GI Cloud Reference Architecture

Version 1.0

Ministry of Electronics & Information Technology,

Government of India

Cloud Management Office

DISCLAIMER

This document has been prepared by Cloud Management Office (CMO) under Ministry of Electronics and Information Technology (MeitY). This document is advisory in nature and aims to provide information in respect of the GI Cloud (MeghRaj) Initiative.

Certain commercial entities, technology, or materials may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by MeitY.

While every care has been taken to ensure that the contents of this Document are accurate and up to date, the readers are advised to exercise discretion and verify the precise current provisions of law and other applicable instructions from the original sources. It represents practices as on the date of issue of this Document, which are subject to change without notice. The readers are responsible for making their own independent assessment of the information in this document.

In no event shall MeitY or its' contractors be liable for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information) arising out of the use of or inability to use this Document

Table of Content

Table of Figures

1 Purpose

Government of India has referenced the Conceptual Reference Model of National Institute of Standards and Technology's (NIST). A requirement to design a GI Cloud Reference Architecture arose to standardize on the nomenclature of terms, various actors and their roles & responsibilities in the GI cloud ecosystem. This document has been prepared to address the requirement of GI Cloud Reference architecture.

The GI Cloud Reference Architecture has been designed to assist the Government Departments to build their Cloud deployment architecture with components, activities and actors as relevant in the GI Cloud ecosystem. The Reference architecture proposed in the document is a vendor neutral architecture and has been designed by adopting widely used and recognized cloud reference architecture and their components.

The document also captures different use case scenarios along with their merits as applicable in today's cloud setup. These use cases are intended to assist Government Departments while designing their cloud solutions. The GI Cloud Reference Architecture is intended to facilitate the understanding of operational intricacies in cloud computing with focus on "what" cloud services provide.

2 Background

Cloud computing has advanced significantly in the delivery of information technology and services by providing an on-demand access to a shared pool of computing resources in a self-service, dynamically scalable, efficient and metered manner.

NIST had published a Cloud Computing reference architecture which identified major actors, their activities and functions in cloud computing. It was a generic high-level architecture intended to facilitate the understanding of the requirements, uses, characteristics and standards of cloud computing. Government of India (MeitY) referenced NIST's conceptual reference model to design the GI Cloud ecosystem and published it in its GI Cloud (Meghraj) Adoption and Implementation Roadmap (April 2013). Apart from NIST, global technology OEMs such as Oracle, IBM have published their own Cloud Reference Architecture which further elaborate NIST's conceptual model and include newer aspects of cloud technology.

MeitY empaneled Cloud service offerings of private Cloud Service Providers for different cloud deployment models (Public Cloud, Virtual Private Cloud, Government Community Cloud) in 2017 thereby including private players in the GI Cloud ecosystem. Government Departments have been leveraging the empaneled services of these players along with cloud services provisioned by NIC to deliver services internally within the Department as well as to the citizens of the country.

MeitY intends to come forward with the updated GI Cloud Reference Architecture which would be designed referencing various globally accepted Cloud Reference Architectures and would identify actors, their activities and functions in line with the GI Cloud ecosystem. The guiding principles leading to creation of the document were to prepare a Reference Architecture that is vendor neutral and does not restrict infrastructure modernization. The Reference Architecture is not tied to any specific vendor products, services or reference implementation, nor does it describes prescriptive solutions that constrain innovation. Also, the GI Cloud Reference Architecture can be used by Government Departments for describing and developing a system architecture using a common framework of reference.

3 GI Cloud Reference Architecture: Introduction

The Government's focus on digitalizing governance under the "Digital India" campaign has led to an increase in computing resource requirements for numerous projects. To meet the existing Infrastructure requirements and to reap benefits provided by the cloud computing, Government Departments are now more inclined towards adopting Cloud. Other factors playing key role in adoption of digital services and reformed Government's outlook to accelerate cloud adoption are accessibility of high speed internet, advent of emerging technologies such as Internet of Things(IoT), Artificial Intelligence (AI)/Machine Learning(ML) , Augmented Reality(AR)/Virtual Reality (VR) and blockchain..

Nowadays, Cloud technology is enabling practices such as DevOps to simplify and speed up the application development process. The near real-time response to Department needs with benefits of cloud would enable the government departments to efficiently deliver internal and citizen centric services leading to increase in adoption of cloud-based infrastructure, platforms and applications. Cloud enables Departments to operate more efficiently, reducing up-front capital costs while providing flexibility in data storage, processing, and other functionalities. As Government Departments are migrating existing applications to the cloud and developing new capabilities/applications on the cloud, understanding and designing cloud deployment architectures with elements of security and management have become crucial while adopting cloud.

In this regard, an architecture is being proposed which shall be referred to as 'Government of India Cloud Reference Architecture (GI CRA)' The reference architecture has been designed using globally prescribed frameworks (addressing security and privacy requirements) and is based on the regulatory and compliance needs for application deployments in the cloud. The design of GI CRA is intended to illustrate and understand the various cloud services in the context of cloud computing and to provide a technical reference to Government Departments to understand, categorize and compare cloud services. The GI CRA comprises of various building blocks and their relationships with each other which ultimately shape to form up a cloud setup.

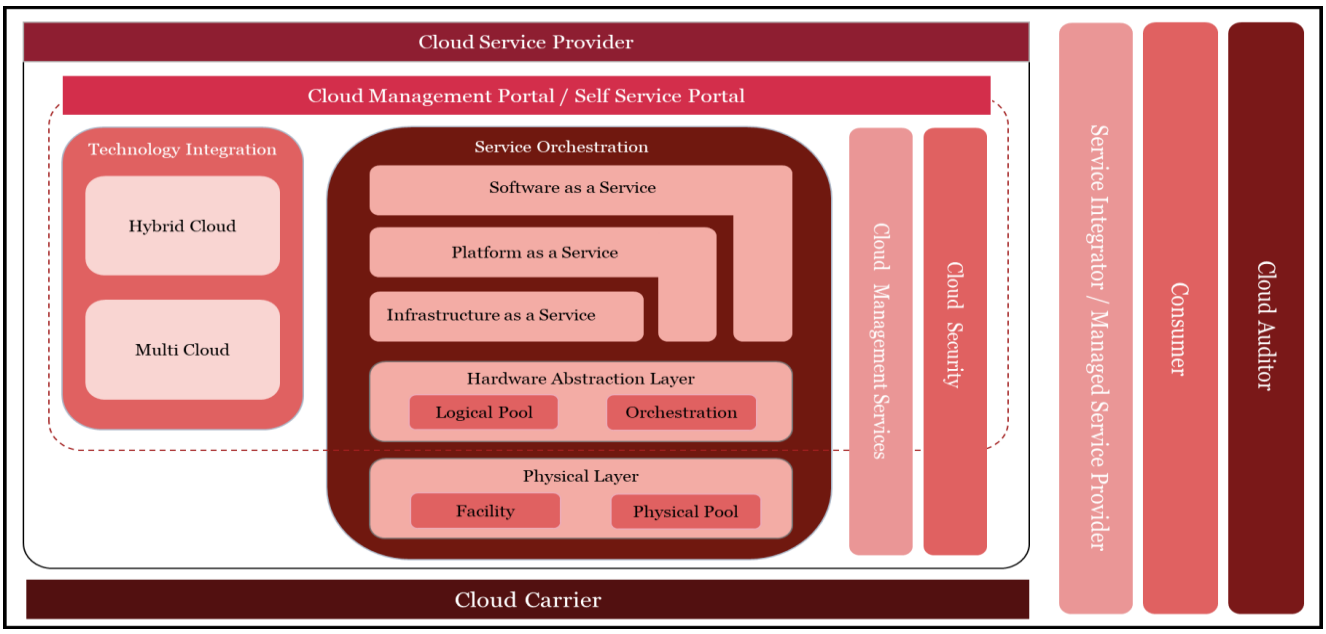

Figure 1: GI Cloud Reference Architecture

The figure above details the various building block which make up the GI Cloud Reference Architecture. This Reference architecture may be leveraged as a framework to build/design Cloud deployments/environment. GI CRA comprises of the following essential components/entities:

- Consumer
- Cloud Service Provider
    - Service Orchestration
    - Cloud Management/Self-service Portal
    - Cloud Services Management
    - Cloud Security and Privacy
- Cloud Carrier
- Managed Service Provider/Service Integrator
- Cloud Auditor

The GI CRA also comprises of an Integration layer which may be utilized for cloud models like Hybrid Cloud, Multi-Cloud and more.

The GI CRA layers/components/entities are described as below:

Components/Entities	Description
Consumer	User or consumer of GI cloud services i.e. Government Departments at Centre and State level, Citizens
Managed Service Provider/Service Integrator	Entity responsible for delivering and managing cloud services for the cloud consumer
Cloud Carrier	Intermediary responsible for connectivity and transport of cloud services from Cloud Service Providers to Consumer
Cloud Service Provider	Entity responsible for operating cloud environment and make cloud services available to consumers
Service Orchestration	Layer covering the management of physical DC facility, IT hardware infrastructure, hardware abstraction layer and provisioning of three cloud service models IaaS, PaaS &

Components/Entities	Description
	SaaS
Cloud Management Platform/ Self Service Portal	Single pane of glass from where consumer or Government Department can provision, manage, and terminate services themselves
Cloud Service Management	Responsible for the smooth execution of cloud build & operate. Includes cloud implementation, operations & maintenance services
Cloud Security and Privacy	Comprehensively address all the security related aspects. Defines guidelines on security addressing the various challenges, risks and for prescribing the approach for mitigating the risks
Cloud Auditors	Responsible for conducting assessment of cloud services, system operations, performance and security of the cloud implementation/deployment.

4 GI Cloud Reference Architecture

This section describes in detail the entities which form the GI Cloud Reference Architecture along with various actors, components and services. Government Department may choose all or some of the services depending on the application requirement while designing the cloud architecture.

4.1 Consumer

The Consumer is the entity that uses or consumes the Cloud services. The Consumer may request for the required service, set up a service contract with the Managed Service Provider/Service Integrator or Cloud Service Provider and consume the cloud service. Consumer lays down the requirement of cloud services and chooses amongst the services offered by the cloud provider .Based on the services consumed, the cloud consumer may need to arrange for payments. Consumers include citizens, government departments, line departments and agencies at the central and state levels.

While opting for cloud services from any of the cloud providers, consumers shall clearly specify the technical requirements. Consumers must also specify the SLAs which shall be fulfilled by the cloud provider. From services perspective, consumer shall identify and specify the quality of services required and which shall be provided by the cloud provider. Any kind of service agreement between customer and cloud provider must include the scope of the cloud provider, security provisions, service level agreement and the finalized payment terms.

A cloud consumer can choose amongst plethora of services offered by cloud providers consisting of IaaS, PaaS and SaaS. For details of the service offerings, please refer the cloud providers individual portals or for empaneled services please refer to Bouquet of Cloud Services and visit (https://www.meity.gov.in/writereaddata/files/Cloud_Services_Bouquet.pdf) for more details.

4.2 Managed Service Provider/Service Integrator

'Managed Service Providers' are defined as below:

- Eligible agencies who would be providing managed services on behalf of the Cloud Service Providers.

- Cloud Service Providers whose services have been empaneled by MeitY and willing and qualified to fulfill role of MSP. They are qualified to register on GeM portal for delivering Cloud Services

Government Departments would contract the Managed Service Providers in case cloud services are being delivered and managed by them on behalf of the Cloud Service Providers. Government Departments can choose to procure cloud services directly from Cloud Service Provider when it already has in place an Implementing Agency/Internal IT Team/expertise that is responsible for managing Cloud resources

There will be a scenario where End to End procurement of cloud services shall be done through a Service Integrator when the cloud services would be a part of the total services procured through Service Integrator (SI) for a turnkey project implementation

Government Departments may refer to the Guidelines for Managed Service Providers offering Cloud Services through Government e-Marketplace for detailed responsibilities of the Managed Service Provider.

MSP/SI will manage the cloud platform and delivery of services along with relations between consumer and cloud provider.

4.3 Cloud Carrier

The Cloud Carrier acts as an intermediary and provides the network connectivity backbone for transport of cloud services between consumers and cloud providers of GI Cloud. Cloud carriers provide access to consumers through network, telecommunication and other access devices.

As part of any engagement, departments shall call out specific SLAs with a cloud carrier to provide services as per the requirements. A cloud carrier may provide dedicated/shared and secure connections between consumer and cloud service provider depending on the department requirement.

4.4 Cloud Service Provider

Cloud Service Provider is the entity responsible for provisioning of the cloud services and making them available for end user consumption. A Cloud Service Provider is responsible for ownership and management of the computing infrastructure required for providing the services, running various software for delivery and management of the services, and ultimately making Cloud services available to the Government Departments through network access. Cloud Provider is the key entity in the GI Cloud Reference Architecture whose roles and responsibilities are extremely vital and critical. Cloud Service Provider is responsible for developing and positioning its offerings through various cloud services model (IaaS, PaaS, SaaS), various cloud deployment models (Public Cloud, Virtual Private Cloud, Government Community Cloud) and managing the delivery of the services. Government Departments based on their requirements may choose the required cloud services on the basis of cloud services model and cloud deployment model being offered by various Cloud Providers.

Cloud Service Provider may offer management and delivery of services to the Government Departments either on its own or through its authorized Managed Service Provider (MSP)/Service Integrator (SI). MeitY has empaneled Cloud Service Offerings of various Cloud Service Providers and laid down multiple technical, functional, regulatory, legal requirements as a part of the empanelment. Increase in the efficiency of delivering cloud services and mitigation of various concerns around security has led to an increase in Cloud adoption within Government Departments.

Government Departments may refer to MeitY's RFP for empanelment of Cloud Service Offerings of Cloud Service Provider for details on the technical, regulatory, legal requirements as well as the Guidelines for Procurement of Cloud Services which outlines the roles and responsibilities of the CSP and MSP/SI on https://meity.gov.in/content/gi-cloud-meghraj

A Cloud Service Provider conducts following activities for all the consumers hosted on the platform pertaining to the areas of Service Orchestration, Cloud Management Platform, Cloud Management Services and Cloud Security & Privacy.

4.4.1 Service Orchestration

Service orchestration is the execution of operational and functional processes involved in developing, designing and delivering cloud services. It refers to the different components required to support Cloud Service Provider activities in positioning and management of cloud computing resources to provide services to Cloud Consumers. Cloud Service Orchestration focuses extensively on process optimizations and takes advantage of different building blocks by reusing them.

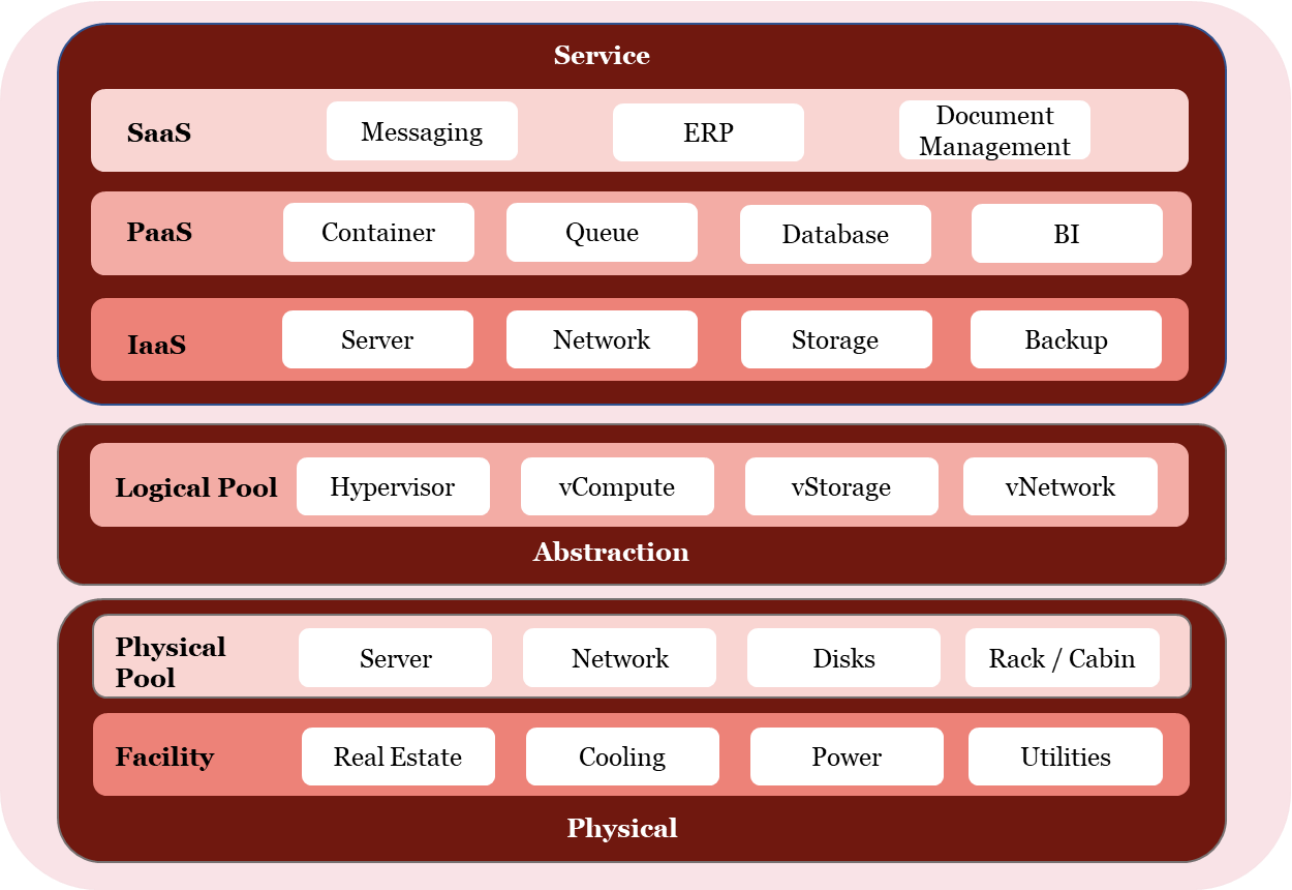

Figure 2: Service Orchestration

The figure above describes the logical view of orchestrated services mainly classified into three sub-layers. The three cloud services model i.e. IaaS, PaaS & SaaS make up the Service Layer whereas Physical DC along with IT hardware constitutes the Physical Layer. The Abstraction layer which includes Hypervisor and virtualized IT infrastructure ties together the Service and Physical layer.

- IaaS: Infrastructure as a Service enables provisioning of compute, storage, networks, and other fundamental computing resources on which Government Departments may deploy and run their applications. The Departments do not manage or control the underlying cloud infrastructure but have control over operating systems, storage, and deployed applications.

- PaaS: Platform as a Service enables deployment of acquired applications or applications created using programming languages, libraries, services, and tools onto cloud infrastructure supported by the Cloud provider. The Government Departments do not manage or control the

underlying cloud infrastructure including network, servers, operating systems, or storage, but have control over the deployed applications and possibly configuration settings for the application-hosting environment.

- SaaS: Software as a Service enables Government Departments to use the cloud provider's applications running on a cloud infrastructure. The applications are accessible from various client devices interface, such as a web browser e.g. web-based email, or a program interface. The Government Departments do not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, except for limited user specific application configuration settings.

It is possible, though not necessary, that SaaS applications can be built on top of PaaS components and PaaS components can be built on top of IaaS components. Government Departments may choose either of the service models depending on their requirement.

The Abstraction layer include software/system elements such as hypervisors, virtualized compute, virtual data storage, virtual network and other computing resource abstractions. The abstraction layer needs to ensure efficient, secure, and reliable utilization of the underlying physical resources by the use of software abstraction. While virtualization technology is commonly used at this layer, other means of providing the necessary software abstractions are also possible. This layer also ensures resource allocation , access control and usage monitoring .The software fabric being leveraged by the Cloud Service Provider that ties together the underlying physical resources and their software abstraction to enable resource pooling, measured service and dynamic allocation.

The lowest layer in Service Orchestration is the Physical Layer, which includes all the physical IT resources along with the physical facility which houses the cloud.

- Facility: Facility include the building in an area that houses essential component to run the Data centres. This facility will have provisions of redundant cooling & power supplies to run data centre equipment's and also includes other utilities like physical security to control and safeguard against unauthorized access.

- Physical Pool: The physical pool comprises of the components placed inside the facility like rack, cabinets which will house IT equipment i.e. server, storage and network devices. This underlying hardware components/equipment will host the virtual environment.

Cloud Consumers are exposed to cloud service interfaces in the Service Layer whereas do not have direct access to the Abstraction and the Physical layer/resources.

4.4.2 Cloud Management Platform

Cloud Management Platform (CMP) would be the centralized access point to manage Cloud deployments and would act as an interface to provision cloud-based IT Services. CMP may provide facility to manage the deployment and operation of applications and associated datasets across multiple cloud service infrastructures, including both on-premises infrastructure and cloud service provider infrastructure. CMP may also provide management capabilities for both hybrid cloud and multi-cloud environments.

CMP has the ability to provide functionalities such as Provisioning and orchestration, Security and compliance, Service Request, Monitoring and logging, Cost Management and optimization and day to day operational activities. These functionalities may be native or orchestrated via third party integrations.

Figure 3: Cloud Management Platform

Government Departments require a feature which allows them to provision, manage, and terminate cloud services themselves through a Web portal or programmed service API calls. CMP is such a feature, a well-coordinated unified management framework that provides an interconnected view of the infrastructure and end-to end visibility.

4.4.3 Cloud Management Services

The Cloud management services provides the key capabilities which are necessary for operations and management of the resources and services required by the consumer.. Cloud Management ensure smooth process flows as per business agreement and the prime objective is to maintain critical services up and running. Cloud management comprises of the administrative tasks involved with creation, maintenance, product/service performance and quality control of the environment within defined scope of work. Cloud management services focuses on processes and services invoked, such as when and where activities occur, who delivers them and how many people or entities they reach. Government Departments should have the ability to create monitors that actively check various metrics, integration availability, network endpoints, and more. Following are some the most widely used but not limited to cloud management services:

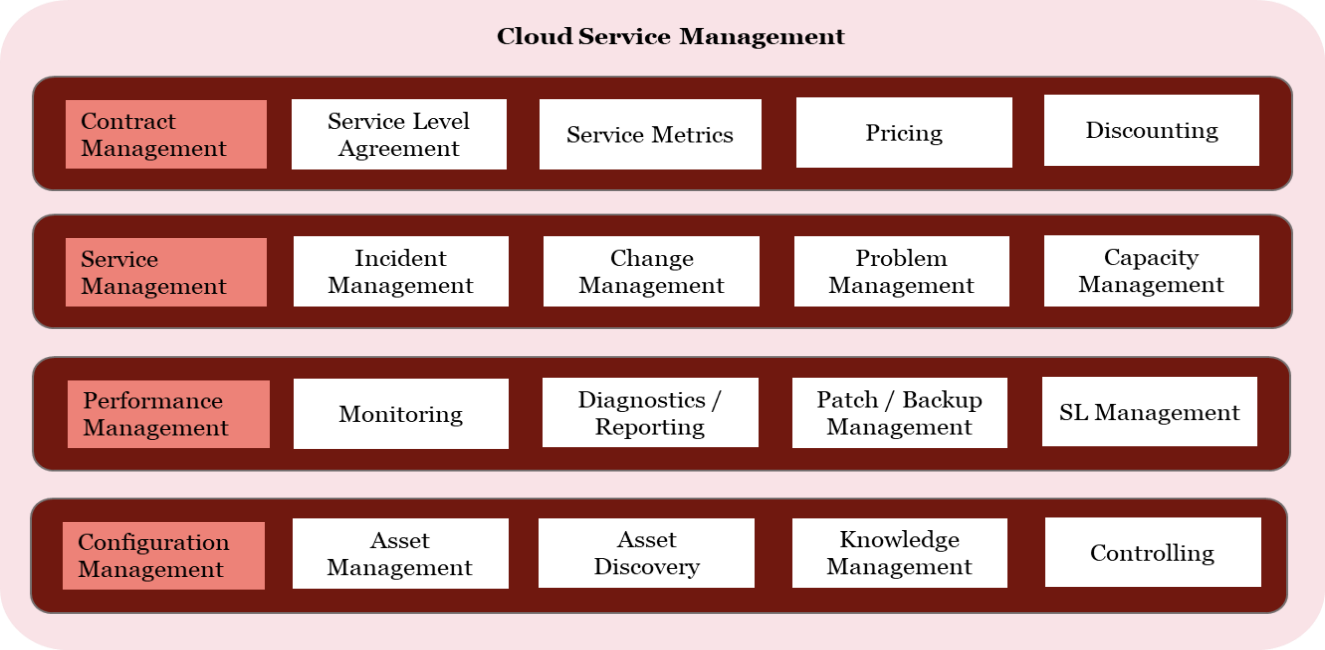

Figure 4: Cloud Management Services

Contract Management – Contract Management is the process of systematically & efficiently Managing contract creation, execution, analysis for financial management & operational performance. Contract Management is the agreement and legal acknowledgment between the Cloud Provider/Managed Service Provider and the Government Departments that ensure to meet the operational, functional & Department's objective. A contract specifies the Service Level Agreement (SLA), agreed period of contract & resources, and activities (Service Metrics) between both Department and provider (who is responsible for each defined activity). It also specifies the discovered prices or agreed pricing between both parties and any other commercial term as a part of contract.

- Service Level Agreement - Service Level Agreement is a documented agreement between the Cloud Provider/ Managed Service Provider and the Government Department to provide a set

of deliverables in a defined timeline. If services are not provided within in defined timeline can lead to penalty depending upon the agreement.

- Service Metrics - Service Metrics defines the roles and responsibilities, defines the owners of the services along with who is responsible for what role or duties between the Cloud Provider and the Government Department.

- Pricing - Pricing is one of the core components of commercial contract, which defines a fix rate or cost of a services given to Government Department

- Discounting - Discounting if any, are based on the price negotiations between the Cloud Provider/ Managed Service Provider and the Government Departments as per the contract terms, for example: It can be 10% discount on a year and 55% on 3 year contract between the Cloud Provider/ Managed Service Provider and the Government Department.

Contract Management activities may be undertaken by the Managed Service Provider in case Government Departments enter into a contract with Managed Service Providers for consuming cloud services.
Government Departments may refer to Master Service Agreement (MSA) for procurement of cloud services (https://meity.gov.in/writereaddata/files/Guidelines_Contractual_Terms_Cloud_Procurement_V1.2.pdf) and Guidelines for User Departments on Service Level Agreement for Procuring Cloud Services (https://meity.gov.in/writereaddata/files/Guidelines_User_Department_Procuring_Cloud%20Services_Ver1.0.pdf) published by MeitY.

Performance Management - The proactive process of collecting, analyzing and using information to track a program or services to guide Government Departments/ Cloud Provider to take decisions to maintain the performance of infrastructure & resources.

- Monitoring - Monitoring focuses on processes and services invoked, such as when and where certain activities occur, who delivers them and how many people or entities they reach. Government Departments should have the ability to create alerts that actively check metrics, integration availability, network endpoints, and many more.

- Diagnostics / Reporting – Diagnostics is tool generated process which ensure health check and measures the performance of an IT environment. Based on diagnostics ran on IT environment a report is generated which is a collection of a data, that can be useful for troubleshooting and future enhancement.

- Patch / Backup Management - Patch management ensure regular deployment of the required patches to keep services, products, virtual machines, Operating Systems and more up to date in order to protect against security vulnerabilities and bugs. Backup Management is one the important aspects of cloud management wherein operational aspects of backup Management include backup and data protection, disaster recovery, restore, archiving and long-term retention, data replication and day-to-day processes on data.

- SL Management - Service Level Management is the process which is responsible for negotiating and meeting the agreed service level agreements, e.g. ticket response and resolution times.

Service Management - Service management refers to implementing, managing, and delivering quality IT services in the best possible way to meet the needs of a Government Department. It ensures that the appropriate mix of people, processes, and technology are in place to provide value. Service Management enables Government Departments to communicate or raise a request in order to resolve any technical issues. Service Management comprises of the following activities/processes:

- Incident Management - Incident Management is a process which ensures that normal service operation is restored as quickly as possible when any issue occurs or any disruption in services.
- Change Management - Change management refers to managing any change request , such as addition/deletion of any cloud services to the existing set of cloud services purchased by the Department.
- Problem Management - Problem Management come into picture when one or more incident with same issue occurs. When Problem Management is into place the repetitive incidents are investigated and fixed. Although Problem ticket may be kept open until a compete resolution of the root cause is found.
- Capacity Management - Capacity Management is an IT process for planning, managing and optimizing the IT infrastructure, Capacity Management ensure that IT resources are right sized to meet current and future requirements in a cost-effective manner.

Configuration Management - Configuration management maintains product's physical attributes with its requirements, design, and operational information and responsible for documenting the configuration of assets that deliver services e.g. Servers, Storage, Network devices – Switches, Routers etc. It ensures the configuration of system resources are known, and trusted.

- Asset Management - Asset Management is the coordinated activity to realize value from assets. It involves management and organization of multiple devices/virtual machines and software licenses to achieve the Department's objectives.
- Asset Discovery - Asset discovery is a process of discovering and collecting data on the technology assets connected to a network for management and tracking purposes. These assets can range from servers to virtual machines and software licenses.
- Knowledge Management - Knowledge management is a process of creating a knowledge base within the Cloud Provider environment to enhance their knowledge on certain activities, learnings from past experiences. Knowledge management also provides training and learning for the employees.

- Version/Configuration Control - Controlling is essential to keep check whether one or more versions of a deliverable or configuration is created. It ensures that all changes to configuration items are controlled.

When leveraging the cloud services the consumers are keen to know whether they shall be move data or application on multiple cloud environments with minimal disruption. A Cloud Service Provider must provide ability of data transfer to and out of the cloud environment to consumers along with supporting elements for migration of services and data from one provider to the other.

4.4.4 Cloud Security and Privacy

The move to cloud-based services has required security programs to extend operations beyond the traditional data centre and to re-evaluate security architectures, processes and controls to maintain effectiveness and efficiency in their efforts to secure various applications. Cloud Security is a crucial and integral component of the Cloud services.

Consumers in the ecosystem would consist of but not limited to Employees/Government Department Users, Application Partners of the Government Department as well as edge devices/ IOT devices (if any, those which would be interacting with the cloud layer).

The Cloud Security would consist of the following layers:

- Cloud Security Governance
- Cloud Security Operations
- Core Cloud Security Capabilities
- Privacy

4.4.4.1Cloud Security Governance

Cloud Security Governance is all about applying specific policies, principles, standards and guidelines to secure data and application deployed in the cloud. These policies and standards are to be applied with existing IT governance policies of the Department and not to be introduced in isolation.

4.4.4.2 Cloud Security Operations

Cloud Security Operations may be represented as a five-step process (Prepare, Prevent, Detect, Respond, Recover) under which various categorizes exist.

One of the crucial categories under the Prepare process is Threat Management and Assessment. It is detailed as follows:

Threat Management – Threat Management is a manual or systematic measurable technical assessment or evaluation for a security of the Government's information system or applications by performing security vulnerability scans, reviewing application and operating system through a unified security controls hub.

- Intrusion Detection & Prevention: Intrusion Detection & Prevention system are threat detection and prevention tool/equipment. IDS/IPS can be provisioned as a physical or a virtual appliance. IDS detect intrusion and malicious activity or policy violations. IDS monitor network and generate logs or report to administrators to act for any suspicious activities. IPS

tool is a Threat prevention tool. IPS is an automated approach which will response well before attacks. IPS continuously monitors network traffic flows and act itself finding any malicious activity or unauthorized behavior.

- Risk Assessment & Audits: Risk assessment is a systematic process of identifying risks to workers safety and health from workplace hazards, Identifying & analyzing potential events that may negatively impact individuals, assets or the environment.

The Prevent process mainly comprises of Vulnerability Scanning and Remediation along with Patch management for the entire cloud landscape.

- Vulnerability Scanning and Remediation: Moving application from pre-production to production requires vulnerability scanning, if application is compromised while developing or in pre-production stage, then infected image will be carried on to production as well. Scanning application for any vulnerability is important. This Process is done through tool which automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. It performs vulnerability scanning of Application which generate an easy to understand report to fix any vulnerability. One the vulnerabilities are identified the same can be remediated as per standard practices by the responsible stakeholders.

- Patch Management: Regular patch management for Operating System, Databases, Anti-virus and other components are ensured by the CSP with acceptance of the cloud consumer. The consumer must be responsible for patching the application periodically. Hence patch management becomes critical in prevention of any breaches which may occur due to vulnerabilities existing in unpatched systems.

The Detect phase comprises of intelligent monitoring around end-point as well as internal monitoring of cloud resources. It is important to monitor cloud resources in order to take effective informed decisions based on the monitoring. The monitoring is to ensure security incidents are timely tracked and documented. A Security dashboard provides a centrally managed and comprehensive view of high-priority security alerts and compliance status. It is single place view tool which monitors cloud environments for vulnerability and check for compliance based on best practices and industry standard.

The Respond phase through incident response management and Cloud forensics would enable Government Departments to respond to cloud security threats in a timely and controlled manner.

- Incident Response and Management: In order to avoid major security issues in the cloud, it is important for Government Departments to have an incident response and management plan in place. Incident response may be a collaborative effort between the Government Departments and the Cloud Service Provider wherein there are clear delineation of roles and responsibilities in case of an incident. It is also important to have a recovery plan in place for certain major incidents.

- Investigation and Forensics: Cloud Service Providers make available certain tools either natively or as third party applications that allow for conducting forensics in case of an incident. In addition to breach investigations, cloud forensics is important in troubleshooting when performing Root Cause Analysis (RCA) for re-building systems lost during disasters or incidents and for complying to compliance and legal requirements.

4.4.4.3 Core Cloud Security Capabilities

Some of the components while evaluating cloud security capabilities of any CSP are detailed below:

Identity & Access Management - Identity and access management (IAM) is the efficient way of giving users access to the right resources at the right time. Security has become a big challenge for identity architects and administrators due to increasing user identity spaces, Statewide policies, complex structure hierarchies and roles, regulatory pressures, and customer facing applications. IAM and User access management is essential to solve complexities arising out of identity silos, securing an increasing number of APIs and endpoints, account management, user password maintenance, regulatory compliances, and licensing.

- Multifactor Authentication - Provides additional layer of security from the prospective of authentication. In Multifactor Authentication users must enter a secure key, can be combination of number or alphabets apart from their username & password. The Auto generated secure key is shared to user on their registered ID or phone number. This type of authentication requires several different forms of authentication and verification before allowing access to secured information.

- Directory Services - Provides functionality to control users, computer & resources. It manages access, controls and privileges within the defined network and manage objects and their attributes. It required to an organization to authenticate employees to login into organization's domain and access certain resource within domain.

- Role Base Access Control - Role-based access control (RBAC) is a process of assigning permissions to users as per their role within an organization. It provides fine-grained control and assigning permissions to users individually. RBAC lets employees to perform action only need to do their jobs and prevents performing task which are not part of their job or role.

- Single-sign-on (SSO) – SSO is an authentication process that allows a user to access multiple applications with one set of login credentials.

Application Security – Application security which primarily deals with protection of cloud applications avoid vulnerabilities such as SQL injection, cross-site scripting, weak authentication and session management, cross site request forgery etc. Vulnerability assessment while deploying the application to cloud should be ensured. Adopting security while designing the application as in the process of DevSecOps is now considered a best practice while evaluating application security in the cloud.

Awareness and Training – Making Government Departments aware about latest developments in the sector of cloud security would enable adopting the right set of tools, policies and procedures while deploying their application on cloud.

Infrastructure Protection – One of the most critical aspect of any cloud deployment is protecting the underlying infrastructure (compute, network, storage) from any security threats. Today Cloud Service Providers are leveraging state of art Security Operations Centre (SOC) facilities for monitoring and managing their deployed infrastructure.

4.4.4.4 Privacy

In any digital economy, data is of strategic importance with many socio-economic and governmental activities being increasingly carried out online. The flow of personal data in the cloud is giving rise to concerns related to storage and using current technologies on cloud services. It becomes more urgent to address various concerns over data and Privacy. The challenge for data protection is in managing the risks and addressing the concerns without restricting or eliminating the potential benefits. The role of Governments and the industry in protecting data-in-transit and data-in-rest is of paramount importance.

- Encryption: Encryption is a way of scrambling data so that only authorized parties can understand the information. Encryption will ensure that no one can read communications or data at rest except the intended recipient or proper data owner. This prevents cyber criminals, from intercepting and reading Government's sensitive data. Encryption helps protection against data breaches, whether the data is in transit or at rest. Similarly, encrypted communications enable the communicating parties to exchange sensitive data without the hassle of data leakages.

- Key Management: When there is an Encrypted program or data to decrypt that information the encryption key is required; encryption key is the unique sequence of bits that protect data from being decrypt. Key Management system is designed to manage, create and protect encryption key and manage encryption and decryption tasks.

- Data Integrity and Data Handling: Data integrity is the maintenance and assurance of accuracy and consistency of data throughout its lifecycle. Data increasingly drives Government Department's decision-making, but it must undergo a various changes and processes to become more practical for facilitating informed decisions. Hence data integrity must be a top priority for all Government Departments. Data integrity can be compromised in a various way hence it becomes pertinent to make data integrity practices an essential component of effective cloud security framework. Location of data and duration of data storage are the main factors to decide on data handling requirements in the cloud. With today's cloud services these factors are addressed to meet any regulatory or Departmental compliances.

  Government Departments may refer to the cloud security best practices published by MeitY for securing their application and cloud deployments.

4.5 Cloud Auditor

The primary role of a Cloud Auditor is to perform an independent examination of cloud service controls. These controls are widespread and range from SaaS to IaaS, Virtualization Controls, Data Management Controls, Data Storage Controls, Infrastructure Controls and more. Audits are performed to verify conformance to standards through review of objective evidence. A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc.

5 Use case scenarios in Cloud

Today Government Departments are focusing on IT modernization where Cloud provides a mechanism to quickly deploy new applications and services at a fraction of the time of on-premise development. The scale of engagement for the Government Departments on the cloud front is rapidly increasing. The Departments have a facility to opt for a pay-as-you-go model to purchase cloud services they consume.

Even today's citizens have become more demanding about the quality of services they receive, hence Cloud gives the flexibility to innovate in how citizen services are today being designed and delivered.

The traditional view–that still holds true in some Government Departments–that data is only secure when held on your own servers in your own data centre, is today becoming a thing of the past. Today, Cloud may be considered more secure than on-premise implementations given the wide variety of security services made available on a "As a service" model. It has been designed for the volume and velocity of the new types of data that all organizations–public and private–must deal with.

Government Departments are today looking to embrace the flexibility, scalability and innovative benefits of Cloud computing. While secure and powerful, Cloud is evolving to support workloads that are stable and contain less sensitive information. The early hybrid alternative was to maintain all sensitive data on-premise and move everything else to the Cloud. Today, there is a more sophisticated path where Government Departments may choose to place workloads on the best platform for their mission needs and budgets. They may create an environment based around a combination of on-premise private Cloud, Hybrid / Multi Cloud and Public Cloud.

Hybrid cloud deployments allow for Government Department to benefit from features of Cloud as well as on-premise deployments. Listed below are the features that would make hybrid cloud attractive for Government Departments:

- Hybrid Integration Styles: Combining app integration, API integration and data integration.
- Hybrid Connectivity: Reach across secure connections to get access to data residing on-premise from Cloud.
- Hybrid deployment: Application and virtual machines can be flexibly migrate or deploy on cloud and on-premises to optimize solution architecture.

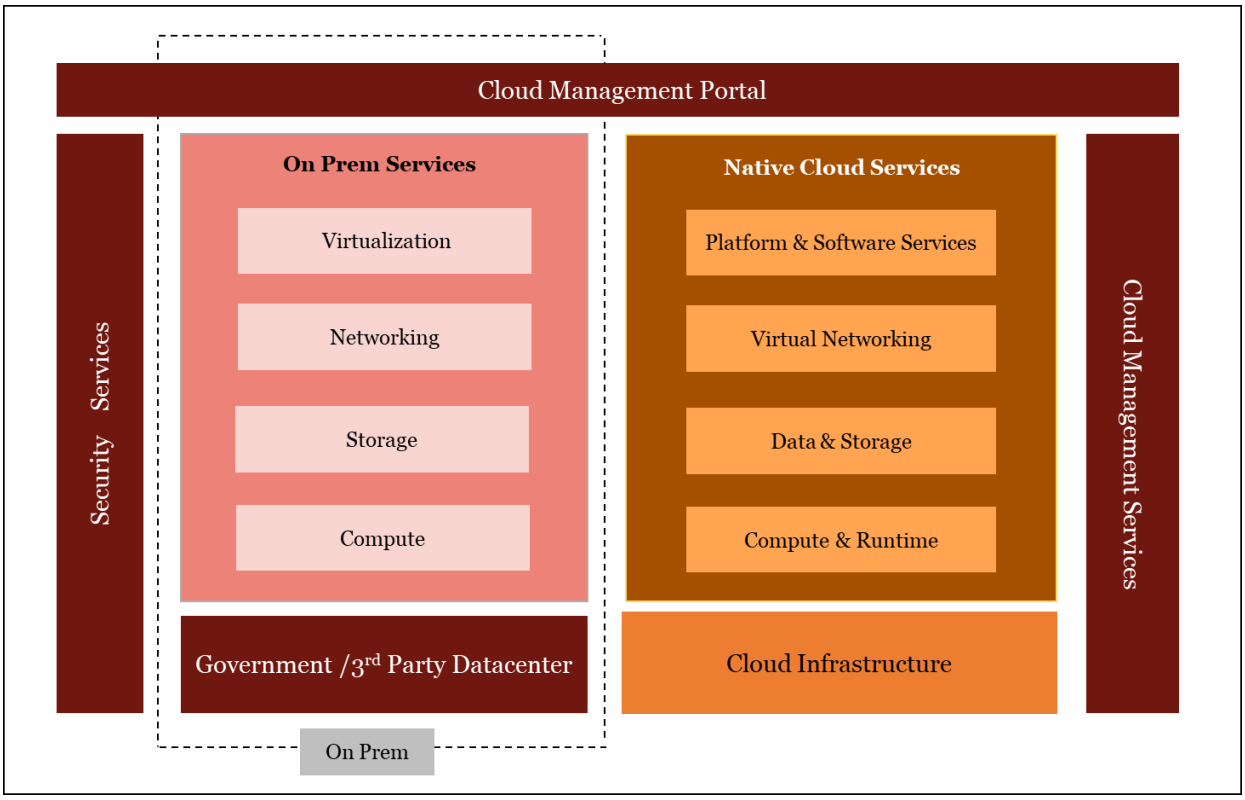

Figure 5: Hybrid Cloud Reference Architecture

The above figure depicts a hybrid cloud reference architecture wherein virtualized IT infrastructure in a third party/Government Data Centre is available (on-premise deployment) and cloud native services are available in the cloud infrastructure. CMP would be the layer allowing for management of resources.

By adopting a hybrid approach to Cloud deployment, Government Departments may overcome any security and data sovereignty issues of the past to deliver a new generation of innovative citizen services.

Some of the common use cases for hybrid cloud as they are settling within digital transformation initiatives are as follows:

- APIs economy: Joining the API economy exposing existing data and functionality from existing system and exposing that as API. API is available to partners to build innovation solutions and service-oriented architecture.

- Automation: Productivity is one of major aspects, automation enable people to spend more time on value added task of their work and less time moving data between system and doing manual tasks which might lead to duplication of data or work.

- Refactor for innovation: Digital transformation leads to digital application, make fundamental shift to a composable application architecture, refactoring from Monolithic to Microservices and moving on to cloud native services.

With Cloud interoperability, Government Departments can leverage services from multiple cloud providers as per their requirement. Multi-cloud is a concept of utilizing more than one cloud service,

from more than one cloud providers, for instance; one cloud provider may provide better IaaS Services while the other Cloud provider may provide better PaaS & SaaS Services.

Government Departments are more likely to meet their mission and operational needs if they're able to carefully select one or more cloud platform best suited for each of their workloads. Cloud Service Providers are now offering Multi Cloud management service, which run on top of existing virtual environment running on-premise and will provide single platform/portal to manage or move workload from on-premise to cloud, and from one cloud to another cloud thereby deriving benefits offered by different Cloud Providers and avoiding vendor lock-ins.

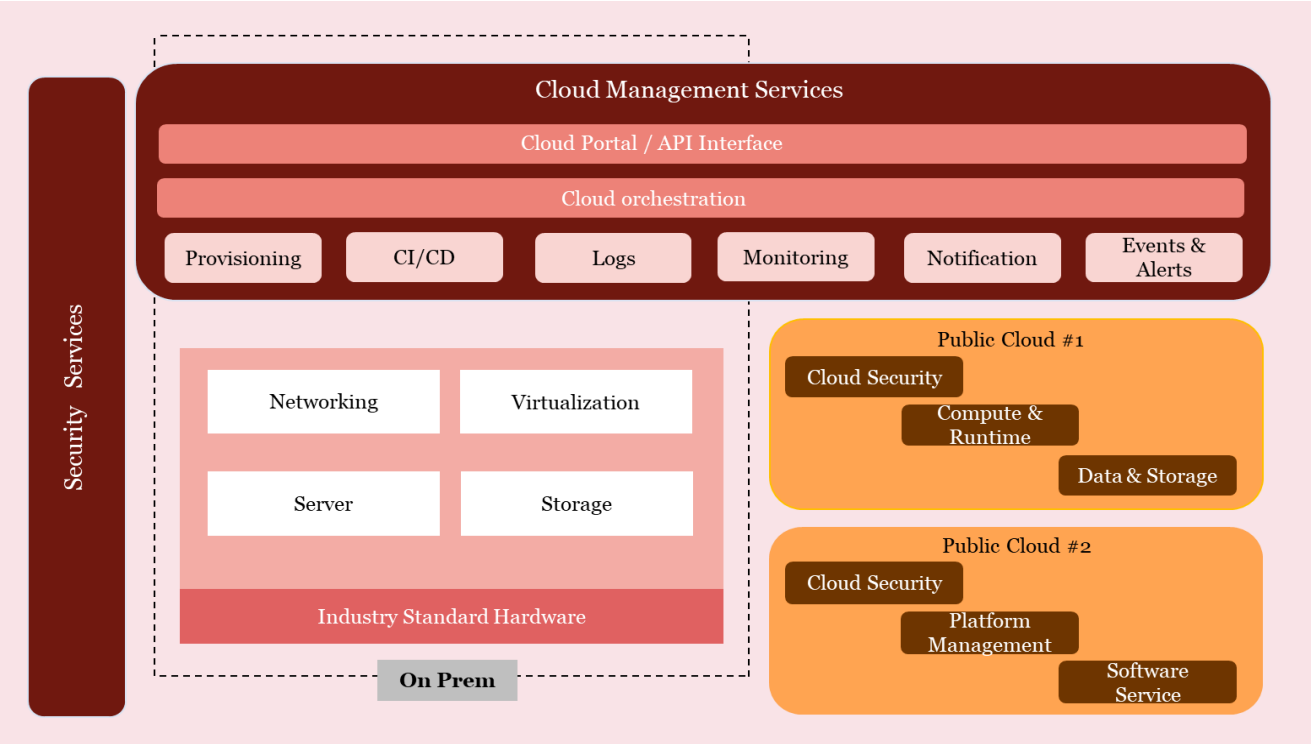

Figure 6: Multi Cloud Reference Architecture

The figure above illustrates the reference architecture devised for Multi-cloud deployments. Virtualized infrastructure on-premise in Government or third party DCs along with IaaS, PaaS and SaaS from different cloud providers. Cloud Management Services through Cloud portal and orchestration allows for management of the different cloud deployments across different Cloud Providers.

Below the are few widely recognized cloud scenarios:

5.1 Database on Cloud

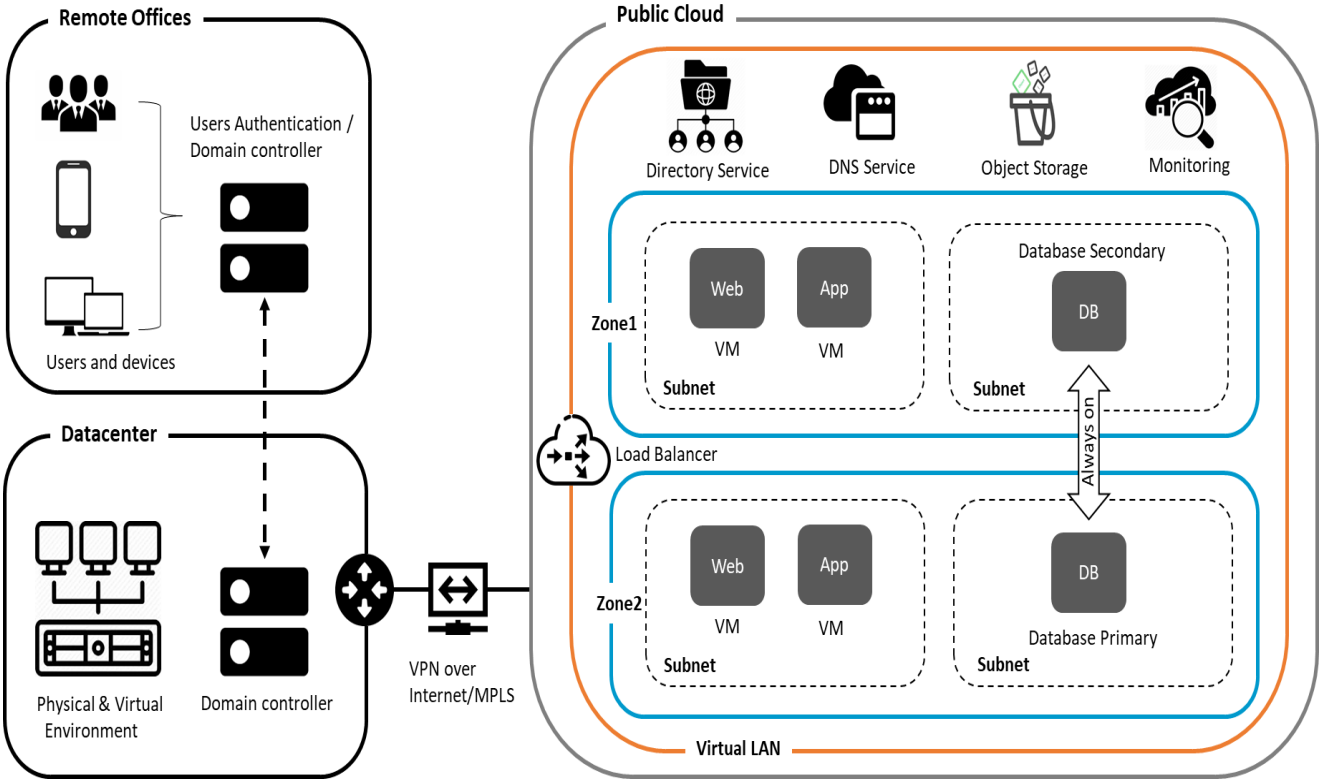

Figure 7: Database on Cloud

The Above Hybrid Cloud Architecture depicts Database on Cloud with active -active database configuration. In this scenario User from different sites and office location are authenticated from Domain controller to access resources, then either through VPN over public internet or MPLS they can access the website or application which is hosted on cloud environment. Having Database on cloud has its many advantages.

Benefits:

- Database services on cloud are automated backed.
- Free up space in production storage reserved for database.
- A copy of the database with read only privilege for load sharing and secondary database for failover or high availability.
- Database volume size can be increased or decreased on the fly, without any downtime.

5.2 Hot Disaster Recovery on Cloud with on-premise Primary DC

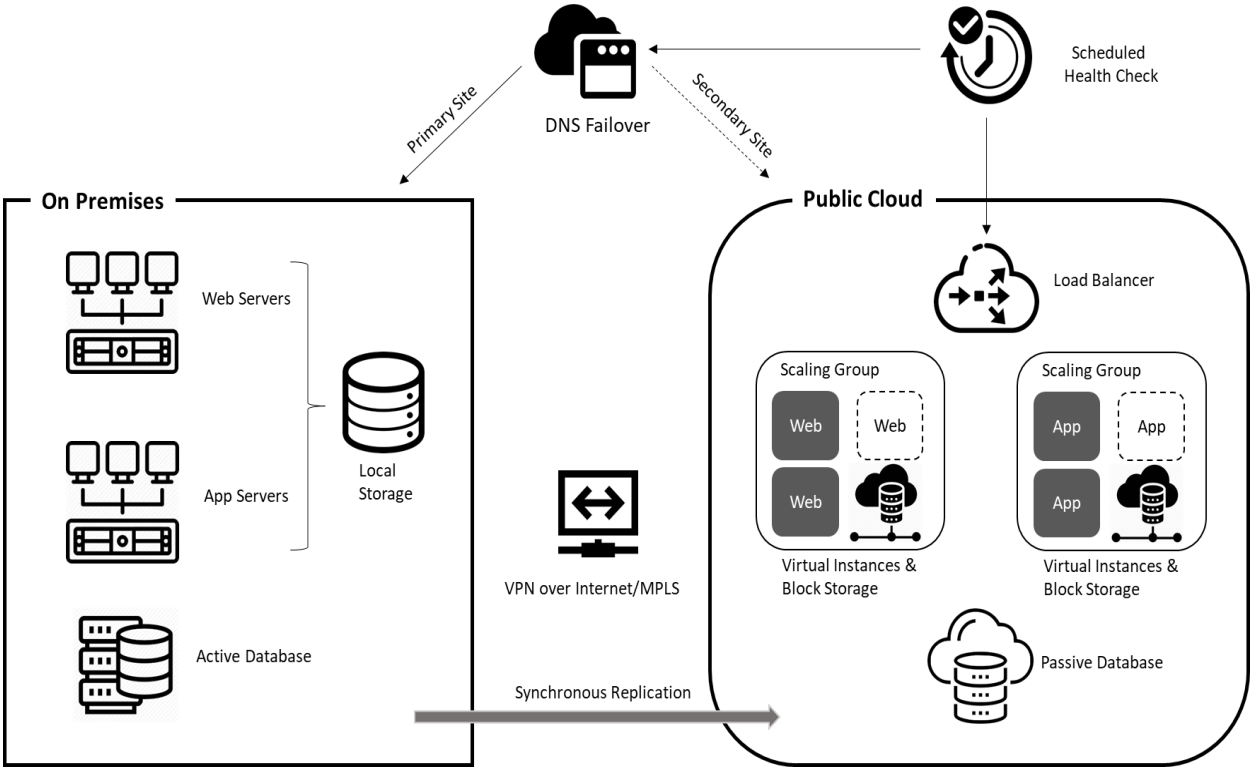

Figure 8: Hot DR on cloud with on-premise Primary DC

With the emergence of Clouds, concepts like High Availability, Data Durability and Infrastructure Elasticity for business continuity have become a reality. Hot Disaster Recovery (DR) can provide near zero RTO and RPO. In case of a Hot DR, services and databases are distributed and synchronized onto another site, geographically apart for the operations continuity in case of a major failure of the on-premise data centre. In this scenario Web, Middleware and Database server are replicated synchronously. Once the disaster strikes or Primary site goes down, the DNS will failover the traffic to secondary site on Cloud. Schedule health check will do regular ping test or heartbeat test as per configured interval of time i.e. Ping test at configured time interval (minutes, seconds) and setup alerts intimating DNS to route traffic to secondary site if ping test fails.

Once the DR site is up, autoscaling (which may already be configured) would start bringing up the virtual machines and would scale- in or scale-out as per requirement. Based on the configuration/algorithm the Load balancer will send load to the Web servers. Passive Database will become active and web & middleware will be in position to access Database.

Cloud Service Providers provide DRaaS (Disaster Recovery as a Service) to end customers with no initial investment in the form of Capital Expenditure.

Benefits:

- Cost effective DR solution for critical applications

- Auto scale would enable right size the virtual machines as per requirement
- Automated failover mechanism requires less human intervention.

5.3 Backup & Archive / Cold Disaster Recovery on Cloud with an On-premise Primary DC

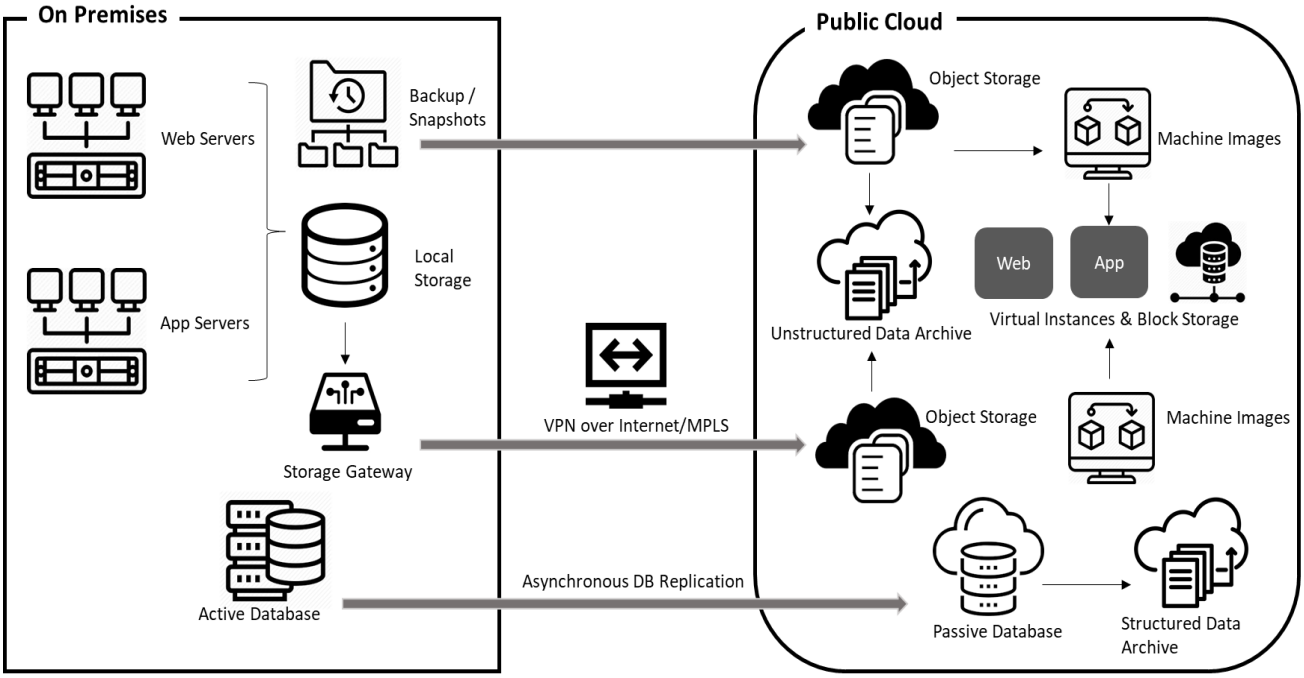

Figure 95: Backup & Archive/ Cold DR on Cloud with on-premise Primary DC

The figure above illustrates the Backup & archival of data on Cloud scenario which is one of the most popular Hybrid cloud use cases. Setting up an on-premise storage for backup and archival demands huge CAPEX. Putting on-premise backup on cloud is of the most significant ways to utilize cloud services. In this scenario Backup / snapshots are sent over cloud through an automated process by the Cloud provider and are kept in an Object storage in encrypted form. Local on-premise storage can also be backed up on cloud. This architecture may also find suitability in designing Cold Disaster Recovery solutions where Departments may not have strict RTO & RPO requirements. If Primary site is down, the CSP or MSP will be able to bring up those virtual machines from Machine image, which were backed up in object storage. Also, as per the Department's backup policy requirement for the availability of data, they can archive their data on cost effective object storage as well.

Benefits:

- Cost effective backup & DR Solution for Non-critical workloads.
- Can archive structure & unstructured data for longer time with minimal cost.
- Free up production storage after analyzing data which required to move on archives.
- Easy retrieval process of archived data.

- No need to procure hardware for backup data on-prem.

5.4 Analytics on Cloud

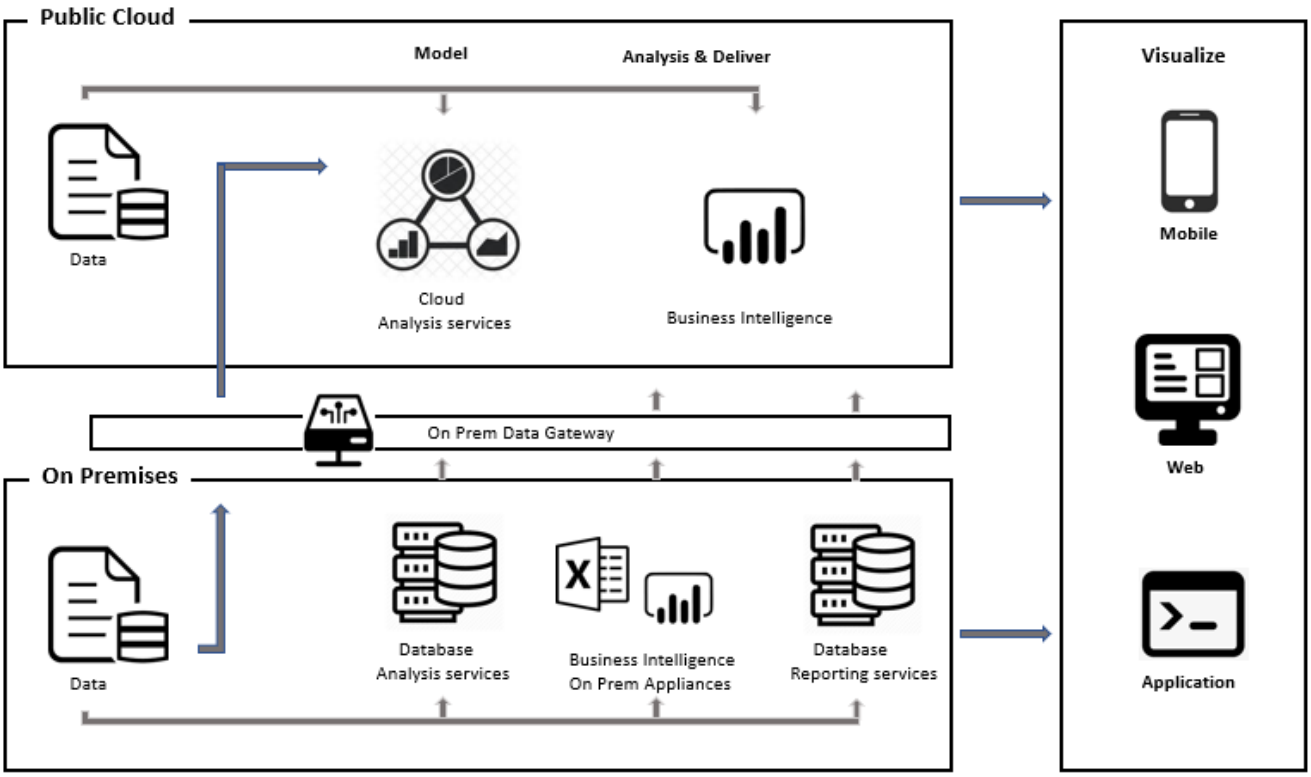

Figure 10: Analytics on Cloud

Running analytics and data scrubbing requires lots of compute power and chain of cluster which is an expensive solution to be built on premises. Government Departments , in order to gain insight from large, complex data sets may utilize data storage and analytics services from CSPs. Users analyze high volumes of data, which might already be stored in the cloud, for example in a Data Warehouse, Cloud provider have enabling BI (Business Intelligence) semantic data modeling capabilities in the cloud. Users can access data sources across on-premises and the cloud infrastructure, model that data and provide business users with a simplified view of their data to enable interactive self-service BI and data discovery using their preferred data visualization tool.

Benefits:

- No need to procure high performance server clusters.
- Gaining useful information out of stored data.
- Consumer can integrate their preferred data visualization tool with Cloud analytics tool.

5.5 Multiple Cloud for Different Functions

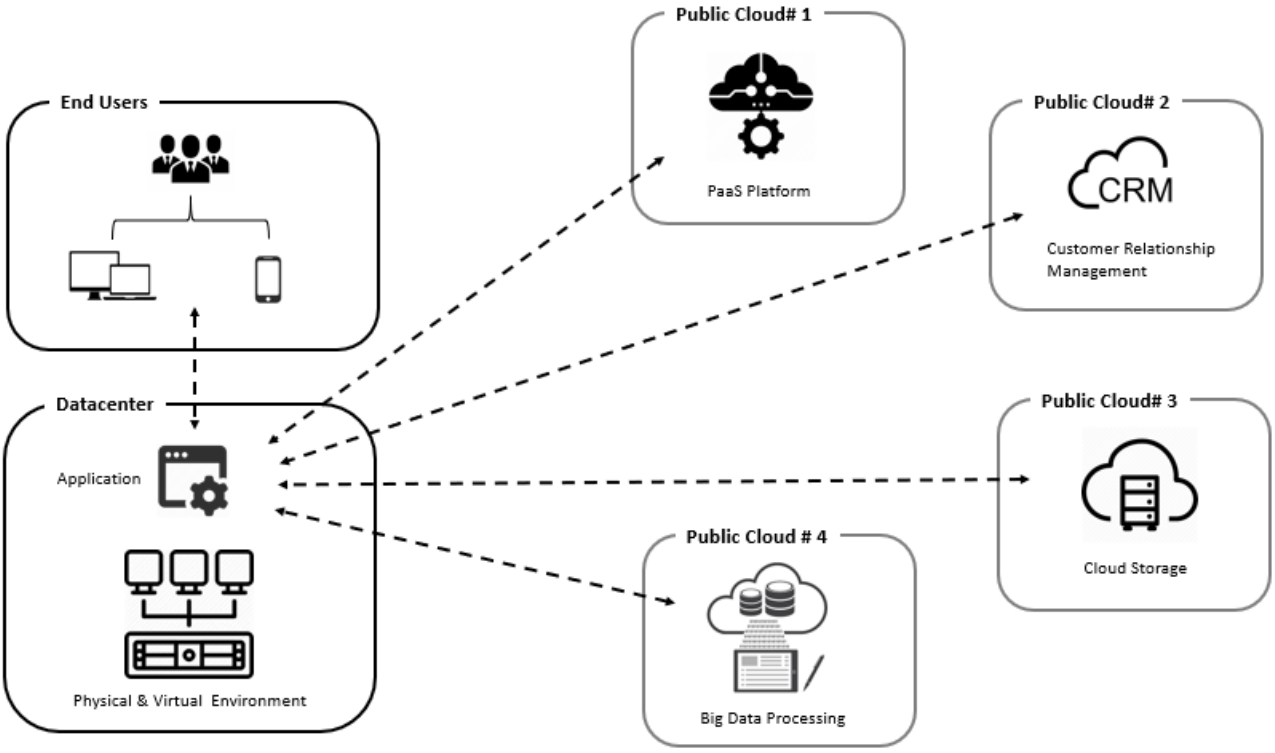

Figure 11: Multiple Cloud for Different Functions

With Multi Cloud strategies, Government Departments can utilize best services (based on functionality and cost) provided by different Cloud providers. In this scenario, application is hosted on Premise, and for Functions and processing, the application is using compute and tools/services provided by different cloud providers. It is a potential cost saving, as Government Departments need not to spend on CAPEX for setting up hardware for data queries and other analytical process.

Moreover, such an arrangement reduces vendor lock-in as well. In a multi-cloud strategy , systems and storage are spread out across multiple cloud platform. Hence, it becomes easier to migrate small-small footprint from on Cloud provider to another's, because most of the infrastructure remains in place during the migration.

5.6 Multi Cloud Scenarios – Migrating to Containers (Monolithic to Microservices)

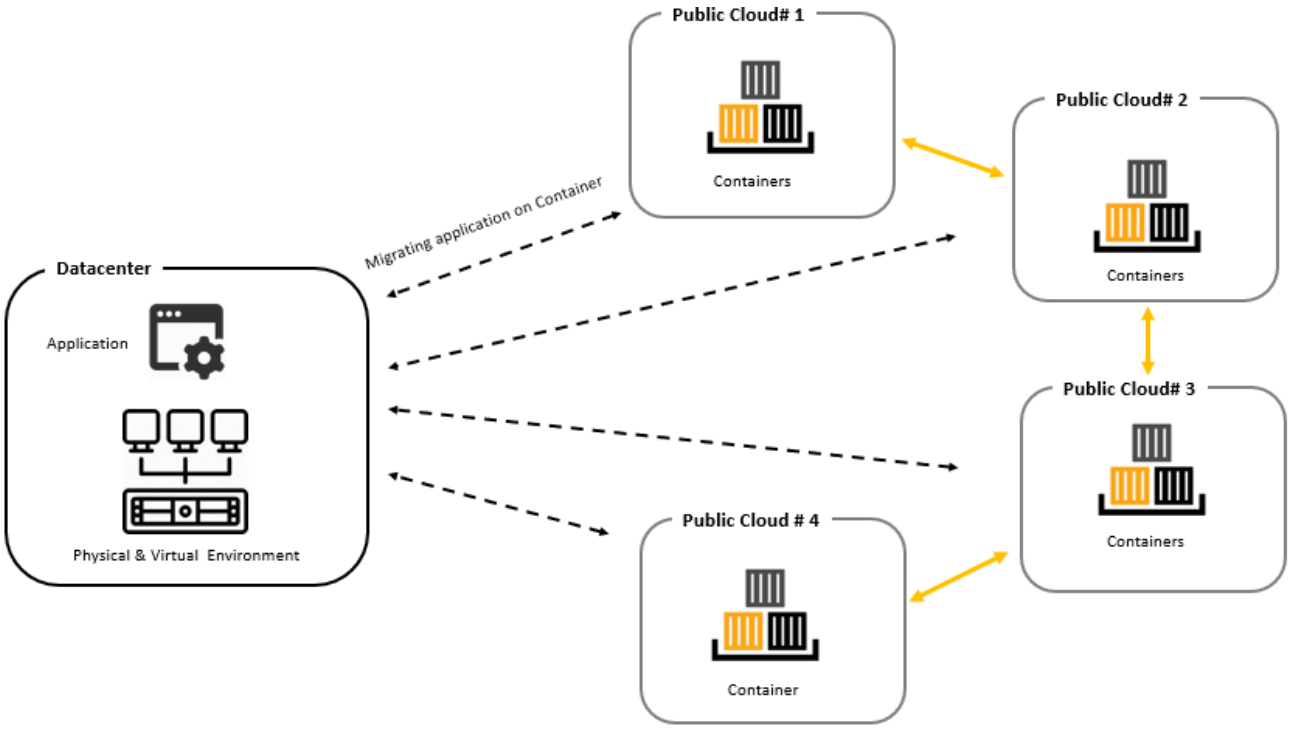

Figure 6: Migration to Containers

Government Departments may not enjoy the complete benefits of cloud technology without using containers and microservices. Microservices and containers are a fast-emerging industry standard that give the Department the flexibility and portability to move data and workloads in and out of different clouds, to deploy more quickly, and to manage applications and data across environments. Microservices belong to a type of architecture in which the applications are split into component pieces, each of which performs a specific fine-grained function. Microservices run inside containers, which include everything a microservice needs to run, such as code, dependencies, and libraries. Containers provide optimal portability across cloud and on-premises environments. Container platforms provide a system for automating deployment, scaling and management of containerized applications. Multiple players whose services are empaneled by MeitY provide container orchestration across cloud platforms. Multi cloud management platform using leading container orchestration, will enable the Government Department to build a cloud, and access cloud services quickly and securely.

It can be helpful to compare microservices to the older monolithic development style of applications, where all an application's components and functions were in a single instance. Many Department applications are still essentially monoliths. Departments may try to identify applications where microservices could be used to improve performance. In these cases, the application should be incrementally broken down into smaller deployable components.

A container and microservices based architecture used consistently across on-premises, private, and public cloud environments provides the ability to seamlessly and securely run workloads across any cloud platform while using a vendor's cloud services.