COEN 329 NETWORK TECHNOLOGY

Project : Cloud Computing

Project submitted by
Benita Rego
ID: W1628656

Nolita Rego
ID: W1628657

Date : 7th November 2021

Under the guidance of Prof. Dr. Keyvan Moataghed

Audience

The focus of the topic "Cloud Computing" focuses on the concept of cloud computing security, with support for the protection and recovery of privileged users, research support, and cloud computing security based on long-term viability. Gives a comprehensive overview. Furthermore, the topic covers data security in cloud computing which emphasizes on cloud service that ensures the data integrity, privacy and protection.

This document covers the architecture, literature review followed by cloud security, data security and privacy, robust cloud security, types of cloud types and deployment models, different cloud automation tools, big data, cloud cryptography, load balancing, containerization, top cloud providers and applications of cloud computing. The literature review section discusses in detail various research papers that describe in detail about the different automation tools with comparison and other features of cloud computing.

The reader is expected to have basic knowledge of networks to be able to understand the architectures and other features of cloud computing. Some background in the field of AWS and other cloud providers is desired to have a better understanding of cloud computing.

This document can be used by cloud engineers, system architects, designers, developers, analysts, business analysts, academicians, researchers and technical authors.

Table of Contents

Table of Figures:

Table of Tables:

1

1. Introduction

We live in a world that is always changing; as a result, every business and corporation is changing as well, and their operations are changing as well. Maintaining our own servers becomes difficult and expensive as scalability, availability, and large volumes of data become commonplace. In this case, cloud computing plays a key role in lowering costs and allowing us to focus on the business challenge rather than the system's architecture. Cloud security, on the other hand, is a big concern with cloud computing.

A growing number of users, ranging from organizations to individuals, are turning to cloud computing. According to a Right Scale 1 poll, the average user utilizes at least four cloud-based applications at any given time and is exploring four more. According to the survey, 41% of commercial firms use public clouds to operate a considerable workload. Cloud computing security is becoming more of a problem as more of our responsibilities are shifted to the cloud. This conclusion is supported by a Forbes 2 report from 2017, which predicts that while cloud solutions will account for 80% of all IT budgets in 15 months, 49% of businesses are delaying cloud adoption due to security skills gaps and concerns. Lack of well-trained resources, maturity, conflicting best practices, and complex business frameworks seem to be part of the problem, to name a few factors. Cloud adoption has reached a turning point as the majority, if not all, for-profit companies, not just the average Internet user, are expected to move more workloads from traditional on-premises storage to the cloud. I am. While there are other concerns to be recognized, investigated, and solved, this document focuses on Cloud computing security, which reflects multiple security vulnerabilities and solutions.

One of the most basic definitions of cloud computing is "a network solution that provides affordable, reliable, simple and easy access to IT resources." Cloud computing not only reduces operational and infrastructure costs, but also gives consumers more freedom and improves performance. Security and data protection are important concerns when storing data in the cloud. Maintaining data integrity, data protection, and security is important for cloud services. Several service providers use various policies and techniques for this goal, depending on the nature, kind, and quantities of data. This article examines how data security is used to protect and secure data in the cloud around the world. It goes over the primary security concerns and the solutions that various service providers have used to protect data.

1.1. Objective

Cloud computing has become a major study topic in both academia and industry.Cloud computing benefits both cloud service providers (CSPs) and users. Security concerns related to cloud computing have been thoroughly studied in the literature. The purpose of this Systematic Literature Search (SLR) is to review current research on the security, risks, and concerns of Cloud Computing. From 2010 through 2020, this SLR looked at research findings published in popular digital libraries. We chose 80 papers to answer the study topics after a thorough examination of current literature. As a result of its findings, this SLR identified Seven Key Security Risks for Cloud computing services. According to the results, data manipulation and breaches were two of the most enthusiastic and controversial topics in the literature. Both data intrusion and data storage have been identified as security flaws in cloud computing environments. According to the results of this SLR, outsourcing of consumer data remains a problem for both CSPs and cloud users. In our survey, the blockchain was identified as a collaborative technology for addressing security issues. The SLR's conclusions include a number of suggestions for future work to protect data security, integrity, and availability.

1.2. Scope

The concept of cloud computing was born out of the distributed software architecture. The purpose of cloud computing is to provide Internet-based hosted services. Cloud Computing has created a number of new user groups and marketplaces in the field of information technology in recent years. Cloud computing services are provided through data centers throughout the world. Microsoft SharePoint and Google Apps are two examples of cloud computing services. security of cloud computing services is an important factor in adopting them. The extant literature focuses on a wide range of security solutions, including technology and policy implementation. The latter study provided additional attacks on the cloud environment from a criminological stance. The proposed reaction to these latest cyber-attacks is based on cloud security criminal ideas. A study [1] discovered several security vulnerabilities that influence cloud computing features. The same study proposes a remedy to the observed cloud security problems. As part of the study, a security guide was prepared to help cloud users understand security weaknesses and attack methodologies.

The use of cloud computing services introduces security challenges and vulnerabilities. The main cause of these issues and vulnerabilities is currently cloud computing models. An attacker exploits a weakness in the cloud model to capture private data from a customer by attacking the processing power of a computer system. The Autonomous Cloud Intrusion Response System (ACIRS) was recently introduced to address the issues mentioned above. Prior to this investigation, the Network Intrusion Detection and Countermeasure Selection System (NICE) worked to determine the best course of action to limit the risk of cloud virtual networks. ACIRS is superior to NICE when it comes to mitigating network risks and problems. Cloud computing (CC) is often used in the field of information technology.However, because essential security technologies have not yet evolved, many service providers are still unwilling to completely deploy the CC. As a result, research shows that service providers should invest in the security of CC-related devices. A few articles that support the investigation of cloud computing security ideas have been uncovered. One of these researches examines security risks and vulnerabilities using an "attack tree map" (ATM). According to study, CC is used in conjunction with the trusted computing platform to provide security services such as confidentiality, authentication, and integrity.

2

2. History

The concept of cloud computing isn't new. Grid computing, utility computing, application service provision, and software as a service are just a few of the stages that cloud computing has gone through. The overarching (overall) concept of supplying Computing resources via a worldwide network, however, was born in the 1960s. By 2020, the cloud computing market is anticipated to be worth $241 billion. Cloud computing explains how you get to the point and how it all began.

The first business and consumer Cloud Computing services websites, hence Cloud computing has a relatively short history. Cloud computing is intrinsically related to the development of the Internet and business technology since it is the solution to the conundrum of how the Internet can help enhance company technology. Business technology has a long and fascinating history, almost as long as business itself, but it was the arrival of computers as real-world solution providers that had the most impact on the history of Cloud computing.

John McCarthy, a computer scientist, came up with the concept of time sharing in the early 1960s, allowing businesses to use a pricey mainframe at the same time. This computing is credited with making a key impact to the development of the Internet as well as being a forerunner to Cloud computing. J.C.R. Licklider, who was important for enabling the creation of ARPANET, proposed the concept of an "Intergalactic Computer Network" or "Galactic Network" (a computer networking concept comparable to today's Internet) in 1969.

(Advanced Research Projects Agency Network).His ambition was for the entire world to be connected, and for people to be able to access programs and data from any location, at any time. In 1970, virtualization tools such as VMware made it possible to run many operating systems in a single isolated environment. A entirely distinct computer (virtual machine) could be run inside a different operating system.

In 1997, Prof. Ramnath Chellappa of Dallas, Texas, coined the term "Cloud Computer," defining it as "a computer paradigm whose processing constraints will be defined by economic rationale rather than technical limits alone." Salesforce.com, founded in 1999, was the first startup to deliver business software through a simple website. The services company paved the door for both specialized and big software companies to sell their products online.

In 2003, the first public version of Xen was launched, which generates a Virtual Machine Monitor (VMM), commonly known as a hypervisor, a software system that allows many virtual guest operating systems to run simultaneously on a single machine. In 2006, Amazon expanded its cloud services. The first was Amazon's Elastic Compute Cloud (EC2), which allowed customers to connect to cloud servers and run their own applications.

After that, the Simple Storage Service was introduced (S3). As a result, the pay-as-you-go concept was introduced to both users and the industry as a whole, and it has since become standard practice. In 2013, the global market for public cloud services reached £78 billion, up 18.5 percent from 2012, with IaaS (infrastructure-as-a-service) being the fastest-growing market offering. Spending on cloud infrastructure and services by businesses worldwide is estimated to exceed £103.8 billion in 2014, up 20% from 2013. (According to Constellation Research).

3

3. Literature Review

3.1. Cloud Computing Security – Trends and Research Directions [2]

In this case, cloud computing plays a key role in lowering costs and allowing us to focus on the business challenge rather than the system's architecture. Cloud security, on the other hand, is a big concern with cloud computing. Cloud security is primarily concerned with cloud infrastructure, software platforms, and user data, as well as access control and identity management.

Common Concerns :

1. Insecure physical and software infrastructure: Here, concerns like the physical and software security of data centers are taken into consideration, as the containers are hosted on common software stacks, also due to the security concerns of the API's provided by the cloud provider.
2. Data Security in the Cloud: Data integrity, confidentiality and privacy, as well as provenance, are the most important concerns in cloud computing. Some important problems here are how data is kept private, how data is prevented from being locked, data security and integrity when several cloud parties are involved in processing.
3. Access to cloud services: User authentication, authorization and access control are one of the most crucial concerns when it comes to cloud computing. It includes unauthorised access, multi level authentication levels, multi-cloud data access etc.

3.2. A Comprehensive Survey on Security in Cloud Computing [3]

This publication compiles a number of peer-reviewed studies on cloud computing security threats and countermeasures. Our research aims to better understand cloud components, security challenges, and hazards, as well as new solutions that could help alleviate cloud vulnerabilities. Nonetheless, the impression of cloud security is that it requires considerable upgrades in order to achieve higher rates of adaptability at the business scale. Many of the challenges surrounding cloud computing, as noted by another study, need to be remedied immediately. The industry has made great progress in combating cloud computing threats.

These concerns, as well as other potential hazards, should be evaluated and addressed. The following are some examples of possible assessments:

A. Organizational capabilities and maturity
B. Risks associated with technology and data
C. Application migration and performance risk
D. People hazards
E. Process dangers
F. Policy dangers
G. Risks associated with a longer supply chain

3.3. Data Security in Cloud Computing [4]

Data security in cloud computing requires more than just data encryption. Data confidentiality and integrity are determined by the tools, procedures, and processes used to protect data. There are two types of data in the cloud that constitute a security risk. Depending on the nature, type, and quantity of data, a variety of policies and approaches are used by various service providers to achieve this goal. This article examines how data security is used to protect and secure data in the cloud around the world. It covers the main security concerns as well as the solutions utilized by various service providers to protect data. There are two types of data that constitute a security concern in most clouds:

1. Data at Rest: Data in the cloud, or any data that can be accessed via the Internet, is referred to as "cloud data." This includes both backup and live data. Because they do not have physical control over the data, it can be difficult for enterprises to protect data at rest if they do not maintain a private cloud. This problem can be remedied, though, by maintaining a private cloud with tightly regulated access.

2. Data in Transit (which means the data stored in the cloud): Data that is traveling in and out of the cloud is referred to as this. This data can be in the form of a cloud-based file or database that can be requested for use at a different location. When data is uploaded to the cloud, it is referred to as data in transit at the time of upload. Data in transit might include highly sensitive information such as usernames and passwords, and it is sometimes encrypted; nonetheless, data in unencrypted form is also in transit.

3.4. Devops a new approach to cloud development and testing [5]

DevOps is a combination of software development and information technology. Its mission is to shorten the system development life cycle and create high quality software on a regular basis.

The connections between DevOps and cloud computing are straightforward:

- The centralized aspect of cloud computing provides a uniform and centralized platform for testing, deployment, and production for DevOps automation. The distributed nature of some enterprise systems used to make centralized software distribution difficult. Many challenges with dispersed complexity can be solved by using a cloud platform.
- DevOps automation is moving to the cloud. On the platform, most public and private cloud computing providers enable DevOps extensively, including tools for continuous integration and continuous development. This tight integration reduces the cost of local DevOps automation while providing centralized governance and control for the success of the DevOps process. Many developers running the process have found that governance does not cause any problems. It's easier to centrally manage from the cloud than to regulate departments.
- The requirement to account for resources used is reduced with cloud-based DevOps. Utilization-based accounting is used in cloud computing to measure resource usage by application, developer, user, data, and so on. This is a service that most traditional systems do not supply. It's considerably easier to track development resource expenditures and make modifications when you use cloud-based resources.

Why is it Important to Automate various Cloud Operations?

Cloud service providers have made it easy for enterprises to gain computing power and storage space on demand, but nothing has been done to minimize the responsibilities associated with managing cloud infrastructure. Hmm. Traditionally, delivering and operating cloud workloads has been a time-consuming process that necessitated extensive manual configuration by IT administrators. Configuring virtual machines, creating VM clusters, configuring virtual networks, and controlling availability and performance were all done manually. One hundred virtual machines would need to be configured one by one if a task needed it.

Today, IT businesses employ cloud orchestration and cloud automation solutions to automate repetitive operations like provisioning virtual resources, defining common configuration items, and constructing infrastructure as code. Developers can use cloud orchestration software products to codify the process of workload deployment and management so that it can be simply repeated in the future. Cloud automation software products take those scripted processes and execute them on their own, with little or no assistance from IT staff. Figure 1 describes the pipeline of DevOps in planning, coding, building and deploying.

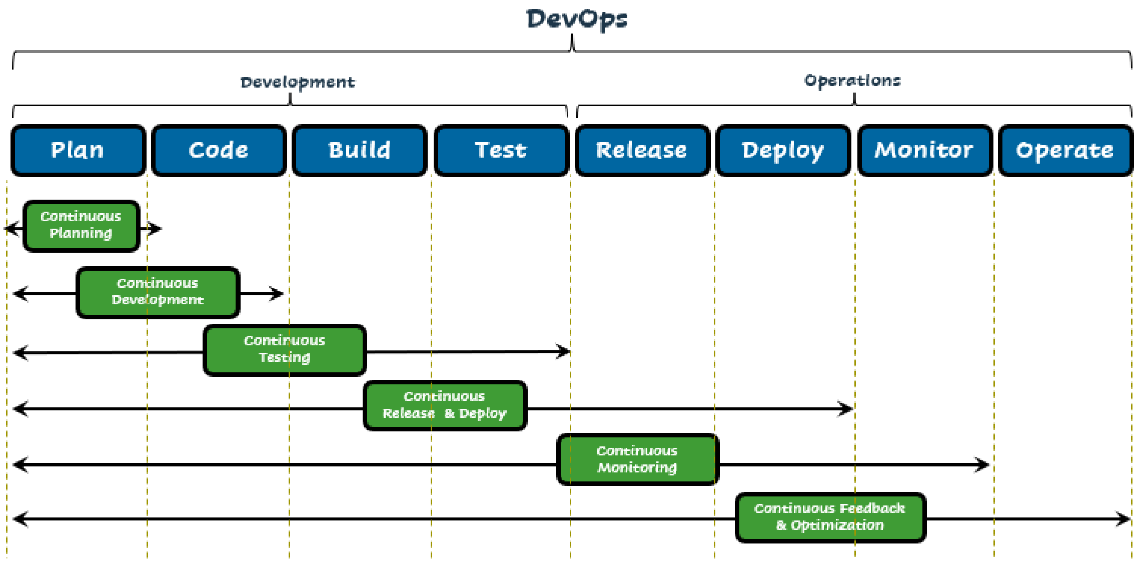


Figure 1. DevOps

3.5. Review of Cloud Automation Tools [6]

Cloud automation is a software solution that allows developers and IT professionals to install, configure, and administer cloud computing services. It enables enterprises to select the appropriate amount of cloud computing resources. It can be used to manage workloads and track application and workload performance. It's a cloud-based IT software solution that's available for free.

3.6. Performance Comparison of Terraform and Cloudify as Multicloud Orchestrators [7]

The cloud orchestrator is a platform for developers to create infrastructure descriptors, and the orchestra follows for autonomous deployment without user interaction. This will make sure that the developer has an updated and tested infrastructure descriptor that can be used to start the infrastructure deployment process by simply providing the orchestrator with the infrastructure description code.

Cloud Orchestrators are a platform where a developer produces an infrastructure descriptor that the orchestrator uses to deploy autonomously without the need for user participation. This ensures that developers have access to an updated and tested infrastructure descriptor, allowing them to start the infrastructure deployment process by simply submitting the infrastructure descriptive code to the orchestrator.

Cloudify:

- Application modeling is a broad phrase that refers to an application and all of its components (infrastructure, middleware, application code, scripts, tool settings, metrics, and logs). The Cloudify language is built on TOSCA (Topology and Orchestration Specification for Cloud Applications) (uses XML and YAML definitions)
- Orchestration is the process of maintaining and running applications. It is possible to execute continuous actions such as scaling, fetching, and maintaining in addition to instantiation.
- Provides a system-wide abstraction of reusable components. For configurations such as management tools, the ability to represent anything in a descriptive language is essential.
- Security - Cloudify Manager uses SSL, which allows clients to verify its validity and ensure that data sent to and from it is encrypted.

Terraform:

- Terraform is a HashiCorp open source technology that allows infrastructure to be defined as code using a simple declarative programming language.
- With just a few keystrokes, you can build and manage this architecture across several public cloud providers (such as AWS, Azure, Google Cloud, and DigitalOcean), as well as private virtualization systems (such as OpenStack and VMWare).
- It also allows you to import existing resources and only target certain ones.
- Plugins make it even more extensible.

GLOBAL RESOURCE ALLOCATION

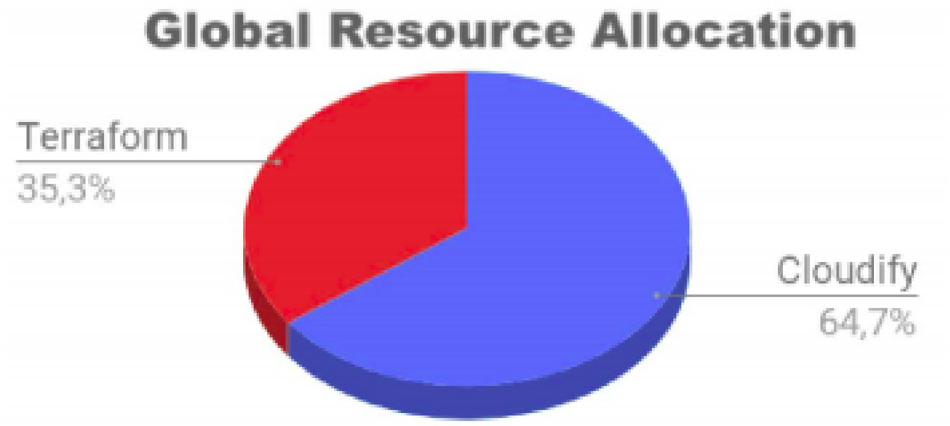


Figure 2. Global Resource Allocation

Figure 2 is a graph that depicts how all of the computational resources used in this experiment were distributed across the orchestrators. Cloudify assigned around 2/3 of the resources used in the process, whereas Terraform only needed 13 of these features to complete the identical operation.

CPU AVERAGE USAGE

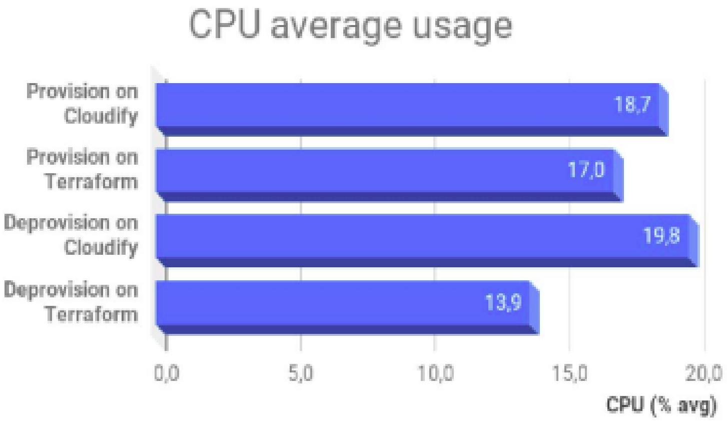


Figure 3. CPU Average Usage

Figure 3 is a graph that describes the following: In the trial situation, Cloudify was less efficient than Terraform, notably in terms of CPU utilization.

AVERAGE EXECUTION TIME

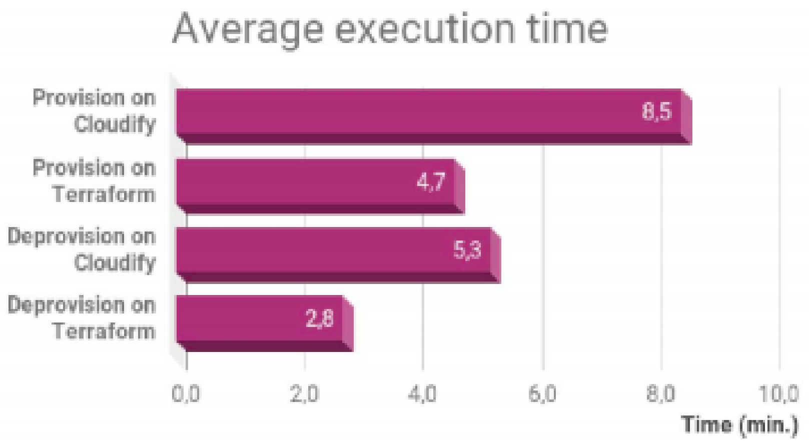


Figure 4. Average execution time

Figure 4 is a graph that describes how Terraform has outperformed Cloudify by 44 percent on the provisioning task. The test environment was provisioned in an average of 4.7 minutes using Terraform and 8.5 minutes with Cloudify. Similarly, Terraform completed the deprovisioning procedure 47 percent faster than Cloudify on average.

I/O AVERAGE ACTIVITY

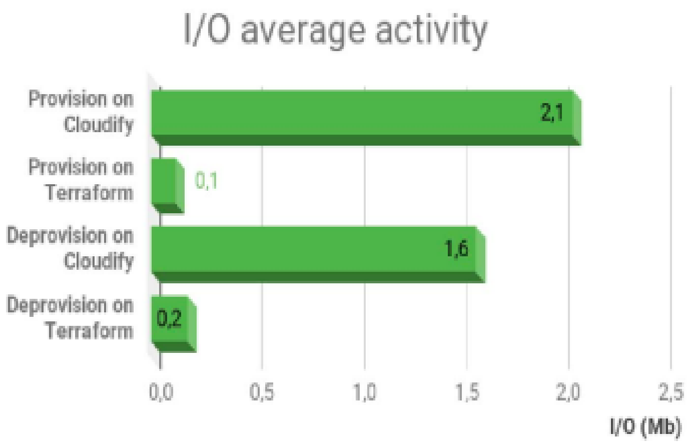


Figure 5. I/O average activity

Figure 5 describes the average disk activity in Cloudify and Terraform. The most noticeable difference is in I/O disk activity. Terraform had modest disk activity on average, accumulating between 0.1 and 0.2 megabytes during the procedures. While Cloudify gathered between 1.6 and 2.1 MB.

Result of Comparison:

- During the experiment that approximated actual orchestration use, the comparison between Cloudify and Terraform revealed a significant gap between these tools.
- Not only does Cloudify consume more resources from the host environment, but it also takes longer to complete tasks than Terraform.
- Cloudify does not support numerous cloud services that are already commonly utilized.
- Terraform showed a remarkable level of maturity during the testing for this project, particularly in terms of error handling and delta operations.
- In addition, a large number of well-documented features and plugins add to the technology stack of this promising application.

3.7. Cloud Computing: Fundamentals and Research Issues [16]

There is a chance that the data-holding machine will fail, resulting in data loss. There's also the possibility of data leakage, which occurs when data slips into the wrong hands, such as hackers or criminals. Aside from that, because the majority of the machines are public, your infrastructure is at danger of data corruption and networking failure. The risk of sensitive data or files being compromised increases with cloud computing. In the prior setup, the access structure was always visible to the CSP. As a result, any hacker or rogue CSP can easily gain access to user information. When using cloud computing, users don't have to worry about software, hardware, or any other external equipment. Users have no idea where their information is stored on cloud servers. Cloud computing provides users with a data-sharing infrastructure. Both the owner and the users are involved.

Users can access the data or files that the Data Owner (DO) has stored on the cloud server. Before any data or services may be accessed, the Cloud Service Provider (CSP) must explain the access control policies. To provide a requested resource to a user, a mapping of access controls between the CSP and organizations with accessible resources is necessary. It's never too late to learn something new.

Features of Cloud Computing:

- Agility: The environment of a system can be changed during any transaction. "Agility" refers to a system's capacity to respond swiftly to its changing surroundings.
- Reliability: The use of multiple sites boosts the reliability.
- Resiliency: Cloud server failures and persistent data storage failures may be ignored by a CSP.
- Performance: In cloud computing, web services are utilized to track performance. The CSP can keep an eye on the cloud server's activity.

To deal with data loss due to machine failure, we can save backups of the data on other machines and save the data using distributed computing techniques, so that even if one system fails, the data can still be accessed from the next available replica of that machine. To combat data leaks and uncontrolled access from the public internet, important data might be stored in a private cloud environment that is only accessible from within the private network, effectively protecting crucial data from the public internet. A new model could be created to handle the access structure problem while maintaining high security.

3.8. Cloud Computing Features, Issues and Challenges: A Big Picture [17]

Since the concept of cloud computing was first presented, there has been a burgeoning interest in studies all over the world. This rapid shift to Cloud computing has sparked worries about a crucial aspect of information systems, communication, virtualization, data availability and integrity, public auditing, scientific application, and information security. As a result, cloud computing research has gotten a lot of attention in recent years. There are also a number of security vulnerabilities in cloud computing that are related to the service layer.

Computing resources have grown cheaper, more powerful, and more widely available than ever before, thanks to the popularity and quick growth of processing and storage technologies, as well as the success of the Internet. Marketing has a tendency to guarantee features that are easily confused with qualities that have diverse implications in other sectors, perhaps leading to cloud. As a result, a detailed characterization of cloud application features is critical for the cloud framework's future development.

This framework sharing, along with the fact that cloud customers require control over the cloud foundation, poses significant security concerns. Clouds have diverse architectures depending on the services they deliver to tackle such difficulties.

Characteristics of Cloud Computing:

- On-demand self-service: By registering, resources can be obtained and used whenever they are needed, without the need for human interaction with cloud administration providers. Processing power, storage, virtual machines, and other computing resources are all examples of computing resources.

- Resource pooling: Cloud administration providers pool their resources, which are then distributed to a large number of customers.
- Rapid elasticity: By scaling out, a client can quickly get more cloud resources and then scale back in by discharging those resources when they are no longer needed.

Service models of cloud computing:

- IaaS (Infrastructure as a Service): provides the flexibility, stability, and scalability that many businesses desire from the cloud while eliminating the need for office hardware. This makes it excellent for small and medium-sized businesses searching for a low-cost IT solution to help them expand.
- PaaS (Platform-as-a-Service): This is a cloud computing model in which cloud computing providers provide infrastructure and software frameworks, but enterprises design and run their own applications. PaaS allows users to construct web apps fast and easily, and the service is versatile and reliable enough to support them. PaaS solutions are scalable, making them excellent for businesses with several developers working on a single project.
- Software as a Service (SaaS): This cloud computing solution entails the distribution of software via the internet to a variety of organizations who pay via subscription or pay-per-use. It's a great tool for CRM and apps that require a lot of web or mobile access.

Security and data accessibility are the two primary research gaps in the aforementioned studies. To boost security, consider combining blockchain with cloud computing so that each request is tokenized with a unique identification that the servers can recognize and send duties to the client instantaneously. Cloud cryptography, which is currently a research area and has significant utility if implemented effectively, can be used to improve accessibility.

4

4 . Architecture

In cloud computing architecture, the front-end and back-end are separated. [8] The front-end and back-end are linked by a network or the internet. The technology components that are combined to create a cloud, in which resources are pooled and shared across a network using virtualization technologies, are referred to as cloud architecture.

The following elements make to a cloud architecture:

A front-end development platform (the client or device used to access the cloud.) One or more back-end platforms may exist (servers and storage). The use of the cloud as a delivery mechanism. A network connects all cloud clients, servers, and storage. These technologies combine to create a cloud computing infrastructure on which applications can run, allowing end users to access cloud resources. Although the name "cloud computing" is new (it was coined in the twenty-first century), the concept is quite similar to mainframe computing, which has been popular since the 1960s and included centralized servers running applications for "dumb" terminals connected to a private network.

The following figure 6 is a diagrammatic illustration of cloud computing architecture:

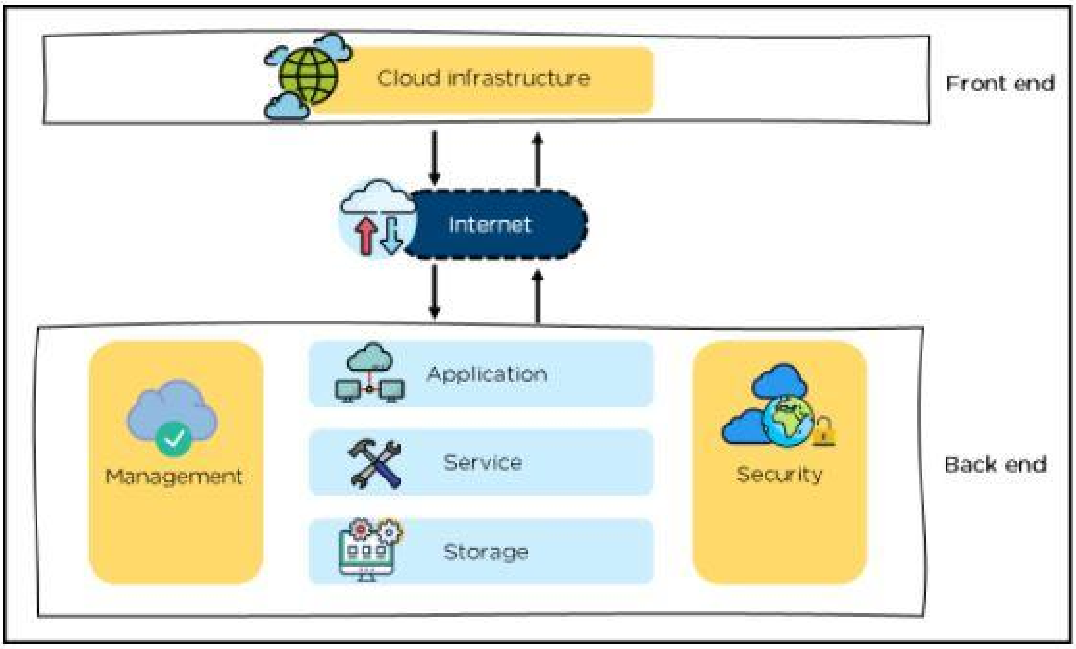


Figure 6. Architecture

Front-end: It provides the necessary apps and interfaces for the cloud-based service. Client-side apps, such as web browsers like Google Chrome and Internet Explorer, make up this system. The only component of the front-end is cloud infrastructure. Let's take a closer look at it. Data storage, servers, virtualization software, and other hardware and software components make up cloud infrastructure. It also gives end-users a graphical user interface via which they may do their jobs.

Back-end: Responsible for tracking all programs running the application on the front end. There are quite a few servers and data storage systems. The back end is an important part of the cloud computing architecture. The back-end cloud architecture's components are listed below.

Despite the fact that no two clouds are the same, there are a few common cloud architectural models. Public, private, hybrid, and multi-cloud architectures are among them. Here's how they stack up:
A public cloud architecture is one in which computing resources are owned and maintained by a cloud services provider. The Internet is used to exchange and redistribute these resources among multiple tenants. Reduced operational expenses, easy scalability, and little to no maintenance are among advantages of the public cloud.
Computing resources are owned and operated by a cloud service provider in a public cloud architecture. The Internet is used to exchange and redistribute these resources between multiple tenants. Reduced operational expenses, easy scalability, and minimal maintenance are all advantages of using the public cloud.
A hybrid cloud system combines the public cloud's operational efficiencies with the private cloud's data security features. Hybrid clouds consolidate IT resources by combining public and private cloud architectures, allowing enterprises to shift workloads between environments based on their IT and data security needs.
A multi-cloud architecture is one that makes use of a number of different public cloud services. A multi-cloud architecture provides more flexibility in terms of selecting and deploying cloud services that are most likely to meet varying organizational requirements. Another benefit is less reliance on a single cloud services vendor, which means more cost savings and less risk of vendor lock-in. Multi-cloud architecture may also be necessary to support microservices-based containerized systems with services distributed across several clouds.

The basic principles of cloud architecture are as follows:

1. **Virtualization:** Virtualization of servers, storage, and networks is the foundation of cloud computing. Virtualized resources are software-based (or virtual) representations of physical resources like servers or storage. Multiple applications can use the same physical resources thanks to this abstraction layer, which improves the efficiency of servers, storage, and networking across the company.

2. **Infrastructure:** There are genuine servers present in the infrastructure. Cloud infrastructure includes all of the elements found in traditional data centers, such as servers, persistent storage, and networking equipment like routers and switches.

3. **Middleware:** These software components, which include databases and communications applications, allow networked computers, applications, and software to communicate with one another in the same way that traditional data centers do.

4. **Management:** These technologies allow for constant monitoring of the performance and

capacity of a cloud system. From a single console, IT engineers can find out the usage, develop new applications, integrate data, and ensure disaster recovery.

5. **Automation software:** Using automation and predefined policies to offer important IT services can drastically reduce IT workloads, streamline application delivery, and lower costs. Automation is used in cloud architecture to easily scale up system resources to handle a surge in computing power demand, deploy applications to meet shifting market demands, and assure governance throughout a cloud environment.

4.1. Benefits and Adoption of Cloud Architecture

Because of three various forms of cloud architecture, businesses are shifting to the cloud. Each of these has its own set of advantages and distinguishing characteristics.

Software as a Service (SaaS):

SaaS architecture suppliers supply and manage programs and software to businesses over the Internet, removing the requirement for end users to install software locally. SaaS apps are often accessed using a web interface that is accessible from a wide range of devices and operating systems.

Platform as a Service (PaaS):

As a service, the service provider provides a computer platform and solution stack, which often includes middleware. Organizations can build applications or services on top of that platform. The cloud service provider provides the networks, servers, and storage needed to run an application, but the end user is responsible for installing and configuring the program.

Infrastructure as a Service (IaaS):

By supplying the essential infrastructure, a third-party supplier reduces the need for enterprises to purchase servers, networks, or storage devices. As a result, businesses can better manage their software and applications while only paying for the capacity they use at any given time.

The adoption of cloud architecture is motivated by a variety of factors.

- Improve the time it takes for new apps to be released.
- To update apps and expedite digital transformation, use cloud-native architecture like Kubernetes.
- Check to see if the most recent regulations are being followed.
- Increase resource transparency to reduce expenses and avoid data breaches.
- Allow for speedier resource provisioning.
- As business demands evolve, use a hybrid cloud architecture to allow real-time scaling for apps.
- Consistently meet service goals
- Use cloud reference architecture to have a better understanding of IT spending patterns and cloud usage.

A well-architected framework for the cloud is more than simply a technology necessity; it is a vehicle for lower operating costs, high-performing applications and satisfied end users.

By following cloud architecture principles and best practices, organizations can gain real business value from their cloud investments and ensure their IT environment in the future.

Up-front planning: When creating a cloud architecture, make sure there is a clear grasp of capacity requirements. Continuously test performance as businesses begin to build up architecture to avoid unforeseen production issues.

Security first: First and foremost, protect clouds from hackers and unauthorized users by encrypting data, managing patches, and enforcing strict standards across all tiers of a cloud infrastructure. For the highest levels of security across the hybrid, multi-cloud company, zero-trust security models should be considered.

Ensure disaster recovery: Automate recovery operations to avoid costly downtime and ensure a quick return to service after a service outage. A highly available architecture can also be ensured by monitoring capacity and deploying a redundant network.

Maximize performance: By continuously monitoring business demands and technology needs, you can leverage and manage the right compute resources.

Cut costs: To save money on cloud computing, take use of automated processes, managed service providers, and utilization tracking.

5

5. Cloud Security

Security in the cloud is a joint duty between the cloud provider and the customer. In the Shared Responsibility Model, there are three types of responsibilities: those that are always the responsibility of the provider, those that are always the responsibility of the customer, and those that change depending on the service model: Cloud email is an example of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS).

Provider security obligations are always related to infrastructure security and access, patching, and configuration of physical hosts and networks where computer instances are operated and storage and other resources are located. Managing users and their permissions (identification and access management), protecting cloud accounts from unwanted access, encrypting and protecting cloud-based data, and managing security status are your tasks (compliance).

Important steps to assess cloud security:

Step 1: Characterize the application's security requirements.

Step 2: Characterize and identify the strengths and weaknesses of cloud provider security.

Step 3: Map application's security characteristics and cloud security characteristics to perform a fit analysis

5.1. General cloud security and impact concerns

1. Insecure physical and software infrastructure:

Concerns such as data center physical and software security are taken into account here, as the containers are hosted on common software stacks, as well as the security concerns of the cloud provider's APIs. It is the obligation of the cloud provider to maintain data security and backups. Internal employees are frequently blamed for serious security breaches and threats. This necessitates a comprehensive set of inspections and audit procedures. Concerns about API security could be solved by requiring all cloud accessible interfaces and APIs to use a key-based digest and integrity verification.

2. Data Security on the Cloud:

The most pressing concerns in cloud computing are data integrity, confidentiality and privacy, and provenance. Some important problems here are how data is kept private, how data is prevented from being locked, data security and integrity when several cloud parties are involved in processing, and so on. Encryption of data using techniques like Homomorphic Encryption is the most efficient way to keep data confidential. Erasure coding and network coding are two types of distributed data coding that have been extensively explored and employed in the cloud, particularly for fault tolerant and highly available storage. Multi-cloud data processing activities such as distributed data mining would necessitate advanced privacy-preserving methods.

3. Access to cloud services:

When it comes to cloud computing, one of the most important considerations is user identification, authorization, and access control. Unauthorized access, multi-level authentication levels, and multi-cloud data access are all examples. Online open identity management communities such as OAuth, for example, are quite successful at preventing illegal access, although they can be challenging to incorporate at times. Different geographical data locations may fall under different jurisdictions, each with its own set of data privacy and security laws, necessitating some level of location awareness.

5.2. Specific areas of security research

Examine three specific areas of security research: Trustworthy Computing, Information Centric Security, and Privacy Protection Models, and explain the impact of Cloud Computing on building a secure cloud computing paradigm.

1. Trusted computing:

Using Trusted Computing, a piece of data can define the Operating System and Application it requires to be opened. In today's environment, you can choose the operating system and program to use to open a piece of data (though some do not make practical sense). Data shows the operating systems and applications that must be used to access with Trusted Computing. With the Trusted Platform Module, you can use strong authentication keys to authenticate users to host and hosts to users to address untrusted execution environment concerns. Remote server attestation is the term for this. A trusted path technique can then be used to validate any future execution on an authenticated host-user pair.

2. Information centric security (ICS):

Information-centric security is a way of approaching the information security paradigm that emphasizes data security over network, application, or even data security. This is accomplished by combining important data security technology with analytics to enable enterprises to detect, monitor, and safeguard sensitive data, including data that transfers to the cloud and is utilized by third parties. With policy-driven encryption and access management, Information Centric Security (ICS) provides total security for personal data throughout its lifecycle.

3. Privacy securing models:

Privacy Protection Data Mining Technology is a way to protect your privacy while allowing you to extract knowledge from data. The idea is to build a storage data protection model (security model) that allows data sharing services to update and control the access and use of shared data. The data hosting faction in multi-party processing might possibly even be passive enemies — they trust each other and execute the contracts, but they may wish to extract "additional" information from the data of other parties.

5.3. Vulnerabilities and open issues

- Cloud computing, like other areas of IT, has a variety of security concerns that must be addressed. These dangers include policy and organizational dangers, technical dangers, and legal and other dangers. The following are some of the open concerns and threats that require immediate attention:
- Shared Technology Vulnerability: Increased resource usage could allow an attacker to launch a single point attack, doing far more damage than it is worth.
- Data Breach: As privacy shifts from cloud users to cloud service providers, the potential for accidental, malicious, or intentional data breaches increases.
- Account of Service traffic hijacking: Access to the cloud over the Internet is one of the major benefits, but it also comes with the risk of account compromise. If you lose access to privileged accounts, you can lose service.
- Malicious Insider: In a cloud environment, a motivated insider can find more ways to attack and cover the trace.
- Injection Vulnerabilities: Vulnerabilities in the administration layer, such as SQL injection flaws, OS injection, and LDAP injection, can pose serious problems for numerous cloud customers.
- API & Browser Vulnerabilities: When combined with social engineering or browser-based assaults, any vulnerability in a cloud provider's API or interface poses a substantial danger; the damage can be significant.

5.4. Countermeasures & Controls

- The cloud's weaknesses and threats are well-documented. Based on their assessment, each cloud service provider and cloud consumer must create countermeasures and controls to limit the risks.
- Encryption from beginning to end: Because data in a cloud delivery architecture may travel to multiple places, it is critical to encrypt the data from beginning to end.
- Examining for malevolent behavior: While end-to-end encryption is strongly recommended, it introduces new hazards because encrypted data cannot be read by a firewall or intrusion detection system. As a result, having proper controls and countermeasures in place to limit the risks of harmful software flowing via encryption is critical.
- Cloud Consumer Validation: Cloud providers must make reasonable efforts to validate cloud consumers to prevent unauthorized use of critical cloud features.
- Secure Interfaces and APIs: Interfaces and APIs are essential for process automation, coordination, and management. All weaknesses need to be mitigated by the cloud provider.
- Insider assaults: To combat insider attacks, cloud providers should do thorough background checks on personnel and contractors, as well as upgrade internal security procedures.
- Securely Used Resources: In a shared / multi-tenancy architecture, cloud providers have secure shared resources such as hypervisors, orchestration, and monitoring tools.
- Plans for Business Continuity: The act of documenting the organization's response to any incidents that result in the unavailability of all or part of a business-critical process is known as a business continuity plan.

5.5. Major Security Challenges

1. Lack of appropriate governance:

The service provider has complete control over cloud computing. By giving this power to the supplier, there is a risk that security will be lost due to a loss of control over authorization parameters. In circumstances when service level agreements with the service provider are not in place, this compromised security poses the additional risk of creating a security gap. Furthermore, the terms of use are open to the user's liberty, i.e., data access can be easily exploited. For example, the Google search engine specifies that the user "agrees that Google has no responsibility or liability for any information and other communication maintained or communicated through use of the service being deleted or failing to be stored."

2. Lock-in:

Another stumbling block is the lack of data format standards, operating techniques, and tools, all of which contribute to a lack of portability between services and applications, as well as between service providers. As a result, the consumer is completely and totally reliant on the provider.

3. Malicious attacks from management internally:

Although this is a rare occurrence, it is a challenging risk to manage. Administrators and managers of cloud service providers are examples of hostile agents who can jeopardize the security of clients using cloud computing applications.

4. Insecure or incomplete data deletion:

When clients ask for data to be erased, either partially or totally, it raises the question of whether the desired portion of their data segment can be deleted accurately. This makes it more difficult for customers to sign up for cloud computing services.

5. Data interception:

Cloud computing data is divided and scattered in transit, unlike traditional computing. Because of the weakness and fragility of computing technologies, such as sniffing and spoofing, third-party attacks, and reply assaults, this offers a greater hazard.

5.6. Protecting Data Using Encryption

Data encryption algorithms for data in transit and data at rest can differ. Encryption keys for data in transit, for example, can be short-lived, whereas encryption keys for data at rest can be kept for longer periods of time. These days, several cryptographic algorithms are utilized to encrypt data. Plaintext is encrypted into cipher text, which is then decrypted using a decryption key in the most basic type of cryptography. Figure 7 talks about encryption and decryption algorithms.

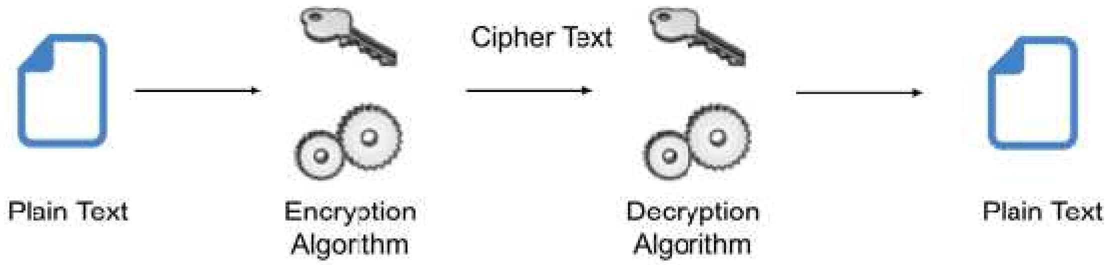


Figure 7. Encryption

Normally there are four basic uses of cryptography:

1. Block Ciphers:

A block cipher is an algorithm for encrypting data (to produce ciphertext) that applies a cryptographic key and algorithm to a block of data rather than per bit. This technique ensures that similar blocks of text in a message are not encrypted in the same way. Normally, the previous encrypted block's cipher text is applied to the following block in the series. The plain text is separated into data blocks, which are typically 64 bits in size. The cipher text is created by encrypting these blocks of data with an encryption key. Figure 8 shows block ciphering of plain text.

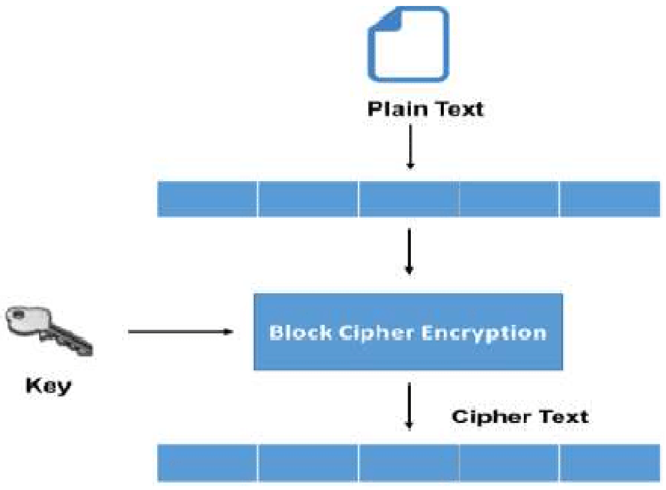


Figure 8. Block Ciphers

2. Stream Ciphers:

Because it is dependent on the present state of the cipher, this method of encrypting data is also known as state cipher. Instead of blocks of data, each bit is encrypted in the thesis technique. Each bit is given its own encryption key and algorithm, which is applied one by one. Because of their low hardware complexity, stream ciphers are usually faster than block ciphers. However, if not handled appropriately, this strategy might lead to major security issues. Instead of encrypting a block of text, the stream cipher encrypts each bit using an encryption key. The cipher text that results is a stream of encrypted bits that can be decrypted later with a decryption key to reveal the plain text. Figure 9 displays stream ciphering of plain text.

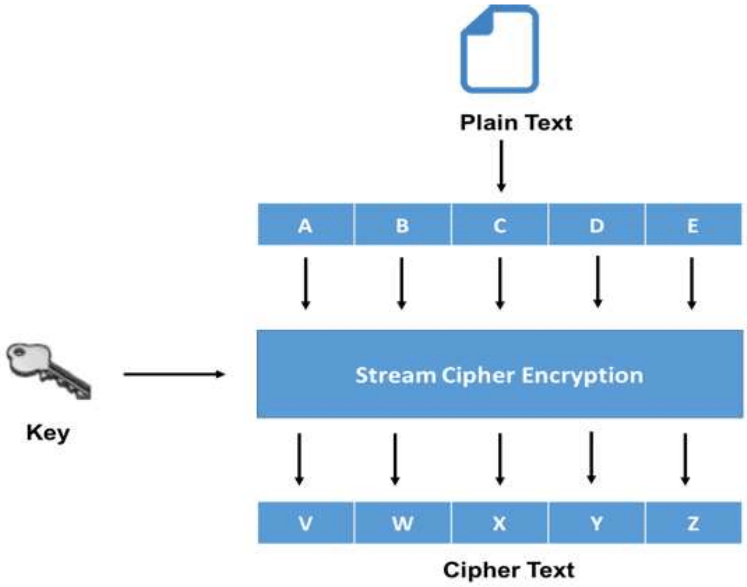


Figure 9. Stream Ciphers

3. Hash Functions:

In this method, an input text is converted into an alphanumeric string using a mathematical formula called a hash function. Normally, the length of the alphanumeric string generated is fixed. This approach ensures that no two strings have the same output alphanumeric string. Even if the input strings are somewhat different, there is a chance that the output strings produced by them will be drastically different. This hash function might be as simple as the one provided in equation (1) or very complex.

$$F(x)=x \bmod 10 \quad (1)$$

Figure 10 shown below is a description of hash functions.

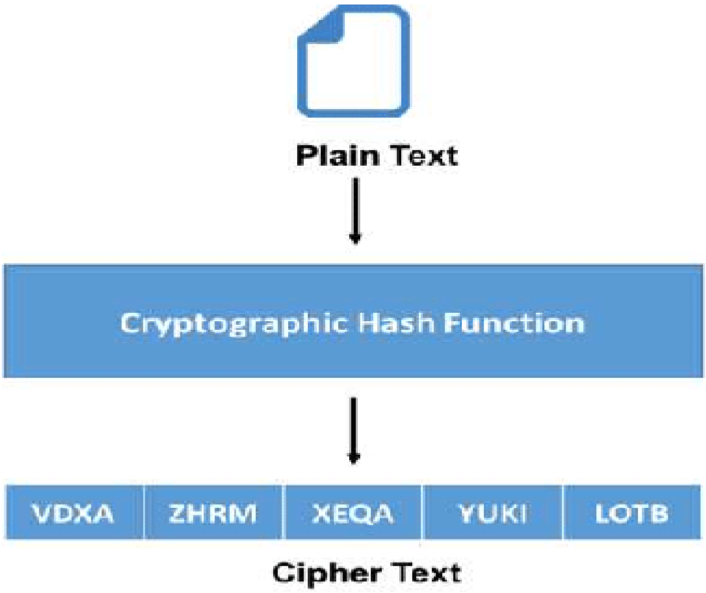


Figure 10. Hash Functions

6

6. Data Security and Privacy

Data security has long been a major concern in information technology. Data is stored in multiple locations around the world, making it more dangerous in a cloud computing environment. Users' biggest concern about cloud technology is about data security and privacy. [10] Data security and privacy are becoming increasingly important for the future growth of cloud computing technology in government, industry and enterprise, but many technologies on the topic of cloud computing are available in both academia and industry. It is being investigated. In cloud architectures, data security and privacy affects both hardware and software. This study aims to improve data security and data protection in a reliable cloud environment, with a variety of security strategies from both a software and hardware perspective to protect data in the cloud. And verify the problem. We conduct a comparative research analysis of existing research on data security and privacy protection approaches utilized in cloud computing in this paper.

Cloud technology has been considered the "next generation" of computer paradigms. Both programs and resources are supplied as services via the Internet in the cloud computing system. Cloud computing is a term that describes a collection of hardware and software components hosted in computer servers that provide a multitude of choices to customers over a network or the Internet.

Grid computing and cloud computing are comparable but not identical [3]. Cloud computing incorporates computational resources operated by multiple operating systems that can provide services such as large-scaled data storage and parallel computing to clients, whereas grid computing merges diverse resources and control systems with just an integrated operating system purpose of providing high manufacturing computing services. The entire picture of grid computing has changed as a result of cloud computing. Data distribution is a new type of cloud computing as compared to grid computing. Figure 11 shows data security and privacy in cloud computing.

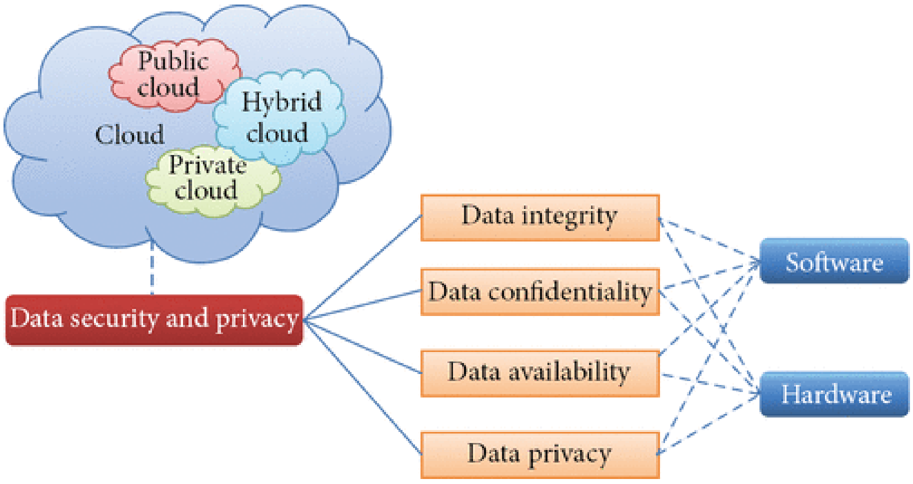


Figure 11. Data Security and Privacy

Data security has always been a major challenge in the IT sector. Data security is extremely crucial in the cloud computing system since data is transferred over various computers and storage systems, including servers, PCs, and other portable devices such as wireless communications and mobile phones. Data security in cloud computing is much more complex than in traditional information systems.

First, let's examine the capabilities of cloud computing before considering data security challenges. On-demand services is another term for cloud computing. There are cloud service providers that enable and monitor services in a cloud computing environment. Cloud providers make all services available over the Internet, and end users use them to meet their business needs and pay the service providers appropriately.

Major issues of data security:

In cloud computing, resource security, resource management, and resource monitoring are all major challenges. Standard norms and standards for installing applications in the cloud are no longer in place, and standardization management in the cloud is weak. Although numerous innovative tactics have been developed and implemented in the cloud, these techniques fall short of providing total security due to the dynamic nature of the cloud environment.

In terms of control in cloud computing, it highlights the inherent issues of data protection, governance, and administration. It also highlights the most pressing security, privacy, and trust issues in today's cloud computing environment, supporting users in understanding the concrete and intangible risks that come with its use. According to the authors, three major potential hazards in cloud computing are security, privacy, and trust. Security is critical in the current era of the long-awaited concept of computing as a utility. The four divisions include safety procedures, cloud server monitoring or tracking, data confidentiality, and avoiding malicious insiders' unlawful actions and service hijacking.

For cloud computing networks, it presents a data security paradigm. The authors concentrated on the security risks associated with cloud data storage. There are a few patents covering data storage security methods as well. A security and privacy architecture for RFID in cloud computing was created for RFID technology mixed with cloud computing, which would connect cloud computing with the Internet of Things.

Security Challenges:

In a word, the most significant difficulties in cloud data security are data privacy, data protection, data availability, data placement, and secure transmission. Threats, data loss, service disruption, hostile attacks from the outside, and multi-tenancy issues are all security concerns in the cloud. When evaluating privacy and security security concerns in cloud - based solutions, it emphasized on information privacy, data segregation, and cloud security. Data security is chiefly responsible at the SPI (SaaS, PaaS, and IaaS) level, and sharing of data is indeed a major roadblock in cloud computing.

In this study, we will look at a variety of security tactics and issues for data storage security and privacy protection in the cloud computing environment. Figure 1 shows a comparative research analysis of existing cloud computing research efforts based on data security elements such as data integrity, confidentiality, and availability.

Data privacy issues and cloud technologies are being explored because data privacy is often related to data security. By securing data, comparative studies on data security and privacy could help to build consumer trust in the cloud computing ecosystem.

6.1. Data Integrity

One of the most important aspects of any information system is data integrity. Data integrity, in general, refers to the protection of data from unlawful deletion, modification, or fabrication. Managing an entity's access and rights to certain enterprise resources helps to guarantee that sensitive data and services are not misused, misappropriated, or stolen.

In a solitary system with a single database, data integrity is simple to achieve. In a standalone system, data integrity is ensured through database constraints and transactions, which are normally completed by a database management system (DBMS). To ensure data integrity, transactions should adhere to the ACID (atomicity, consistency, isolation, and durability) criteria. The majority of databases can support ACID transactions and maintain data integrity.

Authorization is a data access control approach. It's how a system decides what level of access a particular authenticated user should have to the system's secure resources. Data integrity in a cloud system refers to the protection of information integrity. Unauthorized users should not have access to or edit the information. Data integrity is the cornerstone for cloud computing services like SaaS, PaaS, and IaaS. Cloud computing infrastructures usually provide data processing services in addition to storing large volumes of data. To ensure data integrity, techniques such as RAID-type methods and digital signatures can be utilized.

6.2. Data Confidentiality

When storing private or secret data on the cloud, data confidentiality is critical. To ensure data confidentiality, authentication and access control mechanisms are employed. Cloud computing challenges such as data confidentiality, authentication, and access control could be solved by improving cloud reliability and trustworthiness. Users do not trust cloud providers, and it is nearly hard for cloud storage service providers to eliminate potential insider threats, therefore storing sensitive data in cloud storage directly is extremely unsafe. Simple encryption has a key management difficulty, and it can't handle complicated requests like query, simultaneous modification, and fine-grained authorization.

1. **Encryption that is homomorphic:**
   Encryption is widely used to protect the privacy of your data. Homomorphic encryption is presented as a type of encryption method. This ensures that the result of the ciphertext algebra operation is compatible with the result of the delete operation after encryption. Also, there is no need to decrypt the data throughout the process. The application of this technology has the potential to solve data and data company confidentiality issues in the cloud. For secure communication, a Diffie Hellman encryption method, which is fundamentally different from the key distribution management system, has been proposed.

2. **Encrypted Database and Search:**
   Due to the inefficiency of the homomorphic encryption method, researchers are looking at the uses of limited homomorphic encryption algorithms in the cloud. A typical operation is encrypted search. An approach to encrypt storage databases has been proposed for the privacy and security of sensitive data in an untrusted cloud environment. In order to gain

access to the data, a synchronizer exists between the owner and the client. To decrypt the encrypted shared data received from the owner, the client needs the key from the synchronizer. The synchronizer is used to maintain track of both the shared data and the keys that are linked with it.The additional communication with the central synchronizer causes delays, which is a flaw in this technique. However, by using group encryption and limiting communication between nodes and synchronizers, this issue can be overcome.

3. **Distributive Storage:**

   In a cloud setting, distributed data storage is also a promising approach. It explores the security challenges surrounding data privacy in cloud computing, such as data integrity, infiltration, and cloud service availability. One approach for ensuring data integrity is to store data in numerous clouds or cloud databases. The data to be protected from internal or external illegal access is separated into chunks, and each chunk is given a polynomial function using Shamir's secret technique. For safeguarding cloud data, Ram and Sreenivaasan devised a concept known as security as a service. By separating the user's data into pieces, the proposed technique can achieve maximum security. These data pieces are subsequently encrypted and kept in distinct databases, in accordance with the cloud data distribution paradigm. Because each segment of data is encrypted and distributed individually in databases over the cloud, it is more secure against various forms of assaults.

4. **Hybrid Technique:**

   For data confidentiality and integrity, a hybrid solution is presented that combines key sharing and authentication techniques. You can make your connection to your cloud service provider more secure by using a strong key release and authentication mechanism. For safe key distribution between users and cloud service providers, the RSA public key algorithm can be utilized. A three-layered data security technique is proposed: the first layer authenticates the cloud user using one or two factor authentications; the second layer encrypts the user's data for safety and privacy; and the third layer performs quick data recovery using a fast decryption process. TrustDraw, a transparent security extension for the cloud that combines virtual machine introspection (VMI) and trusted computing, is presented as a strategy for event-based isolation of important data in the cloud.

5. **Data Concealment:**

   Data hiding could potentially be utilized in the cloud to maintain data secrecy. It proposes a database security concealing concept. Data concealing techniques combine genuine data with visual false data to distort the volume of the real data. Authorized users, on the other hand, can quickly distinguish between fake and real data. Data hiding technology increases the overall amount of actual data while improving the security of personal data. The purpose of data hiding is to protect sensitive information from malicious users and attackers. The watermarking approach can be used as a key to unlock the data. Only authorized users have access to the watermarking key, hence user authentication is essential to ensuring that the genuine data is available to the appropriate users.

6. **Deletion Confirmation:**

   When users remove their data after receiving deletion confirmation, it is impossible to restore the data. Because more than one copy of data exists in the cloud for security and convenience of data recovery, the situation is highly serious. When users confirm the deletion of their data, all copies of the data should be erased at the same time. However, some data recovery methods exist that can retrieve data from hard disks that have been destroyed by users. As a result, cloud storage providers must ensure that customers' erased data cannot be recovered and exploited by unauthorized users. Data is encrypted in the system before being uploaded to the cloud storage. When users want to remove their data, the system uses a specialized strategy to cover all available storage space with new data, thereby replacing the deletion action.

6.3. Data Availability

When catastrophes such as hard disk damage, IDC fires, and network failures occur, data availability refers to the extent to which a user's data can be used or restored, as well as how users validate their data using techniques rather than relying solely on the cloud service provider's credit guarantee.

Clients are concerned about keeping data on cross-border servers since cloud vendors are bound by local regulations, and cloud clients should be aware of those rules. Furthermore, the cloud service provider must assure data security, including data confidentiality and integrity. All such issues should be shared with the client, and a trust relationship should be established in this connection. Clients should be informed about the cloud vendor's data security guarantees and the jurisdiction of local laws. The paper's major focus is on data difficulties and challenges related to data storage location and relocation, as well as cost, availability, and security.

Users can boost their trust in the cloud by locating data. Cloud storage offers consumers a transparent storage solution, which reduces the complexity of the cloud but also limits users' control over their data storage.

6.4. Data Privacy

Privacy refers to an individual's or a group's ability to keep oneself or information about themselves private and selectively reveal it. The components of privacy are as follows:

1. When a respondent may be more concerned about present or future information than information from the past being revealed.
2. While a user may be comfortable with his or her friends being able to individually request his or her information, he or she may not appreciate alerts being delivered automatically and regularly.
3. Extent: rather than a specific spot, a user's information may be reported as an unclear zone.

When users visit sensitive material in the cloud, privacy means that cloud services can prevent a prospective adversary from inferring the user's behavior based on the user's visit model (not direct data leakage). Oblivious RAM (ORAM) technology has been the topic of research. ORAM technology visits many copies of data in order to conceal the true purpose of users' visits. As a promising technology, ORAM has been widely employed in software protection and in preserving privacy in the cloud. Various cloud scenarios have different privacy concerns, which can be grouped into four subcategories:

1. I how to give consumers control over their data when it's stored and processed in the cloud, avoiding data theft, criminal usage, and illegal sales;
2. How to ensure data replications in a jurisdiction and consistent state, where replicating user data to numerous acceptable places is a common option, while avoiding data loss,

leakage, and unauthorized alteration or fabrication

3. Who is in charge of ensuring that legal obligations for personal information are met?
4. The number of cloud subcontractors involved in processing that can be properly recognized, checked, and verified.

6.4.1. Service Abuse

Attackers can utilize the cloud service to obtain extra data or ruin the interests of other users by abusing it. Other users may misuse user information. Deduplication technique is commonly utilized in cloud storage, implying that the same data is frequently kept once but shared by several users. This reduces storage space and lowers cloud service provider costs, but attackers who know the hash code of the stored files can access the data. The sensitive data could then be leaked on the cloud. As a result, a proof of ownership approach has been proposed to verify cloud users' authentication. The cost of cloud services may rise as a result of attackers. Fraudulent resource use is a type of attack on cloud service payment. Attackers can use the precise data to raise the cost of paying for cloud services.

6.4.2. Averting Attacks

Cloud computing allows for a massive quantity of shared resources to be shared through the Internet. Denial of Service (DoS) assaults should be avoided by cloud systems. It examines the need for cloud computing security services. The authors recommend that trustworthy computing platforms (TCP) and trusted platform support services be included into cloud services. Confidentiality, dynamically growing trust domains, and dynamic services should all be features of the trusted model. Cloud infrastructures demand that users put their data in the cloud solely on the basis of trust. It evaluates cloud services based on trust by analyzing several attack scenarios on the Xen cloud platform.

The key to cloud computing's widespread acceptance is data security and trust. It examines security concerns in the cloud when establishing services and focuses on cloud services from a security standpoint. The important criteria for assuring security in cloud computing are identity management, data recovery and management, security in the cloud secrecy, trust, visibility, and application architecture.

6.4.3. Identity Management

Cloud computing provides a platform for a variety of Internet-based services to be used. However, in addition to its benefits, when a trustworthy third party is involved, it increases the security risk. By involving a trusted third party, there is a risk of user heterogeneity, which has an impact on cloud security. Using a trusted third-party independent technique for Identity Management to use identity data on untrusted hosts could be a feasible solution to this challenge.

It focuses on data leakage and privacy issues in cloud computing. To prevent data leakage and privacy loss in the cloud, many degrees of protection can be implemented. Cloud computing introduces new demand-based commercial services. Dynamic virtualization of hardware, software, and datasets has been used to create cloud networks. Cloud security infrastructure and trust reputation management are critical for cloud service upgrades. The key security challenges in the cloud are Internet access security, server access security, program access security, and database security.

7

7. Pillars of Robust Cloud Security

While cloud providers such as Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Cloud Platform (GCP) provide many cloud native security features and services, enterprise-grade cloud workload protection from breaches, data leaks, and targeted attacks requires additional third-party solutions. The following industry best practices can only be delivered by a cloud-native security pile with integrated visibility and policy-based granular control:

1. **IAM and authentication controls that are granular and policy-based across complicated infrastructures:** To make it easier to update IAM definitions as business requirements change, work with groups and roles rather than individual IAM definitions. Only give a group or role access to assets and APIs that are absolutely necessary for them to do their tasks. The higher the tiers of authentication, the broader the privileges. Don't forget about proper IAM hygiene, such as implementing strong password policies and authorization time-outs. Implementing safe Identity Access Management (IAM) protocols is the foundation of a solid security system. Ascertain that team members have the bare minimum of access to the systems, assets, and APIs they require to do their duties. The level of authentication required to obtain access should rise as privileges increase. Employees should take ownership as well, thanks to password regulations that are enforced.

2. **Across logically segregated networks and micro-segments, zero-trust cloud network security controls:** Use logically isolated areas of the provider's cloud network, such as Virtual Private Clouds (AWS and Google) or vNETs, to deploy business-critical resources and apps (Azure). With granular security settings at subnet gateways, use subnets to micro-segment workloads from one another. In hybrid systems, use dedicated WAN links and static user-defined routing settings to customize access to virtual devices, virtual networks, and gateways, as well as public IP addresses. Keep your mission-critical assets and apps in your cloud network's strategically segregated areas. For instance, on an AWS virtual private cloud or a Microsoft Azure vNET. Separate secure workloads from those that don't require data security standards, and implement rigorous security policies on these micro-segments.

3. **Policy and procedure enforcement for virtual server security, such as change management and software updates**: Cloud security providers offer advanced Cloud Security Posture Management, which consistently applies governance and compliance standards and templates when constructing virtual servers, auditing for configuration violations, and remediating automatically where possible. Use the change management protocols supplied by your cloud security provider to govern change and enforce compliance requirements whenever a change is requested, a new server is provisioned, or sensitive assets are relocated or amended.

Change management applications will include auditing capabilities, monitoring for unusual behavior and deviations from protocol so that you may investigate or trigger automatic mitigation to remedy the problem.

4. **Using a next-generation web application firewall to protect all applications (particularly cloud-native distributed apps):** This will analyze and manage traffic to and from web application servers at a granular level, automatically update WAF rules in reaction to changes in traffic behavior, and be placed closer to workload-running microservices. A web application firewall (WAF) will monitor and alert the administrator of any unusual activity entering or exiting your online application and servers, avoiding breaches and boosting endpoint security.

5. **Enchanted data protection:** Improved data security, which includes encryption at all transport layers, secure file shares and communications, continual compliance risk management, and good data storage resource hygiene, which includes recognizing misconfigured buckets and terminating orphan resources. To ensure data security, your company should encrypt data at every transit layer. Additionally, any file sharing, communication, and other areas of your environment where data is kept, used, or moved should have security safeguards in place.

6. **Real-time threat intelligence that detects and mitigates known and unexpected threats:** Third-party cloud security suppliers provide context to the huge and diversified streams of cloud-native logs by intelligently cross-referencing aggregated log data with internal and external data, such as asset and configuration management systems, vulnerability scanners, and so on. They also offer tools for visualizing and querying the threat landscape, as well as promoting faster incident response times. Unknown threats are caught using AI-based anomaly detection algorithms, which are then forensically examined to assess their risk profile. Real-time warnings on intrusions and policy breaches reduce remediation timeframes, and can even initiate auto-remediation workflows in some cases. Many cloud security providers can give you insight into your cloud-native logs by comparing them to internal logs from other security solutions like asset management, change management, vulnerability scanners, and external threat intelligence. This may support more quick incident response and remediation procedure deployment.

8

8. Cloud Deployment Model

What Is A Cloud Deployment Model?

It acts as a virtual computing environment where you can choose a deployment model depending on the amount of data you store and the users who have access to your infrastructure. The location of the servers used and the users who control them are defined by the cloud deployment model. Decide what your cloud architecture will look like, what you can change, whether you will be serviced, and whether you will have to create everything yourself. Relationships between the infrastructure and your users are also defined by cloud deployment types (what users are allowed to change or implement). When you hear the terms "cloud" or "cloud computing," you automatically think of computing resources that are managed by someone else. However, this is only one of a few cloud deployment options. When we talk about the cloud, we usually refer to the "public cloud." One of the cloud deployment options in which the cloud provider owns and manages all of the servers is this (and other hardware resources).

For various reasons, some businesses are unable to simply migrate to the public cloud. Compliance and data protection requirements, for example, may prevent them from using the public cloud. Alternatively, they may be hesitant to go to the public cloud since they have already spent a lot of money on their own servers and want to make the most of them. As a result, we have a variety of cloud deployment methods to accommodate all possible circumstances.

The types of cloud deployment models are:

1. Private Cloud
2. Public Cloud
3. Hybrid Cloud
4. Multi-Cloud
5. Community Cloud

1. **Public Cloud:**

   Resources are dynamically committed on a fine-grained, self-service basis through the Internet or through a portal in a public cloud. Billing is usually consumption-based and is charged on a pay per use basis. The primary benefits of using the public cloud are scalability and efficiency, as well as the fact that you don't have to buy your own gear. Assume you're building a platform that gets a lot of traffic on occasion. You'd have to make some compromises if you didn't have a cloud. One solution is to purchase enough servers to manage the peak load. However, this would mean that all of those servers would be underutilized the majority of the time.

   Another alternative is to purchase only enough servers to accommodate the normal load, but this may result in your application operating poorly during spikes. You can have both with the public cloud—enough resources for load spikes without making substantial upfront commitments. Furthermore, you'll only be charged for the resources you use, and you'll be able to provide resources on an ad hoc basis as needed, with load-based auto scaling.

Aside from simple virtual machines and storage, cloud providers provide a variety of public cloud services. A public cloud includes Amazon Web Services (AWS), Microsoft Azure, IBM Cloud, and Google Cloud, to name a few. Figure 12 describes public cloud providers.

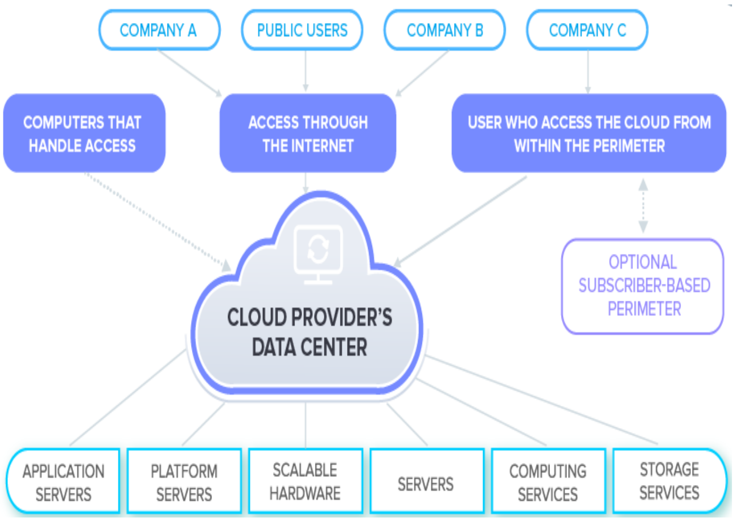

COMPANY A
PUBLIC USERS
COMPANY B
COMPANY C
COMPUTERS THAT HANDLE ACCESS
ACCESS THROUGH THE INTERNET
USER WHO ACCESS THE CLOUD FROM WITHIN THE PERIMETER
CLOUD PROVIDER'S DATA CENTER
OPTIONAL SUBSCRIBER-BASED PERIMETER
APPLICATION SERVERS
PLATFORM SERVERS
SCALABLE HARDWARE
SERVERS
COMPUTING SERVICES
STORAGE SERVICES

Figure 12. Public Cloud

Challenges:
Resources are not committed, but are being used by multiple cloud users, increasing security challenges. This not only adds an additional burden Of ensuring all applications and data accessed on the public cloud, but also has to manage the multitude of external influences such as legislative, data protection etc.

Pros

- Cost savings: Companies can reduce IT operating costs by moving to the public cloud. They are essentially outsourcing these expenditures to a third party who can handle them more effectively. Because the cloud provider may maximize their usage of infrastructure and earnings by offering their services to several customers at once, public clouds are often less expensive than private clouds.
- Less server management: Internal teams don't have to spend time managing servers when using a public cloud, as they do with older on-premises data centers or internal private clouds.
- Security: Many small and medium-sized organizations may lack the financial means to deploy robust security measures. They can outsource some aspects of cyber security to a larger supplier with more resources by using a public cloud service.

Cons

- Security and compliance concerns: Businesses that must adhere to high regulatory compliance norms may be concerned about multitenancy. Multitenancy also carries a minor risk of data leakage, which may be greater than certain organizations in specialized sectors are willing to accept. (In fact, the risk is negligible; most cloud services adhere to stringent security protocols.)

Finally, implementing the same security measures for internal resources and a public cloud that is partially outside of an organization's control might be tricky.

- Vendor lock-in: With cloud technology, this is always a risk. Companies using the cloud will not only save money and gain flexibility, but will also rely on cloud provider services (virtual machines, storage, applications, technologies) to keep their businesses running.

2. **Private Cloud:**

In this deployment model, resources are assigned to a single organization or group of organizations and are treated as intranet features. Billing is usually on a subscription basis and cloud users have minimal obligations. When you run your data center in the same way that public cloud companies do, you have a private cloud. On top of your real servers, you develop an abstraction layer. This gives you the same level of flexibility as a public cloud. If you add more servers to your data center, you won't have to bother about configuring them because they'll (semi)automatically become part of the cluster with a private cloud.

A public cloud provider can also supply you with a private cloud. This means that a cloud provider will isolate specific resources from the rest of its cloud and make them exclusively available to you. The objective is that resources are allocated to a single business, whether you have your own cloud in your data center or from a cloud provider. Private clouds include Red Hat OpenStack, Rackspace, IBM Bluemix Private Cloud, Microsoft Azure Stack, and VMware Private Cloud, to name a few. Figure 13 shown below talks about private clouds used in systems.

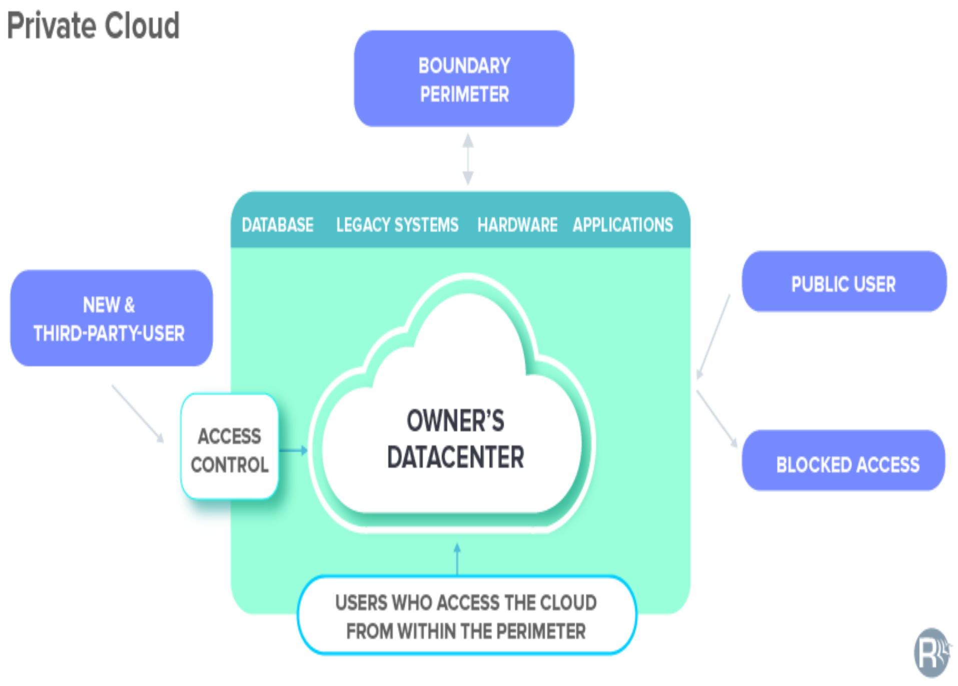


Figure 13. Private Cloud

Challenges

Security challenges include high implementation and management costs, eligibility requirements, and vulnerability management. The scope of security is not comprehensive because cost and ROI are important factors in this deployment model, and security implementations are usually based on risk assessment.

Pros

Those that switch to a private cloud service are only charged for the resources they use. Many enterprises are expected to be attracted to the private cloud because of the benefits it offers.

- High Level of Performance: The tailored aspect of the private cloud enables a corporation to select the hardware on which its infrastructure will be built and to seek a high level of performance to satisfy business needs.
- Resource Saving: Because cloud service providers supply virtual servers, security and monitoring, as well as upgrades and maintenance, most of a company's IT spending is eliminated, allowing more capital to be allocated to the company's core business.
- Availability: Another benefit common to all types of cloud computing is that it frees a company from its physical constraints - files, software, and systems may be accessible at any time and from any location. This availability may be significantly higher in the private model. Because the public cloud must handle a large number of concurrent customers, periods of instability and unavailability are increasingly common, affecting company productivity. Because your infrastructure is tailored to your specific requirements, it's much easier to keep track of delivery and ensure that it's available for as long as feasible.
- Security: The equipment, storage units, and network are configured to perfectly fulfill the standards of IT security managers as well as the compliance limits of its industry. Private cloud services give organizations direct control over their data while lowering IT security risks. Data saved in a private cloud is accessible in a secure environment that is completely dedicated to your company. This detail alone ensures higher data protection and environmental management.

Cons

Because data, especially sensitive data like financial reports and customer contacts, is kept internally in a private cloud, there is more control over it, but it also has significant restrictions.

- Expensive: One downside is the requirement for physical space as well as ongoing hardware and software costs. As a result, this form of cloud computing paradigm is typically more expensive and only suitable for large businesses. Furthermore, in the event of a massive data load, this cloud mode will be less responsive.
- Maintenance: When compared to public cloud services, setting up this infrastructure is more expensive and time-consuming. The corporation might employ a hybrid cloud to gain scalability and consume resources for usage in public cloud settings in this situation.
- Deployment and Support: Only internal hosted resources can be used to extend the private cloud. The organization requires certified skills to maintain deployment. Furthermore, it is extremely difficult to implement on a global basis. It also takes a lot more money and time to realize its full potential.

3. **Hybrid Cloud:**

A hybrid cloud is a deployment model in which a private cloud is connected to one or more external cloud services and managed centrally at the same time. It provides cloud users with a flexible and functional solution that is relatively easy to use. The hybrid clouds have a higher degree of complexity in terms of billing and commercials. A hybrid cloud is one in which a firm uses the public cloud while simultaneously owning on-premises systems and has a link between the two. They work together as a unit. This is a highly beneficial concept since it allows for a more gradual shift towards the public cloud. Some businesses cannot operate solely in the public cloud due to security or data protection concerns, therefore they may choose for the hybrid cloud to meet their needs while also reaping the benefits of the public cloud. They keep mission-critical programs with sensitive data on-premises while storing everything else on the cloud.

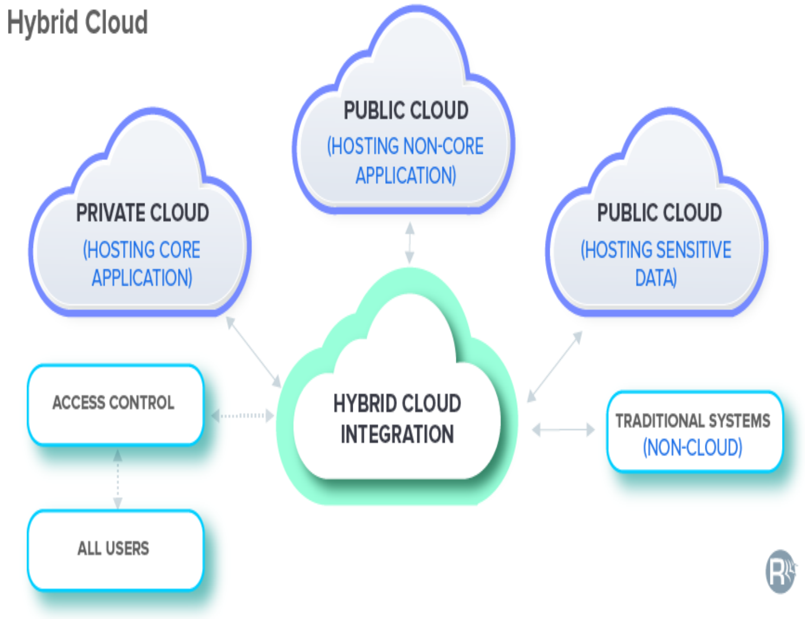


Figure 14. Hybrid Cloud

Figure 14 describes Hybrid cloud integration.

Challenges

Security challenges are relatively high because the deployment model is complex with heterogeneous environments, multiple orchestration, and automation tools. This requires additional administrative burden and puts the supervisor at significant risk.

4. **Multi-Cloud:**

As the name implies, under this paradigm we're talking about hiring multiple cloud providers at the same time. This is similar to a hybrid cloud deployment approach that combines public and private cloud resources. Instead of merging private and public clouds, multi-cloud makes use of many public clouds. You may wonder why you would do such a thing. Mostly for the sake of redundancy. Although public cloud providers provide numerous tools to improve the reliability of their services, mishaps still occur. It's quite rare that two distinct clouds would have an incident at the same moment. As a result, multi-cloud deployment improves the high availability of your services even more. When you need a certain service from public cloud X and another specialized service from public cloud Y, you can use multi-cloud. Figure 15 below describes multi-cloud where multiple clouds used for different functions are shown.

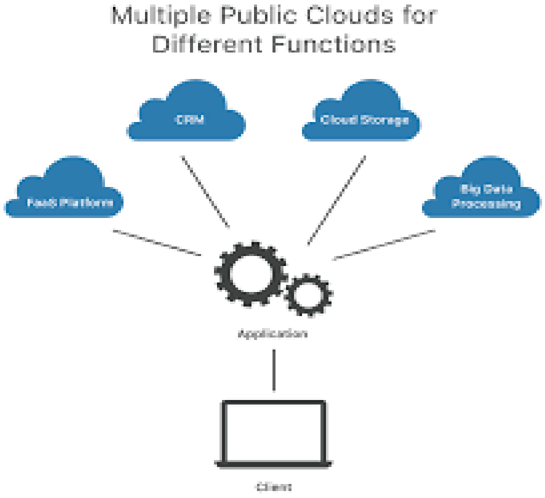


Figure 15. Multi-cloud

5. **Community cloud:**
   This cloud is reserved for a select group of companies from the same "community." As a result, it's not a public cloud because it's not open to the public, but it's also not a private cloud because it's used by multiple users/organizations. A cloud that is used by several different banks is an example of a community cloud. The most significant benefit of a community cloud is that it can be customized to meet the needs of a certain "community." Figure 16 shows community clouds used in various organizations.

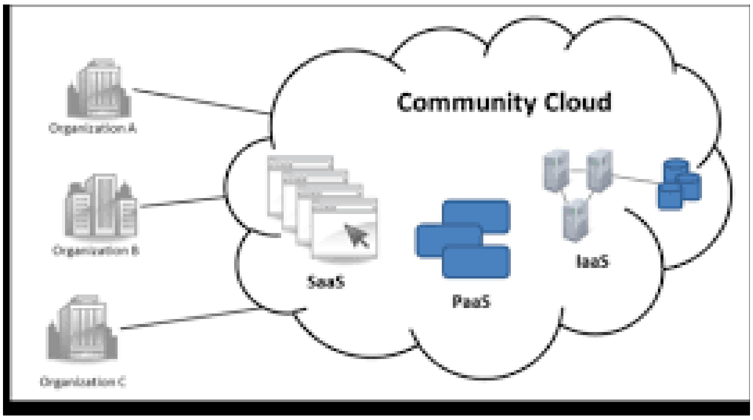
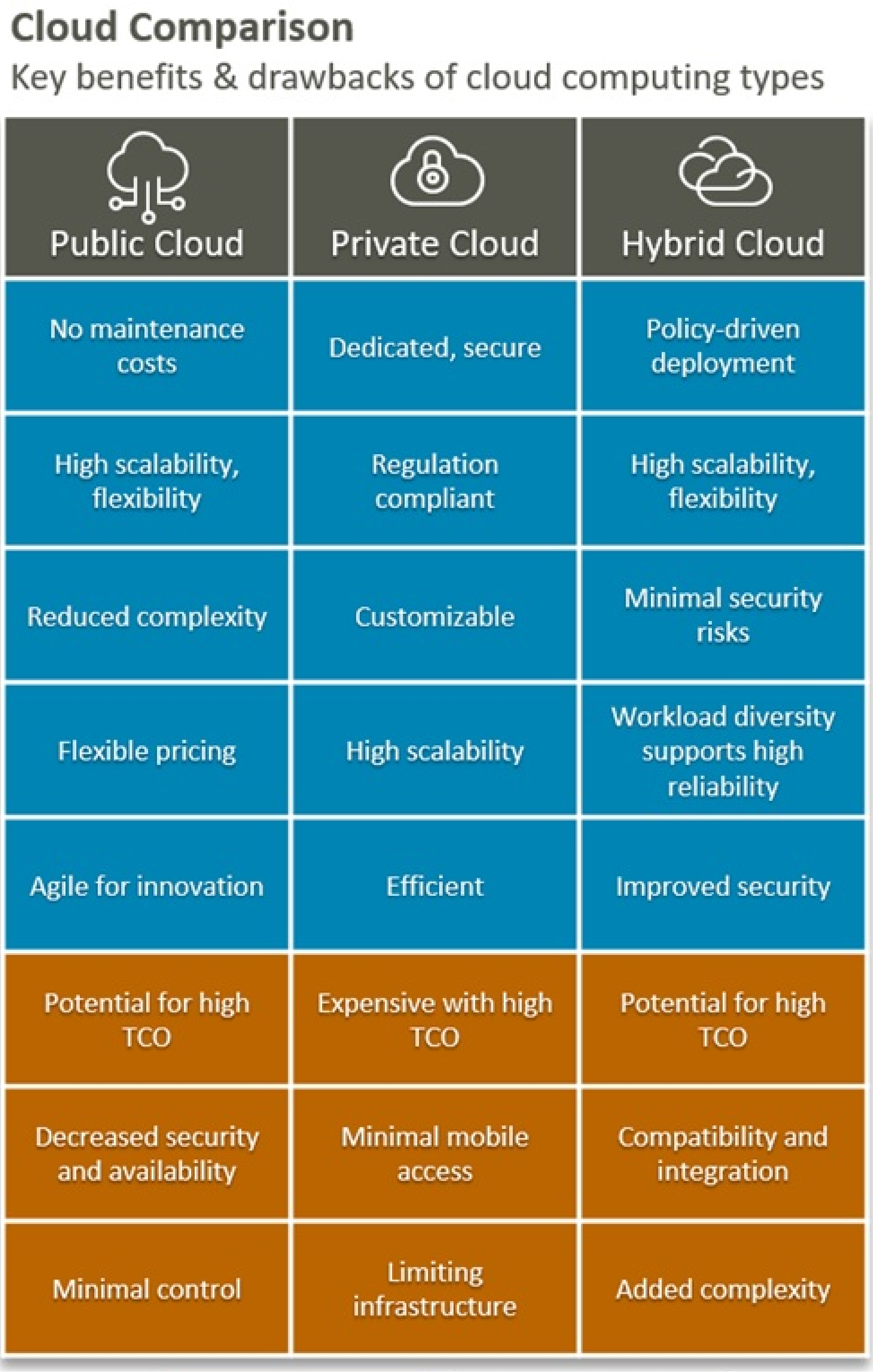


Figure 16. Community cloud



Cloud Comparison

Key benefits & drawbacks of cloud computing types

Public Cloud	Private Cloud	Hybrid Cloud
No maintenance costs	Dedicated, secure	Policy-driven deployment
High scalability, flexibility	Regulation compliant	High scalability, flexibility
Reduced complexity	Customizable	Minimal security risks
Flexible pricing	High scalability	Workload diversity supports high reliability
Agile for innovation	Efficient	Improved security
Potential for high TCO	Expensive with high TCO	Potential for high TCO
Decreased security and availability	Minimal mobile access	Compatibility and integration
Minimal control	Limiting infrastructure	Added complexity

Table 1. Comparison between Cloud Computing Types

In the above Table 1, it compares the various cloud computing types i.e Public, Private and Hybrid Clouds.

9

9. Cloud Automation Tools

Assume you need to establish a number of servers, each with its own memory, disk space, and operating system. This may take several hours to set up, and we may make some errors along the way. Fortunately, tools like Terraform can transform a little code into something that can be planned, deployed, modified, and destroyed on any system.
Cloud automation is a software solution that allows developers and IT professionals to install, configure, and administer cloud computing services. It enables enterprises to select the appropriate amount of cloud computing resources. It can be used to manage workloads and track application and workload performance. It's a cloud-based IT software solution that's available for free. [11]

9.1. Amazon Web Services CloudFormation

Amazon Web Services' CloudFormation tools provide administrators and developers with an easy way to create, deploy, and update a variety of related resources in an organized and predictable way. CloudFormation offers sample templates, or we can build our templates to represent AWS tools, relevant dependencies on our device. After you implement your AWS tools, you can modify and update your tools in a managed and consistent way to effectively add version control to your AWS infrastructure. Figure 17 below shows the AWS CloudFormation Architecture.

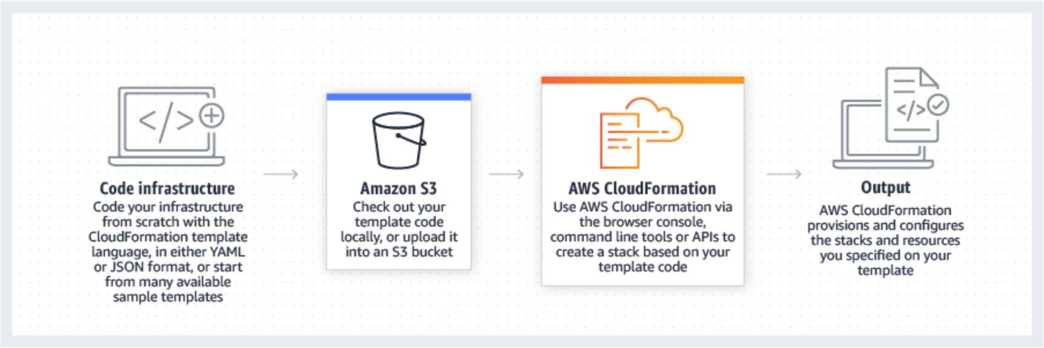

Code infrastructure
Code your infrastructure from scratch with the CloudFormation template language, in either YAML or JSON format, or start from many available sample templates
Amazon S3
Check out your template code locally, or upload it into an S3 bucket
AWS CloudFormation
Use AWS CloudFormation via the browser console, command line tools or APIs to create a stack based on your template code
Output
AWS CloudFormation provisions and configures the stacks and resources you specified on your template

Figure 17. AWS CloudFormation Architecture

Features of AWS CloudFormation are:

- Authoring with familiar programming: The AWS cloud development kit allows users to create apps in familiar programming languages such as Typescript, Python, Java, and.NET. It also allows us to use AWS CloudFormation directly from our IDE to provision our infrastructure.
- Authoring with JSON/YAML: A full network can be modelled in text using AWS CloudFormation. The resources required for setting or developing AWS are defined in YAML or JSON files.
- Safety Controls: AWS CloudFormation automates and secures the provisioning and update of AWS infrastructure. The CloudWatch can be specified using Rollback Triggers. Rollback

Triggers can be used to provide the CloudWatch alert that is monitored by CloudFormation and used for the slack and replace procedure. If any of the alarms are breached, the whole stack operation is preceded back to the deployed state.

- Dependency Management: AWS CloudFormation automatically manages dependencies between our resources during stack management behavior. We don't need to describe the sequence in which the resource is created, changed, or removed. The appropriate actions to be performed for stack actions are determined for each resource.
- Managing Cross-region Cross-Account: AWS StackSets allow us to provide a bundle of AWS tools across different accounts and regions using a single CloudFormation template. StackSets ensures that numerous accounts and regional stacks are automatically supplied, altered, or withdrawn in a secure manner.

9.2. Kubernetes

At its core, Kubernetes is a containerized software that runs and manages a community of machines. It was created using methodologies that ensure the predictability, scalability, and high availability of containerized applications and services throughout their lifecycle. As a Kubernetes user, you get to select how your apps work and how they interact with other apps and the outside world. To test functionality or rollback errors, you can update or remove your services, update gracefully, and transfer traffic between different versions of your apps. Kubernetes provides foundational interfaces and platform composables that allow you to define and manage your application with a high level of flexibility, power, and confidence. It's critical to understand how Kubernetes can support these features, as well as how it's structured and organized at a high level. Kubernetes may be thought of as a layer-based network, with any higher tier resuming the complexity of the lower layers. Figure 18 shows the Kubernetes Architecture.

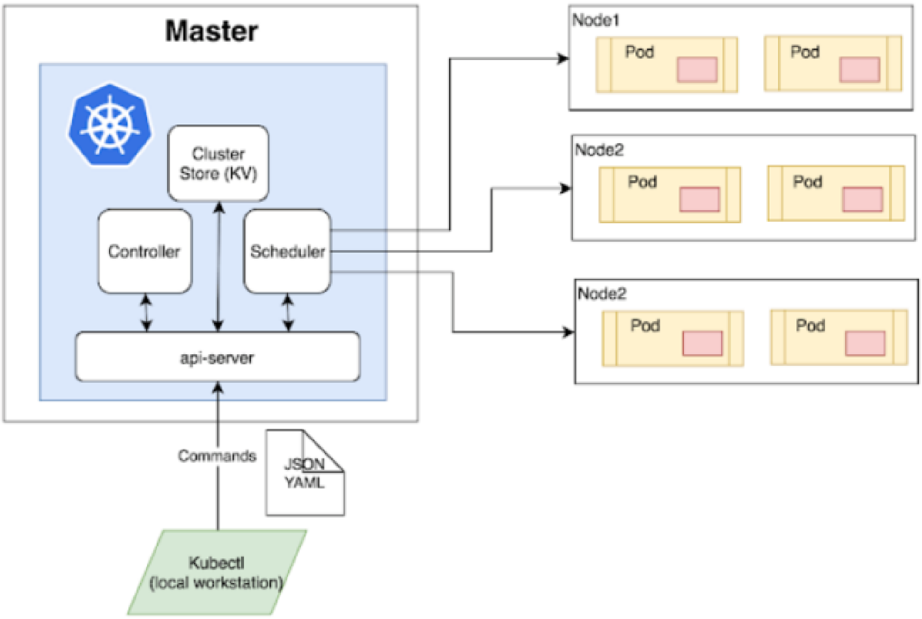


Figure 18. Kubernetes Architecture

Architecture:

It's critical to understand how Kubernetes can support these features, as well as how it's structured and organized at a high level. Kubernetes can be thought of as a layer-based network, with any higher layer resuming the complexity of the lower layers [15]:

- Master Node: The master node is the initial and most important aspect of Kubernetes cluster administration. An administrative entry point for all types of activity. Multiple master nodes in the cluster can monitor fault tolerance. API Server, Scheduler, Controller Manager, and ETCD are just a few of the master node's components.
    - API Server: Serves as the entry point for all cluster commands (REST).
- Scheduler: Node functions are being run by the programmer. Each node's resource utilization is recorded in this file. The workload will be divided by the company. It also allows you to keep track of how the cluster nodes handle the working load. It assists you in balancing the task against available resources and accepting the workload.
- Master/Slave Node: These are worker nodes that play an important role in providing the necessary inter-container networking and collaboration services so that resources can be allocated to scheduled containers. Worker nodes are also important.
    - Kubelet: Get the API server pod setup and verify that the listed containers are working.
    - Docker Container: These Containers run on worker's nodes that operate on the Kube-proxy (the cube-proxy helps in balancing the load and network proxy for the output of a single working node) pods that are configured.

Kubernetes is a container orchestration system that connects numerous virtual and/or physical machines in a cluster via a shared network. This cluster serves as the physical infrastructure for setting Kubernetes' modules, functions, and workloads.

Each cluster's machines in the Kubernetes ecosystem serve a specific purpose. In highly accessible installations, the master machine acts as a machine (or as a small community). As the brain of the cluster, it provides APIs to users and customers, performs security checks on other servers, determines the optimal distribution and allocation of work (“scheduling”), and coordinates coordination with other components. The server acts as both a gateway and a brain. The master server is the cluster's primary point of contact, and it primarily provides Kubernetes' centralized logic.

Nodes are servers with local and external resources for workload acceptance and operation in a cluster of computers. To aid in isolation, flexibility, and management, the software and services are built to run in containers, with each node equipped with the runtime of its container (e.g. Docker). Depending on the instructions received from the master, the containers are either created or destroyed. Changes in network rules are made in response to traffic patterns and transit.

Features of Kubernetes are:

- Automates various manual processes: Kubernetes, for example, will decide which server will host the container and how it will be started.

- Interacts with several groups of containers: Kubernetes can handle several clusters at the same time.
- Provides additional services: In addition to container management, Kubernetes offers security, networking, and storage.
- Self-monitoring: Kubernetes monitors the health of nodes and containers in real time
- Horizontal scaling: Kubernetes enables you to scale resources horizontally as well as vertically, with ease and speed.
- Storage orchestration: To launch apps, Kubernetes mounts and adds a storage system of your choice.
- Automates rollouts and rollbacks: If something goes wrong after you make a change to your application, Kubernetes will rollback for you.
- Container balancing: By computing the "optimal position" for containers, Kubernetes always knows where to put them.
- Run everywhere: Kubernetes is an open source solution that allows you to use on-premises, hybrid, or public cloud infrastructure while allowing you to transfer workloads wherever you choose.

9.3. Puppet

A configuration management solution for private, public, and hybrid clouds that is free source. Puppet DSL (Domain-specific language) is its own configuration language. The system configurations and infrastructu.re as code are defined using a DSL. Puppet Enterprise coordinates task-based multi-device management and command execution. Provides a GUI console for classifying and managing all deployed cloud machines. Figure 19 below describes the architecture of the Puppet automation tool.

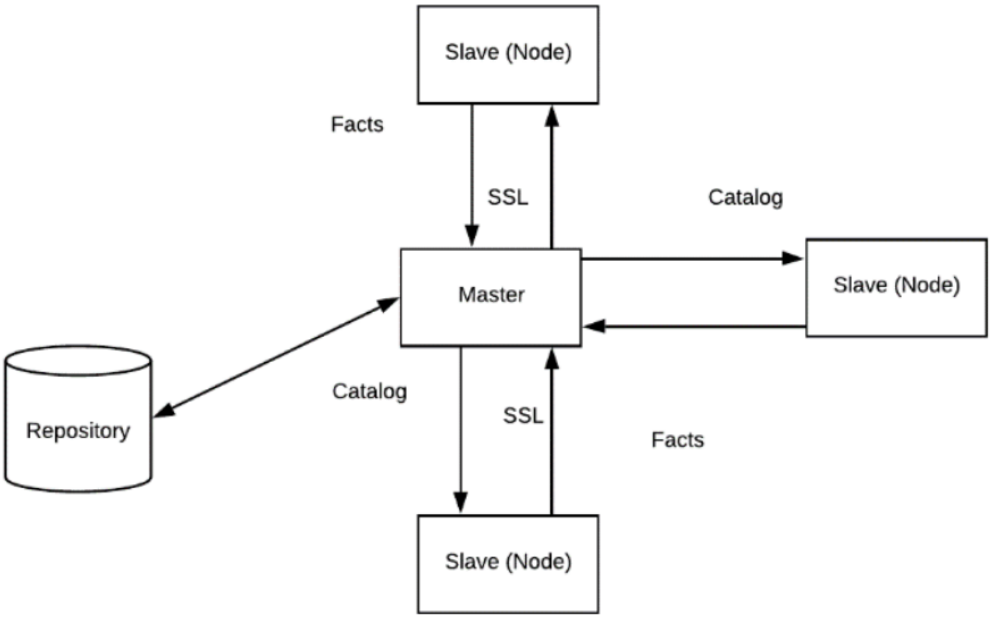


Figure 19. Puppet Architecture

Architecture:

The architecture of Puppet is master-slave. The secure socket layer connects the client and the server. The components of the puppet architecture are as follows [14]:

- Puppet Master: Puppet master is a Linux-based system that uses puppet codes to manage all configuration-related tasks. The master verifies and marks the SSL certificates.
- Puppet Slave: The client uses Puppet Slave as a functional system. The puppet master is in charge of the slave's upkeep and management. Inside the slave, the Puppet agent daemon service executes.
- Repository: The node and server configuration is stored in the repository. Puppet manages the official operating system bundle archives. Puppet collections assist in assembling the majority of the software needed for a basic Puppet deployment.
- Catalog: The compiled format of configuration and manifest files written in Puppet are called catalog. It defines the state and dependency data for all the assets that ought to be overseen by the hub in a specific request.
- Facts: The Facts are a key-value pair that holds data about the node and master computer. The status of any slave is determined by facts, which describe client states such as OS systems, IP addresses, and network interfaces.

Features of Puppet are:

- Idempotency: Idempotency is a feature of Puppet that allows the same set of configurations to be performed numerous times on the same machine[10]. Puppet basically checks the current condition of the target computer and only makes changes if the configuration has changed.
- Cross-platform: Puppet aids in system configuration. The Resource Abstraction Layer handles the implementation details, so they aren't taken into account.

9.4. Terraform

Terraform is a tool developed by HashiCorp that rebuilds your system from well-reviewed templates, checks for accuracy, and allows you to deploy when all the required checks have passed. HashiCorp's tool aids in the provisioning of infrastructure as code. The configuration language used by HashiCorp is. It's used to set up a datacenter's infrastructure. for which I used a tool infrastructure versioning, constructing, and changing in a cost-effective manner. Terraform manages a large number of existing service providers with the use of in-house tailored solutions.

Terraform isn't just for Amazon Web Services. It can theoretically function with any provider and can potentially be used to create its own data center. Ready-made plugins are actively maintained and modified to changing conditions and new features for the most popular providers. You can also contribute your own plugins to the community repository by uploading them. Unlike proprietary tools like CloudFormation, which are only focused on a single provider.

Terraform can build up services like databases or object storage with a variety of IaaS providers. Terraform may be seamlessly integrated into an existing or newly developed deployment pipeline in everyday life. Terraform's main benefit is that the infrastructure configuration is kept in the same repository as the application's source code.

Developers can immediately establish which environment the program is operating in, which machines it is running on, which database it is using, and so on.

Terraform consists of two main parts: the core and the plugin [13].

- **Terraform Core:** GO programming-based command line tool. This is useful for building infrastructure as code, managing resource status, building resource diagrams, executing plans, and communicating over RPC using plugins.
- **Terraform Plugin:** Called by the Terraform kernel as a binary executable via a remote procedure call. The Terraform plugin is used to create the API calls needed for authentication, resource definition, and library initialization.

Terraform works with a variety of cloud providers. For setting up our cloud services, the Terraform config block contains several providers and modules. Providers are obtained and a resource graph is created when the code is compiled using terraform commands. Real infrastructure is configured on the cloud provider, according to the resource graph.

What is the purpose of Terraforming?

- Codify the infrastructure of your application: Provisioning infrastructure as code reduces human error and increases automation.
- Organize infrastructure across many clouds: Using a single procedure, provide infrastructure across 300+ public clouds and services.
- Create infrastructure that can be replicated: With the same configuration, create consistent testing, staging, and production environments.

Figure 20 describes the architecture of the Terraform automation tool by HashiCorp.

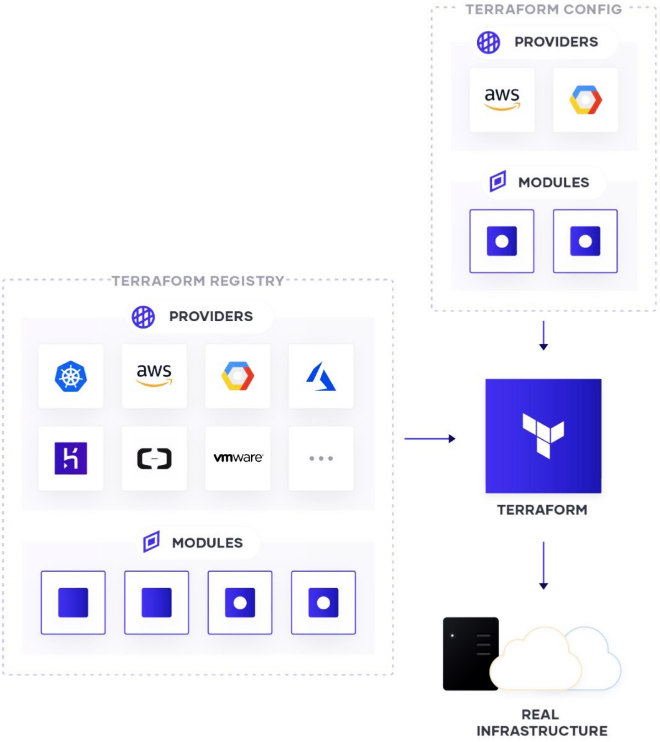


Figure 20. Terraform Architecture

Features of Terraform are:

- Infrastructure as Code: High-level configuration syntax is used to define the infrastructure. This allows you to version control your data center blueprints and treat them like any other code. You can also share and reuse the infrastructure.
- Execution Plans: Terraform features a stage called "planning" that generates an execution plan. When you call apply, the execution plan shows what Terraform will perform. When Terraform manipulates infrastructure, this allows you to avoid any unpleasant surprises.
- Resource Graph: Terraform creates a diagram of all resources and parallelizes the creation and modification of all independent resources. Terraform constructs infrastructure as effectively as feasible as a result, and operators gain visibility into infrastructure dependencies.
- Change Automation: With minimal human input, complex changesets may be implemented to your infrastructure. With the execution plans and resource charts above, you can get an accurate picture of how Terraform changes and in what order to avoid a number of potential human errors.

9.5. SaltStack

A cloud automation tool that automates configuration and deployment using Infrastructure as Code. It's a python-based open-source software that's used for remote execution, configuration management, and cloud control. Salt works with a variety of cloud providers, including Azure, AWS, OpenStack, IBM Cloud, and VMware. Salt Stack uses a common repository to provision servers and infrastructure. Figure 21 shows the architecture of SaltStack.

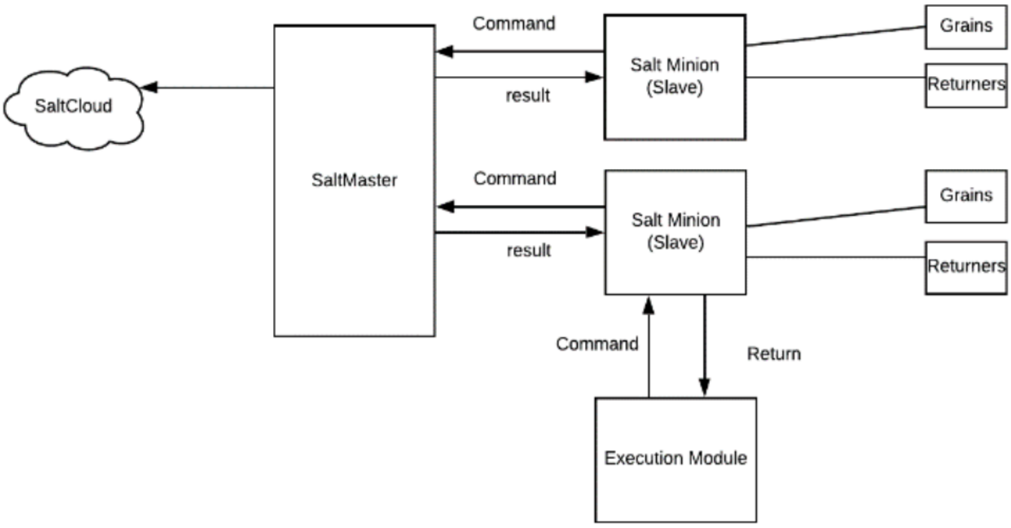


Figure 21. SaltStack Architecture

Architecture:

SaltStack has a highly flexible design that allows it to function with a wide range of servers, from local network systems to data centers. It is based on a simple client-server concept, with numerous daemons cooperating.

The following elements make up salt architecture:

- SaltMaster: Slave daemons receive commands and configuration from a master daemon.
- SaltMinions: Master daemon sends commands and configuration to the slave daemon.
- Execution: Adhoc and module commands against slave daemons are used to monitor in real time.
- Formulas: These are the states that are used for operations like launching a service, checking permissions, and installing packages.
- Grains: System used for detecting diverse facts and storing in RAM.
- SaltCloud: The salt cloud keeps track of cloud hosts.
- SaltSSH: Used to connect to systems through SSH and run commands.
- Runners: The run command of salt was utilized by applications on the master end.

Features of SaltStack are:

- Scalable and fault tolerant: Salt stack has a high failure tolerance, can connect to several masters at the same time, and uses YAML to configure all masters at the same time. Around ten thousand minions can be handled by Salt Master.
- Python API: Salt is a python-based application configuration and monitoring framework with a modular, extendable programming interface.
- Authentication: SSH key pairs are used for authentication, it provides and secures them.
- Execution model: Salt is an utility that allows you to run commands in many computers at the same time.

10

10. Big Data in Cloud Computing

For business and engineering, Big Data is used in the decision-making process to uncover useful insights concealed in the data. Cloud computing has aided the evolution of big data by providing computational, networking, and storage capacity while also posing processing issues. The review, potential, and challenges of transforming big data using cloud computing resources are presented in this study. The major goal of this work is to present a review, opportunities, and challenges of large data applications in cloud computing that demand efficient data processing, as well as some solid design concepts.

"Big Data" refers to data that is large, difficult to store, manage, and analyze using typical databases. For efficient storage, manipulation, and analysis, a scalable architecture is required. Smartphones and social media posts, as well as sensors like traffic lights and utility meters, point-of-sale terminals, and consumer wearables like fit meters and electronic health records, all add to the massive amount of data generated. Various technologies are integrated to find hidden values in this complex data and turn it into usable knowledge, better decision-making, and a competitive advantage.

Cloud computing uses the internet to supply computing services such as servers, storage, databases, networking, software, analytics, and intelligence enabling faster innovation, flexible resources, heavy computation, parallel data processing, and scale economies. By totally abstracting computing, storage, and network resources to workloads as needed and tapping into a wealth of prebuilt services, it allows enterprises to focus on their core business.

Big data has the following qualities:

- **Volume:** The massive amount of data generated every second from a variety of sources, including social media, cell phones, automobiles, credit cards, M2M sensors, photos, and videos, allows users to mine hidden information and patterns.
- **Velocity:** The rate at which data is generated, transported, collected, and analyzed is referred to as velocity. Data is being generated at an ever-increasing rate, and the speed of transmission and access to the data must remain constant to enable real-time access to the various applications that rely on it.
- **Variety:** This term refers to data that has been generated in a variety of formats, both structured and unstructured. Within the columns of a database, structured data such as name, phone number, address, financials, and so on can be organized. This type of information is simple to enter, store, query, and analyze. Unstructured data, which makes up 80% of today's data, is more difficult to sort and extract value from. Text messages, audio, blogs, photographs, video sequences, social media updates, log files, machine and sensor data are examples of unstructured data.
- **Variability:** The high inconsistency in data flow and its volatility during peak periods are referred to as this term. The heterogeneity stems from a plethora of data dimensions

arising from a variety of data types and sources. Variability also refers to the inconsistency with which large amounts of data are consumed into data repositories.

- **Value:** Refers to the hidden value uncovered from data that can be used to make decisions. Big data has significant value in terms of better knowing your consumers, targeting them appropriately, streamlining processes, and boosting machine or company performance.
- **Veracity:** This term refers to the data source's quality and dependability. Its significance is determined by the context and meaning it contributes to the study. Knowledge of the data's authenticity aids in a better understanding of the risks connected with data-driven analysis and business decisions.
- **Validity:** This term refers to the precision with which data has been acquired for its intended application. To maintain uniform data quality, standard definitions, and metadata, proper data governance methods must be implemented.
- **Vulnerability:** This term refers to the safety of the data that has been acquired and stored.
- **Volatility:** Refers to the length of time that data is valid and the amount of time that it must be stored historically before it becomes irrelevant to the current study.
- **Visualization:** Data that is made understandable to nontechnical stakeholders and decision makers is referred to as this. Visualization is the process of turning data into information, information into insight, insight into knowledge, and knowledge into an advantage in decision-making.

10.1. Relationship between the Cloud and Big Data

The terms "big data" and "cloud computing" are often used interchangeably. Big data is primarily about extracting value, but cloud computing is about self-service that is scalable, elastic, on-demand, and pay-per-use models. Big data necessitates vast compute power on demand and widespread storage, while Cloud computing provides on-demand integrated computer resources that are elastic and on-demand. To analyze massive data, you'll need a lot of storage and computational power. Cloud computing also allows for distributed computation processing for scalability and expansion using virtual machines in order to satisfy the needs of the growth of data is exponential.

It has resulted in the growth of analytical platforms that are meant to meet the needs of users, particularly large data-driven enterprises, in terms of providing contextually processed data from all of the stored data. As a result, service providers such as Amazon, Microsoft, and Google have begun to offer big data systems that are both cost-effective and capable of capturing data and incorporating analytics to give proactive and contextual experiences.

The cloud computing environment is a revolutionary new way of delivering IT services. There are numerous providers and user terminals in the cloud computing ecosystem. It encompasses a wide range of software and hardware, as well as pay-per-use or subscription-based services delivered through the internet and in real time. Big data tools are used to collect data, which is then saved and processed in the cloud. For continuous data management, the cloud provides on-demand resources and services. Software as a service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) are the most frequent models for big data analytics (IaaS).

Cloud analytics and analytics as a service (AaaS) are now available on demand for clients. Analytics as a Service (AaaS) is a cloud-based subscription-based data analytics system that connects semi-structured, unstructured, and structured data, transforms it, and analyzes it quickly and scalable.

One of the shared characteristics between Cloud computing and big data is the Internet of Things (IoT). The amount of data generated by IoT devices is enormous, and it must be analyzed in real time. Data can be sent via the internet or over leased lines to cloud providers, who then store it in data stores. The huge data stored in the cloud is then filtered and analyzed using cloud computing techniques and technologies. It creates a way for data to be navigated, stored, and evaluated. IoT and big data require a common platform, which cloud computing delivers. Cloud computing, IoT, and big data are mutually beneficial. The Internet of Things (IoT) is a data source, while big data is a data analytics platform.

11

11. Cloud Cryptography

Cloud cryptography is an encryption method that safeguards data in the cloud. In cloud cryptography, several approaches are employed to add a high layer of protection to secure data, preventing it from being accessed, hacked, or infected with malware. Customers can utilize shared cloud services in a secure and convenient manner because cloud firms encrypt the data they keep. Cloud cryptography safeguards sensitive data without delaying the flow of information. Cloud cryptography is based on encryption, in which text is scrambled into ciphertext using computers and algorithms. This ciphertext can then be decoded with a series of bits and transformed into plaintext using an encryption key. Data encryption can be accomplished in one of the following ways:

Data that is pre-encrypted and synchronised with the cloud: There is software available to pre-encrypt data before it is sent to the cloud, making it hard for anyone attempting to hack it to read.

End-to-end encryption: Messages are sent between senders and receivers, and they are the only ones who can read them.

File Encryption: When data is encrypted at rest, an unauthorized person attempting to intercept the file will not be able to access the information it contains.

Full disk encryption: Any files that are saved on an external disk are automatically encrypted. This is the most important strategy for securing computer hard disks.

11.1. Securing data on the cloud by Cryptography

By encrypting data stored in the cloud, cloud cryptography provides the same level of protection. It has the ability to secure critical cloud data without causing data transfer to be delayed. To strike a balance between security and efficiency, many businesses specify various cryptographic protocols for cloud computing.

The following cryptography algorithms are used in Cloud Security:

- **Symmetric Key Cryptographic Algorithm:**
  Because data encrypted with a single unique key cannot be decoded with any other key, this algorithm provides data authentication and authorization. The most prominent Symmetric-key Algorithms used in cloud computing for cryptography are Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES).
- **Asymmetric Key Cryptographic Algorithm:**
  To protect data in the cloud, this technique uses two different keys for encryption and decryption. Digital Signature Algorithm (DSA), RSA, and Diffie-Hellman Algorithm are the algorithms utilized in cloud computing.
- **Hashing:**
  It is mostly used for indexing and recovering database objects. It also uses two different keys to encrypt and decrypt messages.

11.2. Advantages of Cloud Cryptography

- The information is kept private for the users. Hackers are less likely to commit cybercrime as a result of this.
- If an unauthorized person tries to make changes, the organization is instantly notified. Access is allowed to people who have cryptographic keys.
- When data is transferred from one computer to another, encryption prevents it from being vulnerable.
- In today's data-driven world, cloud encryption is essential because it helps businesses prevent data breaches and cyberattacks.
- Receivers of data have the ability to detect if the data is corrupted, allowing for a quick response and solution to the attack.
- Because encryption complies with the limits established by organizations like FIPS, FISMA, HIPAA, and PCI/DSS, it is one of the safest techniques for storing and transferring data.

11.3. Disadvantages of Cloud Cryptography

- Cloud cryptography provides only a limited level of protection for data that is already in transit.
- To keep encrypted data safe, sophisticated methods are required.
- The systems must be scalable in order to be upgraded, which adds to the costs.
- Overprotective procedures might make it harder for businesses to recover data.

12

12. Load balancing in Cloud Computing

The method of spreading workloads and computational properties in a cloud computing environment is known as cloud load balancing. It allows businesses to manage workloads and application needs by distributing resources over multiple PCs, networks, and servers. The circulation of workload traffic and demands that occur across the Internet is maintained by cloud load balancing. As the internet's traffic grows at a rapid rate, it will soon account for nearly 100% of current traffic. As a result, the workload on the server is rapidly increasing, resulting in server overload, particularly for popular web servers.

Almost all types of services, such as HTTP, SMTP, DNS, FTP, and POP / IMAP, benefit from load balancing. It also improves reliability by incorporating redundancy. A dedicated hardware device or application provides the balancing service. Server load balancing allows cloud-based server farms to achieve more precise scalability and availability.

There are two basic solutions to the problem of server overloading:

First is a single: The first is a single-server approach in which the server is updated to a more powerful server. However, the new server may quickly become overburdened, necessitating even another update. Furthermore, the upgrade procedure is time-consuming and costly.

Second is a multiple: The second option is a multi-server solution, which involves constructing a scalable service system on a cluster of servers. As a result, building a server cluster system for network services is more cost effective and scalable.

12.1. Categorization of load balancing systems

Software-based load balancers: Load balancers that are software-based run on ordinary hardware (desktops, PCs) and operating systems.

Hardware-based load balancer: Hardware-based load balancers are dedicated boxes with specially designed Application Specific Integrated Circuits (ASICs). ASICs allow for high-speed network traffic promotion and are commonly used for transport-level load balancing since hardware-based load balancing is faster than software-based load balancing.

12.2. Benefits of Load Balancing in Cloud

High-availability: When many servers are used together, availability is increased. For example, if one server becomes unavailable, the burden will be picked up by other back end servers, ensuring that incoming traffic is answered and services are not disrupted.

Scalability: Unusual traffic surges can degrade server performance, but load-balancing allows you to add extra servers to the group to handle the increasing number of requests. Rather than switching to a new environment, you can simply raise the number of load-balancers as needed.

Furthermore, you can add or delete the server dependent on the traffic rate and business demand of your website. For example, during a seasonal sale, an eCommerce website may have high traffic, therefore more load-balanced web servers might be added to reduce latency.

Flexibility: Maintaining the system is simple because administrators can route all traffic to one server and put the other load balancer in active/passive mode. This enables them to do maintenance without incurring any disruption. With at least one server up and operating, the technique can be used to undertake maintenance on other load balancers, ensuring that high availability is maintained at all times.

Economical: Load-balancers were formerly prohibitively expensive for SMBs due to their high total cost of ownership. Load-balancing, like the other systems that contributed to the IT bill, necessitated monitoring and administration. The situation is now radically different. The cost of cloud load-balancers is depending on the quantity of resource consumed, which is known as the 'pay-as-you-go' paradigm.

12.3. Examples of Load Balancers

Direct Routing Requesting Dispatching Technique: This request dispatching technique is similar to the one used by IBM's Net Dispatcher. The virtual IP address is shared by both the real server and the load balancer. In this case, the load balancer uses a virtual IP address to create an interface that accepts request packets and directs them straight to the designated servers.

Dispatcher-Based Load Balancing Cluster: A dispatcher provides smart load balancing by regulating where to deliver a TCP/IP request based on server availability, workload, capabilities, and other user-defined parameters. A load balancer's dispatcher module can spread HTTP requests among several nodes in a cluster. The dispatcher distributes the load over multiple servers in a cluster, making the services of various nodes appear as a single virtual service with a single IP address; consumers interact as if it were a single server, with no knowledge of the back-end infrastructure.

Linux Virtual Load Balancer: It's an open source enhanced load balancing solution for creating highly scalable and available network services including HTTP, POP3, FTP, SMTP, media and caching, and Voice Over IP (VoIP). It's a straightforward and effective load balancing and failover solution. The load balancer is the principal entry point for server cluster systems, and it can run Internet Protocol Virtual Server (IPVS), a Linux kernel module that enables transport-layer load balancing, also known as Layer-4 switching.

13

13. Containerization

The container is a building piece in cloud computing that aids operational efficiency, version control, developer productivity, and environmental stability. Because it allows for better control over the granular operations that occur within the resources, the structure has indeed been upgraded. In cloud computing, the usage of containers in online services aids data security, elasticity, and availability. Containers provide various advantages over virtual machines, including a predictable runtime environment, the ability to run almost anywhere, and lower overhead.

For installing and maintaining cloud applications, containers are a popular solution. Containers are used to separate applications from their actual operating environment. A container encapsulates and runs all of the dependencies of a software component in a separate environment.

Containers that run the Docker container engine enable applications to deploy consistently in any environment, whether it's a public cloud, a private cloud, or a bare metal computer. Apps that are containerized are easier to move to the cloud. Containers also make it easy to take advantage of the cloud's massive automation capabilities, as they can be deployed, duplicated, and modified quickly via APIs provided by the container engine or orchestrator.

Containers are becoming more essential in cloud computing systems. Containers are being considered by many businesses as a viable alternative to virtual machines (VMs), which have long been the favoured solution for large-scale enterprise applications.

A Cloud Environment with Virtual Machines and Containers:

A virtual machine is the basic unit used to launch applications in most cloud computing systems (VM). Virtual machines (VMs) are autonomous computing environments abstracted from hardware, similar to containers. Unlike containers, virtual machines (VMs) require a full copy of the operating system to function.

Virtual machines (VMs) can run guest operating systems other than the host, so if the host runs Windows, the VM can run Linux or any other OS. In many technical contexts, VMs outperform containers in terms of isolation and security.

A virtual machine, on the other hand, is effectively a standalone machine with its own operating system, therefore it takes far longer to start up and run than a container. VM images, which are used to generate new virtual machines, are larger and more difficult to automate than container images.

Running containers on top of computer instances, which are technically virtual machines, is the most typical situation in the cloud. Cloud providers are now allowing users to run containers directly on their bare metal servers, bypassing the need for virtual machines (VMs), in a concept known as "container instances."

14

14. Top Cloud Providers

14.1 Amazon Web Services (AWS)

AWS (Amazon Web Services) is Amazon's complete cloud computing platform that includes Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software-as-a-Service (SaaS) packages. AWS services can provide compute power, database storage, and content delivery services to businesses.

Amazon Web Services (AWS) was founded in 2006 as an extension of Amazon.com's internal infrastructure to handle online retail. AWS was one of the first companies to offer a pay-as-you-go cloud computing model, which scales up to match users' compute, storage, and throughput demands.
AWS provides a variety of tools and solutions for businesses and software developers that may be used in data centers across the globe. Government agencies, educational institutions, nonprofits, and private enterprises can use AWS services.

How does AWS work?
AWS is divided into numerous services, each of which can be configured in a variety of ways depending on the needs of the user. For an AWS service, users should be able to access configuration choices and specific server mappings.

Over 100 services, including compute, database, infrastructure management, application development, and security, are available through Amazon Web Services. EC2 Instances, IAM Management, VPC, Elastic Load Balancing, Elastic BeanStalk, Elastic IP, and Analytics are some of the services available.

Why use AWS for web hosting?

- Broad platform support: Any CMS on AWS, including WordPress, Drupal, Joomla can be used. AWS supports and provides SDKs for popular platforms such as Java, Ruby, PHP, Node.js, and .Net.
- Data Centers worldwide: Your consumers could be located anywhere on the planet. With a few mouse clicks, you may have a datacenter or CDN hosting your website in any geography you want.
- Scalable from day one: The amount of traffic to a website might vary greatly. AWS infrastructure can grow and shrink to fit your demands, from peaceful moments in the middle of the night to campaign-driven, social media sharing traffic spikes.
- Flexible pricing models: There are no upfront payments or long-term contracts with AWS; you simply pay for the resources you utilize. AWS provides web hosting with pay-as-you-go or set monthly pricing choices. Figure

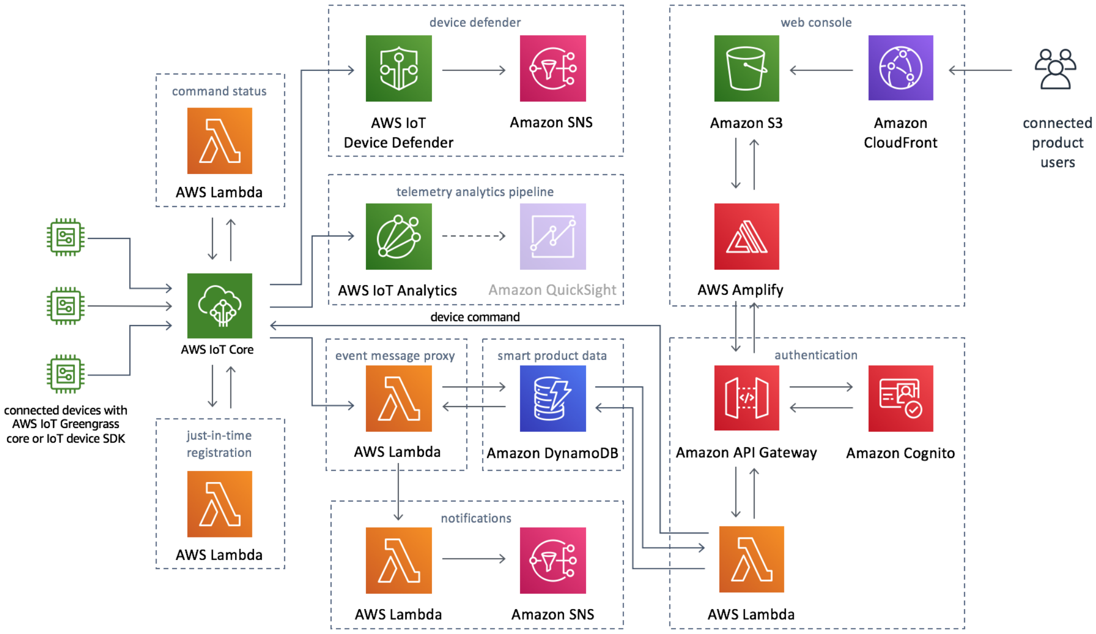


Figure 22. AWS Architecture

Figure 22 above shows the architecture of Amazon Web Services from the AWS Website.

14.2 Google Cloud Platform (GCP)

Google Cloud (also known as Google Cloud Platform or GCP) is a web application development, deployment, and management platform. GCP is primarily a service for creating and managing unique apps that can be published on the web from hyperscale data center facilities. Its cloud architecture hosts applications such as Google Workplace (formerly GSuite and earlier Google Apps).

When you use Google Cloud Platform to host a website, an application, or a service, Google keeps track of all the resources it needs, including processing power, data storage, database queries, and network connectivity. Rather than leasing a server or a DNS address for a month (as you would with a traditional Web hosting company), you pay for each of these resources on a per-minute or even per-second basis, with discounts available if your clients use your services frequently on the Internet.

GCP is a separate business organization within Alphabet, providing the business need for corporations and, in certain circumstances, individuals to install software that can be accessed by Web browsers or Web apps. GCP rents software, as well as the resources required to support it and the tools used to develop it, on a pay-as-you-go basis.

Basic Google Cloud services include the following:
The following are the main services that GCP provides to its customers:

Google Compute Engine:

Compute Engine (GCE) is Google's entry-level service that competes with Amazon's entry-level, premier service: hosting virtual machines. Workloads (applications and services) in data centers are typically run on software-based platforms that may be shifted from one physical computer to another. In fact, a physical server can host more than one of these VMs, increasing efficiency. The virtual machine (VM) concept was established to allow data center mobility; cloud services like GCE use that same format, add a self-provisioning deployment mechanism, and charge consumers for the resources these VMs consume.

A virtual machine instance is a "unit" of virtual machine resources (memory, storage, CPU power, and network throughput) that is put together to run like a physical server with the same amounts of physical resources. In most cases, a service provider will charge a monthly fee for the use of that instance in minutes, as well as any other resources it may consume. GCP charges consumers in seconds rather than minutes in order to be more competitive. It also allows clients to dial in the exact resource buildout they require for their virtual machines, which is useful for businesses that still rely on legacy applications (a nicer way of saying "old programs") that were designed for certain physical machines.

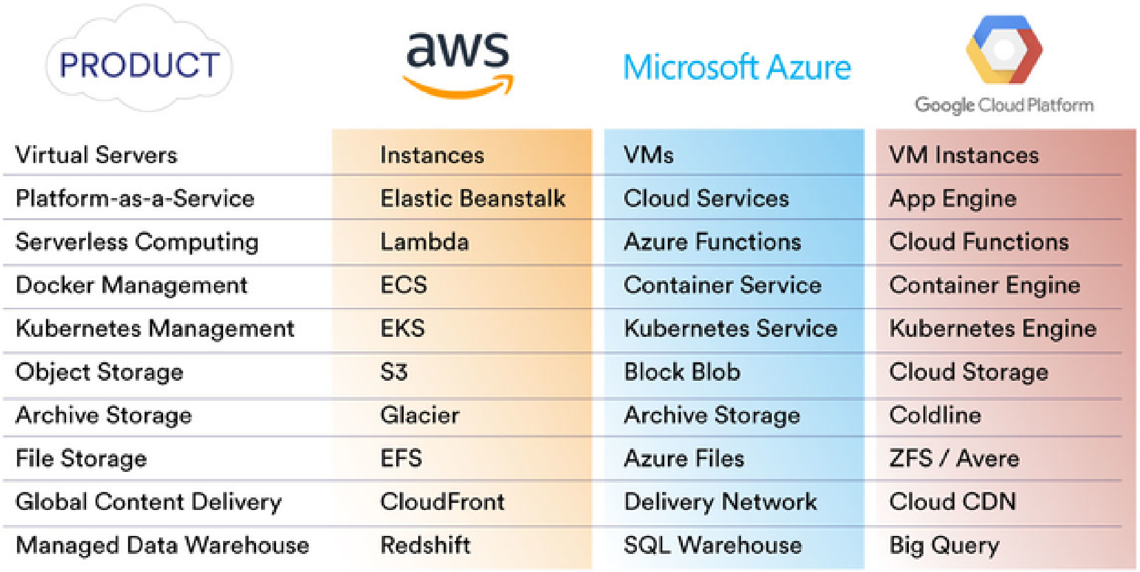
Google Cloud Storage:

Cloud Storage (GCS) on Google Cloud Platform is an object storage system. That is, his record tracks both the ID and structure of each type of data received. Object storage, unlike a standard storage volume's file system, which renders each file or document as a string of digits whose placement is registered in a file allocation table, is an all-purpose block that's leased to customers like parking space at a park-and-lock. It may store full organized databases, raw video streams, or machine learning model matrices.

Google Cloud is a collection of Internet-based services that help businesses digitize. Google Cloud Platform is a subset of Google Cloud, which provides public cloud infrastructure for running web-based applications and is the subject of this blog article.

The following are some of the other Google Cloud services:

- GSuite and Google Apps were formerly known as Google Workspace. This offering includes your organization's identity management, Gmail, and collaboration capabilities.
- Android and Chrome OS have Enterprise Edition. Users can use these phone and laptop operating systems to connect to web-based applications.
- Machine Learning and Business Mapping Services Application Programming Interface (API). These allow the software to communicate with each other.



PRODUCT	aws	Microsoft Azure	Google Cloud Platform
Virtual Servers	Instances	VMs	VM Instances
Platform-as-a-Service	Elastic Beanstalk	Cloud Services	App Engine
Serverless Computing	Lambda	Azure Functions	Cloud Functions
Docker Management	ECS	Container Service	Container Engine
Kubernetes Management	EKS	Kubernetes Service	Kubernetes Engine
Object Storage	S3	Block Blob	Cloud Storage
Archive Storage	Glacier	Archive Storage	Coldline
File Storage	EFS	Azure Files	ZFS / Avere
Global Content Delivery	CloudFront	Delivery Network	Cloud CDN
Managed Data Warehouse	Redshift	SQL Warehouse	Big Query

Table 2. Top Cloud Providers Comparison

Table 2 describes the comparison between top cloud providers i.e Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).

15

15. Cloud Computing Applications

Art, business, data storage and backup services, education, entertainment, management, social networking, and other fields are all served by cloud service providers. The following are the most extensively utilized cloud computing applications:

1. Art Applications

Cloud computing provides a variety of creative tools for creating stunning cards, booklets, and photos quickly and efficiently. The following are the most often used cloud art applications:

- Moo: One of the best cloud art applications is Moo. It's used to create and print business cards, postcards, and mini cards, among other things.
- Vistaprint: Vistaprint makes it simple to design business cards, postcards, booklets, and wedding invitation cards, among other printed advertising material.
- Adobe Creative Cloud: It is invaluable to developers, artists, filmmakers, and other creative professionals. The suite includes PhotoShop image editing programming, Illustrator, InDesign, TypeKit, Dreamweaver, XD, and Audition.

2. Business Applications

Applications and services are built on a base of cloud service providers. To develop their business nowadays, every company needs a cloud business application. It also ensures that corporate services are available to customers 24 hours a day, seven days a week. The following are a few examples of cloud computing's applications:

- MailChimp: MailChimp is an email marketing platform with a number of tools for creating, sending, and preserving email templates.
- Salesforce: Salesforce's platform contains elements such as sales, service, marketing, e-commerce, and more.
- Chatter: We may use chatter to communicate vital organizational information in a timely manner.
- Bitrix24: Bitrix24 is a platform for collaboration that includes tools for communication, management, and social collaboration.
- Paypal: Using a private virtual account, Paypal is the smoothest and also most efficient means of making an online transaction. Paypal transaction via debit cards, credit cards, and Paypal account holders.
- Slack: Slack stands for Searchable Log of All Knowledge and Conversation. It has a user-friendly design that allows us to construct both public and private chat channels.
- Quickbooks: Quickbooks uses the phrase "Run Enterprise anytime, anywhere, on any device" to describe how it works. It supplies businesses with online accounting solutions. It permits more than 20 users to work on the same system at the same time.

3. Data Storage and Backup Applications

We can store information (data, files, photos, audios, and videos) on the cloud and access it using an internet connection using cloud computing. Because the cloud provider is responsible for the security, companies offer a selection of backup and restore solutions to help you recover lost data. The following is a list of cloud-based data storage and backup programs:

- Box.com: Box is a safe and secure online content administration, collaborative, and management service. It enables us to store a wide range of files on the cloud, including Excel, Word, PDF, and images. The key benefit of Box is that it allows users to drag and drop files while also connecting to Office 365, G Suite, Salesforce, and over 1400 other apps.
- Mozy: For our personal and corporate data, Mozy offers sophisticated online backup options. At a certain time, it prepares a fallback schedule for each day or week.
- Joukuu:Joukuu is the most user-friendly platform for sharing and tracking cloud backup data. Joukuu is a popular tool for searching and working on file systems.
- Google G Suite: One of the best cloud storage and backup applications is Google G Suite. These are also Google Calendar, Docs, Forms, Google+, Hangouts, along with data storage and management tools for cloud services. Gmail is the most popular app in the Google G Suite. Consumers can also use Gmail for free email services.

4. Education Applications

Cloud computing is becoming omnipresent in the education industry. It provides students with a variety of online distance learning platforms and student information websites. Powerful virtual classroom settings, simplicity of access, secure data storage, scalability, better reach for students, and minimal hardware requirements for software all make use of cloud computing in education. The following educational applications are available on the cloud:

- Google Apps: Google Apps is the most popular free web-based email, calendar, document, and collaborative study platform.
- Chromebooks: Chromebook for Education has been one of Google's most major programs. It was established with the intention of encouraging educational innovation.
- Tablets with Google Play: It enables teachers to swiftly integrate cutting-edge technology into their classrooms and make it available to their pupils.
- AWS: Universities, community institutions, and schools can use the AWS cloud to create an educational environment.

5. Entertainment Applications

To interact with the target audience, the entertainment industry employs a multi-cloud strategy. Various entertainment applications, such as online games and video conferencing, are available through cloud computing.

- Online games: Cloud gaming has become one of the most popular forms of entertainment.It offers a number of online games that are hosted in the cloud. The best cloud gameplay servers include Shaow, GeForce Now, Vortex, Project xCloud, and PlayStation Now.
- Video Conferencing Apps: Video conferencing apps provide a quick and easy way to connect. We can communicate with our business colleagues, acquaintances, and families

via cloud-based video conferencing. Cost savings, increased efficiency, and the elimination of inconsistencies are almost all benefits of video conferencing.

6. Management Applications

Cloud computing provides a set of cloud management tools to help administrators manage a variety of cloud-related tasks such as resource provisioning, data integration, and disaster recovery. These management solutions also provide management control for platforms, applications, and infrastructure. The following are some important management applications:

- Toggl: Users can use Toggl to keep track of how much time they have budgeted for a project.
- Evernote: Evernote allows you to keep and sync all of your recorded, typed, and other notes in one location. There are two versions, a free version and a premium version. The platform forms used include Windows, macOS, Android, iOS, browsers, and Unix.
- Outright: Administrative users use Outright to track their accounts. It allows you to track your income, expenses, profits and losses in real time.
- GoToMeeting: GoToMeeting provides a video and online meeting app that lets you start a meeting with your colleagues anytime, anywhere from your phone or tablet. You can use the GoToMeeting app to perform management activities such as: For example, you can join a meeting in seconds, view a presentation on a shared screen, or receive notifications for upcoming meetings.

7. Social Applications

Social cloud apps enable a huge number of people to connect with one another via social networking sites like Facebook, Twitter, and LinkedIn. The following cloud-based social applications are available:

- Facebook: Facebook is a social networking site that uses a cloud storage system to allow active users to share files, images, videos, status updates, and more with their friends, relatives, and business partners. Whenever a friend likes and comments on our post, we will be notified on Facebook.
- Twitter: Twitter is a social media platform. It's a system for microblogging. It lets users follow celebrities, friends, and family members, as well as get news. It sends and receives tweets, which are short messages.
- Yammer: Yammer is the greatest team collaboration system for chatting, document sharing, and video sharing among a group of employees.
- LinkedIn: LinkedIn is a professional and student social networking site.

16

16. Conclusion And Future Work

Cloud computing has some security concerns which if not handled efficiently can prove to be lethal to the organizational data as well as the impact of the organization. We have discussed some major concerns which one should pay attention to while migrating to cloud computing and assess the cloud platform in detail. Also, here the information provides a broad-level overview of important current and emerging security concerns in cloud and delineate main research challenges.

Cloud computing security evolves with risk. The risk is that the discovery is often too late to prevent the incident. To effectively mitigate risk, you need to build security at all levels of your cloud computing platform by integrating best practices and new technologies.

Additionally, there is very limited research on training and people's impact on security. You can work to understand the challenges, requirements, and implications of effective safety training for consumers and other providers. The increasing use of cloud computing for data storage certainly reinforces the trend to improve the potential of data storage in the cloud. If data stored in the cloud is not securely protected, it may be at risk. This paper discussed the risks and security threats to data in the cloud and gave an overview of three types of security concerns. Examine virtualization to find threats posed by hypervisors.

Threats from the public cloud and multi-tenancy were also discussed. One of the main concerns of this white paper is data security and its threats and solutions in cloud computing. We've talked about data in different states, along with an efficient method for encrypting data in the cloud. This study provided an overview of the block ciphers, stream ciphers, and hash functions used to encrypt data in the cloud, whether the data is stationary or in motion.

In the first research paper, we see that Cloud computing has some security concerns which if not handled efficiently can prove to be lethal to the organizational data as well as the impact of the organization. We have discussed some major concerns which one should pay attention to while migrating to cloud computing and assess the cloud platform in detail. Here, the information provides a broad-level overview of important current and emerging security concerns in the cloud and delineate main research challenges. In the second paper, we talk about Security in cloud computing that is evolving in step with risks as they are discovered often too late to prevent incidents. Security must be built at all levels of the cloud computing platform by incorporating best practices and new technologies to effectively mitigate risk. In the third paper, we see that the increased use of cloud computing for storing data is certainly increasing the trend of improving the ways of storing data in the cloud.If data stored in the cloud is not securely protected, it may be at risk. One of the main concerns of this white paper is data security and its threats and solutions in cloud computing. We've described data in different states, along with efficient techniques for encrypting data in the cloud. This study provided an overview of the block ciphers, stream ciphers, and hash functions used to encrypt data in the cloud, whether the data is stationary or in motion.

17

17. Acronyms

CC	Cloud Computing
CSPs	Cloud Service Providers
SLR	Systematic Literature Review
ACIRS	Autonomous Cloud Intrusion Response System
NICE	Network Intrusion Detection and Countermeasure Selection System
ATM	Attack Tree Map
ARPANET	Advanced Research Projects Agency Network
VMware	Virtual Machine Ware
VMM	Virtual Machine Monitor
EC2	Elastic Compute Cloud
S3	Simple Storage Service
TOSCA	Topology and Orchestration Specification for Cloud Applications
SSL	Secure Sockets Layer
XML	Extensible Markup Language
YAML	Yet Another Markup Language
DO	Data Owner
I/O	Input - Output
CPU	Central Processing Unit
DevOps	Development and Operations
AWS	Amazon Web Services
GCP	Google Cloud Platform

18

18. References

1. https://ieeexplore.ieee.org/document/9404177
2. Shubhashis Sengupta, Vikrant Kaulgud, Vibhu Saujanya Sharma "Cloud Computing Security – Trends and Research Directions" 2011 IEEE World Congress on Services, Conference Paper · July 2011, DOI: 10.1109/SERVICES.2011.20
3. Gururaj Ramachandra, Mohsin Iftikhar, Farrukh Aslam Khan "A Comprehensive Survey on Security in Cloud Computing" The 3rd International Workshop on Cyber Security and Digital Investigation (CSDI 2017), Procedia Computer Science 110 (2017) 465–472
4. Ahmed Albugmi, Madini O. Alassafi, Robert Walters, Gary Wills "Data Security in Cloud Computing" International Conference on Future Generation Communication Technology (FGCT 2016), Conference Paper · August 2016, DOI: 10.1109/FGCT.2016.7605062
5. Prashant Agrawal, Neelam Rawat, "Devops, A New Approach To Cloud Development & Testing", 2019 2nd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 978-1-7281-1772-0 ©2019 IEEE
6. Varsha C L, Dr. Ashok Kumar A R, "Review on Cloud Automation Tools", International Journal of Engineering Research & Technology (IJERT), Vol. 9 Issue 05, May-2020
7. Leonardo Rebouc¸as de Carvalho, Aleteia Patricia Favacho de Araujo, "Performance Comparison of Terraform and Cloudify as Multicloud Orchestrators", 2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID), 978-1-7281-6095-5/20/$31.00 ©2020 IEEE
8. https://www.simplilearn.com/tutorials/cloud-computing-tutorial/cloud-computing-architecture
9. https://www.vmware.com/topics/glossary/content/cloud-architecture
10. https://journals.sagepub.com/doi/full/10.1155/2014/190903
11. https://www.ijert.org/research/review-on-cloud-automation-tools-IJERTV9IS050156.pdf
12. https://arxiv.org/ftp/arxiv/papers/1912/1912.10821.pdf
13. Terraform Architecture [Online]: https://www.terraform.io/docs/enterprise/before-installing/referencearchitecture/index.html
14. Puppet architecture documentation https://puppet.com/docs/puppet/latest/architecture.html
15. L. A. Vayghan, M. A. Saied, M. Toeroe, and F. Khendek, "Deploying Microservice Based Applications with Kubernetes: Experiments and Lessons Learned," in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 970–973
16. Suyel Namasudra, Pinki Roy and Balamurugan Balusamy, "Cloud Computing: Fundamentals and Research Issues" 2017 Second International Conference on Recent Trends and Challenges in Computational Models, 978-1-5090-4799-4/16, 2017 IEEE
17. Deepak Puthal, B. P. S. Sahoo, Sambit Mishra, Satyabrata Swain, "Cloud Computing Features, Issues and Challenges: A Big Picture" 2015 International Conference on Computational Intelligence & Networks, 2375-5822/15, 2015 IEEE