COIT13236 – Cyber Security Project

**KN University Network Design**

1. **Cloud Integration Plan**

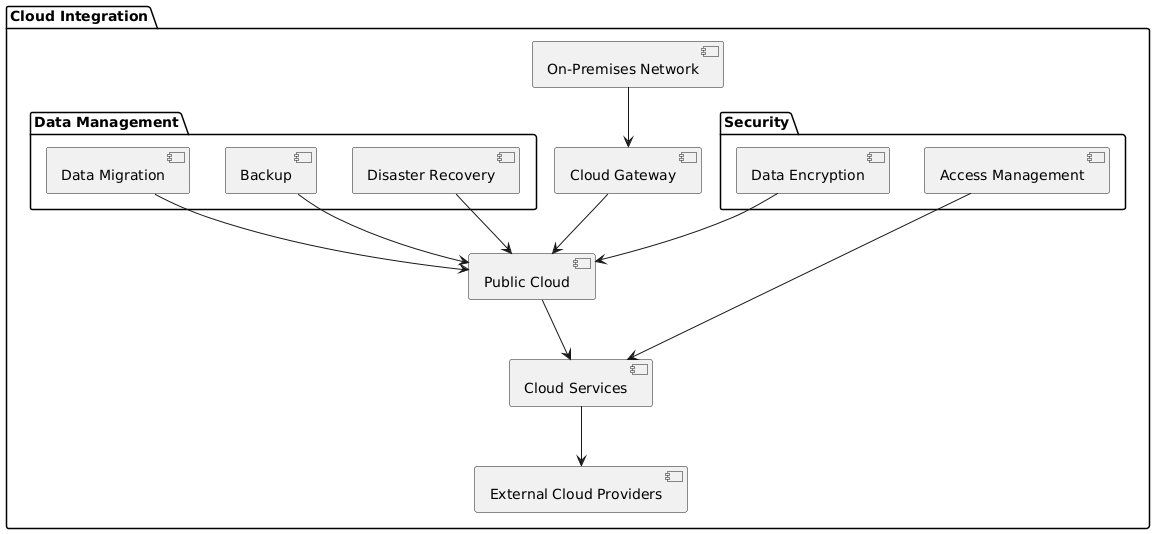
Group 02

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** | **Student ID** |
| Krishan Himesh Abeyrathne | System Administrator | 12217274 |
| Narayan Parajuli | System Security Analyst | 12144248 |

# Cloud Integration Plan

**Cloud Integration Plan:**

A Cloud Integration Plan outlines how an organization will interface its current IT systems and applications with cloud services. The objective is to guarantee consistent communication and interoperability between on-premises frameworks and cloud-based assets, upgrading activities, versatility, and adaptability.



**Fig: Cloud Integration Plan**

With a focus on data management and security to improve the university's Network, the diagram outlines a preferred cloud integration method for KN University. The cloud is used for storing university data to improve access and scalability. Frequent cloud backups guarantee that data may be quickly restored, and a cloud-based disaster recovery strategy continues to function in the event of an emergency. To safeguard sensitive data, university data is encrypted before being stored in the cloud. To guarantee that only authorised individuals can access data and cloud services, strict access controls are in place. The public cloud and the university's on-campus network are connected securely, allowing for seamless data integration and transfer. The primary platform for managing and storing data is the public cloud, with supplementary cloud services available for further capability. By forming partnerships with outside cloud providers, the university gains greater access to specialized resources and capabilities.

KN University seeks to create a more scalable, secure, and resilient IT environment that can accommodate the expanding requirements of its staff, faculty, and students by putting this cloud integration concept into practice. This project will improve data accessibility, expedite disaster recovery, and guarantee that confidential data is safeguarded in accordance with industry best practices for cloud security.

**Components:**

**Cloud Service Providers:**

There are different cloud service providers in the market i.e. Azure Cloud, IBM Cloud, Google Cloud etc. For this project, Azure Cloud will be used for the demonstration as well as for other purposes.

**Cloud Integration Strategy:**

Hybrid Cloud Model: The Hybrid Cloud Model incorporates on-premises framework with public cloud services to establish a unified computing environment.

Cloud Gateway: A Cloud Gateway is an innovation or administration that works with secure availability between an association's on-premises network and public cloud services. It acts as an entry point that manages and secures the data.

**Information and Application Migration:**

Information Migration: Move information to cloud storage with insignificant margin time.

Application Migration: Move applications to the cloud while guaranteeing similarity and execution.

**Security and Consistence:**

Information Encryption: Encode information stored and sent to the cloud.

Access Control: Carry out IAM (Identity and Access Management) strategies for cloud assets.

**Backup and Redundancy:**

Cloud Backup: Routinely back up basic information to cloud storage i.e. Microsoft Azure Cloud Backup.

Disaster Recovery: Use cloud administrations for disaster recovery to guarantee business coherence.

# References

Gartner, Inc. (2021) Hype Cycle for Cloud Computing. Stamford: Gartner. Available at: https://www.gartner.com/en/doc/4482592/hype-cycle-for-cloud-computing (Accessed: 1 August 2024).

Cisco (2024) Cloud Gateways and Integration. Available at: https://www.cisco.com/c/en/us/solutions/collateral/cloud/what-is-a-cloud-gateway.html (Accessed: 1 August 2024).