Technology Architecture

The technology architecture defines the methodology, principles, designs and guidelines for implementation of IT infrastructure for the Government of Bangladesh. It includes all activities to design and implement better technology architecture for digital Bangladesh and provides easy and seamless access to ICT Infrastructure for the ministries to operate on.

Whole of Government: The ICT for Government of Bangladesh

The Bangladesh government is working to achieve Digital Bangladesh Vision 2021 by establishing the seventh five-year plan (2016 – 2020) and the national ICT policy 2015. The technology architecture needs to be defined in a manner that addresses all the challenges of the Government in helping citizens, business and other stakeholders benefit from the digital revolution. Consolidation, resilience and adaptability are the key themes that would drive the design of the ICT Infrastructure

Technology Architecture Principles

The principles listed below are key guidelines for the design, Implementation of IT infrastructure for hosting of applications and hardware computing across the Government of Bangladesh.

These principles are listed below:

- ✓ **TP1 – Technology Independent Architecture**
- ✓ **TP2 – Resilient Architecture**
- ✓ **TP3 – Digital Security**
- ✓ **TP4 – Optimized Hardware**

Name	TP1: Technology Independent Architecture
Description	Technology Architectures are developed in a technology-neutral manner so as to avoid captivity to a specific product or implementation method
Scope	Government hosted ICT Infrastructure.
Implementation Steps	• Industry standards, open architectures and the products/solutions that use them need to be identified. Where conflicts exist between organization and open standards, a cautious approach must be taken to avoid being locked into vendor-centric solutions.
Benefit	• Open, vendor-neutral systems provide flexibility and consistency that will allow government to respond more quickly in an environment of changing business requirements. • Minimizes vendor dependency. • Reduces migration complexity and allows greater flexibility in product replacement. Protects the enterprise against unexpected changes in vendor strategies and capabilities.

Name	TP2: Resilient Architecture

Description	Infrastructure will be selected and implemented with appropriate emphasis on fault-tolerance, stability, and recoverability to ensure the ongoing capability to support ministry applications
Scope	Government hosted ICT Infrastructure.
Implementation Steps	• Infrastructure need to be categorized/ prioritized according to business recovery needs following Continuum of Government guidelines. • Product/ solution maturity should be taken into consideration for implementation of system. • Disaster recovery policies and standards need to be developed.
Benefit	• Minimize infrastructure and application downtime • Facilitates organized disaster recovery capability. • Protects investment in operational data. • Application data will be secured.

Name	TP3: Digital Security
Description	All security requirements should be implemented for IT infrastructure, so that the features, functionality and data will be protected.
Scope	Government hosted ICT Infrastructure.
Implementation Steps	• Security policies, standards, and best practices need to be identified and published • Compliance to security policies, standards, and best practices needs to be monitored.
Benefit	• Provides protection and appropriately controlled access to information • Helps to ensure integrity of data • Enhances public trust • Ensures privacy of data.

Name	TP4: Optimized Infrastructure
Description	All IT system must follow the principle of re-use first then buy, meaning the infrastructure must be shared and re-used by newly developed systems before planning for any procurement
Scope	Government hosted ICT Infrastructure.
Implementation Steps	• All infrastructure listing and mapping with applications • Infrastructure utilization reporting • New deployment scalability requirement submission • Re-use use case and approval

| Benefit | • Reduce end user operation costs
• Reduce service desk problems
• Reduce security breach and impacts
• Reduce data loss and recovery cost.
• Improves in deployment of new application
• Reduce unplanned downtime. |

Future State Technology Architecture

Considering the above principles and the overall vision of integrated digital Government, the future state Technology Architecture has been designed.
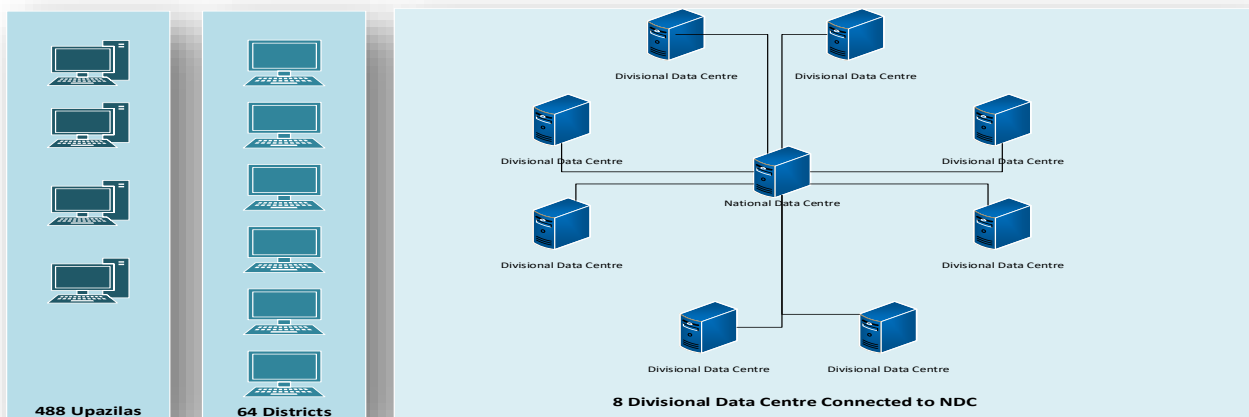
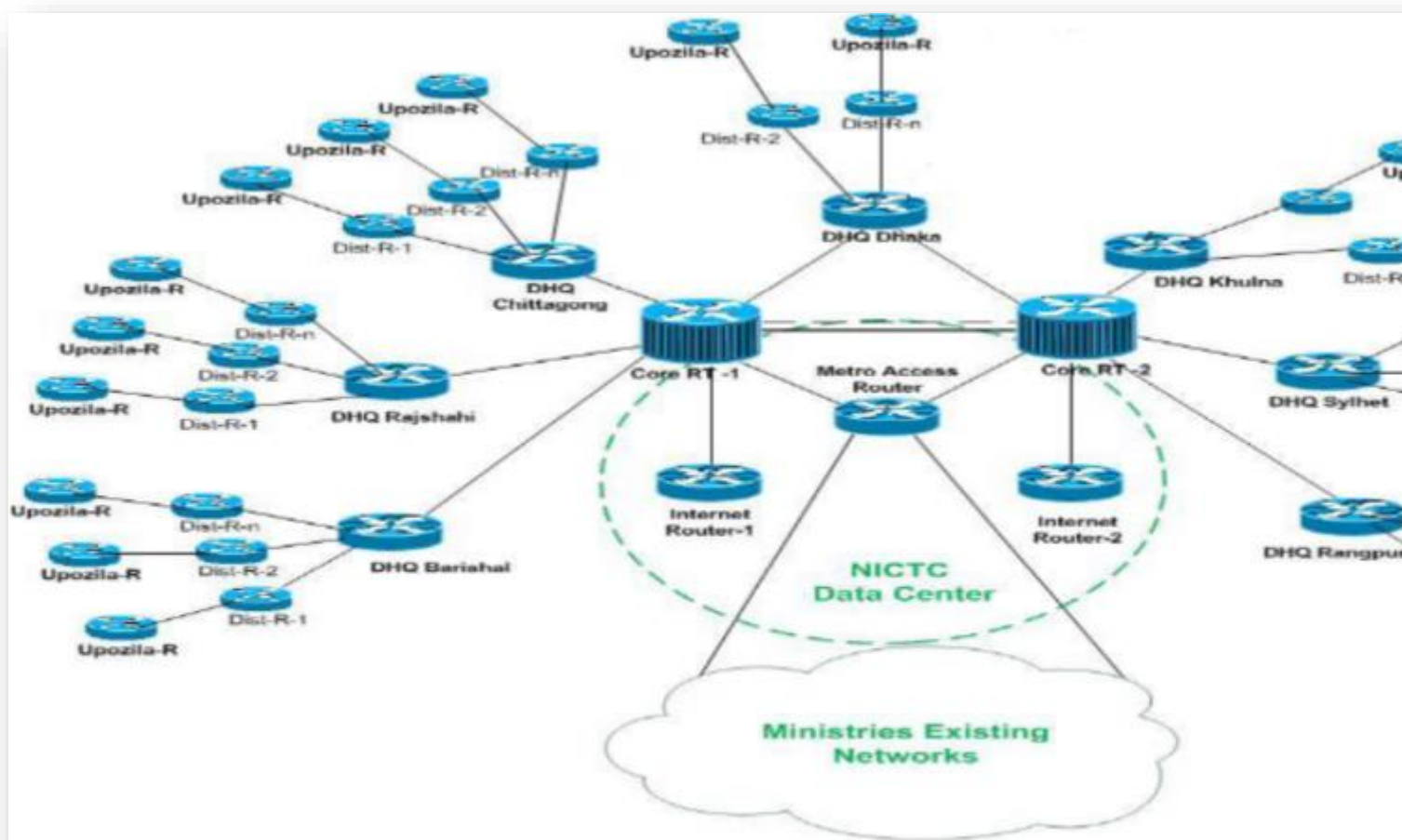Key features of the derived Technology Architecture are:

- ✓ **Scalability to support growth:**
  Based on projected annual growth and scalability measures to ensure ease of expansion and change as per the requirement.

- ✓ **Emerging Technology Ready:**
  The technology architecture is future ready and compatible to new technologies, the new protocols and security requirement.

- ✓ **Secured**
  The design has taken into consideration the unique security requirements to ensure adaptability to changing technology security needs

- ✓ **Cloud Integration**
  The Data Centre must be flexible enough to integrate with the cloud services that is a must for the new era

- ✓ **Resilience**
  The design has taken consideration of making the infrastructure highly resilient yet in the most cost optimized manner
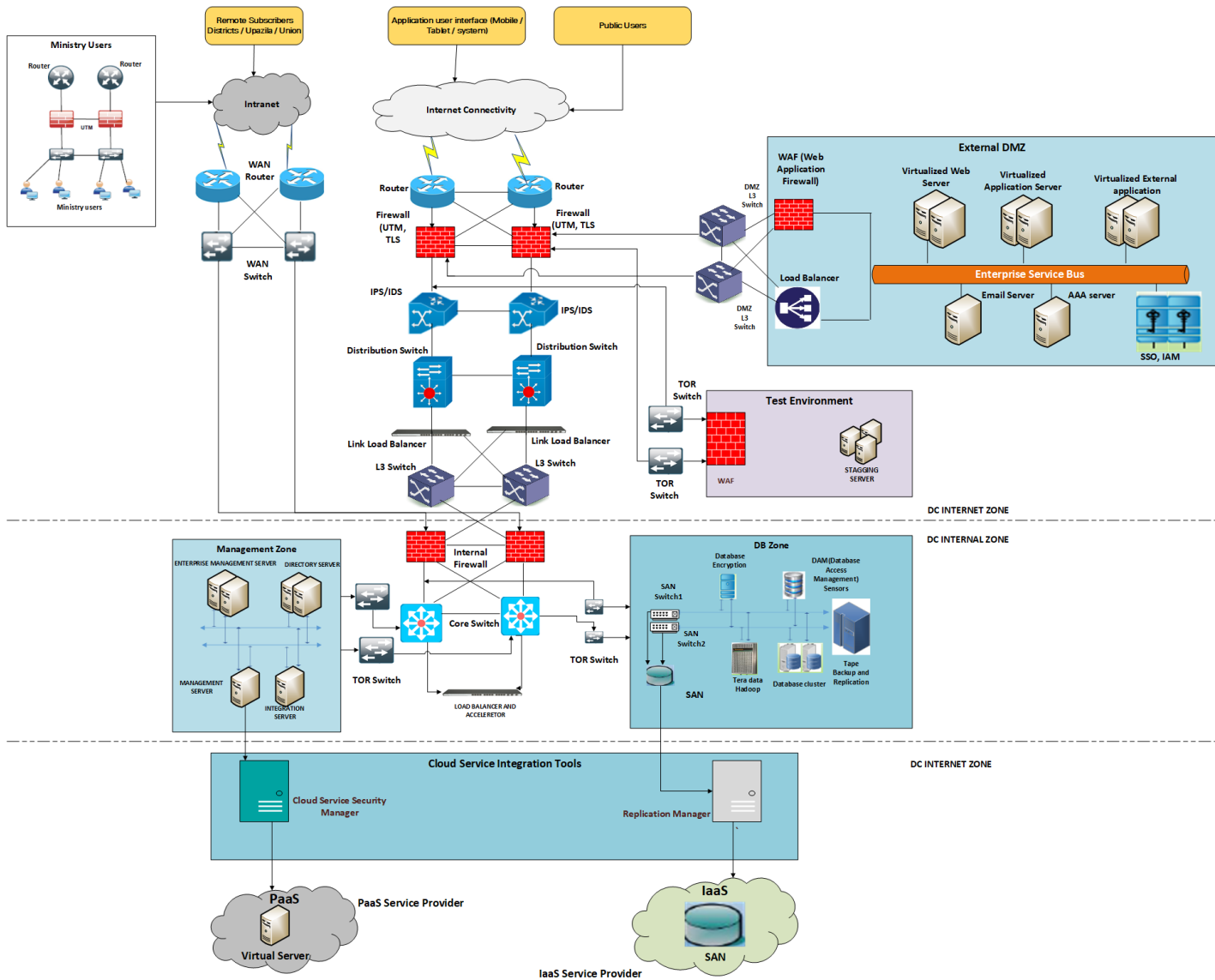
Deployment Architecture - The Future State Data Centre Architecture has been described below. The deployment Architecture has been designed taking into consideration all the above features

Content Delivery Network and Network Topology
The Future State Network Architecture is much derived from the plans of Info Sarkar – III, below is a picturesque description of the same

Disaster Recovery Switching

On premises – National Data centre

Firewall		TLS/VPN
IPS/IDS		Two Factor Authentication
		Load Balancer

APPLICATION FRONT END

| Firewall | | |
| IPS/IDS | | Load Balancer |

Application Portfolio

Machine Critical Applications

Business Critical Applications

Other Applications

Non-Critical Database

DATABASE

DATABASE

DATABASE

DRaaS – Cloud provider

Firewall		TLS/VPN
IPS/IDS		Two Factor Authentication
		Load Balancer

APPLICATION FRONT END

| Firewall | | |
| IPS/IDS | | Load Balancer |

Application Portfolio

Machine Critical Applications

Non-Critical Database

DATABASE

DATABASE

DATABASE

Replication at Regular Intervals

Data Back up service

One Time Configuration setup

DRaaS – Machine Critical Application