Unit 10: Practical Applications and Issues in DR Implementations

Seminar Title: DR Solutions Design and Review

1. Vendor Lock-In Issues and Mitigation Strategies

Vendor lock-in arises when an organization becomes overly dependent on a specific cloud or DR (Disaster Recovery) service provider, making migration to alternative platforms difficult, costly, or disruptive(Weldemicheal,2023).

(i) Proprietary technologies and APIs that hinder data portability and interoperability between cloud providers.

(ii) Inconsistent service level agreements (SLAs) and lack of standardized performance metrics across providers.

(iii) Data format incompatibility, which complicates backup restoration or migration.

(iv) High switching costs, both technical and contractual, when moving DR services to a new vendor.

To mitigate these issues:

- ❖ Adopt open standards and APIs such as the Open Virtualization Format (OVF) and Cloud Data Management Interface (CDMI).
- ❖ Implement multi-cloud strategies to avoid dependency on a single vendor.
- ❖ Negotiate flexible SLAs that include data export guarantees and migration support.
- ❖ Use containerization (e.g., Docker, Kubernetes) to ensure application portability across cloud environments.

2. Security Concerns with the Modern Cloud and Mitigation Measures

Morrow et al. (2021) highlight that while cloud computing offers scalability and reliability for DRaaS (Disaster Recovery as a Service), it introduces significant security challenges, including and not limited to;

(i) Data breaches and unauthorized access, especially when DR sites are hosted in shared environments.

(ii) Insecure APIs, which can be exploited to gain unauthorized system control.

(iii) Loss of visibility and control, since data and recovery processes are managed by third parties.

(iv) Compliance and data sovereignty risks, especially in cross-border DR implementations.

To mitigate these concerns:

(i) Encrypt data in transit and at rest, using strong cryptographic standards (e.g., AES-256).

(ii) Apply identity and access management (IAM) frameworks with multi-factor authentication (MFA).

(iii) Conduct regular third-party audits and penetration testing to verify cloud provider security.

(iv) Implement zero-trust security models, ensuring that every access request is authenticated and authorized(Onwuegbuzie and Alabi,2025).

(v) Use region-specific DRaaS options to comply with local data protection laws (e.g., GDPR)

References

Weldemicheal, T., 2023. Vendor lock-in and its impact on cloud computing migration.

Onwuegbuzie, I.U. and Alabi, O.A., 2025. A Review of Authentication and Authorization Mechanisms in Zero Trust Architecture: Evolution and Efficiency. *Tech-Sphere Journal for Pure and Applied Sciences*, *2*(1).