Educational Administration: Theory and Practice
2024, 30(6), 1789-1798
ISSN: 2148-2403
https://kuey.net/

Research Article

VPC & Public Cloud Optimal Performance in Cloud Environment

Dr. Abdul Bari[1]*, Dr.Imtiyaz khan[2], Dr. Rafath Samrin[3], Dr Akhil Khare[4]

[1]*Associate Professor-CSE, Keshav Memorial Engineering College, Hyderabad, India, Email: abdulbarimohammed11@gmail.com
[2]Professor-CSE, Shadan College of Engineering and Technology, Hyderabad, India, Email: imtiyaz.khan.7@gmail.com
[3]Asst. Professor-CSE, College of Computer Science, King Khalid Univeristy, Abha Saudi Arabia, Email: ralimohammed@kku.edu.sa
[4]Professor-CSE, Maturi Venkata Subba Rao (MVSR)Engineering College, Hyderabad, India, Email: khare_cse@mvscrec.edu.in

***Corresponding Author:** Dr. Abdul Bari
*Associate Professor-CSE, Keshav Memorial Engineering College, Hyderabad, India, Email: abdulbarimohammed11@gmail.com

***Citation**:* Dr. Abdul Bari et al. (2024), VPC & Public Cloud Optimal Performance in Cloud Environment, *Educational Administration: Theory and Practice*, *30*(6), 1789-1798
Doi: 10.53555/kuey.v30i6.5587

ARTICLE INFO **ABSTRACT**

Although cloud computing as a concept has gained widespread acceptance, the security measures used inside the cloud environment remain crucial. Many different methods exist now help safeguard data on the cloud. The Virtual Private Cloud (VPC) service from Amazon is what makes Elastic Compute Cloud (EC2) operate from a networking perspective. A VPC is a virtual private net-work (VPN) in which EC2 instances and other AWS network resources can be located. A Virtual Private Network (VPC) is similar to a regular network in that it consists of a set of IP addresses. Using a virtual private network (VPN) in the cloud is a safe and reliable method for sending data across a public cloud. The public and private clouds may be kept distinctly separate with the use of virtual private clouds. Availability zones are essentially comparable to smaller physical locations like data centres, and only one availability zone may host a given subnet. In this article, we'll go through the Virtual Private Network (VPC) ideas, their components, explain performance metrics differ-ences between public cloud and Virtual Private Cloud (VPC) environments based on several factors.

Keywords: AWS, VPC, SUBNET, GATEWAY

I. Introduction

We now refer to "cloud computing"[1] as the on-demand, internet-based, pay-as-you-go provisioning of computer power, databases, storage space, application software, and other IT resources. A cloud services platform provides you instanta-neous access to flexible and cost-effective IT resources, which can be used for everything from running apps that share photos with millions of mobile users to handling the crucial operations of organization. With cloud computing, we may avoid making expensive hardware purchases and spending a lot of time on admin-istrative chores. As an alternative, we may supply the exact amount and setup of computer resources needed to drive your next clever idea or keep your IT infra-structure. Everything we need is at your fingertips in a flash, and will only be charged for what we really use. Cloud computing simplifies the process of gaining network access to various servers, storage, databases, and application services.[1]

Fig. 1 Cloud Computing resources delivered via internal

II. Different Types of Computing Models

Access to networking capabilities, computers (virtual or on dedicated hardware), and data storage space is provided through infrastructure as a service (IaaS)these are the fundamental components of cloud IT. Compared to other types of cloud computing, The most flexibility is provided by infrastructure as a service. in terms of customizing your setup and the most administrative control over your IT as-sets.[2]

Platform as a Service (PaaS): It allows up resources that would otherwise be spent on controlling businesses to focus on the deployment and management of applications rather than the supporting infrastructure (typically hardware and op-erating systems). Organizations can focus on doing what they do best and not waste time worrying about mundane but necessary tasks such as resource sourc-ing, capacity planning, software upkeep, and patching, etc. [2]

SaaS (software as a service) Your finished product is provided by the service provider, who also operates and maintain for you. When consumers or businesses When people refer to SaaS, they usually mean software aimed at consumers. Busi-nessesneed to concentrate on using a software as a service (SaaS) solution how to put the software to work for them, rather than how to keep it up and running.[2]

AWS (Amazon Web Service): In 2006 [3], Beginning as online services, today referred to as cloud computing, Amazon online Services (AWS) started providing IT infrastructure services to enterprises. Businesses don't have to prepare for and buy servers and other IT infrastructure in advance thanks to the cloud. Instead, they can quickly spin up hundreds of thousands of servers in only a few minutes, accelerating the delivery of results.. Offering more than The most comprehensive and commonly used cloud in the world, Amazon Web Services (AWS) offers 200 fully featured services from data centers across the globe.. In order to save money, be more flexible, and create new products and services more quickly, AWS is used by millions of customers. [4]

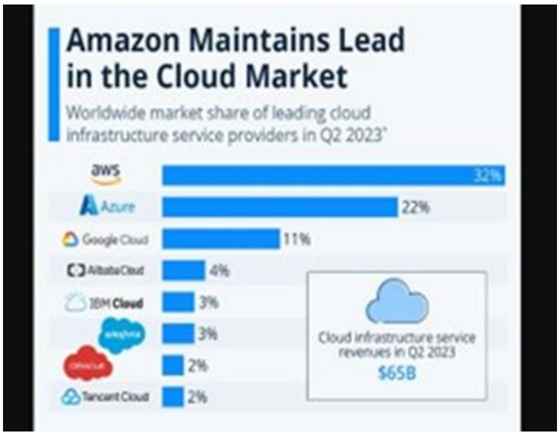

Fig. 2 Leading Cloud Share Market of the world [5]

Introduction AWS resources into a custom virtual network created by the user on Amazon Virtual Private Cloud (Amazon VPC). [6] It allows users to manage every aspect associated with your network, including resources, connection, security, and more. In addition, it specifies the protocols that a network must use to exchange data across various regions or Availability Zones. AWS assets like EC2 instances and RDS instances for storage of data. With Amazon Web Services VPC, user may restrict access to only those who need it. Users may easily alter their Amazon Virtual Private Cloud's (VPC) network settings. power over every aspect of your virtual private network, including its setup, configuration, and dele-tion. [7,8]

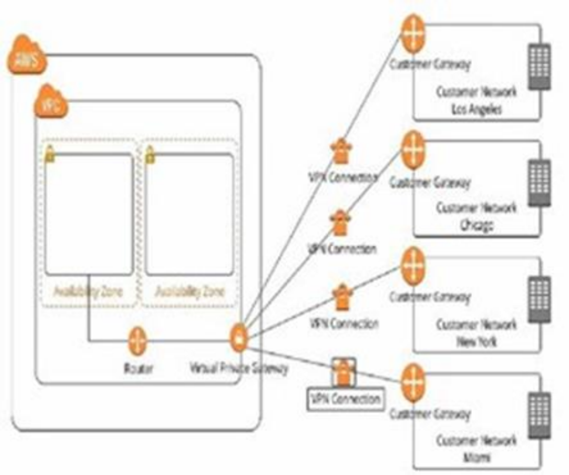

Fig. 3 Virtual Private Cloud's (VPC) [9]

III. Component of VPC [6]:

First, VPC uses the term "subnet," which refers to a group IP address range. A logical collection of IP addresses known as a VPC subnet may store resources such as Amazon EC2 services. Subnetworks may divided into two categories: public, which allows access to the Internet via an Internet Gateway is called public cloud which is available to the public, and private, which does not or it can be called a private cloud. VPCs can spread across many Availabilities Zone, but subnets must remain inside a single Availability Zone

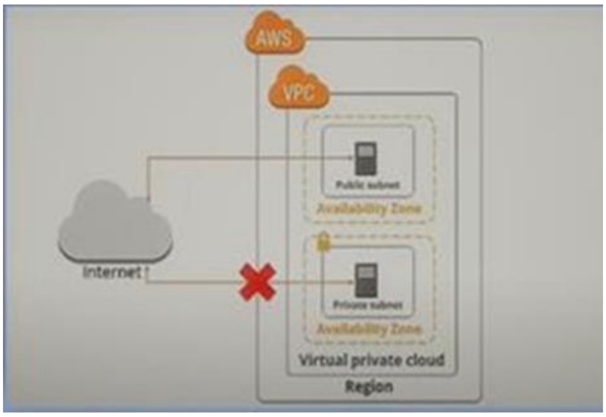

Fig. 4 Virtual Private Cloud's (VPC) with Subset [12]

The template A route table is a list of instructions about how network traffic should be rout-ed. should be directed. Every VPC has a default route table Both The intended recipient's identity and IP address are disclosed. A VPN gateway, NAT gateway, Internet gateway, or any other form of gateway could be the target device. Users can use route tables to plan where their subnet's or gateway's traffic will go.

For encrypted communications between your device and Amazon's servers, you must first connect to the company's Virtual Private Gateway. Users may connect it to their VPC and then establish a VPN tunnel.
A NAT Gateway can be used as an alternative when higher bandwidth and availability with fewer administrative work is required. The private subnet's rout-ing table is expanded to include the IP address of the NAT gateway. It only sup-ports UDP, TCP, and ICMP as protocols.

- All Internet gateways must be linked to the VPC.
- The internet gateway needs to be listed in the subnet's route table.
- Every instance in a given account has its own unique IP address, either a public IP or an Elastic IP.
- The configuration of all security groups and network access controls is re-quired.[12]

Through a Traffic between two VPCs may be routed using either IPv4 or IPv6 private addresses thanks to the VPC peering connection. Users can establish a link between their VPC and another user's VPC by using VPC peering. With this link, data transfer is quick and easy.

Security groups are collections of firewall rules that determine how data from your sample is transmitted and received. Multiple instances can share the same security group. Security groups always permit outgoing traffic by default. Permis-sive, stateful, and modifiable security groups are always available.
A static IP address, also known as an Elastic IP, is a pre-allocated and unchang-ing public IP address that is available for use by any Instance in a specific loca-tion. When the instance with which it is associated is stopped, this IP address stays assigned to your AWS account and is not lost. Make sure you only use an elastic IP address in your VPC when you actually need one. Elastic IP, which is not connected to any instances and is charged by the hour by AWS, is simply de-coupled from one resource and reconnected to another resource [11]
To restrict traffic going in and out of a virtual private network (VPC), network access control lists (NACL) can be set up as an additional security layer. It's a great way to beef up your VPC's .
Your private network or data may be securely sent to your Amazon virtual pri-vate cloud through the Customer Gateway. Presenting your end of the connection is a customer gateway. It might be a piece of hardware or a piece of software. An interface between a private network and an open network. If you copy data Net-work traffic will be promptly diverted to the new instance when switching be-tween instances.
VPC Endpoints enable VPC to communicate with other AWS services locally, bypassing the public internet. Interference nodes and gateway nodes are two dif-ferent types. The components of the VPC are scalable, redundant, and trustworthy.
You can assign IPv4 and IPv6 addresses to your virtual private networks using IP addressing. and networks within networks.

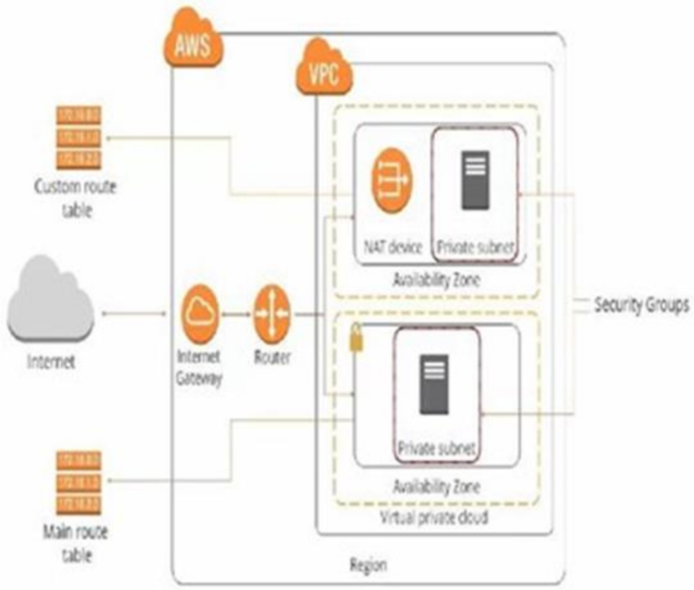

Fig. 5 Virtual Private Cloud's (VPC) Architecture [6]

VPC is divided into two types and they [10]

1. Default VPC.

- Produced when an AWS account is created in each AWS region.
- Has default configurations for the CIDR, Security group, NACL, and Route table.
- comes included with an internet gateway
- We must contact AWS for assistance if we decide to remove the Default VPC.

2. Custom VPC.

- The owner of the AWS account creates the custom vpc.
- The CIDR is chosen by the AWS user building the custom vpc.
- Comes with its own default route table, NACL, and security group.
- Requires the creation of an internet gateway if one is not already present.

IV. PERFORMANCE VARIABLE BETWEEN PUBLIC CLOUD AND VIRTUAL PRIVATE CLOUD (VPC)

There are a number of variables that can affect the degree to which a public cloud and a VPC environment differ in terms of performance. Let's take a closer look at these elements to create a more insightful comparison: Resource Allocation: changes in performance may occur during peak hours since resources in the public cloud are shared among many users. On the other hand, a Virtual Private Cloud (VPC) has dedicated resources, which means more reliable operation.

Latency: which can be exacerbated in public clouds because the data must go over the public internet. As private networks, VPCs have the potential to provide faster connections to on-premises resources.[12]

Scalability: Its often provided via public clouds, allowing you to swiftly deploy extra resources when necessary. Virtual private clouds are scalable, but this may need more hands-on maintenance and configuration. Control: VPCs provide you greater leeway in determining how you set up your network, what kind of security measures you implement, and where you put your resources. Some of these ele-ments are often abstracted away in public cloud systems.

Security: virtual private clouds (VPCs) are safer than traditional networks since they are not connected to the outside world. However, public cloud companies spend a lot on security, and if you set things up right, you may use the cloud with-out worrying.

Cost: public cloud pricing may fluctuate based on how much space and band-width you really use. While VPC costs may be more predictable in the long run, they still may necessitate substantial outlays of capital in the outset.

Data centre and region performance can be impacted by their geographical loca-tion. Since many public clouds offer facilities all around the world, you may pick the one with the best latency and other performance metrics. Virtual private clouds can be used only in certain areas.[11]

Depending on the use scenario, different performance requirements will apply. While public clouds offer scalability, some applications may benefit more from the isolation and low latency of a virtual private cloud (VPC).

Network design and VPC configuration have a significant bearing on perfor-mance. VPC performance may be improved with the right setup of subnets, load balancers, and routing.In order to function at their best, public clouds and VPCs need constant moni-toring and tuning. The distribution of resources and the configuration of the net-work must be reviewed and adjusted on a regular basis.

V. PROCEDURES FOR THE EXPERIMENT

This section describes the experimental setup in great detail, as it was used to measure performance. Settings for Computer Hardware and Programs:
We used the following combinations of hardware and software to conduct our performance analysis:

- Hardware:
  - Servers: Dell PowerEdge R740 with dual Intel Xeon Gold 6254 processors (3.1 GHz, 18 cores each)
  - Memory: 256 GB DDR4 RAM
  - Storage: RAID 10-configured enterprise-grade NVMe SSDs

- Software:
  - Operating System: Ubuntu Server 20.04 LTS
  - Web Server: Nginx 1.20.1
  - Database: MySQL 8.0.26
  - Application Framework: Node.js 14.17.5
  - Load Balancer: HAProxy 2.4.2
  - Monitoring and Metrics: Prometheus 2.30.1 and Grafana 8.1.2
  - Load Testing Tool: Apache JMeter 5.4.1

We chose AWS and Azure are two of the most well-known and commonly used cloud service companies., to conduct our performance analysis because of their dependable systems and extensive suites of services. Since both service providers provide VPC solutions, a direct comparison is possible inside the same cloud environment.

Detailed Services and Locations: Amazon Web Services (AWS): We tested in the extremely popular and accessible Region of the US East (N. Virginia) (us-east-1). Amazon EC2 instances were used. to host our web apps and Amazon Relational Database Service for MySQL for our database management. For the purpose of load balancing, Elastic Load Balancing (ELB) was implemented.

As for Azure, we did our testing in the East US area, which is a highly trafficked and reputable part of Azure. To host the web app, we made use of Azure VMs, managed the database with Azure Database for MySQL, and balanced the traffic with an Azure Load Balancer.[13].To guarantee scientific rigor and uniform evaluation, we used a standardized deployment approach for both the public cloud and VPC settings when releasing the web application or workload.[17]

1. An eCommerce demo built using Node.js, Nginx, and MySQL was deployed as our first online app. In order to mimic a real-world scenario, the program included features such as user identification, a product catalog, and a shopping cart.
2. we set up auto-scaling settings in both cloud environments so that the application could dynamically alter the number of instances depending on CPU usage criteria in order to evaluate its scalability.
3. the application was put through a series of load tests using Apache JMeter to simulate normal and peak usage patterns and see how it performed.
4. Performance measurements such as CPU and memory consumption, response times, and error rates were gathered with Prometheus and shown in Grafana dashboards for monitoring and analysis.[14] We were able to keep a close eye on and assess performance thanks to the real-time monitoring.
5. Security Measures: To ensure a safe and regulated testing environment, standard security measures were used across both the public cloud and the VPC. These included the use of network security groups, firewall rules, and data encryption.

TABLE I: PERFORMANCE EVALUATION BETWEEN PUBLIC CLOD AND VIRTUAL PRIVATE CLOUD'S (VPC)

S.No	Matric	Public Cloud	VPC
1	CPU Utilization (%)	70	50
2	Memory Utilization (%)	80	60
3	Network Latency (ms)	20ms	5ms
4	Response Time (ms)	300ms	150ms
5	Bandwidth Usage (%)	80% of allocation	60% of allocation
6	Scaling Efficiency (Scaling Events)	10 times	5 times
7	Uptime Percentage (%)	99.95%	99.99%
8	Error Rate (%)	2%	1%
9	Cost per Transaction ($)	$0.10	$0.08
10	Security Incidents (Count)	5 incidents	2 incidents
	Compliance (Standard)	Compliant with X	Compliant with Y

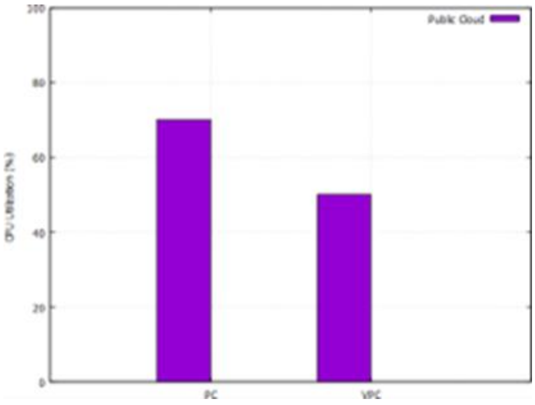

Fig. 6 BAR GRAPH REPRESENTATION OF CPU UTILIZATION BETWEEN PRIVATE CLOUD'S & (VPC)

Comparing the Public Cloud with the VPC, the CPU Utilization (%) in the for-mer is shown to be 70%, while that in the latter is shown to be 50%. The most important aspects of CPU Utilization (%) are as follows: Seasonal Variations, Resource Optimization, and Monitoring Idle, time- tracking gadgets

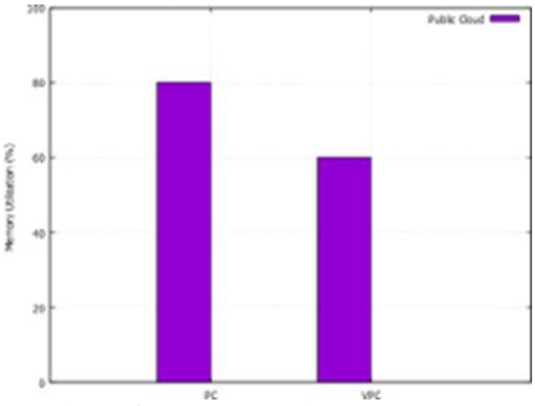

Fig. 7 Bar Graph representation of Memory Utilization between Private Cloud's & (VPC)

Currently, processes and apps in the public cloud consume 80% of the available system memory. 60% of VPC's RAM is being used by programs and processes at the moment. Low Memory Utilization may indicate available memory resources, whereas high Memory Utilization may indicate that the system is consuming most of its available RAM, in which case more memory or memory optimization may be required.

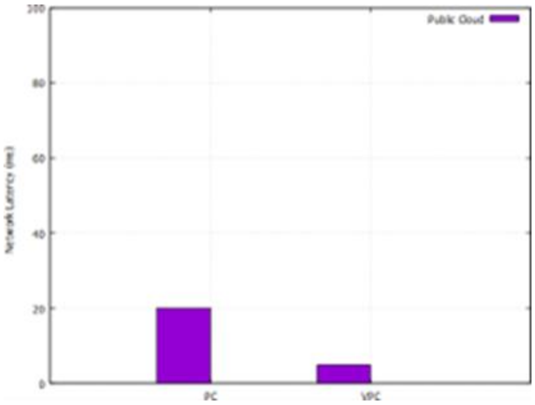

Fig. 8 Bar Graph representation of Network Latency (ms) between Private Cloud's & (VPC)

Latency in a network is the amount of time it takes for data to transit from one location to another. In both public and VPC Cloud settings, it plays a critical role in defining the responsiveness and performance of applications and services. The factors of Network Distance, Network Infrastructure, and Shared Resources all contribute to Network Latency.

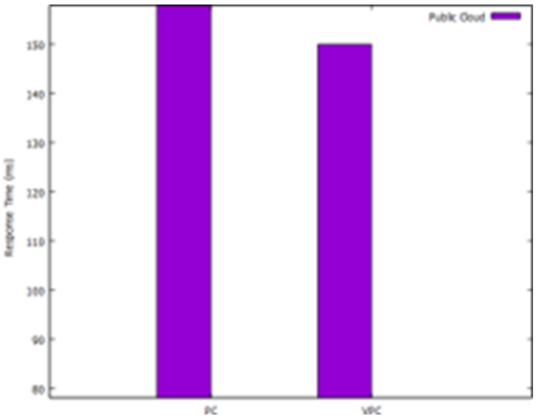

Fig. 9 Bar Graph representation of Response Time (ms) between Private Cloud's & (VPC)

The average response time for a system or service hosted in the public cloud is 300 ms. In most cases, the faster and more responsive a service is, the lower the reaction time should be. The typical response time for a service or system in VPC is 150 ms. The response time is affected by the server processing time, network latency, client-side processing, application load, and resource availability, with a shorter response time indicating quicker and more responsive services.[15]

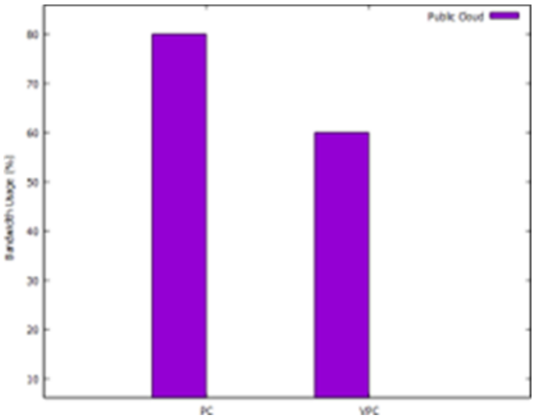

Fig. 10 Bar Graph representation of Bandwidth Usage (%) between Private Cloud's & (VPC)

The network in the public cloud is using up about 80% of its available bandwidth right now. A large percentage of users indicates that there is a lot of competition for available bandwidth. Currently, Virtual Private Cloud, the network is making use of about 60% of its total bandwidth. Since the VPC network is less crowded and has more available capacity when compared to the Public Cloud, the proportion of time it is being used is lower. Indicators of Performance for Bandwidth Utilization (in%) include: Resource allocation, peak vs. off-peak demand, and other network- related issues

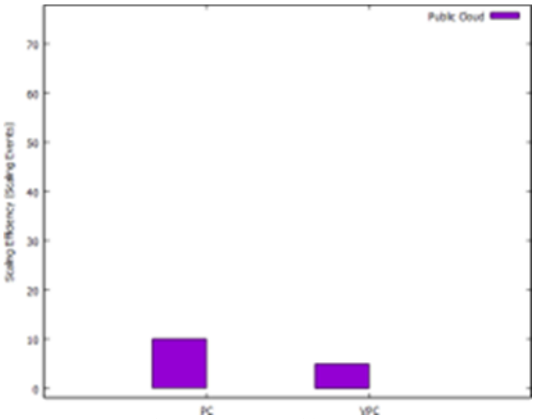

Fig. 11 Bar Graph representation of Scaling Efficiency between Private Cloud's & (VPC)

The key to cost-effectively scaling in the public cloud is to dynamically modify resources to meet workload needs. Finding the sweet spot between performance and cost involves constant monitoring, automation, and the usage of cloud-native capabilities like autoscaling and load balancing. In order to make sure that your AWS VPC can scale effectively in response to fluctuating needs while keeping prices low and performance high, you should automate resource management, optimize instance types, load balance, monitor, and make cost-conscious decisions.

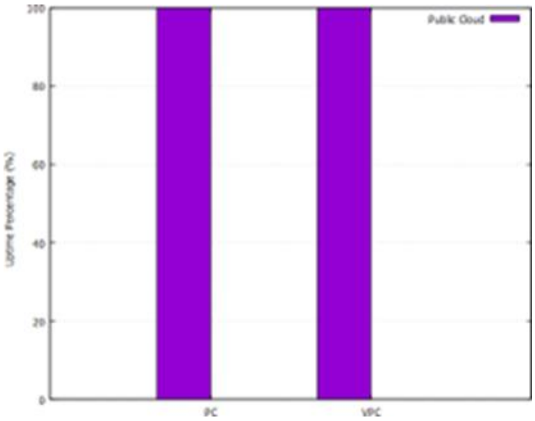

Fig. 12 Bar Graph representation of Uptime Percentage between Private Cloud's & (VPC)

Access to mission-critical applications and services must be guaranteed at all times, and greater percentages imply a higher degree of availability and dependability.

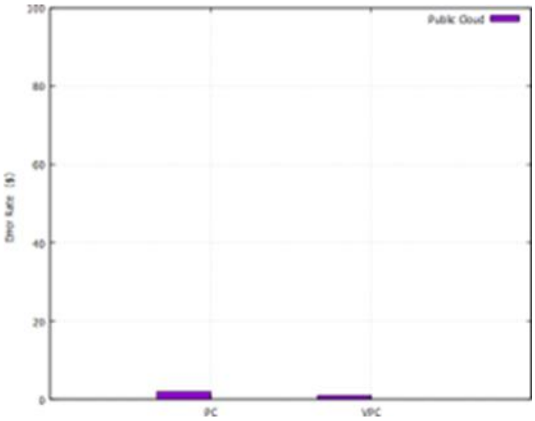

Fig. 13 Bar Graph representation of Error Rate (%) between Private Cloud's & (VPC)

The reported error rate (in percentage) for Public Cloud is 0.5%. In other words, around 0.5% of all transactions or activities are unsuccessful due to defects in the system or service. This percentage is low, suggesting that there is little room for error and that the service can be relied on for the most part. VPC has a documented error rate of 0.2%. Roughly 2% of all transactions or uses of the system are unsuc-cessful due to mistakes.

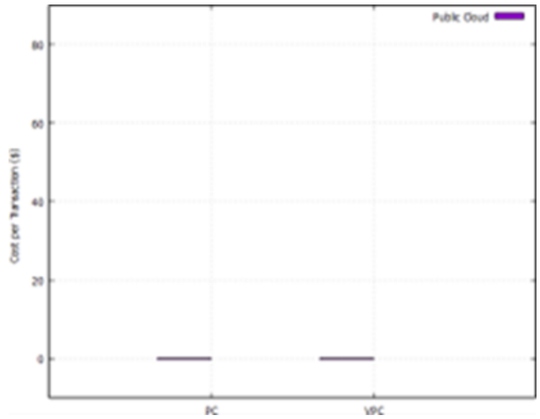

Fig. 14 Bar Graph representation of Cost per Transaction ($) between Private Cloud's & (VPC)

Each transaction incurs around $0.10 in processing fees. Several categories of expenditures, including setup, upkeep, and running costs, are included in this to-tal. About $0.05 is needed to cover the expense of processing each transaction. This is less than what you'd pay in the so-called "Public Cloud," suggesting that VPC transaction processing may be more efficient financially. Budgeting, compar-ing prices, and scalability are all examples of Kye factors.

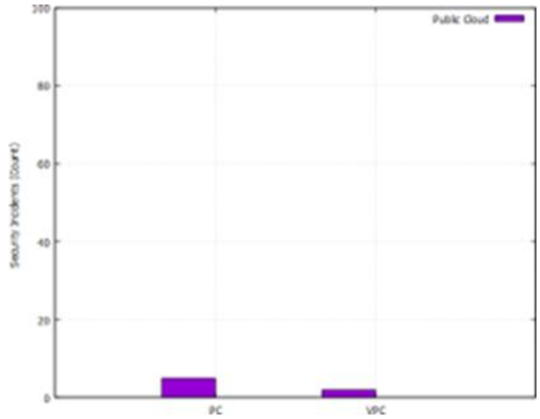

Fig. 15 Bar Graph representation of Security Incident between Private Cloud's & (VPC)

There have been five separate security incidents and/or breaches in Public Cloud. Each occurrence is a distinct vulnerability. During the time period in question, there have been a total of 2 security incidents or breaches reported or identified in VPC. Types of Incidents, Detection, Reporting, Response, Security Attitude, and Constantly Bettering These Are the Core Components

VI. Conclusion and Future work

To make the most of AWS when connecting your off-site networks to Amazon Virtual Private Cloud (VPC), the cloud provider offers a variety of fast, safe ways to establish a connection. We looked at the various AWS VPC parts and tried to explain how they worked together. If the organization wishes to offer cloud com-puting services to its customers, setting up a private virtual private cloud (VPC) is the way to go. Insights into the performance and cost of various cloud environ-ments are provided by the statistics displayed in the table. Differences Between a Virtual Private Cloud and the Public Cloud various measures have shed light on the effectiveness, efficiency, and safety of various setups. Efforts going forward should improve and optimize these settings to accommodate changing business requirements and security standards.

References

[1] AWS White paper," Overview of Amazon Web Services", Amazon Web Services, April 2023

[2] AWS," Types of Cloud Computing", Amazon Web Services, https://aws.amazon.com/types-of-cloud-computing/?WICC-N=tile&tile=types_of_cloud,(2023)

[3] AWS," Overview of Amazon Web Services ", Amazon Web Services, https://docs.aws.amazon.com/whitepapers/latest/aws-overview/introduction.html,(2023)

[4] AWS," Cloud Computing with AWS", Amazon Web Services, https://aws.amazon.com/what-is-aws/,(2023)

[5] Felix Richter," Cloud Infrastructure Market-Amazon Maintains Lead in the Cloud Market", Statista, (2023)

[6] Shubhambhugra," Amazon VPC Networking Components", GeeksforGeeks.org, https://www.geeksforgeeks.org/amazon-vpc-networking-components/,March (2023)

[7] Ritika Pandey," Amazon VPC – Introduction to Amazon Virtual Cloud", GeeksforGeeks.org, https://www.geeksforgeeks.org/amazon-vpc-introduction-to-amazon-virtual-cloud/, April (2023)

[8] Cloudflare," What is a virtual private cloud (VPC)?", Cloudflare.com(2023)

[9] Service Catalog Version ,"VPC Overview ", GruntworkDOCS, https://docs.gruntwork.io/reference/services/networking/virtual-private-cloud-vpc/ ,(2023)

[10] Gaurav-Jethuri," Types of VPC in AWS", Gaurav-Jethuri's Blog, https://gauravdevopsblog.hashnode.dev/types-of-vpc-in-aws#heading-there-are-two-types-of-vpc ,(2023)

[11] Mohammed Nadeem Shareef, Junaid Hussain, Mohammed Khaja Adnan Ali Khan,, Dr. Mohammed Abdul Bari,Crypto Jacking, Mathematical Statistician and Engineering Applications, ISSN: 2094-0343, 2326-9865,Vol 72 No. 1 Page Number: 1581 –1586, (2023)

[12] Mohd Amer,Dr. Mohd.Abdul Bari ,Dr. Akhil Khare," Fingerprint Image Identification For Crime Detection", International Journal For Advanced Researchs In Science & Technology, (IJARST), ISSSN NO: 2457-0362,Vol 12,Issue 10, Page 114,Oct 2022

[13] Hafsa Fatima, Shayesta Nazneen, Maryam Banu, Dr. Mohammed Abdul Bar," Tensorflow- Based Automatic Personality Recognition Used in Asynchronous Video Interviews", Journal of Engineering Science (JES), ISSN NO:0377- 9254, Vol 13, Issue 05, MAY/2022

[14] Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," Smartphone Security and Protection Practices", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01,December 2021

[15] M.A.Bari & Shahanawaj Ahamad, "Code Cloning: The Analysis, Detection and Removal", in International Journal of Computer Applications(IJCA),ISSN:0975-887, ISBN:978-93-80749-18-3,Vol:20,No:7,pp:34-38,NewYork,U.S.A.,April 2011

[16] Mr. Mohammed Afzal, "Reducing Side Effects of Cyber Bullying Using Machine Learning", IJARST, ISSN-2457-0362, Volume 13, Issue 06, June 2023.

[17] Dr. Mohammed Abdul Bari,Arul Raj Natraj Rajgopal, Dr.P. Swetha ," *Analysing AWSDevOps CI/CD Serverless Pipeline Lambda Function's Throughput in Relation to Other Solution*", International Journal of Intelligent Systems and Applications in Engineering , JISAE, ISSN:2147-6799, Nov 2023, 12(4s), 519–526