International Journal of Computing, Programming and Database Management

**E-ISSN:** 2707-6644
**P-ISSN:** 2707-6636
IJCPDM 2022; 3(2): 01-04
Received: 03-04-2022
Accepted: 05-05-2022

**Kishori Chandrakant Budhale**
Assistant Professor,
Department of BCA,
Vivekanand College
(Autonomous) Kolhapur,
Maharashtra, India

**Vijay Bapuso Pujari**
Professor and Head,
Department of BCA,
Vivekanand College
(Autonomous) Kolhapur,
Maharashtra, India

# Cloud computing: A study of mechanism & cloud cryptography

**Kishori Chandrakant Budhale and Vijay Bapuso Pujari**

**Abstract**

Cloud Computing is the on-demand delivery of computing services, databases, storage, applications, networking, and many more through the internet. Cloud Computing technology refers to pay-as-you-go pricing. The cloud delivers a hosting environment that is immediate, flexible, scalable, secure, and available which saves enterprise money, time, and resources. As we are going to use the internet services, security is the major factor to be taken into consideration. Cloud cryptography is a way through which we can secure our data on the internet. Cryptography adds several layers of protection to avoid breaching, hacking, or getting affected by malware. So in this survey, we are going to study the mechanism of cloud computing and how the activities on the cloud can be secured over the internet.

In comparison to private clouds, which can scale effortlessly and on-demand, the public cloud has a massive infrastructure. IaaS is a method of delivering cloud-computing infrastructures such as servers, storage, networks, and operating systems to customers. Customers can get on-demand access to materials here. Cloud cryptography is a type of encryption that employs a number of algorithms to turn plain text into cipher text. Because symmetric cryptography is substantially faster than asymmetric cryptography, it is ideally suited for bulk data encryption.

Using a single key, this technique enables data authentication and permission. The strength of an asymmetric key in assuring the security of information supplied during transmission is significantly greater.

**Keywords:** Cloud, cryptography, decryption, encryption, hybrid, security

## 1. Introduction

Cloud computing provides on-demand services of computer power, database, storage, applications, and other IT relevance through a cloud service platform. It works as pay-as-you-go pricing. Clouds are essentially large distributed computing facilities that make available their services to third parties on demand. The goal of cloud computing is to allow the users to take advantage of technology without having to worry about the software and technical updates and maintenance. In simple terms, cloud computing allows you to pay for use instead of buying your hardware and software outright. It provides speed, scalability, and flexibility which enables businesses to develop, innovate and support business IT solutions. The main point to be focused on in Cloud is Virtualization. Virtualization means creating a virtual hardware platform, storage devices, and computer network resources.

Cryptography, according to privacy experts, is the foundation of security. Cloud cryptography is the encryption of data stored in the cloud, which provides an extra layer of security and prevents data breaches. This method protects data while not impeding data delivery. According to cryptography expert Ralph Spencer Power, "cryptography can better safeguard both information in motion and information at rest." Virtual data must be stored cryptographically while keeping control of the cryptographic key."

## 2. Cloud Storage Device

Storage devices created exclusively for cloud-based provisioning are represented by the cloud storage device mechanism. These devices' instances can be virtualized in the same way that physical servers can spawn virtual server images. In support of the pay-per-use system, they are frequently able to provide fixed-increment capacity allocation. Cloud storage devices can be accessible to the internet for remote access.

The security, integrity, and confidentiality of data, which is more vulnerable to being hacked when entrusted to external cloud providers and other third parties, is a major problem associated with cloud storage.

**Corresponding Author:**
**Kishori Chandrakant Budhale**
Assistant Professor,
Department of BCA,
Vivekanand College
(Autonomous) Kolhapur,
Maharashtra, India

Relocating data across geographical or national boundaries might potentially have legal and regulatory ramifications. Another issue is the performance of huge datasets in particular. LANs provide network dependability and latency levels that are superior to WANs for locally stored data.

## 3. Benefits of Cloud Computing

Cloud computing has numerous advantages for your company. It enables you to set up what is basically a virtual office, giving you the freedom to connect to your business from anywhere, at any time. Access to your data is becoming much easier with the expanding number of web-enabled devices utilized in today's work environment (e.g., smartphones, tablets).

- Working in the cloud, one can store a large amount of data without having to worry about the space, where the device does not need large internal storage.
- Backups and recovery can be done easily.
- Activities like creating, storing, and sharing a file are convenient.
- We can access the cloud from anywhere and on any computing device having an internet connection.
- Using Cloud can help in project collaboration.
- Cloud computing is environment-friendly as it allows multiple workers to work.
- It can be less expensive compared to buying software and hardware.
- Compatible with most computers and operating systems.
- Customers don't need to focus on updates and hardware maintenance.

## 4. General Categories of Cloud Computing

Cloud computing refers to a variety of classifications, types, and architecture models. People's jobs or work have been altered by this networked computing concept. But the cloud isn't just one thing; cloud computing may be divided into three broad categories:

### 1) Private Cloud

A private cloud is a cloud infrastructure designed and developed solely to be used for an organization. The private cloud provides services to limited users. All the data is protected behind the Firewall. These are limited in aspects of size and scalability. Private clouds are managed internally or by a third party and hosted either internally or externally. Here the provider facilitates the exchange of cloud environments with a full guarantee of privacy. This is best suited for those that do not prefer a public cloud due to sharing of physical resources.

### The Advantages of Private Cloud

The following are the most prominent advantages of private cloud computing:

**Exclusive settings:** Environments that are dedicated and secure cannot be accessed by other companies.

**Customs protection:** Organizations can use protocols, configurations, and measures to personalize security based on individual workload requirements, allowing them to comply with tough standards.

**Scalability without compromise**: High scalability and efficiency to satisfy erratic demands while maintaining security and performance

**Effective performance:** The private cloud is dependable in terms of performance and efficiency.

**Flexibility:** The private cloud is adaptable as you modify the infrastructure to meet the organization's ever-changing business and IT requirements.

### 2) Public Cloud

The public cloud is large in infrastructure as compared to private clouds which can provide the ability to scale seamlessly and on-demand. This is a pay-as-you-go model. The public cloud can also be free of charge. Architecturally public and private cloud seems slightly different but as we consider security constraints, it is difficult to manage it on the public cloud as it is shared among multiple customers. All the customers share the infrastructure pool with limited configuration, security, protection, and availability of variances. These are owned and operated by third parties. The public cloud is more efficient and inexpensive compared to the private cloud and hybrid cloud.

### Advantages of Using the Public Cloud

People value the following public cloud advantages:

**There is no CapEx:** There are no investments necessary to develop or maintain the IT infrastructure.

**Technical dexterity**: High scalability and adaptability to meet erratic workload demands.

**Concentration on business:** Because the cloud vendor manages the infrastructure, the complexity and reliance on in-house IT skills are decreased.

**Affordability:** Pricing choices that are flexible based on different SLA offerings

**Cost flexibility:** Cost agility enables firms to pursue lean growth strategies and concentrate their spending on innovative projects.

### 3) Hybrid Cloud

As the name suggests, a hybrid cloud is a combination of both public and private clouds. It allows one to extend either the capacity or the capability of a cloud by aggregation, integration, or customization with another cloud service. A hybrid cloud is capable of providing on-demand, externally provisioned costs. A hybrid cloud preferably serves to eliminate limitations inherent to the multi-access relay characteristics of private cloud networking. The advantages include enhanced runtime flexibility and adaptive memory processing unique to virtualized interface models.

### The Advantages of Hybrid Cloud

**Option based on policy:** Flexible policy-driven workload distribution across public and private infrastructure environments based on security, performance, and cost constraints.

**Scale with security in mind:** Scalability is achieved in public cloud systems without exposing sensitive IT workloads to inherent security threats.

**Reliability:** Service reliability is maximized by distributing services across many data centers, some public and others private.

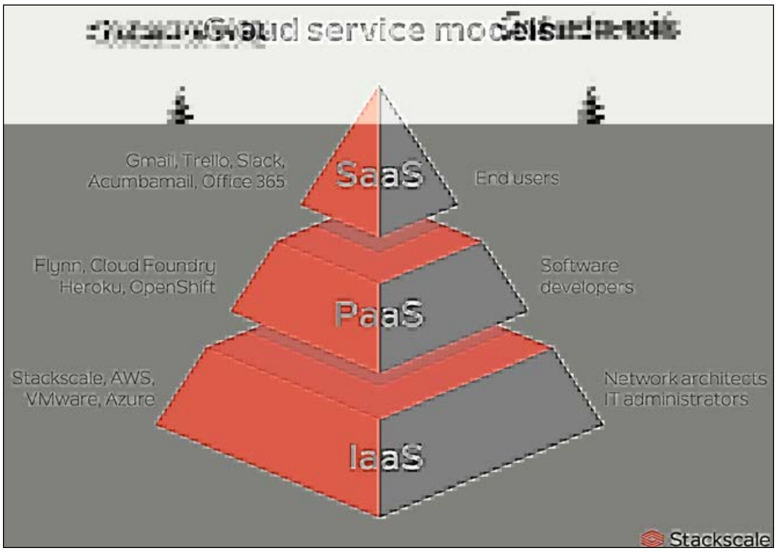
**Cost management**: Improved security posture as sensitive IT workloads run on dedicated resources in private clouds, while normal workloads are distributed across low-cost public cloud infrastructure as a cost-cutting measure.

## 5. Cloud Computing Models

The cloud computing approach enables the delivery of programs over the Internet while eliminating the costs of owning and managing data centers and leveraging the efforts of software developers. Cloud computing and services are typically based on infrastructure ownership (and to whom services are supplied) and the basic architecture visible to consumers (e.g., are they providing a platform for applications, or are they providing complete application software solutions as a service). Cloud computing can be categorized into three primary models based on the services provided:

- Software-as-a-Service (SaaS)
- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)

The Cloud Computing Stack is made up of these three services, with SaaS at the top, PaaS in the middle, and IaaS at the bottom.



**Source**: https://www.stackscale.com/wp-content/uploads/2020/04/cloud-service-models-iaas-paas-saas-stackscale.jpg

**Fig 1:** Cloud service models

In today's world, there are more than three service models in use. More service models are developing as usable models, such as "Data Analytics as a Service" and "HPC/Grid as a Service." The availability of appropriate application software, the need for a product testing environment, the need for impactful computing infrastructure coordination and monitoring, the required distribution of data, services, and infrastructural facilities, and the existence and complexity of enterprise IT, infrastructure, and datacenter/warehouse are all important factors to consider when choosing the right service model. The deployment models can also be used to categorize cloud computing. These classifications are based on an organization's capacity to manage business needs while also securing assets.

**SaaS:** SaaS is known as ‘on-demand software. SaaS is a software distribution model through which applications are shared on a cloud by a service provider. Customers need not have to install applications on their device; rather these are accessed over.

**PaaS:** This environment enables users to develop, manage and deliver applications. In such cloud architecture, users are able to use pre-built tools to develop, customize and test their own applications. Developers can write and deploy the applications easily and directly into the PaaS layer. Paas enables users to focus on development without carrying about the underlying infrastructure. The service providers manage security, operating system, server, software, and backups.

**IaaS:** IaaS was earlier referred to as hardware as a service. Hardware as a service differs from IaaS, in the way that users have to bare hardware on which they can deploy their own infrastructure using the most appropriate software. IaaS is a way to deliver a cloud computing infrastructure like server, storage, network, and operating system. Customers can access here resources as required on-demand. Rather than purchasing servers, software, datacenters space, or network equipment, one can buy them on rent as per the need. one can dynamically select a C.P.U, memory storage, and configuration according to need. Customers can use a vast computing storage space or computing power available on the IaaS cloud platform. This will eventually reduce enterprises' cost of buying and maintaining their own hardware.

## 6. Cloud Cryptography

With the evolution of cloud computing, there is a noticeable need for security solutions over the internet. Cloud Cryptography is a mechanism that safeguards data stored over the cloud. Cloud cryptography is encryption in which several algorithms are used to convert the plain text into cipher text. This cipher text can then be decrypted into plain text by using an encryption key, which will decode it with a series of bits. Hence, Cryptography deals to protect information from unauthorized users by converting the data into non-readable text. Many organizations follow various cryptographic protocols for their cloud computing to keep a balance between security and efficiency. The cryptography algorithms used for cloud security are:

### Symmetric key cryptographic algorithm

This algorithm provides authentication and authorization of the data using a single key used for encryption as well as decryption. Data encrypted using a single unique key cannot be decrypted with any other key. This key is also known as secret-key cryptography or private key cryptography. The symmetric key is best suited for bulk data encryption as it is much faster than asymmetric cryptography. Before communication over the network, both parties must exchange a shared secret key, which should not be shared with other communication partners. Both the parties will produce the same cipher text and plain text at their end. Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES) are the most popular symmetric-key algorithms used in cloud computing cryptography.

### Asymmetric Cryptography Algorithm

Asymmetric cryptography is also known as public-key cryptography which uses two keys to encrypt plain text. These two keys are the public key and a private key. The public key can be available to anyone. The private key is kept secret. A message that is encrypted with a public key can only be decrypted using a private key and vice-versa. Security of public keys is not necessary because it is publically available and can be passed over the internet. The public key is made available to anyone who wants to send you a message while the private key is kept secret so that you can only know. Asymmetric key has far better power in ensuring the security of information transmitted during communication.

### Cloud Cryptography's Advantages

- 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 sent from one computer to another, it gets encrypted. Cloud encryption allows enterprises to be proactive in their protection against data breaches and cyber-attacks, and it has become a need in today's data-driven society.
- Receivers of data have the ability to detect if the data is corrupted, allowing for a quick response and solution to the attack or any technical harm.
- Because encryption complies with the limits imposed by organizations like as FIPS, FISMA, HIPAA, or PCI/DSS, it is one of the safest techniques for storing and transferring data.

## 7. Conclusion

In this paper, cloud computing and its various types are discussed and also types of models of cloud computing are focused on. It also includes cloud security constraints which are also important when we are working on the internet. The study also provides an overview of different algorithms used for data security. I will be working more on balancing security. As the development of cloud computing technology is still under research and development, there will be a better understanding of the design challenges of cloud computing and pave the way for further research in this area.

## 8. Acknowledgment

The authors are thankful to all the friends and Faculty of Vivekanand College Kolhapur for motivating us to write this paper. All the references are hereby acknowledged used in this paper.

## 9. References

1. https://patterns.arcitura.com/cloud-computing-patterns/mechanisms/cloud_storage_device
2. https://www.business.qld.gov.au/running-business/digital-business/digital-risk-compliance/cloud-computing/benefits
3. https://www.bmc.com/blogs/public-private-hybrid-cloud/
4. https://www.greycampus.com/cloud-computing-certifications/cloud-computing-models
5. Kiran Gurbani, Nitesh N Shukla, Raveena Shetty Tilak. Cloud Computing-A Himalaya Publication (2015 certified).
6. Murthy CSV. The Anatomy of Cloud Computing- A Himalaya Publication (2015 certified).
7. https://www.geeksforgeeks.org/an-overview-of-cloud-cryptography/
8. https://www.oracle.com/in/cloud/what-is-cloud-computing/
9. https://www.techtarget.com/searchstorage/definition/cloud-encryption-cloud-storage-encryption.
10. https://www.investopedia.com/terms/c/cloud-computing.asp
11. Sciencedirect.com