Review, Comparison and Critically Appraisal of Microsoft Azure and Google Cloud Technology

A. Introduction

Google Cloud and Microsoft Azure are two of the most well-known cloud computing platforms available today. B noth offer a wide range of features and services that are meant to meet the needs of businesses of all sizes, from fledgling startups to well-established multinationals (Wankhede, 2020). Google Cloud provides a complete range of cloud computing services, including computation, storage, and application services. Only a few of the crucial services offered by Google Cloud are Google Compute Engine, which provides virtual computers for running programmes and services, Google Cloud Storage, which provides data object storage, and Google Cloud SQL, which provides managed database services (Mitchell, 2019). On contrast, Microsoft Azure is a cloud computing platform that provides a variety of services, such as networking, storage, and computation. Azure provides a number of important services, some of which include Azure Virtual Machines, Azure Blob Storage, Managed Database Services, and Azure SQL Database. Azure Virtual Machines provides virtual machines for executing applications and services (Gupta, 2021).

In this report, I have provided an insightful comparison of Kubernetes Engine and Cloud Functions and VPC networking. We can deploy, manage, and grow containerized applications with Kubernetes Engine, a managed container orchestration service. It offers a strong framework with functions like auto-scaling, automatic updates, and load balancing for deploying and managing containers at scale. The serverless computing solution known as Cloud Functions, on the other hand, enables you to run code in response to events without having to manage or provision any infrastructure. Create lightweight, event-driven functions using Cloud Functions that may be activated by a range of events, such as modifications to database data or the arrival of fresh messages in a message queue. On the other hand, both Google Cloud and Microsoft Azure provide robust networking options for VPC networking that let us build private networks and link our cloud services to our on-premises infrastructure. We can build Virtual Private Cloud (VPC) networks in Google Cloud, which give our cloud resources a safe and segregated environment. In order to establish safe connections between our Google Cloud resources and on-premises architecture, we can also use Google Cloud VPN. We may establish Virtual Networks (VNets) in Microsoft Azure, which give us a mechanism to separate and secure our cloud resources. In order to establish secure connections between our on-premises infrastructure and our Azure resources, we can also use Azure VPN Gateway. Additionally, Azure ExpressRoute gives our on-premises infrastructure and Azure a dedicated, private connection (Fowler, 2023).

In this report, I have come to the conclusion that both Google Cloud and Microsoft Azure provide a variety of potent services and capabilities that may aid companies of all sizes in the deployment and management of their apps and infrastructure in the cloud. It's crucial to take the company's unique needs into account when deciding between Cloud Functions and Kubernetes Engine and to select the service that best satisfies those needs. Both Google Cloud and Microsoft Azure offer powerful networking capabilities with VPC networking that can be used to build secure and segregated environments for our cloud assets.

B. Kubernetes Engine and Cloud Functions

A managed Kubernetes service called Kubernetes Engine is provided by both Google Cloud and Microsoft Azure and aids in the large-scale deployment and management of containerized applications. Developers can deploy their apps on Kubernetes Engine without worrying about the underlying infrastructure thanks to the platform it offers. Developers may concentrate on writing code and creating apps while the service takes care of responsibilities like scaling, load balancing, and service discovery while using Kubernetes Engine. Additionally, Kubernetes Engine has capabilities built-in that assist guarantee that applications are always running the most recent versions, such as rollbacks and automatic updates (Shah, 2019).

Developers can run code in reaction to events using Cloud Functions, a serverless compute tool provided by Google Cloud. Developers can use their choice programming language to build code for Cloud Functions, and the service automatically expands the infrastructure to handle any volume of requests. Developers may write business logic with Cloud Functions without having to worry about the underlying infrastructure or server upkeep (Perron, 2020). As opposed to Cloud Functions, which is a serverless computing service that enables developers to run code in response to events, Microsoft Azure provides Azure Functions. Developers can use their choice language to build code for Azure Functions and combine it with other Azure services. Developers can test and debug their code more easily using Azure Functions since it allows them to build locally and deploy to the cloud. It's crucial to keep in mind that there are various use cases that Kubernetes Engine and Cloud Functions serve when contrasting them. Organizations that must install and maintain containerized apps at scale should use Kubernetes Engine, whereas those that must execute quick bursts of code in reaction to events should use Cloud Functions. But we can combine the two services to create more sophisticated apps (Malawski, 2018).

Both Google Cloud and Microsoft Azure's Kubernetes Engine and Cloud Functions services are available on a pay-as-you-go basis. While the cost of running Cloud Functions changes depending on the volume of requests and the amount of RAM utilized, the cost of running Kubernetes Engine depends on the number of nodes and the type of instance used. It is significant to keep in mind that additional elements like storage and network egress could affect the overall cost as well. Both Google Cloud and Microsoft Azure provide comparable VPC networking features to provide secure communication between virtual machines and resources inside a private network. Users of Google Cloud can create their own IP addresses, subnets, and routing tables using the Virtual Private Cloud (VPC) networks that are available. Virtual Network (VNet), a feature offered by Microsoft Azure, is comparable to VPC in terms of functionality. VPC and VNet both offer network segregation, firewall configuration, and VPN connectivity (Tajadod, 2012). Google Cloud and Microsoft Azure offer two well-liked services: Kubernetes Engine and Cloud Functions. While Cloud Functions is perfect for executing little bits of code in response to events, Kubernetes Engine is suited for deploying and maintaining containerized applications at scale. Both services use a pay-as-you-go pricing structure, with costs based on things like the quantity of nodes and requests. Additionally, VPC networking technologies are provided by Google Cloud and Microsoft Azure to provide secure communication within a private network. The decision between Kubernetes Engine and Cloud Functions ultimately comes down to the unique requirements and use cases of each organization. Table 1 provide a comparison of these.

Table 1: A comparative analysis of Google Cloud Kubernetes Engine and Microsoft Azure Cloud Functions

Feature	***Microsoft Azure Cloud Functions***	***Google Cloud Kubernetes Engine***
Type	Serverless computing	Container orchestration
Deployment	Code-based	Container-based

Autoscaling	Yes	Yes
Pricing	Pay-per-use model	Pay-per-use model
Integration	Integrates with Azure services	Integrates with Google Cloud
Ease of use	Easy	Moderate
Monitoring	Built-in monitoring	Built-in monitoring
Maintenance	Managed by Microsoft	Managed by Google
Security	Enhanced security features	Enhanced security features

In a nutshell, both of them are potent cloud technologies that give their consumers particular advantages. For businesses that need to build, maintain, and grow containerized applications, Kubernetes Engine is a wonderful option because it is better suited for container orchestration. On the other hand, serverless computing, which is fantastic for creating event-driven apps that can be scaled on demand, is better suited to Azure Cloud Functions. Both solutions provide built-in monitoring, pay-per-use pricing, and autoscaling. While Azure Cloud Functions is comparatively simpler to use, Google Cloud Kubernetes Engine is only reasonably easy to utilize. Both systems can interface with other cloud services offered by their respective providers and have improved security features. Microsoft Azure Cloud Functions is maintained by Microsoft, while Google Cloud Kubernetes Engine is maintained by Google. This means that the infrastructure's upkeep, uptime security, and customer assistance are all the provider's responsibilities. It is crucial to take the organization's unique needs into account when deciding between Google Cloud Kubernetes Engine and Microsoft Azure Cloud Functions and pick the solution that best satisfies those needs.

C. VPC networking

A key element of cloud computing is virtual private cloud (VPC) networking, which enables users to build private, secure networks within of a public cloud environment. VPCs offer a mechanism to designate a conceptually separate area of the cloud, enabling users to alter their network architecture to suit particular needs. VPC networking solutions are provided by both Google Cloud and Microsoft Azure, however they differ in their methods and functionality (Sfiligoi, 2021).

Google Cloud provides a very flexible and scalable solution to VPC networking that can be tailored to individual needs. Users can construct subnets in Google Cloud's VPC network, which can be configured with custom IP ranges and firewall rules. Users can also construct numerous VPC networks that can be joined via VPC peering or Shared VPC, allowing them to connect resources from various VPCs. Furthermore, Google Cloud allows users to establish unique subnets, providing them more control over their network infrastructure. By connecting two or more VPC networks, users can enable resource communication across VPCs without the need for a VPN connection. On the other hand, shared VPC enables users to share resources between projects while retaining security and isolation by allowing users to use a single VPC network across numerous projects. A popular option for businesses with intricate networking needs, VPC peering and Shared VPC both offer a highly flexible and scalable method of VPC networking (Autio, 2021).

Microsoft Azure has a simpler approach to VPC networking, with virtual networks, subnets, and network security groups serving as the primary components. Users can establish virtual networks that serve as logical containers for resources such as virtual machines, storage accounts, and virtual network gateways. Users can build subnets within these virtual networks to segment resources and govern traffic flow. Network security groups can also be used to impose subnet or VM-level security policies. Although Microsoft Azure's approach to VPC networking is less versatile than

Google Cloud's, it is easier to use and more suited for people without a deep understanding of networking. A basic degree of VPC networking capabilities is provided by Azure's virtual networks, allowing customers to build private network environments inside of the cloud. Both Google Cloud and Microsoft Azure provide affordable pricing for VPC networking. Pricing for VPC networking on Google Cloud starts at $0.04 per hour for the first 10 subnets and goes up to $0.02 per hour for additional subnets. The cost of VPC networking on Microsoft Azure is $0.01 per hour for the first five subnets, and $0.01 per hour for each subsequent subnet.

In conclusion, these two provide reliable VPC networking solutions that may be customized to meet the needs of a wide range of users. VPC peering and Shared VPC from Google Cloud offer a highly flexible and scalable solution to VPC networking, making it a popular option for businesses with demanding networking needs. For customers who might not have substantial networking experience, Microsoft Azure's virtual networks offer a more straightforward and approachable method of VPC networking. The decision between Google Cloud and Microsoft Azure ultimately comes down to the user's individual requirements, so it's important to weigh the features, cost, and scalability of both systems before making a choice.

Table 2: A comparative analysis of Google Cloud and Microsoft Azure w.r.t VPC Networking

Feature	***Google Cloud***	***Microsoft Azure***
Virtual Network	Google Cloud Virtual Private Cloud (VPC)	Azure Virtual Network
Subnetting	Yes	Yes
Load Balancing	Google Cloud Load Balancing, Internal Load Balancing	Azure Load Balancer, Azure Application Gateway
VPN Gateway	Google Cloud VPN Gateway, Cloud Router	Azure VPN Gateway
Firewall	Google Cloud Firewall	Azure Network Security Group, Azure Firewall
Route tables	Google Cloud Route tables	Azure Route tables, User-defined routes
Private IP Addressing	Google Cloud internal IP range, Shared VPC, Alias IP range	Azure Private IP addressing, Virtual network service endpoints, IP address space expansion
Hybrid Connectivity	Dedicated Interconnect, Partner Interconnect, Cloud VPN, Carrier Peering	ExpressRoute, VPN Gateway, Azure Virtual WAN, ExpressRoute Direct
Network Traffic Analysis and Security	Google Cloud Network Intelligence Center, Cloud Armor, VPC Flow Logs, Traffic Director	Azure Network Watcher, Azure Firewall, Network Security Group, Traffic Analytics, Azure DDoS Protection, Azure Bastion

Table 2 compares the VPC networking characteristics of Google Cloud and Microsoft Azure in greater detail. As you can see, both platforms have capabilities like route tables, load balancing, and VPN gateways and firewalls. However, there are some variations in the specific services provided, such as Azure's DDoS Protection for security and Google Cloud's Traffic Director for traffic management. Both platforms have choices for hybrid connectivity; Microsoft Azure offers ExpressRoute, VPN Gateway, Azure Virtual WAN, and ExpressRoute Direct, while Google Cloud offers Dedicated Interconnect, Partner Interconnect, and Cloud VPN. Like Google Cloud's

Network Intelligence Centre and Cloud Armour and Azure's Network Watcher and Traffic Analytics, both platforms also offer network traffic analysis and security tools.

D. Conclusion

I have come to the conclusion that both Google Cloud and Microsoft Azure provide a variety of potent services and capabilities that may aid companies of all sizes in the deployment and management of their apps and infrastructure in the cloud. It's crucial to take the company's unique needs into account when deciding between Cloud Functions and Kubernetes Engine and to select the service that best satisfies those needs. Both Google Cloud and Microsoft Azure offer powerful networking capabilities with VPC networking that can be used to build secure and segregated environments for our cloud assets.

The evaluation of VPC networking on both systems revealed that while Microsoft Azure offers more sophisticated security measures and more customization options, Google Cloud offers a networking experience that is simpler and more user-friendly. Both platforms provide dependable and secure VPC networking solutions, but ultimately it depends on the particular requirements of the organization. Compared to Microsoft Azure's AKS, Google Cloud's Kubernetes Engine is a more developed and feature-rich offering in the context of Kubernetes Engine and Cloud Functions. In contrast to Google Cloud's Cloud Functions, Microsoft Azure's Cloud Functions offer a more simplified and affordable serverless computing option. Overall, each platform has its own advantages and disadvantages, and the choice between the two ultimately depends on the particular demands and needs of the organization. Prior to selecting a choice, it is crucial for organizations to carefully assess both platforms, taking into account aspects like cost, scalability, security, and simplicity of use. Both Google Cloud and Microsoft Azure place a high priority on sustainability and minimizing their carbon footprints, with Google Cloud pledging to run entirely on renewable energy by 2030 and Microsoft Azure pledging to be carbon negative by that same year.

In conclusion, these two technologies provide scalable, dependable cloud computing options for businesses of all sizes. When deciding between the two platforms, organizations can make an informed choice by assessing the unique demands and requirements of the organization and taking into account variables like cost, scalability, security, and sustainability. Organizations must carefully consider their alternatives and select a platform that will fulfil their demands both now and in the future as cloud computing continues to play an increasingly significant part in contemporary corporate operations.

E. References

Wankhede, P., Talati, M. and Chinchamalatpure, R., 2020. Comparative study of cloud platforms-microsoft azure, google cloud platform and amazon EC2. J. Res. Eng. Appl. Sci, 5(02), pp.60-64.

Mitchell, N.J. and Zunnurhain, K., 2019, November. Google cloud platform security. In Proceedings of the 4th ACM/IEEE Symposium on Edge Computing (pp. 319-322).

Gupta, B., Mittal, P. and Mufti, T., 2021, March. A review on Amazon web service (AWS), Microsoft azure & Google cloud platform (GCP) services. In Proceedings of the 2nd International Conference on ICT for Digital, Smart, and Sustainable Development, ICIDSSD 2020, 27-28 February 2020, Jamia Hamdard, New Delhi, India.

Fowler, B., 2023. Cloud Network Engineering. In AWS for Public and Private Sectors: Cloud Computing Architecture for Government and Business (pp. 23-41). Berkeley, CA: Apress.

Shah, J. and Dubaria, D., 2019, January. Building modern clouds: using docker, kubernetes & Google cloud platform. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0184-0189). IEEE.

Perron, M., Castro Fernandez, R., DeWitt, D. and Madden, S., 2020, June. Starling: A scalable query engine on cloud functions. In Proceedings of the 2020 ACM SIGMOD International Conference on Management of Data (pp. 131-141).

Malawski, M., Figiela, K., Gajek, A. and Zima, A., 2018. Benchmarking heterogeneous cloud functions. In Euro-Par 2017: Parallel Processing Workshops: Euro-Par 2017 International Workshops, Santiago de Compostela, Spain, August 28-29, 2017, Revised Selected Papers 23 (pp. 415-426). Springer International Publishing.

Tajadod, G., Batten, L. and Govinda, K., 2012, December. Microsoft and Amazon: A comparison of approaches to cloud security. In 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings (pp. 539-544). IEEE.

Sfiligoi, I., Hare, M., Schultz, D., Würthwein, F., Riedel, B., Hutton, T., Barnet, S. and Brik, V., 2021. Managing Cloud networking costs for data-intensive applications by provisioning dedicated network links. In Practice and Experience in Advanced Research Computing (pp. 1-8).

Autio, T., 2021. Securing a Kubernetes Cluster on Google Cloud Platform.

"Google Cloud VPC Network Overview." Google Cloud. Accessed April 17, 2023. https://cloud.google.com/vpc/docs/vpc.

"Azure Virtual Network Documentation." Microsoft Azure. Accessed April 17, 2023. https://docs.microsoft.com/en-us/azure/virtual-network/.

"Azure ExpressRoute Documentation." Microsoft Azure. Accessed April 17, 2023. https://docs.microsoft.com/en-us/azure/expressroute/.

"Google Cloud Interconnect Overview." Google Cloud. Accessed April 17, 2023. https://cloud.google.com/interconnect/docs/overview.

"Azure VPN Gateway Documentation." Microsoft Azure. Accessed April 17, 2023. https://docs.microsoft.com/en-us/azure/vpn-gateway/.

"Google Cloud VPN Overview." Google Cloud. Accessed April 17, 2023. https://cloud.google.com/vpn/docs/overview.

"Azure Network Security Groups Documentation." Microsoft Azure. Accessed April 17, 2023. https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview.

"Google Cloud Firewall Rules Overview." Google Cloud. Accessed April 17, 2023. https://cloud.google.com/vpc/docs/firewalls.

"Azure Application Gateway Documentation." Microsoft Azure. Accessed April 17, 2023. https://docs.microsoft.com/en-us/azure/application-gateway/.

"Google Cloud Load Balancing Overview." Google Cloud. Accessed April 17, 2023. https://cloud.google.com/load-balancing/docs/overview.

"Microsoft Azure." Accessed April 17, 2023. https://azure.microsoft.com/.

"Azure Virtual Network Documentation." Microsoft Azure. Accessed April 17, 2023. https://docs.microsoft.com/en-us/azure/virtual-network/.

"Azure ExpressRoute Documentation." Microsoft Azure. Accessed April 17, 2023. https://docs.microsoft.com/en-us/azure/expressroute/.

"Azure VPN Gateway Documentation." Microsoft Azure. Accessed April 17, 2023. https://docs.microsoft.com/en-us/azure/vpn-gateway/.

"Azure Network Security Groups Documentation." Microsoft Azure. Accessed April 17, 2023. https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview.

"Azure Application Gateway Documentation." Microsoft Azure. Accessed April 17, 2023. https://docs.microsoft.com/en-us/azure/application-gateway/.

F. Appendix

Codes for VPC Networking:

1. Google Cloud

```
gcloud compute networks create my-vpc --subnet-mode=custom
```

This command creates a custom VPC network named "my-vpc". The --subnet-mode=custom option indicates that subnets within the VPC will have user-specified IP ranges.

```
gcloud compute networks subnets create my-subnet --network=my-vpc --region=us-central1 --range=10.0.0.0/24
```

This command creates a subnet named "my-subnet" within the "my-vpc" VPC. The --network=my-vpc option specifies the VPC to create the subnet in. The --region=us-central1 option specifies the region where the subnet will be located. The --range=10.0.0.0/24 option specifies the IP range for the subnet.

```
gcloud compute firewall-rules create allow-ssh --allow=tcp:22 --network=my-vpc
```

This command creates a firewall rule named "allow-ssh" to allow inbound SSH traffic to the VPC. The --allow=tcp:22 option specifies the allowed protocol and port number (TCP port 22 for SSH). The --network=my-vpc option specifies the VPC to apply the firewall rule to.

2. Microsoft Azure Networking

```
az network vnet create --name myVnet --resource-group myResourceGroup --address-prefixes 10.0.0.0/16
```

This command creates a new VNet named "myVnet" with the address prefix of 10.0.0.0/16. The --resource-group parameter specifies the resource group in which the VNet should be created.

```
az network vnet subnet create --name mySubnet --resource-group myResourceGroup --vnet-name myVnet --address-prefix 10.0.0.0/24
```

This command creates a new subnet named "mySubnet" within the "myVnet" VNet with the address prefix of 10.0.0.0/24. The --resource-group parameter specifies the resource group in which the subnet should be created.

```
az network nsg create --name myNetworkSecurityGroup --resource-group myResourceGroup
```

This command creates a new NSG named "myNetworkSecurityGroup" within the "myResourceGroup". An NSG is a firewall that filters traffic to and from Azure resources.

```
az network nsg rule create --name myNetworkSecurityGroupRule --resource-group myResourceGroup --nsg-name myNetworkSecurityGroup --priority 100 --protocol Tcp --destination-port-range 22 --access Allow
```

This command creates a new rule named "myNetworkSecurityGroupRule" within the "myNetworkSecurityGroup" NSG. This rule allows inbound traffic over TCP port 22, which is used for SSH. The --priority parameter specifies the priority of the rule, with lower values indicating higher priority. The --access parameter specifies whether the rule allows or denies traffic matching the specified criteria.