Weekly Reflections on Key Topics

Reflecting on the module's trajectory, I have selected five pivotal topics that profoundly shaped my understanding of cloud computing's role in modern IT practices.

1. Understanding Cloud Architecture and Frameworks (Unit 2)

Unit 2, "Understanding Cloud Architecture and Implementing Different Frameworks," established the theoretical foundation for designing and managing cloud systems strategically. It moved beyond basic definitions of cloud computing to explore structured methodologies that align technological solutions with business objectives. I found the introduction of TOGAF (The Open Group Architecture Framework) particularly insightful, as it provides a systematic approach to aligning IT architecture with enterprise strategy. The study by Anggraini et al. (2019) demonstrated how TOGAF can be integrated with the ROCCA cloud adoption model to define baseline requirements and ensure that technology initiatives remain business-driven.

The unit also addressed the Software Development Life Cycle (SDLC) in a cloud context, where agility and automation replace linear processes. The concept of Infrastructure as Code (IaC)—automating the provisioning and management of infrastructure—was especially transformative. It illustrated how architecture and deployment can evolve from manual tasks into code-driven, repeatable operations.

Reflecting on this unit, I realised that the success of cloud adoption depends less on specific technologies and more on strategic planning. Enterprise Architecture (EA) frameworks such as TOGAF and ROCCA ensure that cloud initiatives are coherent, adaptable, and measurable (Abd-Elvahab et al., 2023). In essence, technology provides capability, but strategy defines purpose. This understanding shifted my mindset from focusing solely on tools to prioritising governance, value alignment, and scalability in every architectural decision.

References:

Anggraini, N., Binariswanto & Legowo, N. (2019) 'Cloud Computing Adoption Strategic Planning Using ROCCA and TOGAF 9.2: A Study in Government Agency', *Procedia Computer Science*, 161, pp. 1316–1324.

Abd-Elvahab, A. M., Mohamed, A. G. & Shaaban, E. M. (2023) 'Microservices-driven enterprise architecture model for infrastructure optimisation', *Future Business Journal*, 9(1), p. 90.

2. Cloud-Native Technologies and Hybrid/Multi-Cloud Solutions (Units 5 & 6)

These units deepened my understanding of the balance between innovation, agility, and complexity in cloud-native and hybrid models. The study of serverless computing (Ni et al., 2024) revealed both its operational elegance and security challenges. By quantifying security risks through Attack–Defense Trees, the authors showed that even when individual vulnerabilities are mitigated, cumulative exposure remains significant. This insight reshaped my perception of the shared responsibility model, which becomes increasingly intricate as abstraction levels rise.

Simultaneously, exploring microservices architectures (Abd-Elvahab et al., 2023) demonstrated how modular systems enhance scalability and agility but introduce challenges in integration, monitoring, and governance. The reflection on hybrid and multi-cloud models, exemplified in Anggraini et al. (2019), reinforced that while these architectures optimise control and compliance, they also expand the attack surface. Critically, I learned that agility without robust governance is unsustainable. The NIST Cybersecurity Framework 2.0 (NIST, 2024) emerged as a vital tool—providing a common language and measurable outcomes to manage risk across heterogeneous environments. Reflecting on my own professional practice, this unit reinforced the importance of embedding security and architectural discipline as core design principles rather than reactive measures.

References:

Abd-Elvahab, A. M., Mohamed, A. G. & Shaaban, E. M. (2023) 'MicroServices-driven enterprise architecture model for infrastructure optimization', *Future Business Journal*, 9(1), p. 90.

Anggraini, N., Binariswanto & Legowo, N. (2019) 'Cloud Computing Adoption Strategic Planning Using ROCCA and TOGAF 9.2: A Study in Government Agency', *Procedia Computer Science*, 161, pp. 1316–1324.

National Institute of Standards and Technology (NIST) (2024) *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

Ni, K., Mondal, S. K., Kabir, H. M. D., Tan, T. & Dai, H. N. (2024) 'Toward security quantification of serverless computing', *Journal of Cloud Computing*, 13(1), p. 140.

2. Cloud Security and Compliance (Unit 7)

This unit challenged me to rethink cloud security as a continuous, integrated discipline rather than a set of reactive measures. The works of Baldini et al. (2016) and Gundu et al. (2020) highlighted that the move towards serverless and multi-cloud architectures has redefined the traditional security perimeter.

Firstly, the shared responsibility model has evolved. In serverless environments, the cloud provider handles operational layers such as runtime and patching, but clients retain accountability for identity, configuration, and application logic (Baldini et al., 2016). This underscores the need for "shift-left" security—embedding protection mechanisms at the earliest stages of development.

Secondly, the multi-cloud paradigm introduces an expanded attack surface. Gundu et al. (2020) noted that managing consistent security policies across providers is complex, often leading to configuration drift and increased data transit risks. Reflecting on this, I understood the criticality of centralised visibility and governance to meet compliance obligations such as ISO/IEC 27001 and GDPR.

Finally, I learned that emerging architectural responses—such as multi-cloud exchanges and direct interconnects—can enhance performance and reduce exposure but

simultaneously centralise risk. This duality reminded me that every optimisation introduces trade-offs. Overall, Unit 7 reinforced that effective cloud security demands proactive governance, automation, and a culture of shared accountability across teams.

References:
Baldini, I. et al. (2016) 'Serverless Computing: Current Trends and Open Problems', *Proceedings of the International Conference on Mobile Software Engineering and Systems (MOBILESoft '16)*, ACM.
Gundu, S. R., Panem, C. A. & Thimmapuram, A. (2020) 'Hybrid IT and Multi Cloud – An Emerging Trend and Improved Performance in Cloud Computing', *SN Computer Science*, 1(256). https://doi.org/10.1007/s42979-020-00277-x

3. Disaster Recovery and Cloud Migration (Units 8 & 9)

These units emphasised the strategic interdependence between cloud migration and disaster recovery (DR). Through the readings by Carson and Rodrick (2024), I learned that modern DR strategies are inseparable from the migration process itself. Cloud platforms enable Disaster Recovery as a Service (DRaaS), allowing organisations to maintain cost-efficient, scalable standby environments that meet strict Recovery Time and Point Objectives (RTO/RPO).
A key takeaway for me was the shift from capital-intensive redundancy to elastic resilience. However, migration success depends on understanding the shared responsibility model across IaaS, PaaS, and SaaS. While providers guarantee infrastructure resilience, customers must architect and test their own recovery processes. This reinforced my view that DR planning is not optional but a strategic design imperative.

Security emerged as another crucial dimension. The use of direct interconnects such as Azure ExpressRoute ensures secure, high-bandwidth replication channels—mitigating risks from public internet exposure. Yet, as Dunbar (2024) warned, the extensive use of proprietary cloud services introduces vendor lock-in, complicating future migrations or multi-cloud DR.

Reflectively, I realised that flexibility and resilience must coexist. A well-architected DR strategy is not just a safety net—it is an operational capability that sustains business continuity and customer trust in the digital era.

References:
Carson, R. & Rodrick, M. (2024). *Business Continuity and Disaster Recovery*. Packt Publishing. (Ch. 2 & 3).
Dunbar, W. (2024) 'Vendor-Locked DevOps Strategies', *Communications of the ACM*.
Zheng, Y. et al. (2024) 'Optimization model for vehicular network data queries in edge environments', *Journal of Cloud Computing*, 13, pp. 1–15.

4. AI and Cloud Computing (Unit 11)

The convergence of Artificial Intelligence (AI) and cloud computing emerged as one of the most transformative themes of the module. While the lectures emphasised technical integration—AI leveraging cloud scalability and cloud leveraging AI for optimisation—the paper by Carugati (2023) expanded my understanding by situating this relationship within the broader digital-economy power dynamic.

The interdependence between cloud hyperscalers and AI developers represents a mutual dependence that drives innovation and competition. Cloud platforms provide the computational infrastructure necessary for training large-scale models, while AI workloads generate massive demand for cloud resources, reinforcing growth for providers. As Carugati (2023) notes, this creates a self-reinforcing cycle in which technological and economic forces are intertwined.

I found it particularly enlightening to explore how this dynamic spans all service layers: at the IaaS level, hyperscalers differentiate through proprietary hardware such as TPUs and Trainium; at PaaS, platforms like Azure OpenAI Service curate AI ecosystems; and at SaaS, AI integration transforms productivity suites such as Microsoft 365 Copilot.

However, this symbiosis also poses risks—vendor lock-in, market concentration, and hardware bottlenecks—which threaten innovation and fair competition. Reflecting on this, I now view cloud–AI integration not only as a technical achievement but as a strategic and ethical frontier. As regulatory frameworks like the EU Digital Markets Act (DMA) emerge, the industry must balance progress with fairness and transparency.

References:

Carugati, C. (2023) 'The competitive relationship between cloud computing and generative AI', *Bruegel Working Paper 19/2023*.
Alshareef, H. N. (2023) 'Current development, challenges, and future trends in cloud computing: A survey', *International Journal of Advanced Computer Science and Applications*, 14(3).