IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 6, June 2023

DOI: 10.17148/IARJSET.2023.10639

CLOUD COMPUTING AND GRID COMPUTING

Sachin B.K[1], Prof. Mohammed Mueen Pasha[2]

MCA student, School of CSA, REVA UNIVERSITY[1]

Assistant Professor, School of CSA, REVA UNIVERSITY[2]

Abstract: The advent of cloud computing is a watershed moment in the evolution of the information technology industry. The term "cloud computing" is used to describe the practice of using on-demand, scalable, and shared server space. In addition to just having to pay for the resources they really use, companies also don't have to worry about things like setting them up or keeping track of their use. Google Cloud Platform (GCP) is a top cloud application programming interface (API) nowadays. GCP's portfolio of public cloud services, built on a massive, stable infrastructure, has contributed to significant growth in the short time since the company's inception five years ago. The Google Cloud Platform is a collection of cloud computing services that aims to satisfy the requirements of a broad variety of cloud computing users. These services include computation, storage, and networking. Google Cloud Platform (GCP) is a public cloud provider that provides a wide range of computing services, such as data management, web and video content delivery via the internet, and artificial intelligence (AI) and machine learning (ML) applications. Using Google's own infrastructure, you can create, deploy, and scale your own apps, websites, and services using Google Cloud Platform. With its roots in the Google App Engine architecture, GCP is a collection of cloud computing services that allows websites to be hosted in Google's data centers. Customers of Google Cloud are the rightful owners of their data and have the right to decide how that data is used. All data stored, transmitted, or processed using Google Cloud is encrypted at every stage. Your data, apps, infrastructure, and customers are all safeguarded on Google Cloud by the same infrastructure and security services that Google employs to prevent fraud, spam, and abuse.

Keywords: Cloud computing, Google cloud platform, APIs.

I. INTRODUCTION

Customers of Google Cloud are the legal custodians of their data and should have the last say in how it is utilized. Stored information in Google Cloud is automatically encrypted when resting. Our Cloud Key Management Service (Cloud KMS) platform gives you better control over the whereabouts and safety of your encryption keys and data at rest [1]. Customers using Google's application and storage services on the Google Cloud Platform (GCP) have the option to encrypt their data, as is the case with other cloud service providers.

The Cloud KMS platform is a cloud service provided by Google Cloud to its customers [1] that allows for the centralized management of cryptographic keys for use with Google Cloud resources and applications. Using Cloud Key Management Service, you may do all of your cryptographic tasks in the cloud, including creating, importing, and managing cryptographic keys. To generate and utilize keys using Cloud KMS, Cloud HSM, Cloud External Key Manager, or Customer-Managed Encryption Keys (CMEK), all you need is a Google Cloud connection to another service. With Cloud KMS, you have a verifiable and monitorable root of trust over your data, and you are the data's ultimate custodian. Cryptographic keys may be handled on the cloud in the same manner they are handled locally. Key management may be done remotely using CloudKMS.

Maintain the same level of command over cloud-stored cryptographic keys as you do locally [4].

Key Management Service

In certain cases, a Key Management Service (KMS) may make managing cryptographic keys easier. Use a Key Management Service (KMS) to generate cryptographic keys and control how they are used across different applications and operating systems. Using encryption keys and Cloud KMS's REST API, sensitive data such as passwords may be safely stored. Google's encryption services are managed in the cloud through Google Cloud Key Management Service (KMS). By using the Google Cloud Key Management Service (GMS), which is an integral part of the Google Cloud Platform (GCP), customers may effortlessly manage encryption keys for data stored in the cloud. Using a cloud-based Key Management Service (KMS), users may securely store, produce, and share their cryptographic keys. Data in Google Cloud Storage is secured while it is resting. Users have more say over the security of their data at rest and the safety of their encryption keys when they use a platform like Cloud Key Management Service (Cloud KMS).

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 6, June 2023

DOI: 10.17148/IARJSET.2023.10639

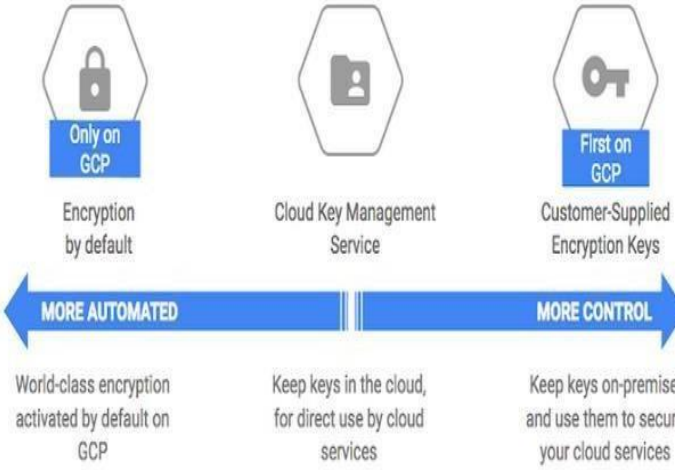


Figure 1.1 Key Management Service

The following are the available choices for key generation while using Cloud KMS::

[1] Cloud Key Management Service) to encrypt data using a symmetric or asymmetric key that you control.
[2] If you're in need of a hardware key, Cloud HSM can assist you restrict access to just FIPS 140-2 Level 3-validated HSMs, where your symmetric and asymmetric keys will be safe.
[3] If you need to employ cryptographic keys that you produce yourself, Cloud KMS allows you to import them.
[4] If you'd like, you may utilize your 5Cloud KMS key with Google Cloud's other services. The initials "CMEK" stand for "customer-managed encryption key." The CMEK function may be used to produce, utilize, rotate, and remove encryption keys needed to secure data in other Google Cloud services.
[5] Keys may be generated and managed outside of Google Cloud via Cloud External Key Manager (Cloud EKM), and then the Cloud KMS platform can be set up to make use of those keys, further bolstering the security of data at rest. [1]

Figure 1.2 Google Cloud portfolio

Cloud KMS Platform Overview

The Cloud KMS platform allows for the use of both hardware and software-based keys for encryption and digital signing, and it supports a variety of cryptographic techniques. The Cloud Identity and Access Management (IAM) and Cloud Audit Logs platforms are coupled with the Cloud Knowledge Management System (KMS) so that you can:

Control access to keys and monitor their activity.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 6, June 2023

DOI: 10.17148/IARJSET.2023.10639

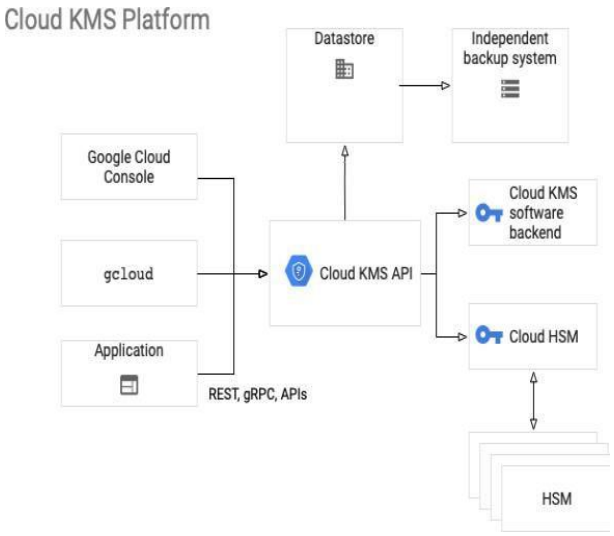


Figure 1.3 Cloud KMS Architecture

The graphic demonstrates how the Cloud KMS platform is put together.

The Google Cloud Control Panel, the gcloud order line tool, and apps that make use of the REST or gRPC APIs are the primary entry points via which administrators interact with the primary authoritative services. Both the REST API and gRPC are available to apps for communicating with the key management service. [1]

The usage of customer-managed encryption keys (CMEK) enables an app to access any Google service. In contrast, CMEK uses the Cloud KMS API. The Cloud KMS API may be used to combine the functionality of software-based key management systems (Cloud KMS) with that of hardware-based key storage modules (Cloud HSM). Both hardware- and software-based keys may access Google's security features.

After a client receives a key through the cloud KMS platform, they may choose a granularity at which the key backend will be responsible for key generation and cryptographic operations.

The Cloud KMS platform, in contrast to Cloud EKM, gives users access to not one but two backends via the Cloud KMS API. The protection level of a program determines the safety of keys that may be unwrapped by a software security module to carry out cryptographic operations. To decode keys protected by an HSM, all cryptographic operations must be performed inside the HSM itself.

Cloud Storage, BigQuery, and Compute Engine are just few of the Google Cloud Services that work with CMEK. Customers may use the Cloud KMS platform and CMEK to manage the encryption keys used by these services.

Modules that have been verified against FIPS 140-2 execute all cryptographic activities in the cloud for KMS.

Benefits of Key Management Service

Raise the bar on worldwide protection: Take use of Google's worldwide reach to rapidly expand your user base while you relax knowing that Google is handling the complexities of key management on your behalf.

To assist you in satisfying mandated requirements, An External Key Manager, customer-provided keys, FIPS 140-2 Level 3-approved HSMs, and software-backed encryption keys all make it feasible to secure cloud data simply.

Take advantage of Google Cloud product integrations: To manage data encryption across Google Cloud products and take use of extra security features like Google Cloud IAM and audit logs, use customer-managed encryption keys (CMEK).

Key features

Use a cloud-based key management service to control and monitor all of your cloud services' symmetric and asymmetric cryptographic keys from one convenient place.

Use HSM to protect hardware keys: Easily switch between two different types of encryption keys, one secured by

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 6, June 2023

DOI: 10.17148/IARJSET.2023.10639

software and the other by hardware. Use Hardware Security Modules (HSMs) verified to FIPS 140-2 Level 3 to store and process encryption keys.

EKM's ability to accommodate external keys is crucial. Your encryption keys for BigQuery and Compute Engine data may be stored and managed in an externally hosted key management system..

Cloud KMS allows users to create, store, rotate, and remove symmetric and asymmetric cryptographic keys, including AES256, RSA 2048, RSA 3072, RSA 4096, EC P256, and EC P384.

To avoid unintentional or malicious data loss, Cloud KMS includes a 24-hour wait before destroying crucial material.
API-based key management service (KMS) that encrypts, decrypts, and signs data such as secrets before storing it.
For minimal latency and maximum uptime, host your service anywhere you choose using Cloud KMS, since it is accessible in several areas across the world. [3]

II. ENCRYPTION CONCEPTS AND KEY MANAGEMENT AT GOOGLE

Some key management phrases and meanings are laid forth here, with reference to Google's elaborate key management system.

Key: A specific thing with a name that stands in for a cryptographic key. As we rotate the keys or generate new copies of the keys, the bits that this pointer references may change.

Cloud KMS may be used with either symmetric or asymmetric keys. To protect sensitive information, symmetric encryption techniques like AES-256 in GCM mode may be used in conjunction with a symmetric key to cipher a block of plaintext. You may generate digital signatures and encrypt data using asymmetric keys.

A key ring is a convenient way to keep all of your keys together. Each set of keys is associated with a particular Google Cloud project and has its own home. IAM policies are sent down to keys from the key ring they are stored in. Rather than having to manually give, cancel, or adjust permissions for each key, you may do it at the key ring level by grouping them with keys that share similar rights. If you don't find the organization provided by key rings to be helpful, you may always adjust rights on individual keys.

Key metadata: Names of resources, information on the characteristics of KMS assets including IAM policies, key types, and key sizes key state, and any information generated from the above. Metadata of critical importance may be handled independently of the critical content.

Key version: Key information at a given period is shown here. The most important version of a resource is the one that provides the most important information. Each subsequent version is given a higher number. After a key is spun, a fresh version of that key with brand new key material is produced. Over time, several iterations of the same logical key might emerge, reducing the utility of any one variant. There will always be a “primary” form of a symmetric key. By default, encryption is performed using this version. Decryption using symmetric keys in Cloud KMS is handled automatically by determining which key version is required. [1]

Key hierarchy

The following diagram depicts Google's internal Key Management Service's key hierarchy. Cloud KMS makes use of Google's own KMS by having Google KMS encrypt and sign Cloud KMS keys. The trust foundation for Cloud KMS and Google KMS are the same.

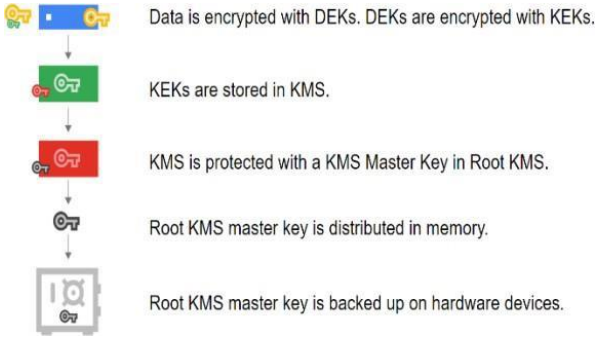


Figure 2.1 Internal key hierarchy

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 6, June 2023

DOI: 10.17148/IARJSET.2023.10639

What is meant by “data encryption key” (DEK)?
A KEK is a cipher key that is used to encrypt another cipher key. When using a Cloud KMS, whether it be software, hardware, or an external backend, you are in full control of the encryption key at all times.
.
KMS Master Key: The KEK encryption key is the key used to encrypt the KEKs itself. This secret code is disseminated through

memory. Hardware devices provide as backups for the KMS Master Key. Your keys are encrypted using this key.
Root KMS: Key administration service used internally by Google. [2]
A Cloud KMS key is a named object that may store information and multiple copies of a key. There is only one set of keys for a given address.

Permissions and roles in Identity and Access Management (IAM) may be used to provide or revoke access to keys. Controlling who has access to a master copy is impossible. When a key is disabled or destroyed, all copies of that key are either useless or destroyed as well.

III. CREATE KMS KEY IN GOOGLE CLOUD PLATFORM

Create a key ring

STEP 1: Go to the key management page in the cloud console.
STEP 2: Click Create key ring.

STEP 3: In the Key ring field, enter the name for your key ring.
STEP 4: From the key ring location dropdown, select a location like “us-east1”.
STEP 5: Click Create. [5]

Cloud KMS Pricing
Cloud KMS's Cloud Key Management Service, Cloud External Key Manager, and Cloud Hardware Security Module all have their own rates, which may be found on their separate websites. The price of employing a cloud-based key management service depends on three variables: the total number of active key versions, the security level of those versions, and the use rate. Separate pricing models exist for the Cloud Key Management Service, Cloud Hardware Security Module, and Cloud Outer Key Director.

Cloud External Key Manager
Users of GCP have access to the Google Cloud Key Management Service (KMS), which supports Cloud External Key Management (EKM). While your encryption keys are safely held in an external key management provider, your GCP data is safeguarded by Key Broker for Google Cloud EKM. To encrypt data in ComputeEngine or BigQuery, or to safeguard data using a symmetric key, users generate encryption keys in Key Broker for Google Cloud EKM, generate a Cloud EKM key, and then identify the externally managed key in Google Cloud KMS using a key URI. An external key encryption key (KEK) may be used as a wrapping key in GCP projects, and Google Cloud External Key Manager (EKM) is a cloud native service that allows access to such a KEK. If you use Google Cloud EKM to add keys to your key ring, you may use the CCKM interface with GCP EKM to manage the endpoints for those KEKs. You may also utilize Thales or Fortanix, two examples of external Key Managers that can be used with Cloud External Key Manager (Cloud EKM) [8]. Customers using Cloud EKM and the related EKM service must make an explicit risk tradeoff between the availability of their cloud workloads and the security of their data. Using off-cloud encryption keys to encrypt data at rest in the cloud introduces additional failure modes that might lead to inaccessibility or even loss of data saved un Google Cloud services. High availability and fault tolerance included into the EKM service's architecture are crucial for dealing with these issues [13].

Customer-managed encryption keys (CMEK)
Clients have greater say over the encryption keys used in their Google Cloud projects thanks to Cloud Key Management Service (Cloud KMS), a component of several Google Cloud services. The term “customer-managed encryption keys” (CMEK) refers to the fact that the customer is responsible for maintaining these keys. When encrypting data using Google Cloud Services, the CMEK key remains under your control at all times.
There is no guarantee that using CMEK will make your data safer than using Google's built-in encryption features. There are also Cloud KMS-related fees to consider while utilizing CMEK. More of the system's parameters can be adjusted with CMEK's help.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 6, June 2023

DOI: 10.17148/IARJSET.2023.10639

keys, including (but not limited to) the following skills pertaining to their lifespan and management:

a. Disabling Google's access to the keys used to decrypt your data at rest gives you control over Google's ability to access your data.
b. Your data may be encrypted using a key that satisfies jurisdictional or residency restrictions.
c. The encryption keys protecting your information may be changed either automatically or by hand.
d. A Cloud HSM key, a Cloud External Key Manager key, or an existing key imported into Cloud KMS may all be used to encrypt your data. [7]

A service is considered to be CMEK-integrated if and only if it supports the CMEK protocol. When it comes to securing various forms of service-related data, certain services, like GKE, offer several CMEK interfaces.

Temporary data is encrypted by a CMEK-compliant service using a key that is generated in memory and never persisted to disk. The temporary key is removed from memory when the data is no longer being used, making the encrypted data inaccessible even if the storage resource is still available.

To verify that CMEK is being used consistently throughout an organization, Google Cloud provides two organizational policy limitations. Administrators of an organization may use these controls to mandate the use of CMEKs and restrict access to certain Cloud KMS keys for CMEK security. [7]

With CMEK, you may encrypt data at rest in Cloud SQL with your own private keys. After adding customer-managed encryption keys, Cloud SQL will utilize your key anytime an API request is performed. Data encryption keys (DEK) and key encryption keys (KEK) are controlled by Google and used to encrypt Cloud SQL. [6]

Customer Supplied Encryption Keys

Client-supplied encryption keys (CSEK) are supported by both Google Cloud Storage and Google Compute Engine. You may encrypt and decrypt your data using Google's collection of randomly generated keys, or you can give your own encryption key. You have the option of adding your own AES-256 key, encoded in the industry-standard SHA-256 format, on top of the encryption keys handled by Google.

Base64. A customer-supplied encryption key is the term for this kind of key. Cloud Storage does not permanently retain or manage a customer-supplied encryption key on Google's servers. Both Google Cloud Storage and Google Compute Engine support CSEK, or customer-supplied encryption keys. If you provide your own encryption key, Google will use it to encrypt and decode your data using a set of randomly generated keys provided by Google. All stored data is encrypted by default on Google Compute Engine. You don't have to do anything special to have Compute Engine manage and handle this encryption; it happens automatically. You may, however, provide your own encryption keys and take charge of this encryption yourself. [10]

Figure 2.2 Cloud Key Management service

Google cloud HSM

You may store encryption keys and conduct cryptographic operations in a group of cloud-hosted Hardware Security Modules (HSMs) that have been certified as compliant with FIPS 140-2 Level 3. The HSM cluster is managed by Google, so you won't have to stress about clustering, scaling, or patching. Cloud HSM's front end is Cloud KMS, so you get all the benefits of that service as well [11].

Although all client data-at-rest is encrypted by Google Cloud, certain customers, particularly those concerned with compliance rules, want access to the encryption keys. Google Cloud provides Cloud HSM for such users.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 6, June 2023

DOI: 10.17148/IARJSET.2023.10639

protection service for keys using a hardware security module.
Key generation and other cryptographic operations may be carried out on FIPS 140-2 Level 3 certified HSMs in the cloud using Cloud HSM. With this service, you can be certain that your most critical workloads are secure without incurring the administrative burden of running an HSM cluster [12].

Cloud HSM is available everywhere in Google's cloud, from the smallest to the biggest. When you turn on Cloud HSM, you may immediately begin utilizing HSM-backed keys to encrypt data in other Google Cloud services like BigQuery, Cloud Storage, and Persistent Disk.

Cloud HSM and the HSM hardware are managed by Google, relieving you of the burden of coordinating the usage of HSM-backed keys in production or worrying about compromising data security due to resource sharing with other Google Cloud tenants or services. Cloud HSM's data plane API is a breeze to work with, and it's included in Cloud Key Management Service API.

Anywhere that Google Cloud supports customer-managed encryption keys (CMEK), Cloud HSM may be used to provide additional protection through a hardware security module (HSM). You may encrypt your Cloud Storage buckets and Cloud SQL tables using a key stored in your own Cloud HSM.

Legal requirements, regional restraints, and other corporate rules may all be enforced with the help of cloud HSM. In the section under “Security and regulatory compliance,” you will learn how to utilize Cloud HSM to determine the legality of your existing keys. safely import them into Cloud HSM, and track where they came from.

IV. GRID COMPUTING

Grid Computing may be thought of as a collection of computers working together to do something that would be too taxing for any one system to handle alone. A virtual supercomputer is created when all the computers on the network adhere to the same protocol. Their job might include tasks like the analysis of massive databases or the simulation of complex scenarios, both of which call for a lot of processing power. Each computer in a network provides services such as processing time and data storage.

As a subclass of distributed computing, grid computing creates a virtual supercomputer out of several computers on a network. The Internet or an Ethernet-like bus. It's also a sort of parallel computing, however its cores aren't all located in one place like traditional parallel computing. Although grid computing is not a new idea, it has not yet reached its full potential due to the lack of widely acknowledged standards and conventions.

Working:
A Grid computing network mainly consists of these three types of machines

[1] **Control Node:** A computer, often a server or cluster of servers, that controls and monitors the network's resources.
[2] **Provider:** The computer's resources are added to those of the network.
[3] **User:** The machine doing the networked job.

In response to a request from a client computer, the network's control node makes available to the client all of the network's resources. It is preferable that it donate its resources to the network while it is not in use. That's why any ordinary computer on the node may switch roles as needed, acting in one of two roles: buyer or seller. In a homogeneous network, all of the computers use the same OS, whereas in a heterogeneous network, the computers use a broad range of OSes. This is the main distinction between grid computing and other distributed computing models.

Authorization of network processes is yet another function of middleware. Permission is granted by a provider in a grid computing system. Middleware is a software/networking protocol used to manage a network and its resources. The network is managed by this, and the control nodes just carry out its orders. Because the grid computing system is meant to use only idle computer resources, the control node is responsible for ensuring that no one provider is overwhelmed with work.

allows the user to execute any program on its computer, which poses a serious security risk to the system. As such, a middleware's job is to check that the network isn't being used for any malicious purposes.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

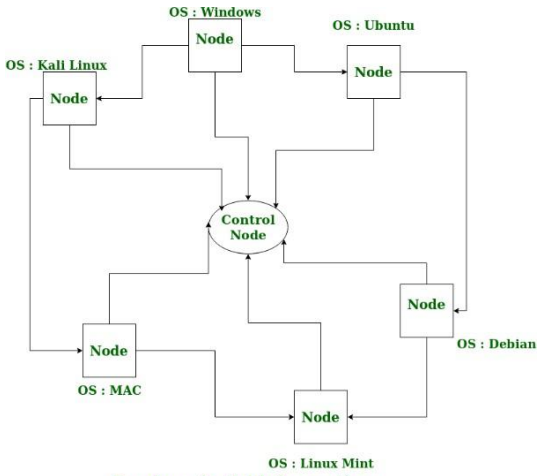
International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 6, June 2023

DOI: 10.17148/IARJSET.2023.10639

The notion of Grid Computing was first conceived in 1999 with the publication of "The Grid: Blueprint for a new computing infrastructure" by Ian Foster and Carl Kesselman. Grid computing was formerly seen as a centralized server farm, but nowadays it's more like a decentralized team effort.

Grid computing is now being employed by several universities to address many analytical, mathematical, and physical challenges.



Topology in Grid Computing

Advantages of Grid Computing:

1. There is no need for a centralized administration or processing power since no servers are needed outside of a single control node.
2. A single grid computing network may be used by a collection of diverse computers.
3. Users don't have to pay anything to have their work done simultaneously in many places.

Disadvantages of Grid Computing:

1. The grid's underlying software is still maturing.
2. The current situation calls for an extremely rapid connection between various computing resources.
3. It may be cost-prohibitive for certain applications due to the licensing requirements for several servers.
4. There is reluctance to share across many communities.
5. When the control node has issues, the whole network might grind to a standstill.

How is Grid Computing Used?

And the two outcomes taken together may yield When several professionals in various fields need to work together on a project but don't have easy access to one another's data and computer resources, grid computing may be an invaluable tool. The scattered teams are able to pool their strengths and make a greater impact by working together despite their separation in location. In other words, all of the available processing power may be devoted toward accomplishing different parts of the larger whole. As an example, one study group may look at weather patterns in the North Atlantic area, while another group looks at the South Atlantic region.

V. CONCLUSION

Google's Cloud Key Management Service (Cloud KMS) is primitive in comparison to other cloud services that also offer key management services and especially to Enterprise Key Manager Systems, which provide customers unique and exclusive access to their encryption keys during their whole existence. Only cloud-based data storage services can be protected by Google Cloud KMS. For instance, Google Cloud KMS does not support the OASIS Key Management Interoperability Protocol (KMIP), an open standard for key management. Manage cryptographic keys for your cloud services with ease with Cloud KMS, a service hosted in the cloud. Generate, deploy, rotate, and delete cryptographic keys with the help of a cloud-based key management service. With the help of Cloud IAM and Cloud Audit Logging, you can control who has access to which keys and keep tabs on their activity. Symmetric and asymmetric key generation and payload encryption have always been available in Cloud KMS. Since our secrets will be encrypted and

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 6, June 2023

DOI: 10.17148/IARJSET.2023.10639

decrypted by Cloud KMS, we won't need a safe place to keep the keys. Encryption and decryption are restricted to only those with permission or via a service account. KMS is a completely managed solution that allows your company to handle encryption keys in one place. With Cloud KMS, the difficulties of managing cryptographic keys for cloud services and on-premises applications are abstracted away, and a set of simple APIs is provided. Cloud KMS will keep your cryptographic keys in the same location as your resource deployment.

We've also covered why and when Grid Computing disciplines should be used, as well as some of the considerations developers and service providers should keep in mind throughout deployment. Now that we have an overview, we can go into the specifics of Grid Computing, its history and development across sectors, and the ongoing architectural initiatives throughout the globe.

REFERENCES

[1] https://cloud.google.com/docs/security/ke y-management-deep-dive
[2] www.appviewx.com/blogs/deep-dive-into- google-cloud-key-management-services/
[3] cloud.google.com/security-key- management#section-4
[4] https://cloud.google.com/kms/docs
[5] https://cloud.google.com/kms/docs/creatin g-keys
[6] cloud.google.com/sql/docs/mysql/cmek
[7] https://cloud.google.com/kms/docs/cmek
[8] https://thalesdocs.com/dpod/services/key_ management_services/ekms/index.html
[9] k21academy.com/google-cloud/google- cloud-kms/https://cloud.google.com/docs/security/enc ryption/customer-supplied-encryption- keys
[10] https://cloud.google.com/kms/docs/hsm
[11] https://cloud.google.com/docs/security/clo ud-hsm-architecture
[12] https://cloud.google.com/docs/security/reli able-ekm-architectures
[13] cloud.google.com/sql/docs/mysql/cmek
[14] cloud.google.com/docs/security/encryptio n/customer-supplied-encryption- keys#:~:text=Customer%2DSupplied%20Encryption%20Keys%20(CSEK,encrypt% 20and%20decrypt%20your%20data.