International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

ESTABLISH SECURE PRIVATE CONNECTIONS TO SERVICES USING AWS PRIVATELINK

Siva Kumar Mamillapalli
siva.mamill@gmail.com

Abstract

Amazon Virtual Private Cloud (Amazon VPC) enables AWS users to establish a virtual private network within the AWS Cloud. This setup allows customers to securely deploy services within an Amazon VPC and grant access to these services both internally and externally using standard methods like internet gateways, VPC peering, NAT, VPN, and AWS Direct Connect. This paper explores how AWS PrivateLink maintains network traffic privacy and facilitates secure, scalable connectivity between Amazon VPCs and AWS-hosted services and data.

Keywords: AWS Cloud, VPC, Private Connectivity, Secure Access, VPC Peering, NAT, VPC EndPoints.

I. INTRODUCTION

Amazon Virtual Private Cloud (Amazon VPC) was introduced in 2009, allowing customers to create a logically isolated segment of the AWS Cloud, where they can launch and manage AWS resources within a network they define. This capability gives users full control over their virtual network configuration, enabling them to isolate and secure their resources in the cloud. By using Amazon VPC, customers can establish a private, secure environment while still benefiting from the scalability and flexibility of the AWS Cloud.

To access third-party applications or public AWS services from within an Amazon VPC, customers can use various traditional methods. These include configuring an internet gateway to connect to the broader internet, setting up a Virtual Private Network (VPN) for secure communication, leveraging AWS Direct Connect with a virtual private gateway for dedicated network connections, or establishing VPC peering to enable seamless communication between VPCs. These options provide flexibility in how customers choose to connect to external services, ensuring they can tailor their network architecture to meet their specific needs while maintaining control over security and performance.

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

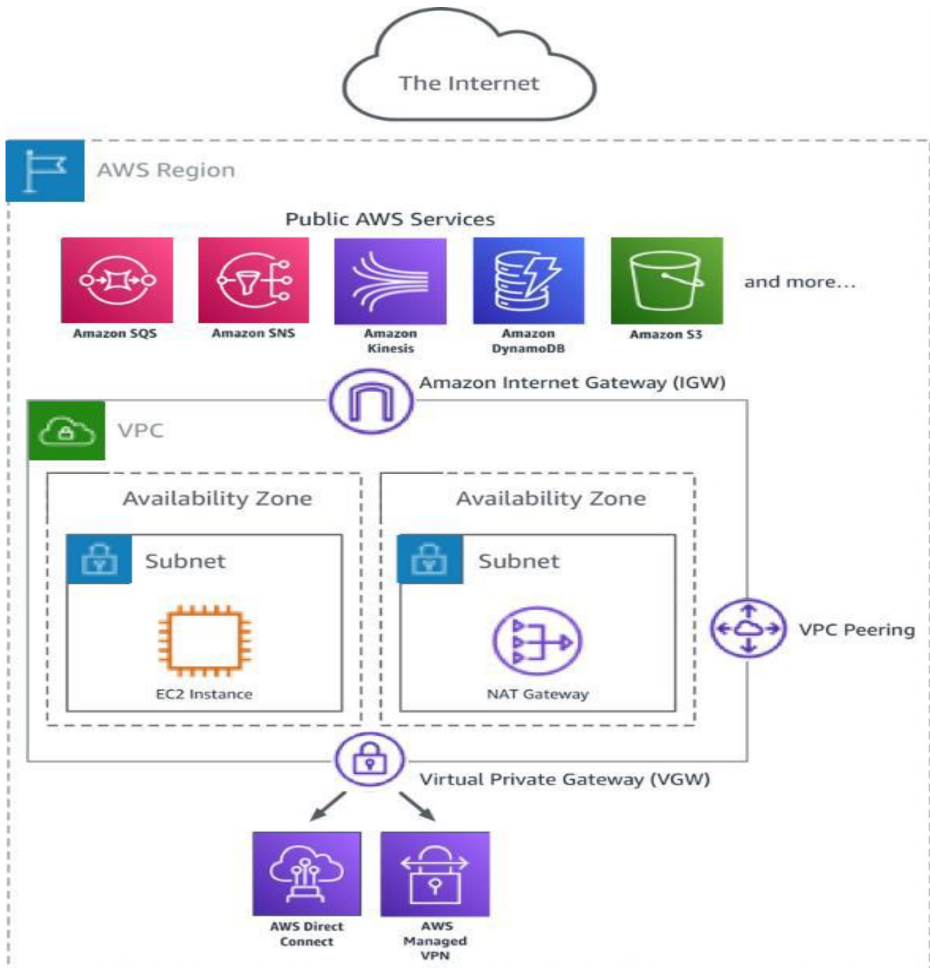

Figure 1: Traditional access from an Amazon VPC

1.1 What is AWS PrivateLink

AWS PrivateLink offers secure, private connections between Amazon VPCs, AWS services, and on-premises applications over the AWS network. This enables customers to easily and securely access AWS services through the private Amazon network, facilitating connectivity to AWS services via interface Amazon VPC endpoints.

AWS PrivateLink also enables customers to build an application within their Amazon VPC, known as a service provider VPC, and make that application available as an AWS PrivateLink-enabled service or VPC endpoint service. A VPC endpoint service allows customers to host a service within their VPC and provide access to it for other users through AWS PrivateLink.

1.2 Why Use PrivateLink

Before AWS PrivateLink, services within a single Amazon VPC were connected to multiple Amazon VPCs either through:

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

- Public IP addresses via each VPC's internet gateway, or
- Private IP addresses using VPC peering.

With AWS PrivateLink, service connectivity over Transmission Control Protocol (TCP) can be securely and scalably established from the service provider's VPC to the service consumers' VPCs.

AWS PrivateLink offers three primary benefits:

- Use Private IP Addresses for Traffic

AWS PrivateLink enables Amazon VPCs to securely and efficiently connect to AWS-hosted services using private IP addresses. Unlike traditional methods that rely on public IP addresses or traverse the internet, PrivateLink keeps the traffic within the AWS network, ensuring that services behave as though they are hosted directly within an Amazon VPC.

- Simplify Network Management

AWS PrivateLink eliminates the need for complex configurations like managing internet gateways, NAT gateways, or firewall proxies. It removes the challenges of allowlisting public IPs and simplifies networking across multiple VPCs. Additionally, connectivity between services across different AWS accounts and VPCs is streamlined, with no need for route table changes or the setup of VPC peering or Transit VPCs.

- Facilitate Cloud Migration

With AWS PrivateLink, on-premises networks can securely connect to AWS services via AWS Direct Connect. This makes migrating traditional on-premises applications to the cloud easier while ensuring that the traffic remains private and secure, providing customers with greater confidence in the process.

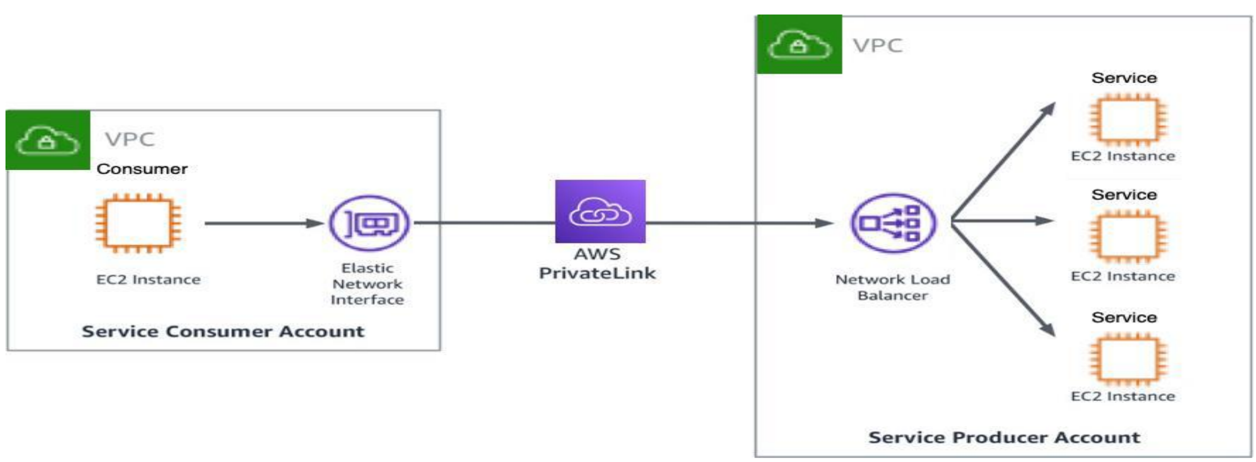

Figure 2: VPC-to-VPC connectivity with AWS PrivateLink

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

1.3 What are VPC Endpoints

A VPC endpoint allows customers to securely connect to supported AWS services and VPC endpoint services powered by AWS PrivateLink. Amazon VPC instances can communicate with these services without needing public IP addresses, and the traffic between an Amazon VPC and the service stays within the Amazon network.

VPC endpoints are virtual devices that are horizontally scalable, redundant, and highly available. They enable communication between instances in an Amazon VPC and services without introducing availability issues or bandwidth limitations. There are two types of VPC endpoints:

1. Interface Endpoints

Interface endpoints facilitate connectivity to services over AWS PrivateLink. These services include AWS managed services, services hosted by other AWS customers and partners in their own VPCs (known as endpoint services), and supported AWS Marketplace partner services. The entity offering the service is the service provider, while the entity using the service is the service consumer. An interface endpoint consists of one or more elastic network interfaces with a private IP address, serving as an entry point for traffic destined for a supported service. Interface endpoints currently support many AWS managed services. For a full list of services available over AWS PrivateLink, refer to the documentation for VPC endpoints.

2. Gateway Endpoints

Gateway endpoints direct specific IP routes in an Amazon VPC route table (in the form of a prefix list) for traffic destined for Amazon DynamoDB or Amazon S3. Gateway endpoints do not support AWS PrivateLink. More details on gateway endpoints can be found in the Amazon VPC User Guide.

Instances in an Amazon VPC do not need public IP addresses to communicate with VPC endpoints, as interface endpoints use local IP addresses within the consumer's Amazon VPC. Gateway endpoints, on the other hand, are accessible within an Amazon VPC through prefix lists in the VPC's route table. For an illustration of connectivity to AWS services using VPC endpoints, refer to the figure below.

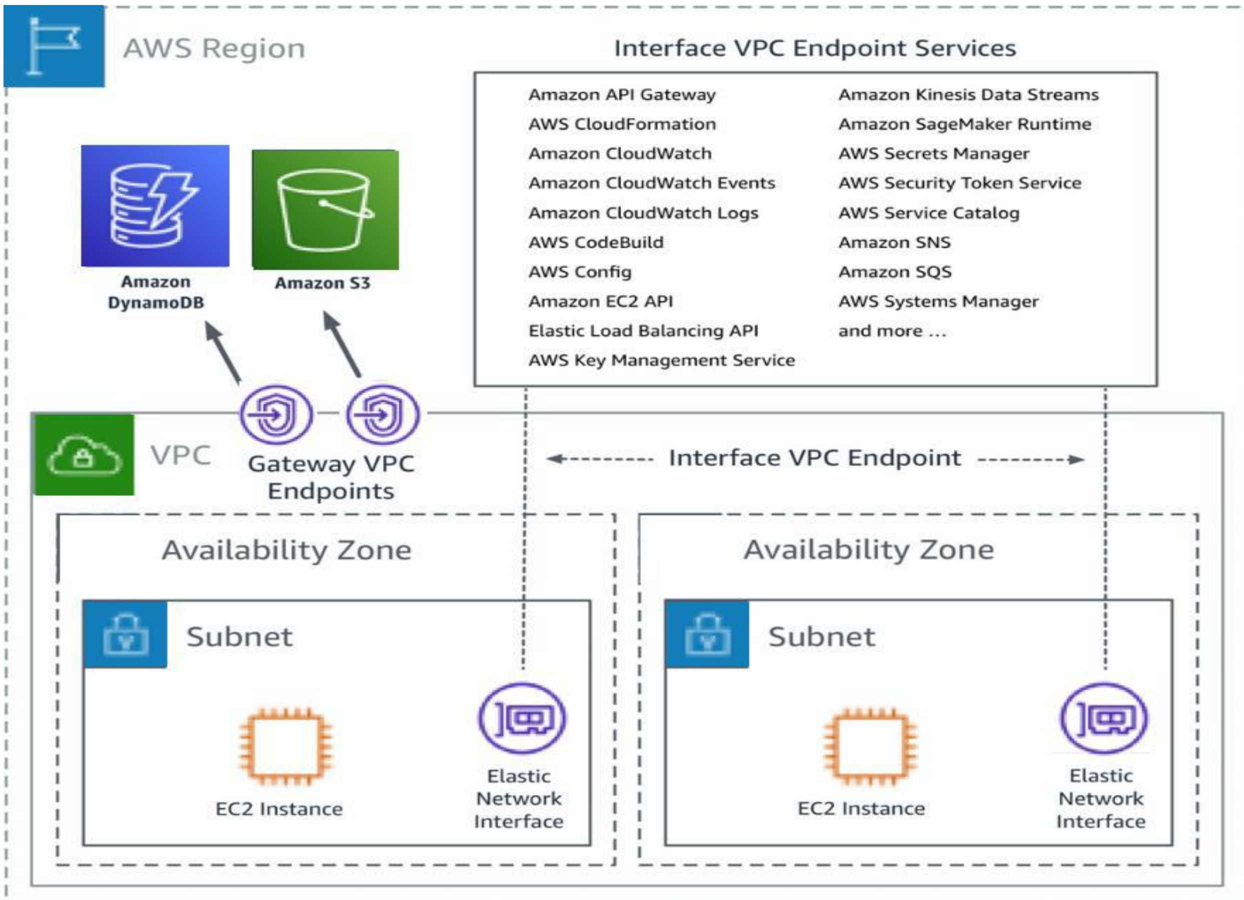

Figure 3: Connectivity to AWS services using VPC endpoints

1.4 How does AWS PrivateLink work?

AWS PrivateLink utilizes Network Load Balancers to link interface endpoints with services. A Network Load Balancer operates at the network transport layer (Layer 4) and is capable of handling millions of requests per second. For AWS PrivateLink, this is represented within the consumer's Amazon VPC as an endpoint network interface.

Customers can enhance the resilience of their service by specifying multiple subnets across different Availability Zones. This ensures that the service remains operational in the event of an Availability Zone disruption. To accomplish this, customers can create endpoint network interfaces across multiple subnets, each mapped to different Availability Zones.

1.5 Creating highly-available endpoint services

The creation of VPC endpoint services involves four stages, which we outline here: generating a DNS hostname, using a private IP address, deploying the endpoint, and configuring it.

As shown in the diagram below, the account owner of VPC B acts as the service provider and has a service running on instances within subnet B. The owner of VPC B has a service endpoint

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

(vpce-svc-1234) associated with a Network Load Balancer that directs traffic to the instances in subnet B. Instances in subnet A of VPC A access the services in subnet B through an interface endpoint.
When an interface endpoint is created, DNS hostnames specific to the endpoint are generated, allowing communication with the service. Once the endpoint is established, requests can be sent to the provider's service using one of the following methods:

Endpoint-specific Regional DNS hostname: vpce-0fe5b17a0707d6abc-29p5708s.ec2.us-east-1.vpce.amazonaws.com

Zonal-specific DNS hostname: vpce-0fe5b17a0707d6abc-29p5708s-us-east-1a.ec2.us-east-1.vpce.amazonaws.com

Private DNS hostname: myservice.example.com

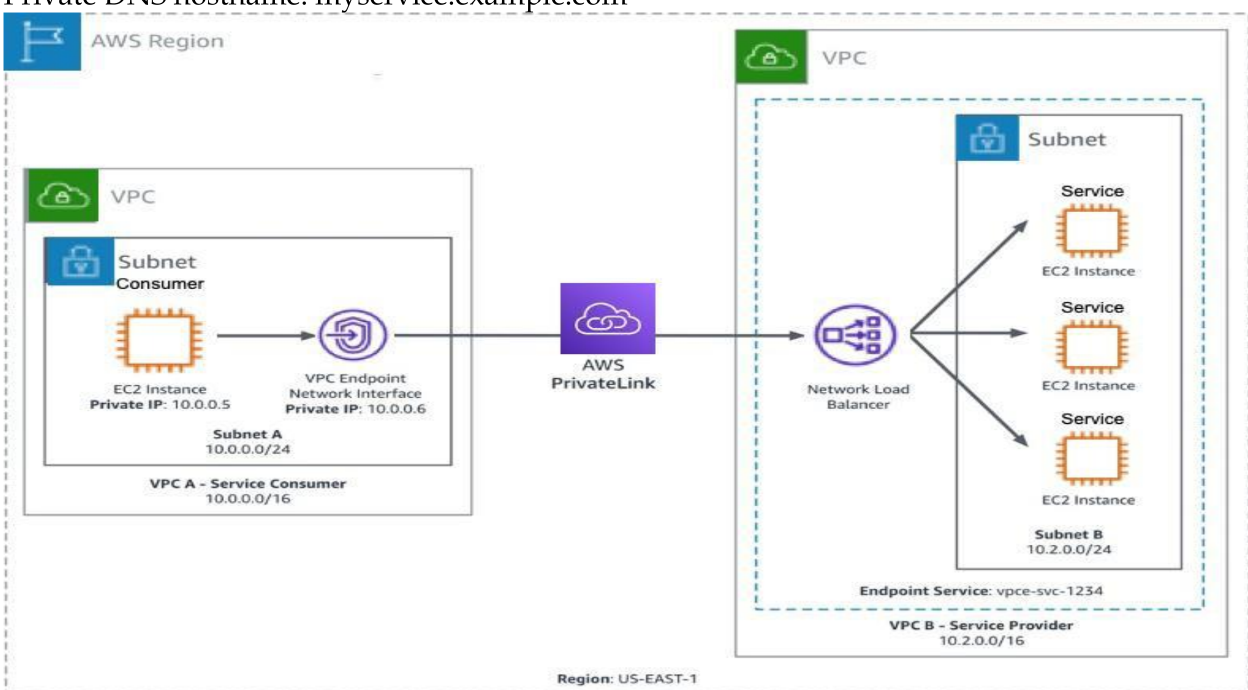

Figure 4: Detailed Amazon VPC-to-VPC connectivity with AWS PrivateLink

II. USE-CASES

This section showcases some of the most common use cases for consuming and providing AWS PrivateLink endpoint services.

2.1 Private access to SaaS applications

AWS PrivateLink allows Software-as-a-Service (SaaS) providers to securely and privately offer their services on AWS to thousands of customers. Service providers can use a Network Load Balancer to direct traffic to instances in their Amazon VPC, creating an endpoint service. Customers can then create an interface VPC endpoint in their own VPC to access the service privately.

For high availability and low latency, it is recommended to create a PrivateLink endpoint in each Availability Zone within the region. Non-AWS customers can connect to the service using AWS Direct Connect for private access.

For example, a customer wanting to analyze log data can use a logging analytics SaaS hosted on AWS. By using AWS PrivateLink, they can securely transfer logs to the service through a private interface VPC endpoint, avoiding public-facing AWS endpoints.

2.2 Shared Services

As customers deploy workloads on AWS, common services like security, logging, monitoring, DevOps tools, and authentication often emerge across different workloads. These services are typically centralized in a Shared Services VPC, which can be accessed by workloads in other Amazon VPCs. Traditionally, VPC peering is used for this communication, but it has limitations, including a cap of 125 peering connections per VPC and the need for fine-grained access controls.

AWS PrivateLink offers a more secure and scalable solution by allowing common services in the Shared Services VPC to be exposed as endpoint services, accessible by workloads in other VPCs. The service provider creates a PrivateLink endpoint service using a Network Load Balancer targeting specific instances. Consumers can then create an interface endpoint in their VPC to access the service securely.

To ensure low latency and high availability, it's recommended to deploy Network Load Balancers across multiple Availability Zones. Service consumers can access the endpoint service using private DNS hostnames or the endpoint's IP addresses.

2.3 Hybrid services

As customers migrate to the cloud, a common approach is to use a hybrid cloud environment, where workloads are gradually moved to AWS while continuing to use on-premises resources. In a Shared Services VPC, AWS PrivateLink allows the endpoint service to extend to on-premises data center resources.

The Network Load Balancer for the PrivateLink endpoint service can target both AWS resources and on-premises systems. Service consumers on AWS create an interface VPC endpoint associated with the endpoint service, with requests forwarded to on-premises resources. This setup facilitates easy migration, cloud bursting, or failover to the cloud.

As the migration progresses, on-premises targets can be replaced by AWS instances, transitioning the environment from hybrid to fully cloud-based. For a visual representation of hybrid connectivity using AWS Direct Connect, refer to the following diagram.

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

2.4 Presenting microservices

Customers are increasingly adopting scalable, modern architectures for their workloads, with microservices being a popular approach. A microservice is a type of service-oriented architecture (SOA) where applications are structured as collections of loosely coupled, specialized services.

AWS PrivateLink is well-suited for microservices environments. Teams can create and deploy their microservices in an Amazon VPC. Once ready to share, they can expose the service as an endpoint service, which typically involves a Network Load Balancer targeting Amazon EC2 instances or containers on Amazon ECS. Service consumers can then request access to the endpoint service by creating an interface VPC endpoint in their VPC to consume the microservice.

In this architecture, microservices are segmented across different Amazon VPCs, potentially managed by different service providers. Consumers can access these services by creating interface VPC endpoints for each service. The communication happens via DNS hostnames generated for the endpoints.

Microservices often interact with each other in a call stack throughout a request's lifecycle. A service consumer can also act as a service provider by aggregating consumed services and presenting itself as a higher-level microservice.

III. CONCLUSION

The AWS PrivateLink scenarios and best practices presented in this paper provide valuable insights for building secure, scalable, and highly available architectures tailored to your services on AWS. These guidelines are designed to help you make informed decisions about how to leverage AWS PrivateLink to connect services privately and securely while optimizing performance and ensuring reliability.

Before deciding on an Amazon VPC connectivity architecture, it's important to thoroughly evaluate your application's connectivity needs. For instance, consider the following factors:

- **Traffic Volume:** Determine how much data needs to be transferred between services and between your AWS environment and external clients. High traffic volumes may require an architecture that supports large-scale, low-latency communication, such as AWS PrivateLink with multiple Network Load Balancers and interface VPC endpoints.
- **Data Sensitivity:** If your application handles sensitive data, such as financial or healthcare information, you may need to ensure that all traffic remains private and doesn't traverse the public internet. AWS PrivateLink offers private connectivity, helping to mitigate the risks associated with public-facing endpoints.
- **Geographical Distribution:** Evaluate whether your services need to be accessed from multiple regions or Availability Zones, or if you need to integrate with on-premises data centers. AWS PrivateLink allows you to build resilient architectures that span multiple regions and ensure your services are highly available with low latency.
- **Hybrid Connectivity:** If your organization is still transitioning to the cloud or operates

iJCEM
International Journal of Core Engineering & Management

International Journal of Core Engineering & Management
Volume-7, Issue-03, 2022 ISSN No: 2348-9510

in a hybrid environment with both on-premises and cloud resources, consider using AWS PrivateLink to connect your on-premises systems securely to AWS-hosted services. This approach is ideal for businesses that need to gradually migrate or burst workloads to the cloud while maintaining on-premises infrastructure.

By carefully considering these factors, you can select the appropriate Amazon VPC connectivity solution that best meets your needs. Whether you use interface endpoints for private service connections, gateway endpoints for services like Amazon S3 or DynamoDB, or combine AWS PrivateLink with other AWS services for advanced scenarios, choosing the right connectivity method will ensure that your architecture is secure, scalable, and performs optimally. This careful planning and implementation can also facilitate smoother future growth and allow your services to scale as your business needs evolve.

REFERENCES

1. Layo, I. 2013. Cloud Computing Advantages for SMEs. Available online: http://cloudtimes.org/2013/09/18/cloud-computing-advantages-for-smes/ .
2. Amazon Web Services. https://aws.amazon.com/
3. https://aws.amazon.com/whitepapers/
4. Managing security responsibilities for Amazon Virtual Private Cloud, https://docs.aws.amazon.com/vpc/latest/userguide/security.html(Accessed on Feb,2022)
5. Control access to VPC endpoints using endpoint policies, https://docs.aws.amazon.com/vpc/latest/privatelink/vpc-endpoints-access.html (Accessed on June,2022)
6. What are VPC Endpoints, https://docs.aws.amazon.com/whitepapers/latest/aws-privatelink/what-are-vpc-endpoints.html(Accessed on 8th July 2022)
7. Modi, C., Patel, D., Borisaniya, B., Patel, A. and Rajarajan, M., 2013. A survey on security issues and solutions at different layers of Cloud computing. The journal of supercomputing, 63(2), pp.561-592.8.
8. Strckland, J. (2020). How Cloud Computing Works. How Stuff Works. Available online: https://computer.howstuffworks.com/cloud-computing/cloud-computing.htm(Accessed on 12th Feb 2021)
9. National Institute of Standards and Technology, NIST.2011. The NIST Definition of Cloud Computing. Available online: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (accessed on 6 December 2021)
10. AWS Architecture Blog: https://aws.amazon.com/blogs/architecture/reduce-cost-and-increase-security-with-amazon-vpc-endpoints/(Accessed on 12th Apr 2022)