Microsoft Corp, Google, IBM, and Oracle. Cloud computing, itself, is revolutionizing the IT landscape; service providers are now offering cloud computing services. It attributes its widespread adoption to availability through sharing resources, elasticity, the huge potential for scalability, easier access and usage, easy maintenance, and low costs, among others.



Figure 6: Major-Cloud-Computing-Service-Providers

6.1. Amazon Web Services (AWS)

How could we build services at Amazon? By running lots of smaller evenly sized teams owning the services end to end, small cross service communication resulting in a larger service that delivers value to a customer without any head. Embracing operational ownership by the team triggered a great feedback loop of understanding the pain points of customer running the production. The service owners stopped doing undifferentiated heavy lifting to be able to innovate even better and quickly for the customer.

Today, connectors are built for a vast number of services, and AWS provides a container service. This means that we have this very well-oiled machine where things automatically and seamlessly have API convergence across different services. On top of that, what we are capable of releasing is not just a VM or an instance of compute, but an entire region or a whole data center-like infrastructure on the cloud with all these fabric controllers, and networking fabric. [19] You can also use services to a

dizzying degree to do anything. This allows us to service providers around the world and, thanks to Apex and everything that is going on, we are being able to deliver industries specific clouds as well as these general-purpose regions which serve customers across any sector.

[38] One major thing that Amazon identified with AWS was the need for automation through API. Thus far, the industry was being run by virtualization and data center managers were familiar with anything and everything involving virtual machines. But you couldn't perform SQL queries on connected virtual machines, which would be a problem if you were building the infrastructure for a multitenant platform. So, Amazon's fundamental premise was that all the services they would bring out would be controlled using an API. We have had this from the outset, and that is one of the key components of the platform.

6.2. Microsoft Azure

Security is an important issue in cloud computing, as client confidentiality is of major concern [19]. As Microsoft Azure runs applications on Microsoft servers, with high security measures, it is around ISO/IEC 27001, SOC 1 and SOC 2, PCI DSS, HIPAA, and others. Transactions are encrypted and transmitted on a highly secured network from on the endpoint to the cloud, using SSL/TLS. Further, Azure has secure customer key management systems in place. Microsoft has a highly structured Shared Responsibility Model (SRM). This model divides the labor and resources essential for cloud computing and security services. In other words, it allows users to take full control of their virtual machine, such as operating system configuration and software installation. It is a significant compliance approach that provides the best possible customer shared responsibility to Azure users.

Microsoft Azure is a major player in cloud computing, offering Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models [39]. As a member of the Microsoft cloud service family, Azure has many advantages such as software services like Windows server, SQL server, and SharePoint. These provide Azure users an added benefit to transform their existing applications onto the

Windows Azure environment. Microsoft Azure can also prove to be a preferred choice for enterprises already using Microsoft products as their enterprise applications [40]. Microsoft Azure operates in 54 regions, around the world, with 67 announced. It is divided into regional cloud units, known as Regions. Departures could cater to these needs of the clients, which are price, durability and fault tolerance. The on-premises deployments are based on currently available capabilities provided by Azure, like, Azure Stack, a set of tools that allows an organization to increase patron advantage by using cloud technology. Global regions and availability zones in Microsoft Azure use a set of policies and configurations to manage network policies for applications. Application gateways are instances within the DataCenter that help in transferring network packets to their destined location.

6.3. Google Cloud Platform

Azure and AWS offer a large set of services in terms of cloud storage. AWS offers "Amazon S3" in its simplest type. The data stored are found in a collection called bucket and they are not placed in a folder. S3 buckets have their own URL's. The import-export solutions are amazon machine image (AMI), amazon cloud front key and AWS Storage gateway. IAM is a service for authoring AWS environments, and it allows defining roles, policies and users. As of 2021, AWS offers more than 200 services. Some other AWS services include "Amazon Transcribe" a voice service, "Amazon Fargate" a compute engine, "Amazon Music" streaming application, and "Amazon Connect" a contact center solution. Some additional services include "Amazon Cognito" a service for user authentication. One final AWS product is "AWS Elemental", a platform that offers encoding, dynamic ad insertion, and video monetization for video delivery.

Google Cloud Platform is a service of Google that offers a number of cloud solutions. In the field of application services, it offers intelligent analytics system, API platform and Internet of Things (IoT). In the field of computing, GCP offers products like "Compute Engine" and "Kubernetes Engine". Under the area of storage and databases, it offers services like a storage platform, SQL, and NoSQL databases. For networking, GCP offers

services like "Network service", "Hybrid and Multi-Cloud" and a communication service for connecting IoT devices with Google Cloud. In the field of hosting, it provides "Cloud Endpoints" for creating, deploying and managing APIs. [17] Statistically, Google Cloud has a market share of around 7.5% and is the third most popular cloud service as of 2021, behind Amazon Web Services (AWS) and Microsoft Azure. [41]

7. Chapter 6: Cloud Computing in Business

When businesses opt to move to the cloud, organizations need to create shifts to a different operating environment. This is not just at the technology level, but also in the system's style and governance of records. Cloud computing faces numerous issues, such as over-rated security and confidentiality, and there continues a concern about whether providers of the cloud possess the capability and potential to handle disasters. The development of infrastructure as well as services for receive and transmit the information is growing along with cloud research and has become popular in industry applications. Users do not possess to have know-how of the internal configuration of the cloud server; end user service details are classified and operational characteristics are hidden. The move to Total Cloud Computing is showing ongoing, and organizations employing electronic sector e.g. Facebook, LinkedIn, and businesses like Amazon, Microsoft are relying heavily on cloud infrastructure providers' services such as AWS, Azure.

[42] Cloud Computing can offer multiple benefits to businesses, such as increasing accessibility, flexibility, reducing IT expenses, moderating hardware resources, and scalability. Recent technological advancements have brought broad shifts not only to businesses but more specifically IT applications. Because of its recurrent evolution in a variety of sectors of the job life, the Cloud has become so prominent that some note that it evolves to the team. [5]

Vision of Cloud Computing

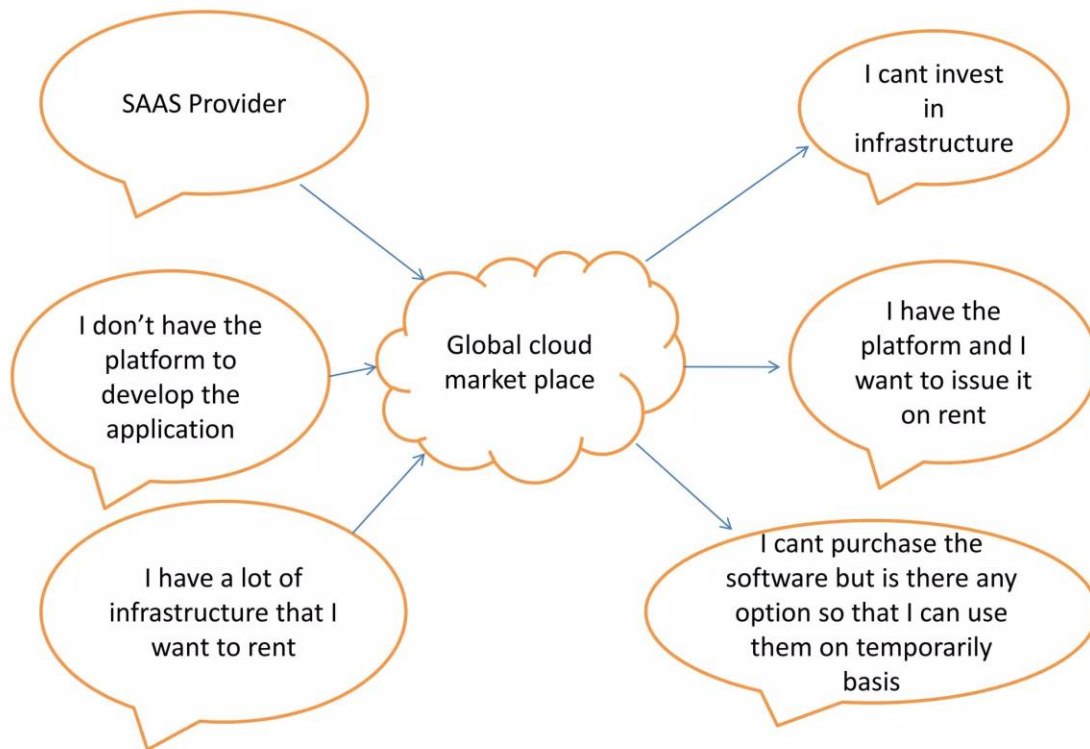


Figure 7: Vision of cloud computing

7.1. Cloud Adoption Trends

In researching the usage of cloud computing based on X-as-a-service, businesses shifted to cloud-centric digital infrastructure as a choice for Internet or software platform connected operations and services. The businesses delineate cloud computing and X-as-a-service platforms based a phases on the spectrum of cloud-based digital communications for various levels of infrastructure while associating platforms with their listings. The transition to Cloud computing and communication technology infrastructure is broadening possibilities, copy, range and abilities in the platform schema. Given the utility of Amazon web services (AWS) infrastructure for a cloud computing platform is clear that due to a backlog of tasks and responsibilities AWS is a common choice for SaaS, IaaS, and PaaS matrix. For instance, AWS CDK - The AWS cli and EC2 are the prime factors of

AWS as a generic service and cloud computing platform Infrastructure service.

[43] Cloud computing optimization focuses on local hardware capacity and software security properties for seamless launch on mobile devices. Cloud computing is actively marketed in businesses to enable faster delivery of processes, services, and software. Industries use cloud computing to underpin platform-level resolutions for disaster recovery and business continuity. The main cloud computing services of IAAS (Infrastructure as a Service), PAAS (Platform as a Service) and SAAS (Software as a Service) also offer several beneficial features like demand and automatic scalability, decreased time to market and ceaselessly replicable user encounters.[44] Cloud-center computing is the desired platform for businesses nowadays, and the transition to Cloud-centric digital infrastructure is getting a position where it's even more accelerated post-pandemic. Cloud computing changes hardware facilities and data centers, from investment-intensive and infrastructural projects to on-demand services. Advanced features like elastic-ios, serverless and high availability render cloud infrastructure more cost-and-time-effective. X-as-a-service depicts the delivery service models that are provided online. Cloud computing not merely modifies the intelligence but likewise the way different mods of platforms are utilized online.

7.2. Use Cases and Case Studies

The performance improvement in the traditional enterprise systems still demands the efficient use of IT resources as per user priorities. In view of increasing demand for cloud infrastructure, the work seems to be quite essential and worthy [45]. Cloud computing technology is promising and challenging because of its architecture and specific type of user demands. Schedules generated by the algorithm for instance, will provision those resources in the cloud to the end users and offer them though requests. A number of task instances were the subject of investigation without knowledge of proper workflow scheduling strategy. On account of that, a performance evaluation for worst case priority with respect to other

strategies was provided in the article. The algorithm is responsible for generating an optimal schedule with respects to minimizing the performancebased makespan under guaranteed SLAs. A maximum number of tasks can be incorporated into this model.

Despite the current expansion of information technology (IT) and computational power, enterprises are still looking for ways to optimize the usage of those assets according to the requirements. Cloud computing is an innovative topic of contemporary interest which has opened up the business opportunities for outsourcing of the IT infrastructures and enterprise applications. According to Buyya et al. [46], cloud computing can be used in the following areas: private, public, community clouds, and hybrid clouds. Generally, organizations tend to create their own private cloud. This is mainly because of the sensitive data handling issues that are the essence of organizations. Community cloud is specified for the collective organizations for a partnership and collaborative purposes. On the other hand, public cloud is customized for the public users. Hybrid cloud is a combination of two or more different cloud entities where they keep their own entities separate but they use to communicate with each other. In general, cloud computing offers a number of benefits, which enable rationalization of the operational costs and costs of ownership of ICT systems, during organizational efforts by these systems. In addition, cloud computing can provide support in the area of management of energy and environmental resources; thus, more environmentally friendly solutions can be achieved and the reduction of CO₂ emissions can be obtained [47]. The use of a number of parallel resources available in the cloud is realized in the form of a model consisting of a number of virtual IaaS systems, platform PaaS, software systems as SaaS services, and cloud data storage systems under a model of DaaS (Data-as-a-Service). Cloud computing deliver services in three categories: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). SaaS offers traditional application functions through the web, PaaS offers virtualized servers for web application deployment, and IaaS provides basic computer infrastructure services.

8. Chapter 7: Future Trends in Cloud Computing :

Cloud computing attributes the highest priority to managing security, trust, privacy, encryption, and key exchange among servers using IoT-based communication, big data in the cloud, server-based and cloud system intrusion, and system analysis and authentication. Despite these enhancements, future trends in cloud computing address the major issues of the energy consumption of cloud server systems, data redundancy and utilization, and resource management. Extended research in available OS with a secure communication strategy for cloud-based computing has gained top priority in the field of cloud security. IoT cloud user platforms are in high demand and can effectively maintain the dynamic system changes with updates [48]. Additionally, maximum secure data protection is addressed through the query-based solution in health care-sector cloud mobile platforms. The maximizations of communication are accomplished with enhanced data transfer in cloud systems, where encryption is considered equally important to enhance data privacy and protection [46].

Cloud computing is a novel service model, developed to address the challenges of today's information technology sector. The increasing demand for cloud services resulted in changes to the information technology industry. Cloud computing is experiencing a continuous increase in demand, which has highlighted an urgent need for a new architecture. In the past, a major disadvantage of cloud computing was its inability to guarantee data security in the public cloud infrastructure [40]. However, significant advancements in cloud service has made it possible to create more secure and stable systems with high performance and reliability.

8.1. Edge Computing :

[49] Edge computing has emerged as a new paradigm to manage the increasing aggregate IoT traffic distributed to the cloud and to meet real-time service requirements in the era of 5G [50]. Edge computing shifts IoT computations from a centralized data center to network edge devices. This enables immediate processing of data generated by PID devices with limited public cloud assistance. Edge computing provides support to implant artificial

intelligence (AI) algorithms, including the training and execution of AI models, in the network environment to allow coordination and cooperation among different IoT devices in the 5G environment. Edge computing can significantly enhance scalability and reduce the cost of service deployment and operations. As part of edge computing, advanced technologies of fog computing, edge-based recognition, and localization are emerging.[51] The only downside, if one exists, is that every cloud provider has at least four generations of data centers, built in 1989, 1999, 2009, and 2020, which consume a lot of energy. Edge data centers, on the other hand, can facilitate computation and data processing in the heart of the IoT network and thus save at least 2.3% of the internet power, which is a significant power saving for less than \$8.99. This gives the IoT a short-response time but with significant power and cost savings, with \$30 billion. It therefore has the potential to significantly reduce power consumption or cost, two of the three major objectives of the cloud, while the latency reduction is insignificant, hence this implies the third major objective being maintained while the cloud provides rear-end services.

8.2. Serverless Architectures :

The most important features of FaaS are, one, security: the isolation of every Logiccode for each function; two, efficiency: short code deployment times; three, very high scalability through the invocation of IaaS resources per function. They are called serverless frameworks, but they are not, in fact, devoid of servers: the servers on which the functions run are only managed by the cloud provider. Popular serverless providers include Microsoft Azure, Google Cloud, and AWS. The possibility that serverless computing can manage the unstructured data generated by each individual is well documented. The ability to guarantee rapid noSQL write and read accesses encourages developers to rely on serverless services for IoT usage. At a higher level, it is possible to manage incoming data in real time, perform inferential control and post processing in cloud storage, without having to build an infrastructure ourselves or rely on platform virtualized solutions. petits [52].

Serverless computing, a new technology in the cloud system domain, solves IoT application development, management, and deployment challenges. This technology is also to trigger functionalities in response to events. This infrastructure avoids the traditional client/server model of managing resources, but most of the serverless applications are currently being run on servers. I'll explain why we need serverless architectures and why businesses observed at third party service providers for serverless. Comparatively, traditional web applications have to access these components all the time, which causes more idle state access, which is critical in cloud-based deployment including SaaS [53]. The significant architecture includes web server needs to be robust enough to store states of different users. Further, to extract the logs of script for extra storage cost and frequent fetch multiplies the computation cost. We discuss how the new technology compared to web servers is helpful to solve the challenges efficiently.

9. Chapter 8: Legal and Ethical Considerations in Cloud Computing :

File requests to the cloud are forwarded through the client front-end API [54]. Allows the client to upload, delete, change, rename and retrieve cloud files. Coronaviruses can penetrate end-user applications, they can be caught faster as they can be transferred to server endpoints for scams and they get sensitive information and traits files from cloud clients this need not be difficult. In the new release, several creators are in the Eastern domain and use unsecured customer options. The application goes to using incorrect setting variations, darts public bills, and complex electronic growth can be used to produce free Bluetooth® applications [55].

Common problems in cloud systems are hacking, data theft, and lack of ubiquitous connectivity. Data loss, insider theft, and connection eavesdropping are the top three cloud security threats that managers must prioritize. Lower down the list are inefficient application programming interfaces and obsolete interfaces. The top five security concerns included in the classification by OWASP's Top 10 Web Application Security Risks ranked client-side attacks in the first position. In the low levels, injection and women attacks, XML external entity ban, broken authentication, SROI loss, security housing confusion, and reckless distribution of sensitive data can be found. The ten most critical security errors now assessed. Web security is explained by three hypotheses: attacks in the Cloud (side client), inefficient interfaces, and obsolete interfaces [34].

9.1. Data Protection Regulations :

The Vietnam government issued guidance for building cloud computing scenarios, a national cloud computing platform establishment decision, and guidance on condition and procedures for import of used information technology. The Ministry of Information and Communications of Vietnam is required to develop a strategy for building e-government. This process will allow for strategy use, measurement, results, and stages. Furthermore, there will include procedures for protecting users on the internet,

monitoring, protecting personal data, account lockout mechanisms, and suspect activities.

There are different technologies present in cloud computing. Some are open while others are close source. All types of technologies suffer from different types of threats and vulnerabilities. At a different layer, different types of attacks are performed, such as DoS attacks and privacy threats. Different types of On cloud platforms, security is a backup for safety requiring users to trust cloud providers for the services. Most cloud providers require starting with bigger packages and guide to data center and technologies, resulting in data loss and management and leakage of personal data.

Cloud security is a primary issue in cloud computing systems [5]. Cloud computing occurs at multiple levels: device, edge, fog, and technology, and has suffered from various attacks such as information leakage, denial of service, and advanced persistent threats. Cloud-based services have converted from commercial to personal, and hosted apps require real-time connectivity, internet bandwidth, and big data processing power. Combined cyber-physical systems for cloud contain multiple individual systems with multiple safety-critical domains and attack vectors. Furthermore, applications employ continuously inadequate inventory, quality, and compatibility.

9.2. Vendor Lock-In :

While the availability of public cloud services results in convenient provisioning of resources, providers have different solutions for achieving similar goals. This can result in parks of services from a cloud provider being difficult to substitute with services from a different provider [56]. Understanding the essential differences between cloud services from different providers in relation to service levels, software development, and operated applications is conceptual analysis. While multi-cloud environments aim to avoid vendor lock-in by distributing critical solutions across clouds, multi-cloud introduces a different set of lock-in solutions with unbalanced managed responsibilities and sharing of identical business logic. Hybrid

clouds are containers for client cloud services and pools of computing capabilities provisioned in multiple clouds. In contrast to multi-cloud, hybrid cloud is an approach for adding cloud-native applications to the park of client services in a modular manner.

Cloud computing is beneficial for organizations of all sizes [57]. Companies can avoid significant investments in information technology by renting resources for specific purposes, only paying for what they use. On the other hand, migrating to cloud computing introduces potential risks. Companies could end up being bound to a specific provider for a prolonged period, sometimes facing obsolescence or high costs when attempting to change to a different provider [58]. This undesirable position corresponds to vendor lock-in. Strategy, design, and solution alternatives such as multi-cloud or hybrid clouds can be relevant here. Thus, vendor lock-in is a significant and dominant risk that enterprise architects face when introducing cloud computing solutions in organizations.

10. Chapter 9: Multi-Cloud Strategies :

Promoting consumer democracy with migration flexibility and freedom to choose what is best in the context of the specific demands and problems that you solve. There are many examples of common business use cases that can benefit from these advantages, becoming multi-cloud service users for specific or general scenarios. Unique cloud computing is subject to service interruption, intrusion into the data center, or physical disasters that can keep the application and service environment offline and, in some cases, result in data loss. For these situations, maintaining high availability, that is, guaranteeing that your service is accessible and that the data is safe and up to date, is crucial. That is why you should create an automatic distribution system that contains copies of its services in different parts of the world and in properly regulated data center environments, using proper safe cloud provider replication and backup strategies. Many companies decide to execute some of the critical systems produced in another cloud provider, which is placed in a disaster recovery data center that is maintained in different environments.

Use multi-cloud offerings for their own individual service strengths. Choose one cloud provider as the core and another one for specific services or particular categories of services. Choose a cloud provider to use exclusive services from discrete cloud provider environments. Choosing cloud services with political motivations, while getting unlimited flexibility to migrate your services and, in addition, minimizing possible vendor lock-in risks. Migrating an existing application from provider A to provider B that is compatible with the required provider A application environment. Maintaining high availability: not depending on a single cloud provider. List of owners of any type of single component vendor lock-in. Develop high-performance massive distributed systems - focus on the implementation of a specific function, taking advantage of the features and low costs of different providers - while ensuring that your system services are correctly reached, with low latencies and high availability.

10.1 Benefits and Challenges of Multi-Cloud Environments :

Despite the challenges, management and data-centric image methods are few and have little consideration. This is because customers are forced to know and programmatically handle cloud services. This would artificially complicate and inflexibly program, and generate a single core focused code, boosting a high rate of errors. Despite basic techniques like integrated data management, security, and graph processing, these services at the cloud level consist of daily operations for customers. These operations include customer data encryption, extensive user access verification, zone transfer restrictions in global visible matrix transport, and the support of social authenticity by enabling the management of user data to ensure enduring authentication integrity. In addition, the user data control methodologies storage and transmission costs at the customer level with the management of integrity, confidentiality, and trust.

The multi-cloud environment also presents many advantages. These advantages include reducing risk by not relying on a single cloud provider, better quality of service through the location of services near customers, and customers who demand trust, privacy, and better performance. In a multi-cloud environment, sensitive parts of the data can be distributed to more conservative CSPs that handle crucial requirements in compliance with regional standards. However, taking full advantage of a multi-cloud environment is not trivial. This is due to the different characteristics and acquisition fees for each cloud and the trade-off for housing, moving, or processing sensitive data in different cloud service providers.

In recent years, many organizations have turned to a multi-cloud environment with at least two public cloud providers. Despite the development of cloud computing, there are still challenges in cloud computing. These challenges include security concerns, service level agreements with service providers, avoiding lock-ins, cloud data distribution, data migration, and data confidentiality.

While cloud computing presents many opportunities for organizations to be flexible, on-demand, and have on-demand data queries, the ever-increasing

number of free cloud services can bring many benefits. These benefits include access to various capabilities and data, cost savings, fault tolerance, and performance improvement. However, they can also lead to data privacy issues and complex cloud management in multi-cloud environments.

10.2 Implementing Multi-Cloud Architecture :

A multi-cloud architecture ensures these features.

- Geo-distributed data - Compliance with laws and regulations - Minimize risk exposure - Business continuity and disaster recovery - Performance and availability - Best-of-breed services - Financial hedging - Simplification and consolidation of IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) in a multi-tier Internet architecture (MTIA) - Differing multi-stakeholder partitioning

Limitations, including performance issues related to overused resources offered by a single cloud computing provider, may be resolved through forming a multi-cloud architecture. There are several strategies to be considered to form a multi-cloud architecture. A few consider the favorable utility of public cloud services to be a main concept behind a multi-cloud architecture, including:

10.3 Best Practices for Managing Multi-Cloud Deployments :

- ✓ Encourage a developer mindset: Today's IT responsibility is to manage not just the IT infrastructure (keeping the lights on, delivering lower cost, etc.), but to deliver IT as a service (ITaaS) and to create an environment where "younger, developing a collection of digital native tools used to operate that infrastructure. These tools are used to deliver digital led business services faster, while still ensuring the availability, security and compliance required by business leaders and executive customers. This requires culture, skills, tools and processes as well as business online ready IT infrastructure assets.
- ✓ Assess the need: Re-architect (if necessary): Using a multi-cloud strategy for the sake of using multi-cloud is not strategic. Not every workload will be suitable for multi-cloud architectures, and not every application should use these cloud deployment operations. Keep applications and data aligned with their best execution venue. Although the need for better alignment between

technology planning and business goals is the primary business driver globally, it is also driving IT refactoring issues.

- ✓ Identify stakeholders: One of the most important steps in defining a multi-cloud strategy is identifying, and aligning, stakeholders within the business. If managed poorly, shadow IT threats and rogue applications become an increasingly common issue, but if a cloud-smart and thoughtful strategy is maintained, then those same stakeholders can help to create better IT service delivery outcomes for their lines of business.
- ✓ Assess your multi-cloud strategy: Before pursuing a multi-cloud strategy, leaders must assess what role multi-cloud can play in their enterprise strategy. Because of the complexity and management challenges of multi-cloud environments, experts say that these architectures should not be pursued unless absolutely necessary. When used, multi-cloud should be employed only where business justification demands such a configuration and where a clear use case is required. Multi-cloud deployments are not beneficial in every scenario, as they increase the operational complexity immensely.
- ✓ These best practices include:
 - A) Because multi-cloud environments are extremely complex, it is essential for IT leaders to consider best practices when managing their cloud infrastructure.
 - B) Best practices for managing multi-cloud deployments.

11. Chapter 10: Hybrid Cloud Solutions :

Cloud computing is changing the business models of IT. Cloud solutions are now readily available, competitively priced, of high quality, and highly available. Public cloud efficiencies are now well-documented and available to resolve a plethora of business problems. However, to the cloud skeptic, public cloud solutions have a set of disadvantages, such as animate with duration and overall cost. Given that customer workloads are stored in one cloud, this directly reduces the potential for cloud workload redundancy. Also, given that public price points are based on "pay-as-you-go," the overall cost (CAPEX and OPEX) might, in fact, be higher than having customer workloads provisioned in-house, particularly over a long multi-year time period.

11.1 Hybrid Cloud Solutions :

Introduction Ensuring a successful transition to a cloud solution is the primary goal of this chapter. This chapter will explore a variety of cloud solutions that are currently available. In addition to IaaS-based cloud, this chapter will also augment IaaS-based solutions with PaaS-based solutions. This chapter will examine the various cloud platforms that exist in today's cloud ecosystem. This will include both the private cloud, the public cloud, and the hybrid cloud. This chapter will also evaluate whether a hybrid cloud strategy is advantageous. Practical examples and use cases will be examined and developed in order to rationalize the hybrid cloud idea. The de facto standard for cloud orchestration and provisioning is OpenStack. OpenStack is used today extensively in both public provider clouds as well as in private enterprise data center clouds. Therefore, the deployment and use of OpenStack will be explored in Chapter 2.

11.2 Hybrid Cloud Models and Use Cases :

There are two main approaches organizations can follow: First, they maintain the ownership of certain workloads, certain data, and part of the IT infrastructure in a certain and implement cloud-based aspects, e.g., scaling for others, or backing up the ERP systems. Or second, level-loads and

"normal" bursting works might be off-loaded to the cloud and on-premises infrastructures be dimensioned to suffice. With this hybrid environment in mind, it's no doubt that the organization needs to manage the cloud in single-pane-of-glass mode.

The objective of cloud-based solutions, as aforementioned, is to improve the efficiency of IT services. One might expect that this means that the cloud "destroys" the standard IT infrastructure, but that is not the case. Many organizations look for ways in which to smartly balance costs and other locations between on-premises resources and a cloud. The former for all its experience in customization, control, adherence to certain legal or administrative rules, etc., and the latter for its agility, pay-per-use characteristics, etc.

11. 3 Integration Strategies for Hybrid Cloud Environments :

After the successful integration with cloud computing and its service models, software, platform, and infrastructure, it is recognized as an alternative fulfillment model for inherent limitations and infoys of standard information technology deployment and management based on formats. Its combination with company resources, internal private clouds, and inquiring with public cloud vendors makes reaching cloud solutions a substantial strategic option for those organizations. It provides solutions and services to gradually adjust, label, and retain cloud distances through a process of replacement for ending legacy systems, updates to libraries and solutions, or where significant strategic risks cannot be covered. High and asymmetric dependence on response time optimization, reliance, legal, and level of required service for solving lattice work, cloud, or hybrid implementation.

Cloud computing is a rapidly expanding and adaptable technology trend. A key role is to drive companies and government organizations towards greater profitability and resource efficiency. In addition to the economic benefits, cloud services offer massive potential for superior service quality. The process of integrating cloud computing requires careful planning. This includes establishing and sustaining connections, smooth operation, and aligning traditional or standard Information Technology with new cloud case.

This chapter seeks to better understand the benefits, challenges, and different aspects of integration strategy for hybrid cloud environments.

11.4 Security Considerations in Hybrid Cloud Deployments :

The increased connectivity between the internal IT systems and the public cloud systems leads to a higher chance of cross-contamination between botnets. Routers and other internet acceleration equipment should have an option to not form Full State Translation tables which remember the correlation between the NATed interaction, unless the load is really huge. The combination of perimeter and internal security layers as in the old days, but now applied in the virtual security world, creates a step-layering defense. While this defense can now be applied in the virtual world, it is still a bit of an optical illusion that unless the underlying network both the overlay and the hypervisor security consists of are secure, the security concept remains a fallacy. This requires a new set of components (FIPS, intrusion prevention systems, next-generation firewalls) which are accepted by the security departments. While logically they are quite close to the physical counterparts, the performance and scalability of the physical components cannot be applied to the virtual components. The lowest-cost hypervisor abstraction (Type 1 or Type 2) devices which bypass the cloud or removed in sniffer mode, should be able to secure the communication. Securely deploying physical firewalls in conjunction with cloud-based deployments is specifically addressed in. Relying on certain features, the interconnection company place virtual machines at a Service Provider edge, thereby creating a new dimension of the corporate perimeter. The number of packet interceptors grows linearly with the number of public addresses owned because the virtual machines use these public addresses. A company's new routing rule to the Virtual Machine's neighbor router is ported in either the copper or the fiber full state table, which only knows traffic to and from the internal company networks and the virtual machines. Shadowed from the Virtual Machine, they intercept any and all communication without the public IP full-state table knowing that the intercepted clients, although the virtual machine is active, actually exchanged information with a public IP. Thanks to the single mode operation, they do not require a full business

relationship or a service contract. In this fashion, it should be possible to intercept more information that is sent from and to the virtual machine before full state entries need to be added, although some interception can still be done.

There are several security challenges that are specific to hybrid cloud deployments which are different from either public, community, or open cloud deployments. Federated identity management, which allows a user to use the same login and password across the various IT domains they have access to, is a huge requirement for the success of the hybrid cloud. As part of the hybrid cloud deployment, it is simple and customary for the public cloud to be used as a massive and scalable disaster recovery environment. Therefore, a Unified Threat Management (UTM) solution has to take care of ensuring that the data that goes back and forth between the enterprise and the public cloud complies with the corporate security and information compliance standards.

12. Chapter 11: Cloud-Native Architecture :

This section will explore these concepts again. Service container provides a standard way of packaging code or runtime configuration that can run or scale within a cloud-native environment. It can deliver on the promises of "build anywhere" of modern development for microservices. Platform abstraction introduces isolating technology standards and APIs that define how a service is run, networked, scaled, and managed. It offers developers control over very large amounts of resources, and it enforces your organization's break glass policy by controlling all resource access via two-factor authentication and location controls. In Kubernetes, these policies are manifest in the extensive use of role and role binding. The microservices paradigm, with autonomous, collaborating entities concentrated on business capabilities, obviates many of the difficulties of traditional N-Tier application systems. Resilient applications discover (and then avoid) common failure modes in distributed systems. Resilient applications are designed to prevent compromise and are continuously monitored for compromise via a network security platform. Automating the software development process can greatly reduce deployment frequency, change lead time, change failure rate, and mean time to restore service when compared to manual change. Automating toil can also dramatically reduce the relevance of software failures, thus greatly reducing corresponding disruption and work and burnout.

Cloud-native consists of modern, innovative technology and processes for enterprises to build scalable services on public, private, and hybrid clouds. The cloud-native toolchain includes several key technology categories, such as service container, platform abstraction, microservices principles, resilient applications, automation throughout the software development life cycle, and data as a first-class citizen. The ultimate goal of cloud-native for most companies is to deliver value to customers at a faster speed. There have been many discussions on these cloud-native concepts and standards.

12.1 Key Principles of Cloud-Native Design :

For The Fowls of the Air Both microservices and traditional application monoliths can and have lived in on-premises environments and can be ported to the cloud. It's the microservices architecture that has unlocked the full potential of the cloud and therefore microservices are what enable and essentially define a cloud-native design. Build microservices instead of monoliths so that each service can take advantage of all the best capabilities available in the cloud.

Cloud-native design is based on several key tenets. These are some of the key principles that you must incorporate in your design to evolve your software application to cloud-native maturity.

13 . Chapter 12: X Multi-Cloud Strategies:

Promoting consumer democracy with migration flexibility and freedom to choose what is best in the context of the specific demands and problems that you solve. There are many examples of common business use cases that can benefit from these advantages, becoming multi-cloud service users for specific or general scenarios. Unique cloud computing is subject to service interruption, intrusion into the data center, or physical disasters that can keep the application and service environment offline and, in some cases, result in data loss. For these situations, maintaining high availability, that is, guaranteeing that your service is accessible and that the data is safe and up to date, is crucial. That is why you should create an automatic distribution system that contains copies of its services in different parts of the world and in properly regulated data center environments, using proper safe cloud provider replication and backup strategies. Many companies decide to execute some of the critical systems produced in another cloud provider, which is placed in a disaster recovery data center that is maintained in different environments.

Use multi-cloud offerings for their own individual service strengths. Choose one cloud provider as the core and another one for specific services or particular categories of services. Choose a cloud provider to use exclusive services from discrete cloud provider environments. Choosing cloud services with political motivations, while getting unlimited flexibility to migrate your services and, in addition, minimizing possible vendor lock-in risks. Migrating an existing application from provider A to provider B that is compatible with the required provider A application environment. Maintaining high availability: not depending on a single cloud provider. List of owners of any type of single component vendor lock-in. Develop high-performance massive distributed systems - focus on the implementation of a specific function, taking advantage of the features and low costs of different providers - while ensuring that your system services are correctly reached, with low latencies and high availability.

13.1 Benefits and Challenges of Multi-Cloud Environments :

Despite the challenges, management and data-centric image methods are few and have little consideration. This is because customers are forced to know and programmatically handle cloud services. This would artificially complicate and inflexibly program, and generate a single core focused code, boosting a high rate of errors. Despite basic techniques like integrated data management, security, and graph processing, these services at the cloud level consist of daily operations for customers. These operations include customer data encryption, extensive user access verification, zone transfer restrictions in global visible matrix transport, and the support of social authenticity by enabling the management of user data to ensure enduring authentication integrity. In addition, the user data control methodologies storage and transmission costs at the customer level with the management of integrity, confidentiality, and trust.

The multi-cloud environment also presents many advantages. These advantages include reducing risk by not relying on a single cloud provider, better quality of service through the location of services near customers, and customers who demand trust, privacy, and better performance. In a multi-cloud environment, sensitive parts of the data can be distributed to more conservative CSPs that handle crucial requirements in compliance with regional standards. However, taking full advantage of a multi-cloud environment is not trivial. This is due to the different characteristics and acquisition fees for each cloud and the trade-off for housing, moving, or processing sensitive data in different cloud service providers.

In recent years, many organizations have turned to a multi-cloud environment with at least two public cloud providers. Despite the development of cloud computing, there are still challenges in cloud computing. These challenges include security concerns, service level agreements with service providers, avoiding lock-ins, cloud data distribution, data migration, and data confidentiality.

While cloud computing presents many opportunities for organizations to be flexible, on-demand, and have on-demand data queries, the ever-increasing

number of free cloud services can bring many benefits. These benefits include access to various capabilities and data, cost savings, fault tolerance, and performance improvement. However, they can also lead to data privacy issues and complex cloud management in multi-cloud environments.

13.2. Implementing Multi-Cloud Architecture :

A multi-cloud architecture ensures these features.

- Geo-distributed data
- Compliance with laws and regulations
- Minimize risk exposure
- Business continuity and disaster recovery
- Performance and availability
- Best-of-breed services
- Financial hedging
- Simplification and consolidation of IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) in a multi-tier Internet architecture (MTIA)
- Differing multi-stakeholder partitioning

Limitations, including performance issues related to overused resources offered by a single cloud computing provider, may be resolved through forming a multi-cloud architecture. There are several strategies to be considered to form a multi-cloud architecture. A few consider the favorable utility of public cloud services to be a main concept behind a multi-cloud architecture.

13.3. Best Practices for Managing Multi-Cloud Deployments :

These best practices include:

1. Encourage a developer mindset: Today's IT responsibility is to manage not just the IT infrastructure (keeping the lights on, delivering lower cost, etc.), but to deliver IT as a service (ITaaS) and to create an environment where "younger, developing a collection of digital native

- tools used to operate that infrastructure. These tools are used to deliver digital led business services faster, while still ensuring the availability, security and compliance required by business leaders and executive customers. This requires culture, skills, tools and processes as well as business online ready IT infrastructure assets.
2. Assess the need: Re-architect (if necessary): Using a multi-cloud strategy for the sake of using multi-cloud is not strategic. Not every workload will be suitable for multi-cloud architectures, and not every application should use these cloud deployment operations. Keep applications and data aligned with their best execution venue. Although the need for better alignment between technology planning and business goals is the primary business driver globally, it is also driving IT refactoring issues.
 3. Identify stakeholders: One of the most important steps in defining a multi-cloud strategy is identifying, and aligning, stakeholders within the business. If managed poorly, shadow IT threats and rogue applications become an increasingly common issue, but if a cloud-smart and thoughtful strategy is maintained, then those same stakeholders can help to create better IT service delivery outcomes for their lines of business.
 4. Assess your multi-cloud strategy: Before pursuing a multi-cloud strategy, leaders must assess what role multi-cloud can play in their enterprise strategy. Because of the complexity and management challenges of multi-cloud environments, experts say that these architectures should not be pursued unless absolutely necessary. When used, multi-cloud should be employed only where business justification demands such a configuration and where a clear use case is required. Multi-cloud deployments are not beneficial in every scenario, as they increase the operational complexity immensely.

Because multi-cloud environments are extremely complex, it is essential for IT leaders to consider best practices when managing their cloud infrastructure.

14. Chapter 13: Hybrid Cloud Solutions :

Cloud computing is changing the business models of IT. Cloud solutions are now readily available, competitively priced, of high quality, and highly available. Public cloud efficiencies are now well-documented and available to resolve a plethora of business problems. However, to the cloud skeptic, public cloud solutions have a set of disadvantages, such as animate with duration and overall cost. Given that customer workloads are stored in one cloud, this directly reduces the potential for cloud workload redundancy. Also, given that public price points are based on "pay-as-you-go," the overall cost (CAPEX and OPEX) might, in fact, be higher than having customer workloads provisioned in-house, particularly over a long multi-year time period.

Ensuring a successful transition to a cloud solution is the primary goal of this chapter. This chapter will explore a variety of cloud solutions that are currently available. In addition to IaaS-based cloud, this chapter will also augment IaaS-based solutions with PaaS-based solutions. This chapter will examine the various cloud platforms that exist in today's cloud ecosystem. This will include both the private cloud, the public cloud, and the hybrid cloud. This chapter will also evaluate whether a hybrid cloud strategy is advantageous. Practical examples and use cases will be examined and developed in order to rationalize the hybrid cloud idea. The de facto standard for cloud orchestration and provisioning is OpenStack. OpenStack is used today extensively in both public provider clouds as well as in private enterprise data center clouds.

14.1. Hybrid Cloud Models and Use Cases :

There are two main approaches organizations can follow: First, they maintain the ownership of certain workloads, certain data, and part of the IT infrastructure in a certain and implement cloud-based aspects, e.g., scaling for others, or backing up the ERP systems. Or second, level-loads and "normal" bursting works might be off-loaded to the cloud and on-premises infrastructures be dimensioned to suffice. With this hybrid environment in

mind, it's no doubt that the organization needs to manage the cloud in single-pane-of-glass mode.

The objective of cloud-based solutions, as aforementioned, is to improve the efficiency of IT services. One might expect that this means that the cloud "destroys" the standard IT infrastructure, but that is not the case. Many organizations look for ways in which to smartly balance costs and other locations between on-premises resources and a cloud. The former for all its experience in customization, control, adherence to certain legal or administrative rules, etc., and the latter for its agility, pay-per-use characteristics, etc.

14.2. Integration Strategies for Hybrid Cloud Environments

After the successful integration with cloud computing and its service models, software, platform, and infrastructure, it is recognized as an alternative fulfillment model for inherent limitations and infoys of standard information technology deployment and management based on formats. Its combination with company resources, internal private clouds, and inquiring with public cloud vendors makes reaching cloud solutions a substantial strategic option for those organizations. It provides solutions and services to gradually adjust, label, and retain cloud distances through a process of replacement for ending legacy systems, updates to libraries and solutions, or where significant strategic risks cannot be covered. High and asymmetric dependence on response time optimization, reliance, legal, and level of required service for solving lattice work, cloud, or hybrid implementation.

Cloud computing is a rapidly expanding and adaptable technology trend. A key role is to drive companies and government organizations towards greater profitability and resource efficiency. In addition to the economic benefits, cloud services offer massive potential for superior service quality. The process of integrating cloud computing requires careful planning. This includes establishing and sustaining connections, smooth operation, and aligning traditional or standard Information Technology with new cloud case. This chapter seeks to better understand the benefits, challenges, and different aspects of integration strategy for hybrid cloud environments.

14.3. Security Considerations in Hybrid Cloud Deployments

The increased connectivity between the internal IT systems and the public cloud systems leads to a higher chance of cross-contamination between botnets. Routers and other internet acceleration equipment should have an option to not form Full State Translation tables which remember the correlation between the NATed interaction, unless the load is really huge. The combination of perimeter and internal security layers as in the old days, but now applied in the virtual security world, creates a step-layering defense. While this defense can now be applied in the virtual world, it is still a bit of an optical illusion that unless the underlying network both the overlay and the hypervisor security consists of are secure, the security concept remains a fallacy. This requires a new set of components (FIPS, intrusion prevention systems, next-generation firewalls) which are accepted by the security departments. While logically they are quite close to the physical counterparts, the performance and scalability of the physical components cannot be applied to the virtual components. The lowest-cost hypervisor abstraction (Type 1 or Type 2) devices which bypass the cloud or removed in sniffer mode, should be able to secure the communication. Securely deploying physical firewalls in conjunction with cloud-based deployments is specifically addressed in. Relying on certain features, the interconnection company place virtual machines at a Service Provider edge, thereby creating a new dimension of the corporate perimeter. The number of packet interceptors grows linearly with the number of public addresses owned because the virtual machines use these public addresses. A company's new routing rule to the Virtual Machine's neighbor router is ported in either the copper or the fiber full state table, which only knows traffic to and from the internal company networks and the virtual machines. Shadowed from the Virtual Machine, they intercept any and all communication without the public IP full-state table knowing that the intercepted clients, although the virtual machine is active, actually exchanged information with a public IP. Thanks to the single mode operation, they do not require a full business relationship or a service contract. In this fashion, it should be possible to intercept more information that is sent from and to the virtual machine

before full state entries need to be added, although some interception can still be done.

There are several security challenges that are specific to hybrid cloud deployments which are different from either public, community, or open cloud deployments. Federated identity management, which allows a user to use the same login and password across the various IT domains they have access to, is a huge requirement for the success of the hybrid cloud. As part of the hybrid cloud deployment, it is simple and customary for the public cloud to be used as a massive and scalable disaster recovery environment. Therefore, a Unified Threat Management (UTM) solution has to take care of ensuring that the data that goes back and forth between the enterprise and the public cloud complies with the corporate security and information compliance standards.

15. Chapter 14: Cloud-Native Architecture

This section will explore these concepts again. Service container provides a standard way of packaging code or runtime configuration that can run or scale within a cloud-native environment. It can deliver on the promises of "build anywhere" of modern development for microservices. Platform abstraction introduces isolating technology standards and APIs that define how a service is run, networked, scaled, and managed. It offers developers control over very large amounts of resources, and it enforces your organization's break glass policy by controlling all resource access via two-factor authentication and location controls. In Kubernetes, these policies are manifest in the extensive use of role and role binding. The microservices paradigm, with autonomous, collaborating entities concentrated on business capabilities, obviates many of the difficulties of traditional N-Tier application systems. Resilient applications discover (and then avoid) common failure modes in distributed systems. Resilient applications are designed to prevent compromise and are continuously monitored for compromise via a network security platform. Automating the software development process can greatly reduce deployment frequency, change lead time, change failure rate, and mean time to restore service when compared to manual change. Automating toil can also dramatically reduce the relevance of software failures, thus greatly reducing corresponding disruption and work and burnout.

Cloud-native consists of modern, innovative technology and processes for enterprises to build scalable services on public, private, and hybrid clouds. The cloud-native toolchain includes several key technology categories, such as service container, platform abstraction, microservices principles, resilient applications, automation throughout the software development life cycle, and data as a first-class citizen. The ultimate goal of cloud-native for most companies is to deliver value to customers at a faster speed. There have been many discussions on these cloud-native concepts and standards.

15.1. Key Principles of Cloud-Native Design

For the fowls of the Air Both microservices and traditional application monoliths can and have lived in on-premises environments and can be ported to the cloud. It's the microservices architecture that has unlocked the full potential of the cloud and therefore microservices are what enable and essentially define a cloud-native design. Build microservices instead of monoliths so that each service can take advantage of all the best capabilities available in the cloud.

Stateless Services Applications are frequently built handling their own state—such as handling session states—which is fine in a traditional environment but often creates serious scaling and redundancy issues in a cloud environment. Stateful services are limited in how they can scale or be made redundant and must carefully orchestrate state sharing across instances in a manner that may make leveraging cloud elasticity suspect. Eliminate session state where it is inappropriate, focusing on stateless design where possible and keep doing so until you can't find any more stateful bottlenecks in your services. You will find that your software solutions are easier to scale and maintain and your cloud bill shrinks, all because you're playing to the strengths of the cloud environment.

Cloud-native design is based on several key tenets. These are some of the key principles that you must incorporate in your design to evolve your software application to cloud-native maturity.

15.2. Containerization and Orchestration Technologies

A large volume of emerging applications is created from microservices, regardless of the size of the organization and available resources. Considered as an operating system, within a container, all files and settings comprised by a Linux distribution are included, rendering it possible to run a wide range of Linux applications. This is achieved via the combination of the following elements: an operating system kernel (Linux and Windows are the most common options) that efficiently leverages hardware resources; a tool providing the virtualization of processes, storage volumes, and network interfaces; an available hardware infrastructure that allows for the

container to be considered as a virtual system, without the need of a hypervisor, unlike the Virtual Machine.

Considered as one of the principal cloud giants, these services offer a range of benefits for users, cloud administrators, and cloud developers. Cloud platforms such as AWS, Microsoft Azure, and Google Cloud offer developers a reliable, highly elastic, and inexpensive infrastructure platform. When used correctly, this platform supports running workloads with very specific resource requirements that cannot be easily met by investing in traditional IT infrastructure. In short, public cloud platforms support a wide range of use cases. Offering support for both container and virtual machine image formats, major cloud providers such as AWS, IBM Cloud, Microsoft Azure, Oracle Cloud, and Google Cloud are putting an emphasis on supporting container formation workloads.

15.3. Benefits of Cloud-Native Applications

The real magic of the cloud is not by reducing the infrastructure cost by 80% by moving from a traditional data center to Amazon Web Service to use an EC2 instance. Practically any enterprise moving to the cloud will realize infrastructure savings even just by moving to any public cloud provider. The real magic of the cloud is from cloud-native applications. In the traditional data center, when we build an application with a capability such as payment processing, we will typically develop a single payment application. In the cloud-native development paradigm, we will build our payment processing capability as multiple microservices. These small self-contained services could be developed, deployed, and scaled independently. Then we use a combination of some mix of these services to build out the payment processing capability. Combining these services can also be dynamic because microservices are built to scale.

Most enterprises that are moving to the cloud are moving existing legacy applications running on-premises data centers to Infrastructure-as-a-Service (IaaS) providers such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure. By moving to IaaS, the enterprises can save money by not paying for data center or co-location costs, and they can

quickly scale the hardware usually by a simple API call. While it is a move in the right direction and you are getting real benefits, you won't realize the significant benefits that the cloud has to offer. The real benefits will be from migrating to cloud-native applications that are entirely built in the cloud using microservices.

16. Chapter 15: Microservices and Cloud Computing

Despite the likely robustness of microservices, including those upon which information from the so-called "Internet of Things" (IoT) is based, the data and the programs that manipulate them remain vulnerable to attack and to damage that may threaten the integrity, availability, or the confidentiality of data. Additionally, in meeting business needs, and in using cloud computing services to do so, sensitive data often is passed to third-party microservices that provide additional cloud functionalities that neither your existing service nor your business provide themselves. Privacy laws, and sometimes such laws are the reason for putting business computing solution on cloud resources, often limit sending data streams to those select upper layers that should have access. Software solution designers have to find ways to secure the links between microservices that communicate different data amounts, while keeping compliance to the laws when doing so in public clouds.

Microservices are an architectural style for application development based upon disassembling complex applications into simple microservices that have individual responsibilities and that work together in concert to produce software artifacts. Microservices provide durable and adaptable integrations between different software solutions needed by an enterprise in meeting its business objectives. These services depend upon open technologies popular in enterprise solutions, including the cloud computing resources that host them. As microservices communicate via messages over networks, and are often built to act upon data harvested from either the data streams within an organization, or upon data streams from autonomous sensors acting upon the real world, securing messages between microservices that have both internal and external communication paths has become complex. Several approaches to securing microservices beyond the point of message have arisen to meet this challenge.

16.1. Microservices Architecture Overview :

In many ways, microservices are not a brand-new concept, but a re-badging of older ideas such as SOA (Service Oriented Architecture), domain-driven

design, UNIX small tools, OO components and distributed processes. Elearning and MOOCing services are an area where very rapid scaling and failure of parts of the system are common, both in commercial and academic organizations. Docker use cases are another rich source of information. These are perhaps too high a level to be complete examples, but their domain-specific nature may make them useful for someone looking to do something similar. Taking the advice of the people who have gone before can save considerable time.

The emergence of the cloud as a major application platform emphasizes the need for cloud software developers to consider the implications of a microservices-based development methodology for next generation cloud applications. Microservices applications are a network of loosely coupled independently deployable back-end applications, with a common end-user front end or composite presentation layer. They promote agility and easy scaling of system components, and can solve some of the common challenges with cloud applications such as proprietary vendor lock-in, and large system code base complexity. In this paper, we discuss the major wiki-based resources available for those considering using microservices for their cloud applications, and reflect on the challenges and opportunities of using microservices for cloud applications.

16.2. Microservices Deployment Strategies

Two major strategies gained attention in recent literature. Canonical service decomposition such as routing is used over a consistent set of capabilities provided by a microservice, and every service request is handled by Nginx Web server and MySQL backend databases. Seven small datasets are introduced from Coursera to release the challenge of load at that level. To handle all data effectively, four microservices are introduced around the partitioning strategy. A publish-subscribe model is invoked to preserve consistent observable state updates within the application's data.

There are numerous ways to deploy microservices in a production environment. This is due to the increasing need to decompose monolithic applications across multiple teams working on different parts and

functionalities of the application. Coffea and Roehm employ the microservices architectural style in an online meeting management application using several deployment strategies to reduce their 22 unique services operating over 433 containers in nine data centers. They propose five deployment strategies including merge, split, and custom. Turnbow reviews 12 functional service deployment strategies at Coursera to implement its function call across the site. The functions were executed every time there was a new service invocation, creating a site-wide and highly dynamic service deployment challenge. In this work, a list of the microservices deployment strategies and tools available and employed in the area of cloud microservices.

16.3. Microservices Communication and Orchestration

A better solution for service-to-service communication got standardized as gRPC. This is much better than REST regarding ease of use, standardization, hard client features, and better performance. Our experience is that most modern microservices are realized using gRPC. Even if REST is not very efficient due to the overhead of headers being sent for each message, it can be a preferred choice, especially for integrating applications and legacy systems. REST can be simply used over HTTP/2 (and not only over HTTP/1.x) to use TCP instead of TLS if we do not need (or already have) the extra security of TLS. We have used this approach for synchronous communication, especially in Big Data environments, to get a significant increase in performance.

Among different models for creating effective microservice orchestration, the two models having a strong effect are service-to-service communication and message-driven communication. For service-to-service communication, the well-known approaches are gRPC and its counterpart from Facebook, Thrift. Another well-known solution for service-to-service communication is REST. This is very easy to use. You just create some endpoints in your microservice for different purposes, e.g., POST for adding something new, GET for getting the resources of the microservice, etc. A related service accesses these endpoints and executes the provided instruction. However,

lack of standardization, no built-in support for streaming, and lack of hard client features are some of the disadvantages of REST.

17. Chapter16 : Advanced Security Strategies in Cloud Computing :

The deployment of the virtual cloud network distributes Gateway Control Descriptors (GCD) to the service node to connect the gateways in Cluster Head Buildings in a communication-secure way between cloud nodes, and to control the software programmable defined network infrastructure in cloud computing environments. The virtual cloud network is applicable to the virtual network created on the same or different service buildings. In addition, the virtual cloud network is designed to enhance the global SBS performance and the cyberspace reliability of the cloud networking and cloud service security in cloud computing environment, comprising at least one Service Stack Node (SSN) implemented on at least one service node. The service node is a virtual machine (VM) or service computer. The VM is a reusable, scalable, and ultra-small computer that can replace or buy a web server, quickly implement development, experiment, or manage corporate backend systems.

In Chapter 1, the cloud service is composed of multiple environmental layers. As shown in Chapter 1, the majority of cloud nodes in these layers are implemented by virtual machines. The primary purpose of this chapter is to secure communication and data in the cloud environments within each of the environmental layers. Virtual networks, the GCHB system in SBS, and unique data structures are to be used for protecting communication and data in the cloud service herein. The virtual network, unique data structure, and cyberspace protection for service node communication are presented.

Cloud computing is tending to become an ideal platform for researchers, in addition to corporate users, because of the various available computing resources capable of conducting many experiments or processing many petabytes of data. However, data in the cloud has to be shared among cloud nodes and has various characteristics like volume, velocity, variety, and value. One of the dominant issues is the security of data handled, stored, or controlled by these cloud nodes.

17.1. Zero Trust Security Model

Zero Trust infrastructure is an information security framework that has been applied more broadly. The main idea is that one cannot join a network simply because they have some incoming packets with the right destination or are at the physical place where the definitive infrastructure is located. However, network protection is no longer an adequate security approach. Zero trust must also cover users, applications, and processes independently of their protection system, and the data should always be considered vulnerable. It must cover every single resource, regardless of whether they are legacy systems or existing communication protocols, with the purpose of supporting several services such as sensors, state estimation, or actuations. In redundancy conditions, when two security models access the network, it should be possible to identify incoming data access and decide who allows access. If the allowed model is unable to accomplish this, then the network has to leave the redundancy condition to avoid potential attackers accessing compromised systems.

Zero Trust is a proactive security model that "trusts nothing" and verifies everything. It traditionally assumes that bad actors already exist, so verification is required for everything accessing the network. Its core tenet is "never trust, always verify" via Zero Trust networking, with a focus on every access and entity (identity) across corporate, private, distributed, or cloud resources. Zero Trust protects the network at its finest granularity: the interaction itself. It inspects a request to ensure that the privileges and conditions of the entity, the environment, and the request align with the security protocols. All device access is handled the same, thus greatly reducing potential security vulnerabilities. Designed to protect modern on-prem and cloud networked infrastructures for distributed workforces, it is applicable to any device requesting access to resources outside of corporate headquarters.

17.2. Threat Intelligence and Security Automation

Security through Automation in cloud computing is becoming the next revolution in defending against the rapidly changing threats and malware

trends of the cloud. It is no secret that the primary problem in securing a cloud environment is the scale, the intensity of traffic that needs to be inspected around the clock for primary security protection and enhancing development. Defending such networking infrastructure is a daunting task, which requires high throughput, scalability, and speedup without performance degradation. Cloud-based security solutions have provided an intelligent means to deal with these challenges. It is a symbiotic relationship that allows enterprises to leverage the strength of the CSPs to provide value add-on to enhance the security protection. Security through automation allows rapid protection against suitable and emerging needs in the networking infrastructure and ensures proper security measures in a more efficient way. By integrating best-of-breed cloud automation with security platforms, we can reduce risk posture from internal or external attacks and threats, assure HIPAA and GDPR based security compliance and minimize threat vectors using Network and Cloud resources, and enhance the quality of SD-WAN networks. These early Government and Public commercial cloud spirit of "You Build, You Innovate, and You Deploy" the new theme, "You rent, You Compute, We Secure" which is more strategic in case of contraceptives and control of cloud access, data security, and security endpoint in Internal infrastructure relocation.

Threat intelligence is a critical concept in ensuring data protection of an enterprise solution. It is a combination of services, sources, and even products termed as threat feeds that provide actionable information to provide real-time threat details and enhance security. This requires security analysts to identify and prevent probable issues and exploit and incident activities in the networking infrastructure. The task of threat intelligence is performed within the concept of the cyber kill chain and assists in taking proactive measures to protect the privacy of the system. Threat intelligence is provided by both commercial and open-source intelligence sources. This threat intelligence should be integrated with security solutions to provide contagious security solutions, dealing with the rapidly changing and highly scalable cloud networking infrastructure, making the information flow smooth. The setup provided for threat intelligence should be alert driven,

using telemetry from multiple sources such as SIEM solutions to get attack information about probable security breaches and then performing incident response actions required based on the received intelligent threat scores. Candidly, the information or control centers should be able to hunt for malicious connections or suspicious activities, preferably using GUI-based solutions.

17.3. Secure Access Control Mechanisms

The rapid growth in digital data has been driven by a significant expansion and wide adoption of cloud services and technologies. For the cloud user, placing sensitive data into the cloud involves strong security, privacy, and trust. Attribute-based encryption (ABE) was introduced to enable fine-grained access control over encrypted data with specified attribute sets and/or policies. In recent years, many cloud storage access control mechanisms requiring fine-grained access control and effective user authorization process have been addressed. The user does not need to possess information on whether and where the data item resides, and that location privacy is basically protected. Existing encrypt before outsourcing techniques are not secure to prevent illicit data retrieval, and the user's searchability requirement cannot be fully satisfied.

Recently, various cryptographic key generation mechanisms were implemented to make the encrypted file search and access control mechanisms practical. The goal of a secure ABE system is to give a data owner control over who can search. Furthermore, sets of data are finally grouped into neighborhoods or databases. A cloud user only obtains data that his/her credentials allow him/her to access. Existing ABE schemes are not originally designed for keyword search over encrypted data and thus are not suitable for real-world data stored in the cloud. To realize a secure and efficient ABE model, they subsequently utilized weak ABE to define attribute-based searchable encryption (ABSE), a next-generation cryptography mechanism.

18. Chapter 17: Compliance Standards in Cloud Computing :

Cloud computing can be described as computing that takes place on remote servers, using resources provided by others. Users access the required information over the internet. An analogy for cloud computing is how users use electricity, plugging into the cloud and using as much or as little of the service as needed. The goal of cloud computing is to apply high-performance computing to solve complex business and technical problems using scalable, upgradable, and energy-efficient systems. The cloud is flexible, scalable, cost-effective, and fast. Users can upload information to the cloud for processing and download the results. They can also rent hardware, software, infrastructures, and platforms as a service. Cloud providers offer different platforms with varying capabilities to different groups of users. For large-scale computation or real-time high-performance computing, cloud providers offer services that allow users to calculate on computers with the desired number of processors, storage, and on-demand connectivity using live migration of clustered guest operating systems within the data center.

To address these concerns, cloud service providers have created service-level agreements, but these agreements are considered weak and do not provide sufficient protection for users. In order to ensure that users have the same level of protection as the providers' own employees, it is suggested that cloud service providers should be required to allow users to monitor the processing of their information and communication to authorized or potentially interested third parties, unless the provisioning is private.

Currently, cloud service providers are organizations that provide various services to users. However, there are concerns about their practices. They are accused of tracking users, selling their information to marketing companies, conducting attacks on behalf of government and organized crime, denying service to users, modifying data, sending false updates, and increasing the threat surface for users and their data.

18.1. Overview of Key Compliance Regulations (HIPAA, GDPR, etc.)

The General Data Protection Regulation (GDPR) is the reformed data protection law and replaces the Data Protection Directive 95/46/EC of the

European Union (EU). GDPR further strengthens privacy compliance and applies to any organization that stores personal data on EU citizens - if you are a US company with an EU presence, the GDPR still applies to the data you hold on behalf of the EU citizens. The former Safe Harbour agreement has been replaced by the Privacy Shield framework and the EU-US data protection "umbrella" agreement.

In this section, we'll start by identifying the key worldwide compliance regulations and standards, then highlight regulations from a few specific countries and discuss their details. In the healthcare industry, ensuring compliance with IT security and privacy regulations is a high priority due to the requirement to protect electronic protected healthcare information (ePHI). This data, once breached, can result in privacy, identity theft, and financial damage to patients, heavy penalties for healthcare organizations, a damaged reputation, and a significant loss of patient confidence. The HIPAA is the most important regulation for the healthcare industry to comply with.

18.2. Compliance Challenges and Solutions

Policies are defined as OPA rules, and they are used to monitor compliance in near-real time. Cloud administrators can define policies to track compliance with the regulatory standards to which their organization must adhere and either terminate or migrate a virtual system if a violation is detected. ACS uses the Xen hypervisor and the Cloud Service Provider, Eucalyptus environments as its base. In addition to the ACS tools, VMware vSphere and vCloud also offer some compliance support functionality. These tools analyze the VMware ESX environment to verify that configurations align with best practices and offer solutions to fix problems. Openpages is a tool that uses an engine to analyze configuration information, and configuration alerts for policies can be exported by the Openpages Enterprise business GRC Module. The vCloud Compliance Checker includes a database that can evaluate if vCloud is configured and used according to a subset of the TCG virtualization guidelines. Unova et al. suggest another approach to verifying compliance with a given policy in a cloud environment. Their plugin for the OpenNebula IaaS platform offers segregation between users and application domains,

and secure sharing and access of both applications and data among final users. Their system works with Linux KVM but does not support data connection topology changes that could harm network isolation.

Ensuring that information systems comply with internal or regulatory policies has always been a key function of operational management, but it becomes even more important when governmental or industry standards are involved. A significant body of work exists in the area of Enterprise Risk Management (ERM), and existing tools are beginning to provide ERM assessment capabilities for cloud solutions. Q-Compliance is a project designed to provide compliance assessment and satisfaction in the cloud. The ACS (Agile Compliance Secure Hosted Hypervisors) cloud model extends the Xen Hypervisor and adds four new components: an isolated domain, a cloud manager, a domain manager, and secure storage.

18.3. Auditing and Reporting for Compliance

ISO 27001 Clause 4.3 is part of the ISO 27001 standard that covers compliance obligations. It provides requirements for establishing operational processes, plans, and controls to ensure that the Todorific Service Management System remains in compliance with relevant legal and regulatory requirements. The major audits ensure that the management system is working efficiently and effectively, creating comfortable overall conditions for great compliance. If the organization's management system does not signal noncompliance or occupational consequences, conducting management review meetings and auditing management reviews will not be required.

Organizations need to ensure that the service management system has been properly configured and data is being handled according to security policies and regulatory guidelines. This means that information security personnel require access to security solution data and tools to manage security controls and prove compliance upon request to internal or external auditors. Cloud service providers must be prepared to provide independent external audit reports if they wish to maintain their existing security certifications.

19. Chapter 18: Identity and Access Management (IAM) in the Cloud :

Identity and access management (IAM) is the first line of defense. It prevents unauthorized access to an organization's infrastructure, applications, and data. At the same time, an effective IAM approach enables the right people to do the right things at the right times. It manages who has access to what and collects and analyzes information and sets rules and links them to users' access. It does this by first recognizing the people who are attempting to access infrastructure, applications, and data and then authenticating them. Once it knows who is attempting to sign in, it determines whether that person should be granted access.

Identity and access management (IAM) in the cloud is the first line of defense. It prevents unauthorized access to an organization's infrastructure, applications, and data while enabling the right people to do the right things at the right times. It recognizes and authenticates who is attempting to access assets and then determines whether that person should be granted access. This chapter discusses IAM in various cloud technologies. Then, it demonstrates how to secure an Azure SQL Database, a popular managed database in the cloud via IAM and other technologies.

19.1. IAM Concepts and Components :

In the traditional data centers that companies operate and have control over the physical servers and networks, only their employees would have access, and only authorized roles and people can add/remove users and assign permissions to users to access various resources. Even for the cloud service providers like Amazon Web Services (AWS) or Google Cloud Platform (GCP), there will be one or more centralized accounts, and role-based access will be managed for the employees. Thus, relationship authorization at the enterprise level and cross-functional roles for authorization and authenticating logs across functions would be managed across multiple trust levels.

Cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform operate and manage data centers for providing cloud computing services such as Infrastructure as a Service

(IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The key control of the cloud resources is the Identity and Access Management (IAM) tool, which we can use to configure who is authenticated and authorize what authenticated users and services can do. Every cloud service has the capability to create and manage users and mechanisms to manage access, and the IAM should be used in tandem with features of the cloud resources like encrypted volumes, key management service, and continuous asset management. The cloud customers would have the data that is associated with their enterprise placed in the servers that are managed by the cloud service provider. So, it is important to know how our user data is protected, how data is segregated, and who will have access to the data.

19.2. Role-Based Access Control (RBAC) in IAM :

After consideration, it is found that the IAM relationship and attributions are an essential transcendent business for each cloud endorser, which can be lonesome of implicit IAM attributes. It is outlined with the device parts as the basic existence of the cloud-setting-up parts. The cloud endorser part needs common business devotee and cloud provider parts. It is related to the business, which is allowed to produce different cloud-based strategic economic effects as previewed by the profile and different industry opportunities. Cloud consumer commercial cloud seeker soft attribute set mapping attribute set classification function of the consumer and the capabilities requested from the cloud cloud provider soft attribute set mapping attribute set function of the queue provider and the identifier in the consumer. These references should analyze the tokens. The soft tokens are considered given for audience case analysis. Soft references are considered based offerings. The cloud business process is considered from the aspect of the demand and supply diam and represents a business and related activity model.

As a conclusion, cloud-based identity management should have a rule-based system to make IAM work more efficiently. Suppose we create a basic architecture for the users and applications that are in the cloud environment. In that case, we must analyze the type of rules and

attributions fusing in the environment, create a certain relaxation throughout unique location, isolate the envisioned model parts, and utilize which kind of architectural list is a prerequisite.

Role-based access control (RBAC) provides the least privilege principle as well. This term mainly originated from NIST-based production, which goes by the RBAC idea. We assign rules to subjects to enforce who does what. With this content, we can use policy agents in IAM as well. Those agents are transitive and located systems. We can shape, integrate, and apply membership and entitlement analyses using the IAM policy rules. Integration and application points such as Windows runtime policy, XACML XML runtime, and policy enforcement points are also mentioned.

19.3. IAM Best Practices and Implementation Tips :

Identity and Access Management (IAM) is very integral to the security of the cloud, especially to AWS. With several identity and access management features created to be used effectively and efficiently, it is important to understand best practices and optimal implementation scenarios that are in conformance with AWS security best practices. This section highlights best practices that organizations need to consider when creating IAM resources.

IAM Best Practices and Implementation Tips

Overview of IAM Best Practices Best practices clearly define identity and access management as a shared responsibility. Best practices are put in place to secure and protect cloud resources from unauthorized access. These best practices assist in ensuring that identities have fewer privileges with permission. Creating IAM policies consisting of explicit permissions and disabling permissions or changes in AWS account security functionalities, such as creating users and deleting users from the root account, increases the security levels of an AWS account. This practice helps to minimize any security risk associated with the AWS root account and helps to promote accountability with service usage.

20. Conclusion and Future Outlook

These types of needs are fulfilled by cloud computing technology, in which if a company has a lot of data of users or something and if they want to work on the data and also live the data. Users who want to keep the company's name remember and to also get revenue as soon as possible. Then, in this case cloud computing is useful because it can quickly search the data and get answer fast because it uses online discoveries like Google API.

[59] [60]In cloud computing, users can access cloud-based applications and services online from anywhere with an internet-connected device. To use these cloud-based services and applications, users are not required to store or manage any data locally; the data and services are accessible through a connected device over the internet from cloud storage, databases and servers. Cloud computing also brings new challenges in the field of computer science and engineering. One of the important challenges is security. Because of cloud storage's flexibility, there are many security concerns when it comes to cloud chains. Existing solutions to many storage systems struggle with protecting data and preserving users' privacy. Data privacy is also a big challenge in cloud computing.[4] With the help of cloud computing technologies we can adopt a kind of policy with our data that data is a feature of the system rather than a feature of the site. By using this policy, we can fetch our data from tied up systems from the cloud for use in our local systems which is known as cloud synchronreacheable online storage and the process to use this data to the local application consists of mainly five major steps; Discovery, Translation, Adoption, Consumptionor Visualization. As we all know about a very famous open source operation system named red hat Enterprise Linux. It is known for its perfect stability. It provides smoothness in the office technologies market. As we all know, nowadays, companies are looking forward to new technology so that they can manage all kinds of work ina very small amount oftime. They are looking for better storage technologies or technology which can reduce their space in local servers and the workload of the local machines.

20.1. Summary of Key Points

The most important pieces of advice from the literature regarding effective cloud services strategy, are to: (a) obtain early high management support in cloud adoptions (thus, sustain advocates), (b) to engage with information technology so as to innovate in or with third-party cloud services, (c) engaging in dialogues with providers and first dots (in the form of employees) and look at both short-and long-term implications. This simple framework has been chosen, as its architecture is well known from the literature, and the sub-components are considered individually throughout the chapter as they are of interest. Our results have relevance for IT management in across industries, and results should be of interest for researchers in other industries and host countries. Future research could look at the potential for strategic opportunities for smaller first party to co-create new third-party value from cloud. Follow up research could focus on new and emerging technologies such as the blockchain, which could also hold opportunities for co-created in combination with third party cloud providers. For public cloud customers conducting best privacy protection when features haven't been mature, combining tactics are recommended, which is also in line with a better service delivery model of cloud computing.

Cloud computing involves transferring aspects of an organization's operations or service delivery model to off-site data centres owned by third-party providers and accessed via the internet. Depending on the way an organization uses the cloud and its service-offerings, this business model can have significant implications, ranging from the choice of technical services over cost savings to strategic benefits and the ability to quickly realise product innovation ideas [61]. Beyond that, the cloud may allow organizations to offload mundane operational or maintenance tasks and provide better service coverage for existing customers. Proponents argue that cloud services (along with big data, artificial intelligence/AI, and other technologies composite cloud) can enable strategic goals such as cost savings, operational efficiencies, and even business model innovation (e.g. the development of complementary products) or increased customer acquisition. However, external customers tend to have different expectations and

demand a user-focused approach. By delivering services through separate but interrelated technology layers from shared and standardized resources, (multi)tenant isolation still remains one of the chief problems. The remainder of the chapter discusses methods in finding cloud's strategic benefits in detail.

20.2. Emerging Technologies in Cloud Computing

I am nervous and excited about Artificial Intelligence (AI) in general, as well as the data-exploded World Wide Web (Web) and 'success breeds complacency' kind of practices that are being practiced. What excites me is the new AI gold rush of recent years, the massive novel data and compute initiatives and implementations, and the multitude of AI driven innovative possibilities. This translates into large scale depersonalised and personalised intelligence in extracting inferences, insight and knowledge for a variety of applications ranging from entertainment to natural and life sciences, cyber military and space science to cyber education, the environment to abstract cyber spaces, and a plethora of areas and territories of human endeavors. AI is being applied in industry, science, education, health care and national security, among others. The AI technologies have brought about a step change in the way the processing and exploitation of these vast amount of data is undertaken. [62] Indubitably, cloud is becoming a new normal for processing large scale data next to AI, the productivity improvements that comes along due to machine learning and AI, together with very large data sets and big data statistics are delivering a quick and significant value. The cloud architecture does have endowment of ability to store and process information about huge numbers of users in scenarios such as social networks, sciences and social security data. In companies huge numbers of employee's activities, their performances, their data of birth, passport, residential details and all other details can be stored and processed and/or it is also elaborately employed in other applications.

The explosion in the amount of data generated and the need for real-time and quick access to very large datasets has resurrected interest in Parallel and Distributed Computing. Cloud centric approach, where core parallel and

distributed computing including HPC resources, databases, software packages, etc., are accessible using Web based protocols and interfaces has matured and seems to be a successful commercially viable option. [1] This is helping in making Cloud Computing suitable for executing a number of High Performance Computing (HPC) applications. The Cloud infrastructure gives users access to HPC systems over a scalable reliable, high performing and secure dedicated computing infrastructure.

21. Appendices

Several offerings actually come in the shape of services. For instance, the most important benefit for most companies using cloud today is the savings in capital expenses for software and equipment. The cloud allows companies to pay only for the amount of resources they use. Linq is fundamentally a distributed system, where it uses Hadoop cluster as cloud technology, to process data on a cloud. As a result, it divides data set into partitions and process these partitions in parallel. But, due to the use of different buffering mechanisms for data processing, it shows considerable amount of data processing time, which in turn extends completion time of the processes. So, proper buffering techniques are needed, that can minimize it's completion time effectively [2].

[63] Throughout the book, we have seen many service models that the cloud offers. But, what if you are a developer, an academic researcher, or a person who is not into any tech job domain? Then it's unlikely you'll find something of your interest that isn't covered yet, right? Not really. There's so much more than just the basic services a cloud can offer. People have been creating valuable services and software for cloud and will continue to do so. With the concept of PaaS, which is the initial of platform as a service. In PaaS, we get tools and services that can be used via a SaaS service, hence we don't have to worry about any kind of installation, updates, and no need to maintain it. Eg. Salesforce, Google AppEngine, Wordpress, etc.

Appendices A: A Comprehensive Guide to Docker and OpenStack: A Practical Approach for Students

1. Introduction to Docker and OpenStack

Docker is a technology that emerged in 2013. It is a tool that is used to facilitate development, deployment, and execution in the production environment of applications encapsulated into lightweight and portable containers. With Docker technology, it is possible to create containers that perform specific functions, leaving the developer free from spending time and effort configuring the machine, the entire run-time environment of the application, the operating system (OS), and the dependencies of the applications (libraries, frameworks, etc.). This allows the development of portable applications that can function independently of the type of OS or machine on which it will be executed. On the other hand, OpenStack is an Open-Source software/hardware platform for building own public- and internal cloud computing infrastructures. It is initially a project from RackSpace and NASA and currently has various contributors. OpenStack has a modular architecture, which, at high levels, divides its components into object storage, identity service, block storage, networking, compute, and dashboard.

It is observed that every day we are faced with new challenges in the management of corporate computing environments. For this reason, the area of Information Technology (IT) keeps evolving in terms of technology as well as in managing complex and large hardware environments. These challenges gave rise to a research area called Cloud Computing. In practice, engineering professionals and academia today use tools and technologies such as Docker and OpenStack for Cloud Computing. In this context, this text has as main objective to introduce concepts and to demonstrate how to use the Docker and OpenStack technologies, focusing on undergraduate students. Initially, we demonstrate the basic features of the Docker and OpenStack tools.

Then, we describe practical examples of the use of both technologies, illustrating with simplified examples. When we finish the description of these tools, we will have demonstrated the basic knowledge about them (installation, basic configuration, main commands, and use cases), which will enable the student to develop complete projects using these technologies.

1.1. Overview of Containerization and Virtualization

Docker is currently the most popular system container technology, and its resemblance to regular packaging, as it was previously utilized, has brought about a high level of interest compared to other container solutions. A typical usage of Docker enables temporary, stateless deployment or development of isolated application instances. However, the software also supports more advanced deployment and development tasks. In these cases, it is often utilized together with other container-based software, such as Kubernetes, DC/OS, or OpenStack, which are used for maintenance and management support purposes.

Comparing to the VM-based approaches, the system container (container) approach also allows multiple isolated systems to run on a single host. These containers share the same operating system kernel, running one of the supported operating systems, and allow different application instances or processes for the guest user. The approach can offer better execution performance, reduction of system maintenance effort, and it enables different vendors' approaches to providing and supporting a restricted security context, subject to some limitations.

Nowadays, virtualization technology refers to a way of running multiple isolated systems, known as virtual machines (VMs), on a host. Each isolated system is known as a guest system and can be managed to run different operating systems and allowed user-space binary.

In the late 1950s, during the mainframe computing era, people developed virtualization technology. It allowed individuals to operate multiple isolated systems, each with its own operating system, efficiently sharing valuable mainframe resources. Later, from the 1980s to the early 2000s, during the

personal computing era, most computer systems were managed to run a single specific operating system and intended applications at a time. Workstations and servers were the computation devices connecting remote users using early network technologies to run an instance of an operating system.

2. Getting Started with Docker

This section aims to demonstrate how to get started with Docker, including how to install it and manage containers. It also presents the application of Docker on a real use case. After reading this chapter, readers are expected to understand how to use Docker commands to pull images and run containers for a specific purpose. This knowledge will be applied in a future chapter in conjunction with OpenStack for application deployment.

Docker is an open platform that allows developers and system administrators to build, package, ship, and run distributed applications in containers. A container is a lightweight, stand-alone, executable package of a piece of software including everything needed to run it: code, runtime, system tools, system libraries, settings. Containers are an abstraction at the app layer that packages code and dependencies together. Multiple containers can run on the same machine and share the OS kernel with other containers, each running as isolated processes in user space. Containers take up less space than VMs (container images are typically tens of MBs in size) and start almost instantly. Docker helps developers put everything they need to develop and run their software into portable containers that can be run anywhere.

2.1. Installation and Setup

Before installing Docker, we must make sure that the operating system is fully updated to the latest version. Installation of an operating system on a cloud, a hypervisor in the case of server virtualization, and OpenStack, in the case of using an infrastructure-as-a-service (IaaS) cloud with AppFS that we will see next are more advanced topics. Therefore, learning to use Docker first is a simpler solution. Next, set up the lab environment by updating the operating system.

2.1.1. Prerequisites for Docker Installation

2.1. Installation and Setup

In the third chapter, we will quickly learn what Docker is and how it works. We then look at the prerequisites we need to install Docker on the Ubuntu computer that we will use to play with DevStack with Docker. After that, we install Docker and finally test it so that students are familiar with its basic commands.

3. Docker Basics

Docker is a platform that is easy to use and is designed to simplify the creation, deployment and running of applications in the form of containers. What makes Docker unique is it enables an easier, more robust, and more efficient way to benefit from containerization technology. A container is simply a model for a unit that allows a developer to wrap up a piece of software in a complete filesystem that contains everything it needs to run including the code, runtime, system tools, libraries and anything else a running application needs to work. Containers can be moved from one server to another hosting the Docker platform without any changes to the application itself. They do not have the traditional overhead found in a virtual machine; the container operates as an isolated process running on a single Linux instance. Today, Docker has become one of the fastest-growing technologies, being adopted by many companies around the world including larger software providers such as OpenStack, Google, and Red Hat.

In this chapter, students will be introduced to the basic concepts of creating and running Docker containers. Workshop-style activities are included for students to use what they have learned by using self-guided exercises. To follow along with the workshop activities, students need to have access to a Fedora Linux development operating system including access to the Superuser account.

3.1. Containers vs. Virtual Machines

However, containers have no resource reservation policy or inefficient utilization of resources, such as machine learning workloads in OpenStack.

The second limitation is their need for patchy access; they require fast access to a limited subset of host hardware. Providing such access may be difficult or impossible in existing setups, which are designed for general-purpose virtual machine modernization.

A container is a small, fast, and portable runtime system that can run on any platform that supports containers, independent of the operating system. It offers an enormous increase in speed, flexibility, and success over traditional operating systems.

3.1.1. Containers

Containers take virtualization to the next level. They are more efficient than hypervisors in breaking down barriers between the applications running on a single physical machine. Although containers can isolate applications from each other and perform the same tasks as a VM, they are not a VM replacement. Each model has its advantages. VMs offer more security, while containers can be run on everything.

Virtual machines (VMs) are an abstraction of physical hardware, turning one server into many servers. The hypervisor allows multiple VMs to run on a single machine. Multiple operating systems can run on one physical machine, and multiple applications run on each system.

4. Docker Commands and Operations

You can run a Docker container with the following command: `docker run IMAGE`. By issuing this command, you will start a new instance of the specified image. The `OPTIONS` setting will allow you to run the container as you need. If you do not want a new container every time you execute the command, you can start from the existing list or a new instance of a previous container that has exited. The `IMAGE` argument is the image to be executed to create a new instance. You have the option to choose `CMD`, the command to run in the container for the new run. `ARGS` are the arguments that will be passed to the `CMD` at the instantiation.

A Docker container is created from an image. An image is a set of files that contain system libraries, system tools, code, and other files that can be used as the base for the running environment of your containers. The file collection is created on your machine and turns into an image you can run. The container is the instance of the created image. To start, stop, list, or interact with a container, we use the Docker client, which is a command-line tool.

4.1. Building and Running Containers

First, I pull the alpine image and run a few commands in it. The commands are enclosed in double quotes and executed. Then I pull the python:2-onbuild version and see what the difference with the last case is. Finally, I build this version from a Dockerfile, run a container and try to verify that all the necessary elements for a working environment for Flask are there. With a correct command, Flask runs and we see the welcome page. These three base Docker images represent well the fastest approach to deploy code inside a container, even when it needs external libraries—Clang, in this case—to be built. The fourth base image, python:2 is a slim version, and the verification for Flask's setup is not executed.

In this section, I focus on the creation of containers, which I carry out using the Docker engine. Docker containers can be created in a few different ways, including Dockerizing existing applications and creating a container from scratch. After experimenting with some base images, I find that the Docker Engine is a highly efficient tool for developing and testing application code that will run in an OpenStack environment, as it reduces the time needed to set up an OpenStack environment on my computer. To experiment with some existing base Docker images, I first download the latest Docker engine and run the command `docker run hello-world`.

5. Docker Networking and Volumes

Endpoints The network is composed of endpoints. Each time we specify to use an adapter (use `--net` in the Docker create command line, for example), we are basically specifying the creation of an endpoint. When an instance

uses an IP from the group led by a specific adapter (ifconfig for Linux), that instance has a network endpoint set up and running. Docker creates a Virtual Ethernet (veth) device for the endpoint. However, the Veth device possibly created by Docker or perhaps already created and not yet used (in which case the command is run after setup Docker force). The actual configuration of an endpoint (including the IP address) is performed using the adapter. For the adapter to work, infrastructure connected to the physical network (it does not matter which, i.e. Wi-Fi, Ethernet, or others) has to be installed. If everything is well configured, communication should flow seamlessly within the infrastructure.

Docker Networking Similar to Docker volumes, the network also belongs to the group of certain aspects of a container that are disposable. When a container is removed, so are the "virtual" settings applied at the time of its startup. However, in the network, there is an interesting aspect: while a volume is a file of the host system that is "connected" to a directory inside the running container, a network is a completely separate system that is available to the Docker engine, i.e. it is linked into the Docker runtime. Let us start emptying some concepts related to containers and Docker network.

Introduction The previous discussion on Docker focused only on deployment, but actually having your applications running is not the only thing that matters. You have to be sure your applications are only using what you intended, i.e. the correct network settings, only those directories that you upload files to, etc. This paper introduces the essentials of Docker networking and Docker volumes. It is important to note that these features have different settings depending on the OpenStack cloud that the user uses. This will be addressed in due course. Figures 65 to 71 show how to set Docker networking and what they mean each time, as well as how Docker volumes work for you.

5.1. Connecting Containers

Listing 5.15 shows a simple way of connecting a Docker container to an OpenStack Nova instance. The container creates a plugtap interface (plugtap0 in this example) and connects it to the host (the eth1 interface in

this case). In the `nova.boot()` command, the `"nic_model"` and `"hw_vif_model"` parameters give the name of the implemented module (`vif_libvirt`) and fake driver (`vif_type_tap`) for the OpenStack instances. The IP of the fake interface is configured in the DHCP configuration file. If security improvements are necessary, a static IP configuration or security group can be applied. When more than one plugtap is created, its IP, interface, and Nova's NIC type should be managed to ensure the proper solution. This example describes the most basic way of connecting a container to OpenStack. More complex VM solutions are out of the scope of this abstract.

Unlike the VM and OpenStack integration, connecting a Docker container to an OpenStack instance requires more coding. In this section, we present a simple way of connecting a Docker container to physical hosts, Linux bridges, or OpenStack instances. The Linux bridge way of connecting containers to VMs is preferred and is the standard networking used by OpenStack Neutron agents. The second way of connecting a container to an OpenStack instance uses a host or bridge that is connected to the outside of a host and uses NAT to forward packets. The description of both sequences using the OVS is almost similar to the Linux bridge. First, we need to create and configure the type of connection defined by the series, and then connect the container's interface to the Docker host or `dockerbr0` bridge.

6. Introduction to OpenStack

The OpenStack project is a global collaboration of developers and cloud computing technologists producing the open standard cloud computing platform for both public and private clouds. Backed by the largest IT companies in the world, OpenStack is used by service providers, enterprises, government agencies, and academic and research institutions serving a variety of workloads. OpenStack software controls large pools of compute, storage, and networking resources throughout a datacenter, managed through a dashboard or via the OpenStack API. OpenStack works with popular enterprise and open-source technologies, making it ideal for heterogeneous infrastructure.

OpenStack is a collection of open-source software that enables enterprises to create and manage large groups of virtual machines through a unified GUI or API. OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources throughout a datacenter, all managed through a dashboard that gives administrators control while empowering their users to provision resources through a web interface. It allows businesses to control large pools of compute, storage, and networking resources by using OpenStack technology either through a web-based dashboard, through a command-line client, or through RESTful web services. It has a modular architecture with various code names. OpenStack Compute (code-name Nova) fabric controller.

6.1. What is OpenStack?

The OpenStack cloud operating system can provide the processing resources for Internet-scale applications in a way that is attractive to both the users of the service and within the datacenter design. The key technology to providing and growing the computing power of OpenStack is virtualization. As cloud computing emerged and quickly grew, virtualization became a key enabling technology for both of the primary modes of service delivery: Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). The online web tools that contribute to providing these compute resources are typically backed by server farms that can scale. These tasks and services that can be hosted in a cloud for a business partner or the public are diverse in quality and quantity, but all vendors want the ability to supply these resources to their customers as a way to generate revenue.

OpenStack is a very ambitious open source project. It is usually termed as a cloud computing operating system. It is a huge project with a lot of moving parts. There are so many components in OpenStack that it has been divided into sub-projects which are more manageable. These projects usually manage compute, storage, and networking resources in a cloud environment. OpenStack is best suited in the Infrastructure as a Service domain. This means that infrastructure is delivered as a virtual service and clouds can be used for deploying virtual machines which offer resources of a physical

machine. OpenStack is becoming the de facto standard for providing cloud solutions in the IT industry because it has a very active community, it is being deployed extensively, and companies in the IT sector have already started briefing OpenStack solutions in their roles and products.

7. Key Components of OpenStack

7.1 OpenStack Dashboard (Horizon) The dashboard in OpenStack is called Horizon. Horizon is the web interface used to interact with OpenStack. If you have installed OpenStack, administrator credentials will allow you to perform any function; whereas, normal users will only be allowed to perform certain functions. For example, users can create and boot instances, manage advanced images, and define availability zones and host aggregate configurations; however, only administrators can manage tenants, users, roles, flavors, security groups, key-pairs, network allocations, quotas, customizations of the dashboard display, and so on. Therefore, it is always good to give administrative privileges to users once OpenStack is installed in a production environment.

In this chapter, we are going to look into some of the key components of OpenStack and their importance. We will see how we can use OpenStack's dashboard, Horizon, to actually work on it. But first things first; before we do anything, let's first log in to OpenStack with our browser.

7.1. Nova (Compute)

Compute service - Nova interacts with the hypervisors. A hypervisor is software that emulates a hardware architecture enabling guest OS to run. It is also referred to as a VMM (Virtual Machine Manager). KVM, QEMU, and other VT extensions (Intel Virtualization Technology, and other processors with at least x2APIC and the EPT can expand the logical address space through hardware assistance), and VT-x (Intel Virtualization Technology for x86, processor-extended page tables) and AMD-V (Virtualization Technology for AMD) are commonly used hypervisors in clouds. Such software like Virtual Box, VMware, or Vagrant is also a hypervisor but not used for production environments because of its licensing

model. If you want to use such hypervisors, you need to override the default and public use your own hypervisors because OpenStack only defaults to the public clouds. It is multi-vendor in technology. If you can override the default hypervisors, the images need to be built manually using hypervisor-specific slice (when using shared glance you sent up the operating system images by yourself? Then regardless of the hypervisor selection, it needs to be specified while booting from the image service) in the hypervisor group and need to update flavor specifications to include the exclusive property to the hypervisor. Virtual machines created by KVM need specific properties like `VOLUME_BACKING_FILE_FORMAT` or `RBD_DEFAULT_FORMAT`. The image cannot be only shared and built by KVM. You must maintain nova-compute's settings constant and correct image metadata with nova flavor commands.

Each OpenStack project has its own dedicated purpose. The Compute project is called Nova. It provides a way to manage a hypervisor on a physical machine. Some people refer to this as VMM or the hypervisor. By default, the hypervisor used for Nova is QEMU.

7.2. Neutron (Networking)

Neutron provides advanced networking services through its API, plugins and drivers. A typical networking example is VLANs. To use this kind of network, the VMs need physical ports and they typically have to be VLAN-aware. Moreover, all the actions involving VLAN technology are set up through VLAN management software such as switch and router VMs. Switch and router VMs need to configure themselves to be connected to each VLAN and must also update the switch and its router tables. VLAN-aware software has the accounting information that describes how many VLANs a host supports and that also lists the supported VLANs. The computational effort to integrate together the VLAN-aware software with the switch and router VMs should not be underestimated. It would be easier to use the direct connection method, as in a phone call, instead of the VLANs method, with its relays as seen in the incoming data flow. However, such plugins or drivers are

not simple pieces of code; some like Open vSwitch are an independent project.

In cloud computing context, creating and managing virtual machines (or any type of VM) is not a big deal. However, running applications distributed over multiple virtual machines requires a lot of complex driver configurations such as for networking. Normally, the security policies for each virtual machine need to be implemented on the virtual network components by the network administrators. A network is a key factor that affords connectivity between the various services offered by cloud. Neutron can, for example, create NIC (network interface cards), GRE (generic router encapsulation) tunnels or layer-2 tunnels aimed at the VMs management. It also needs to create networks, manage databases, update identity and compute services and other configurations.

7.3. Glance (Image Service)

The Glance system consists of the following broad components that are important to its correct functioning: (1) Pluggable backends, which take care of the storing and fetching of images, and allow the system administrator to determine what backend to use. (2) A registry and a store that the dispatch calls to, responsible respectively for storing and retrieving image properties/data. (3) The image schema that provides a proper data storage type according to the selected image backends. The interaction with the backends and the handling of the above two are managed by the resource.

Glance is the image service in OpenStack and is backed by either the local file system, Ceph or Swift. This component was created to store and manage virtual images, and it offers the possibility of sharing across users. Glance has a registry service to store information about images and information about where the actual image can be loaded from. The image service also allows developers to add metadata to the image and to add their own metadata. Glance is normally a starting point when working with the rest of the OpenStack services, as you first select an image to be used by an instance, then utilize the network and compute services once the instance is

running. The Neutron client, available in the free download, provides a set of easy-to-use commands to manage the various Glance functions.

8. Setting up an OpenStack Environment

8.3 Three-Tier and Four-Tier Applications Application designs that use one or two network interfaces (like the ones depicted in the previous sections) may not be super interesting/useful/compelling. Generally in the real world, applications have more than two network interfaces. One of the advantages of using OpenStack clouds is in fact this ability to manage the network (and the services).

8.2 Improving Your Skills by Building More Realistic Scenarios The burden of deploying and operating OpenStack grows with the amount of features required by a particular OpenStack cloud. In real-world production deployments, many features and service configurations that are beyond the scope of this text may be required. However, once an introductory level of OpenStack has been understood and applied via the DevStack and Dockerized DevStack setups, there are better ways to understand OpenStack rather than using the Keystone Docker container.

8.1 Planning the Setup Note that even if our actual OpenStack setup may or may not fulfill the conditions required for Dockerized OpenStack: The idea is to provide a general guide to OpenStack installation with specific emphasis on creating a multi-node OpenStack setup for corporate and private use and installing OpenStack as an add-on to an existing DevStack setup.

While OpenStack is a collection of disparate services, each service can be run independently of OpenStack. Due to this modular nature of OpenStack, an actual deployment of OpenStack involves using the services required for the desired set of requirements. In a large datacenter, only a fraction of OpenStack services are used, while in a small or medium datacenter setup, a larger fraction of services may be used.

8.1. Installation Steps

The installed parts that are described in the instructions are only the apt functionalities. The repositories that are used in this procedure are the official repositories for the Ubuntu distributions. Some precautions must be taken if the Ubuntu version that is being used is a testing version. The current process assumes that the Ubuntu version is 20.04, which is a Long Term Support version.

c. Use the official GPG key of Docker to add the repository to the system. \$
curl -fsSL

b. Install the packages that allow apt to work with repositories over HTTPS by using the following commands: \$ sudo apt-get install apt-transport-https
ca-certificates curl software-properties-common

Step 1: Set up the repository a. Update the list of packages \$ sudo apt-get
update

There are several ways to install Docker using the Ubuntu operating system. The fastest and easiest one requires executing the following commands in the command line of the operating system:

It is time to practice how Docker operates. To do this, we need to install Docker on our machine. The process of installing Docker is not a difficult task. It only requires executing a bunch of commands and then validating that the program can be used correctly. Once Docker is installed and running, the student can create and destroy virtual containers without causing any catastrophic damage to the base OS. That is why Docker is so useful for learning purposes. The Docker community has focused a lot on making the whole installation process user-friendly. If you do not believe me about the simplicity of the installation process, let's have a look at the installation instructions for Docker on the [docker.com](https://docs.docker.com/engine/install/) website.

9. Creating and Managing Virtual Machines in OpenStack

Step 1: Launching, Pausing, and Resuming Virtual Machines At this moment, the virtual machine status is already active, so to remove it from the

environment, you have to first put it in a paused status. When the VM is paused, you can go back to the active state and then delete it. Below, we listed the commands to pause and resume the VM. A virtual machine, in the perspective of an end user, is a combination of vCPU (virtual CPU), RAM, and disks residing in a compute node. These abstracted resources are unified and presented as a big compute resource. Later, we are going to discuss further how this association is done. First, it is important to launch the virtual machine to better explain how this resource is going to be assembled by the Nova and Neutron services. Before launching the VM, verify if the previous network has already been removed from the environment and create a new network based on the OpenStack.

Introduction In this section, we are going to talk about one of the most important tasks in the cloud ecosystem related to OpenStack: the virtual machine. We will reproduce several steps to demonstrate how the user has to interact with an OpenStack system to create and manage VM (Virtual Machine) resources dynamically. Removing, suspending, resuming, and rebooting the virtual machine are part of the management task that we will also introduce. We have divided the information into three steps as follows: Step 1: launching, pausing, and resuming virtual machines; Step 2: rebooting and removing virtual machines; and Step 3: live migration and evacuation.

9.1. Launching Instances

Our first command will be to check the list of images that we can use to create the instances. To do this, we just need to execute the command "openstack image list". Note that we need to select the image to use for our instance. This command will show a long list of images. To filter the images that we actually have available in our cloud, we can add "| grep ubuntu" at the end. This will show us the available Ubuntu images. The image format is required to create the network. We can execute the command "openstack image show NAME-OF-THE-IMAGE", where "NAME-OF-THE-IMAGE" will be the name of the image we selected.

Now we are going to launch an Ubuntu guest virtual machine in our Kolla environment. We only need to execute a few commands. We will start by

looking for the name of the image to start up an instance, creating a network, and a public key to login to the guest virtual machine. We will be using the OpenStack CLI for these activities. After that, we can launch the instance itself. Next, we need to find the external IP where the deployed instance will be accessed. We will look within the available IPs in the public network and match the IP to the guest virtual machine instance. We will then allocate a floating IP and finally associate it with the instance.

10. Networking in OpenStack

The OpenStack networking components are shown in hybrid mode in the above figure (Neutron, Nova-network). The first figure above shows the default networking setup in a typical DevTest OpenStack setup. By default, the hybrid mode for networking is used in Devstack. It gets further by a multi-node scenario, where a multi-node setup in Devstack is explained. In Neutron, you can use the Open vSwitch software switch or a similar software switch, such as the Linux Bridge module. Devstack will use the OpenVSwitch plugin and agent for Neutron. Two default bridges, named "br-ex" and "br-int," were used in the "OpenvSwitch agent" and the "OpenvSwitch plugin" and direct all north to south traffic through the OVS-BR-LAN bridge. It isolates each tenant or diagonal traffic with the OpenvSwitch agent. Clients and servers of different instances can communicate across different projects on the same node, but cannot communicate with instances of other nodes and projects.

There are three key concepts related to OpenStack networking you should familiarize yourself with: 1) Default networking setup in Devstack or DevTest, 2) Additional configuration for Neutron, and 3) Additional configuration for Nova networking. This chapter discusses these topics in detail with specific configuration options. Depending on the Devstack branch and how your Devstack localrc and localrc file are configured, you may get a slightly different installation. On DevTest, the Prerequisites installation will be standard and the initial steps required to set up Devstack will be similar to ones provided in the online documentation. The general installation settings and changes in localrc and localrc file will be done as required.

10.1. Software-Defined Networking (SDN)

Docker containers (L2) operate at the link layer, meaning that they are tied to a Layer 2 network. A Layer 2 virtual network is an isolated network that extends across a LAN. It treats each physical device as though it is directly attached to each other physically or logically. Frames transmitted from devices in the Layer 2 virtual network are transmitted to all of the interfaces within the edge bridge and are then forwarded only to the interface that leads to the destination device. An example of this is the bridge networking in Docker. Although it is easy to use and allows containers to have connectivity, it does not resolve the inherent scalability and other limitations of bridges. It still needs an SDN solution to enable Docker to easily add containers to the network.

SDN is a logical evolutionary step in the development of network technologies. SDN extends virtualization concepts to the network components. Network as a Service (NaaS) is the operation and management of network infrastructure where most parts of NaaS, like switches, routers, load balancers, security appliances (firewalls, etc.) and WAN optimization, are installed, configured, and managed from an external source. SDN allows dynamic network reconfiguration to support new requirements. It allows carriers to expand their product offerings and improve service delivery. It helps data center operators to connect tenants to resources more quickly by simplifying network provisioning. Programmatic control of SDN helps resolve issues in current networking models.

11. Container Orchestration with OpenStack

After completing the GlassFish distributed deployment and manual container configuration, this lab introduces Kubernetes and K8s using OpenStack as an alternative to Minikube, and describes the process of these two methods in a comparative way. In summary, the completion of this lab enables students to use recent state-of-the-art container orchestration platforms to implement load balancing services.

Our lab curriculum provides the students opportunities to gain practical experience, in addition to gaining a general understanding of containers and OpenStack. In recent years, DevOps has shown the potential to bridge the gap between development and deployment. While using OpenStack to deploy and manage VM is very helpful for students to understand IaaS, using OpenStack to deploy and manage container orchestration or using containers to provide OpenStack services can provide personalized services to students, which enriches the teaching methods.

In this section, we introduce an aggregated course of using OpenStack container and Kubernetes in the Computer Science and Technology Infrastructure System Architecture course for students in their junior year. We make them learn the related domains deeply and implement a load balancing application that can deploy and manage web instances automatically under Kubernetes.

There are a lot of challenges and technical issues for cloud service providers, such as high network cost and distributed deployment. During the Infrastructure System Architecture course, students also need to understand these challenges and practice the deployment process in the real world.

11.1. Using Magnum

First, let's use the OpenStack CLI commands to make it easier to understand, then we'll show you how to use Horizon, OpenStack's graphical interface. We will create and install a running web server with a simple content and an external Floating-IP that is accessed from outside the OpenStack cloud. You can do the same steps using the GUI - OpenStack Horizon. After running the commands below, you will also know how the process is performed using the GUI. I especially prefer Horizon as it facilitates resource visualization, but using OpenStack CLI facilitates understanding.

Magnum is a project to use containers to provide as a service of OpenStack. It deploys and manages clusters of machines for the management of

containerized applications using OpenStack services. We used Helm with Keystone and OpenStack Images in the cloud, interface with Magnum. We will now use Magnum, an Orchestration service container.

In this section, we will learn how to use Magnum to deploy clusters using containers instead of virtual machines. We will work with basic load balancing. This will install Magnum (Kubernetes+Flannel+Docker registry), create the bay, then create a simple application running a web service. To follow this tutorial, you need basic experience in OpenStack. Although almost everything uses OpenStack Horizon, this is also shown using the OpenStack CLI.

Conclusion and Next Steps

Educationally, OpenStack enables the empirical study of and configuration of infrastructure to the size of actual computing services according to demands. Furthermore, by using it along with a set of Docker containers, several basic and advanced study possibilities can be achieved, among which, basic possibilities (such as the configuration of environments with different operating systems), automation possibilities (related to the creation and control of computing resources using software) and optimization (relating to minimizing costs and even seeking the best computational performance for specific applications). In addition, it is possible to make comparisons of different settings, performance comparisons, and behavior of services when comparing different application behaviors in different operating systems and/or different combinations of hardware.

In this section, we have examined several materials, examples, scenarios, and use cases involving Docker containers and OpenStack services. We have seen how OpenStack allows the automatic management of virtual resources through a set of modules and interfaces and how Docker, in turn, allows the creation of portable and easily installable computing environments. We can improve container services on OpenStack through the utilization of the Magnum service and DelayedLoad. The combination of the flexibility of the OpenStack infrastructure services that are already well established in the market with the advanced configuration and management possibilities of the Docker containers make OpenStack and Docker an excellent solution for companies and educational institutions. For educational institutions, Nova, Neutron, Keystone, Glance, and Magnum have the ability to purchase computing and storage resources (IaaS) and control platform outputs when necessary, leaving computational resources free for use by their students.

Glossary of Terms

The hash of terms included here is simply an outcome of the operational investigating of resources briefly summarized within the section and possibly selected to hold the more widespread procedures in cloud technology. The most regularly used phrases by the community are used here and, when required, are defined using standard texts and Wikipedia, as those are generally accepted by industry and academia. Although results can be understood without references to any kind of resource and flow smoothly throughout the chapter, such references could be helpful for curious readers to dig deeper into specific areas that they particularly enjoy, ensuring the construction of a broad knowledge pool. As an unforeseen side effect of its own nature, this glossary is in perpetuum under updating. [17]

The essential purpose of this chapter is not to bother the reader with the more comprehensive terms, but to provide a reference to the non-normal concepts that might be fairly common in this region. It does not pretend to cover all the jargon and slang words used in literature, only the one frequently used to describe a generic term, a new technology, or an advancement in cloud computing. For the most profound understanding of the subject, it is also important to have an updated glossary of phrases(le) that cover the latest insights and experiments about cloud technologies. [63]

Additional Resources

Shelvino, F., & Tamm, G. (2010). Cloud computing -devastation or just blindness?. In 9th European Conference on e-Gov. Ljubljana, Slovenia.

Prasad, A., & Chana, ICSC, (2010). Towards an Ontology for Cloud Computing. In Proceedings of the 2010 EMIC, International Workshop for Educational and Engineering of Computer Science and ISE, Innovation in Software Engineering, PhD Forum.

Jung Woo, V., Hsin-Liu, K., Saurabh, K., Youngill, K., Raja, S., Eric, B., Kashi, V. (2009) Above the Clouds: A Berkeley View of Cloud Computing. Berkeley: University of California, Berkeley, Reliable Adaptive Distributed Systems Laboratory.

Galeri, D., & Gigante, J. M. (2010). Cloud Computing and its Environmental Impact. In Federation of Enterprise Architecture and Business Process Analysis (FEABIA), International Conference. Gävle, Sweden.

Emeakaroha, V., Brandic, I., Maurer, M., & Dustdar, S. (2010). Low Level Virtual Machine (LLVM) Live Migration and Workload Estimation Enhancements for Cloud Computing. In aP2PS'10, 2nd International Conference on Advances in P2P Systems. Barcelona, Spain.

Daugherty, Paul. (2009) "What the Enterprise needs to know about Cloud Computing." Gartner, Inc.

Anon (2009). An introduction to the financial analysis of cloud computing. The European Financials Analyst Project. Research Institute of Computer Science, Applied to the Economic Corporation (IRIT-IRISA), Université Toulouse I Capitole, Universities Rennes 1 and Rennes 2, France.

Assunção, M. D., da Silva Veith, Anca I., & Buyya, R. (2009). A cost-benefit analysis of Cloud Computing. In: Proceedings of the 18th International Heterogeneity in Computing Workshop. Washington, D.C.: IEEE Computer Society.

References:

- [1] N. Almurisi and S. Tadisetty, "Cloud-based virtualization environment for IoT-based WSN: solutions, approaches and challenges," 2022. ncbi.nlm.nih.gov
- [2] Q. Hu, "Optimization of Online Course Platform for Piano Preschool Education Based on Internet Cloud Computing System," 2022. ncbi.nlm.nih.gov
- [3] I. Sommerville, "Teaching cloud computing: a software engineering perspective," 2012. [\[PDF\]](#)
- [4] S. Qamar, N. Lal, and M. Singh, "Internet ware cloud computing :Challenges," 2010. [\[PDF\]](#)
- [5] A. Ometov, O. Liombe Molua, M. Komarov, and J. Nurmi, "A Survey of Security in Cloud, Edge, and Fog Computing," 2022. ncbi.nlm.nih.gov
- [6] J. Hassan, D. Shehzad, U. Habib, M. Umar Aftab et al., "The Rise of Cloud Computing: Data Protection, Privacy, and Open Research Challenges—A Systematic Literature Review (SLR)," 2022. ncbi.nlm.nih.gov
- [7] F. Boucenna, "Semantic, Efficient, and Secure Search over Encrypted Cloud Data," 2020. [\[PDF\]](#)
- [8] S. Benabied, A. Zitouni, and M. Djoudi, "A Cloud Security Framework Based on Trust Model and Mobile Agent," 2020. [\[PDF\]](#)
- [9] S. P. Mirashe and N. V. Kalyankar, "Cloud Computing," 2010. [\[PDF\]](#)
- [10] S. Ahmad, S. Mehfuz, F. Mebarek-Oudina, and J. Beg, "RSM analysis based cloud access security broker: a systematic literature review," 2022. ncbi.nlm.nih.gov
- [11] Q. Lu, X. Xu, H. M. N. Dilum Bandara, S. Chen et al., "Patterns for Blockchain-Based Payment Applications," 2021. [\[PDF\]](#)
- [12] C. Kelly, N. Pitropakis, A. Mylonas, S. McKeown et al., "A Comparative Analysis of Honeypots on Different Cloud Platforms," 2021. ncbi.nlm.nih.gov

- [13] R. Almajalid, "A Survey on the Adoption of Cloud Computing in Education Sector," 2017. [\[PDF\]](#)
- [14] R. Lakshminarayanan, B. Kumar, and M. Raju, "Cloud Computing Benefits for Educational Institutions," 2013. [\[PDF\]](#)
- [15] A. Anasuya Threse Innocent, "Cloud Infrastructure Service Management - A Review," 2012. [\[PDF\]](#)
- [16] J. Kwao Dawson, F. Twum, J. Benjamin Hayfron Acquah, and Y. Marfo Missah, "Ensuring confidentiality and privacy of cloud data using a non-deterministic cryptographic scheme," 2023. ncbi.nlm.nih.gov
- [17] N. Singh, M. Raza, V. Vardhan Paranthaman, M. Awais et al., "Internet of Things and cloud computing," 2021. ncbi.nlm.nih.gov
- [18] R. Fouad AlCattan, "Integration of Cloud Computing and Web2.0 Collaboration Technologies in E-Learning," 2014. [\[PDF\]](#)
- [19] R. Shyam Thakur, R. Bandopadhyay, B. Chaudhary, and S. Chatterjee, "Now and Next-Generation Sequencing Techniques: Future of Sequence Analysis Using Cloud Computing," 2012. ncbi.nlm.nih.gov
- [20] R. Buyya and K. Sukumar, "Platforms for Building and Deploying Applications for Cloud Computing," 2011. [\[PDF\]](#)
- [21] M. Rizwan Ali, F. Ahmad, M. Hasanain Chaudary, Z. Ashfaq Khan et al., "Petri Net based modeling and analysis for improved resource utilization in cloud computing," 2021. ncbi.nlm.nih.gov
- [22] R. Gong, N. Ge, and J. Li, "Real-Time Detection of Body Nutrition in Sports Training Based on Cloud Computing and Somatosensory Network," 2022. ncbi.nlm.nih.gov
- [23] G. Briscoe and A. Marinos, "Digital Ecosystems in the Clouds: Towards Community Cloud Computing," 2009. [\[PDF\]](#)
- [24] I. Fé, R. Matos, J. Dantas, C. Melo et al., "Performance-Cost Trade-Off in Auto-Scaling Mechanisms for Cloud Computing †," 2022. ncbi.nlm.nih.gov

- [25] D. Timur Mirzoev and R. Alvarez, "Leveraging VMware vCloud Director Virtual Applications (vApps) for Operational Expense (OpEx) Efficiency," 2014. [\[PDF\]](#)
- [26] A. S. Ibrahim, J. Hamlyn-Harris, and J. Grundy, "Emerging Security Challenges of Cloud Virtual Infrastructure," 2016. [\[PDF\]](#)
- [27] N. Asiri, "Security and Privacy Issues in Cloud Storage," 2024. [\[PDF\]](#)
- [28] P. Kumar Shukla, A. Aljaedi, P. Kumar Pareek, A. R. Alharbi et al., "AES Based White Box Cryptography in Digital Signature Verification," 2022. ncbi.nlm.nih.gov
- [29] J. Becerra Guerrero, G. López Pérez, and A. Rueda Zoca, "Some results on almost square Banach spaces," 2015. [\[PDF\]](#)
- [30] J. Sen, S. Zhao, X. Wang, G. Zhang et al., "Cloud Computing - Architecture and Applications," 2017. [\[PDF\]](#)
- [31] N. Cong Luong, P. Wang, D. Niyato, W. Yonggang et al., "Resource Management in Cloud Networking Using Economic Analysis and Pricing Models: A Survey," 2017. [\[PDF\]](#)
- [32] M. Mirza, M. Kratz, D. Medeiros, J. Pina et al., "Building the Foundations of an Informatics Agenda for Global Health - 2011 Workshop Report," 2012. ncbi.nlm.nih.gov
- [33] K. Jungck and S. Rahman, "Cloud Computing Avoids Downfall of Application Service Providers," 2015. [\[PDF\]](#)
- [34] D. Mukhopadhyay, G. Sonawane, P. Sarthi Gupta, S. Bhavsar et al., "Enhanced Security for Cloud Storage using File Encryption," 2013. [\[PDF\]](#)
- [35] S. Kumar, M. Abdul Wajeed, R. Kunabeva, N. Dwivedi et al., "Novel Method for Safeguarding Personal Health Record in Cloud Connection Using Deep Learning Models," 2022. ncbi.nlm.nih.gov
- [36] A. M. Alwakeel, "An Overview of Fog Computing and Edge Computing Security and Privacy Issues," 2021. ncbi.nlm.nih.gov

- [37] D. Sikeridis, I. Papapanagiotou, B. Prasad Rimal, and M. Devetsikiotis, "A Comparative Taxonomy and Survey of Public Cloud Infrastructure Vendors," 2017. [\[PDF\]](#)
- [38] W. Yu and J. Chen, "The state-of-the-art in web-scale semantic information processing for cloud computing," 2013. [\[PDF\]](#)
- [39] S. Ilager and R. Buyya, "Energy and Thermal-aware Resource Management of Cloud Data Centres: A Taxonomy and Future Directions," 2021. [\[PDF\]](#)
- [40] B. Bhandari and J. Zheng, "A Preliminary Study On Emerging Cloud Computing Security Challenges," 2018. [\[PDF\]](#)
- [41] G. D'Angelo, S. Ferretti, and M. Marzolla, "Cloud for Gaming," 2015. [\[PDF\]](#)
- [42] S. Goyal, S. Bhushan, Y. Kumar, A. ul Hassan S. Rana et al., "An Optimized Framework for Energy-Resource Allocation in a Cloud Environment based on the Whale Optimization Algorithm," 2021. ncbi.nlm.nih.gov
- [43] R. Nair, S. Nasrullah Zafarullah, P. Vinayasree, P. Singh et al., "Blockchain-Based Decentralized Cloud Solutions for Data Transfer," 2022. ncbi.nlm.nih.gov
- [44] W. Pourmajidi, L. Zhang, J. Steinbacher, T. Erwin et al., "A Reference Architecture for Observability and Compliance of Cloud Native Applications," 2023. [\[PDF\]](#)
- [45] A. Aggarwal, S. Kumar, A. Bhatt, and M. Asif Shah, "Solving User Priority in Cloud Computing Using Enhanced Optimization Algorithm in Workflow Scheduling," 2022. ncbi.nlm.nih.gov
- [46] S. Mishra and S. Kumar Panda, "Cloud Computing: Applications, Challenges and Open Issues," 2023. [\[PDF\]](#)
- [47] H. Li, "Computer Security Issues and Legal System Based on Cloud Computing," 2022. ncbi.nlm.nih.gov

- [48] D. Bermbach, A. Chandra, C. Krintz, A. Gokhale et al., "On the Future of Cloud Engineering," 2021. [\[PDF\]](#)
- [49] M. Whaiduzzaman, A. Barros, M. Chanda, S. Barman et al., "A Review of Emerging Technologies for IoT-Based Smart Cities," 2022. ncbi.nlm.nih.gov
- [50] Z. L. Shao, C. Huang, and H. Li, "Replica selection and placement techniques on the IoT and edge computing: a deep study," 2021. ncbi.nlm.nih.gov
- [51] S. Ali, undefined Abdullah, T. Poupi Theodore Armand, A. Athar et al., "Metaverse in Healthcare Integrated with Explainable AI and Blockchain: Enabling Immersiveness, Ensuring Trust, and Providing Patient Data Security," 2023. ncbi.nlm.nih.gov
- [52] N. A Angel, D. Ravindran, P. M Durai Raj Vincent, K. Srinivasan et al., "Recent Advances in Evolving Computing Paradigms: Cloud, Edge, and Fog Technologies," 2021. ncbi.nlm.nih.gov
- [53] V. N. Potapov, "Constructions of Pairs of Orthogonal Latin Cubes," 2019. [\[PDF\]](#)
- [54] R. H. Weber and D. Staiger, "Part 3: Practical Implementation of Data Protection Environment," 2017. ncbi.nlm.nih.gov
- [55] L. kacha and A. Zitouni, "An Overview on Data Security in Cloud Computing," 2018. [\[PDF\]](#)
- [56] B. de Bruin and L. Floridi, "The Ethics of Cloud Computing," 2017. ncbi.nlm.nih.gov
- [57] N. Kratzke and R. Peinl, "ClouNS - A Cloud-native Application Reference Model for Enterprise Architects," 2017. [\[PDF\]](#)
- [58] A. Bisong, undefined Syed, and M. Rahman, "An Overview of the Security Concerns in Enterprise Cloud Computing," 2011. [\[PDF\]](#)

- [59] B. Magotra, D. Malhotra, and A. Kr. Dogra, "Adaptive Computational Solutions to Energy Efficiency in Cloud Computing Environment Using VM Consolidation," 2023. ncbi.nlm.nih.gov
- [60] Y. Kalyani and R. Collier, "A Systematic Survey on the Role of Cloud, Fog, and Edge Computing Combination in Smart Agriculture," 2021. ncbi.nlm.nih.gov
- [61] C. Stab and I. Gurevych, "Parsing Argumentation Structures in Persuasive Essays," 2016. [\[PDF\]](#)
- [62] S. Singh Gill, M. Xu, C. Ottaviani, P. Patros et al., "AI for Next Generation Computing: Emerging Trends and Future Directions," 2022. [\[PDF\]](#)
- [63] I. Sriram and A. Khajeh-Hosseini, "Research Agenda in Cloud Technologies," 2010. [\[PDF\]](#)