Title	Cloud Security Architecting
Long Title	Cloud Security Architecting
Credits	**5**
NFQ Level	**Expert**
Module Author	**Anila Mjeda**

Module Description:

In this module, students will explore the world of cloud security and the critical importance it holds in today's digital landscape. Students will gain an understanding of approaches to designing and implementing rigorous security strategies, complemented by monitoring and detection methodologies that provide real-time insights and proactive responses. Students will gain an understanding of Identity and Access Management (IAM) best practices, including centralized management of authentication, authorisation, roles and policies, logging and auditing. Students will be equipped with necessary practical expertise to protect varied cloud resources such as storage services (Object, Block, File, Queue), database platforms, compute offerings (Virtual Machines, serverless functions, containers), and networking configurations (Virtual Networks, Subnets, Firewalls, VPNs). Students will develop a holistic understanding of the challenges and intricacies of securing multi-faceted cloud-hosted environments and an awareness of the encompassing compliance and regulatory landscapes. This module was developed under the Cyber Skills HCI Pillar 3 Project. Please refer to consortium agreement for ownership

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1 Examine the foundational principles of cloud security, distinguishing it from traditional IT security and the nuances of various cloud architectures and service models

LO2 Recognize the role of identity & access control in cloud environments as the security perimeter in the cloud, and design strategies for effective identity management and access controls

LO3 Evaluate and secure the components that comprise cloud-hosted solutions ensuring the confidentiality, integrity and availability of digital assets.

LO4 Design and implement an overarching Cloud Security Posture Management (CSPM) strategy tailored to specific business needs and cloud architectures

LO5 Examine the implications and complexities of compliance and regulatory standards in cloud security, adapting strategies to ensure adherence

Indicative Content

Evolution of Cloud Security:
Origins and rise of cloud platforms & responsibility shifts. Major cloud providers. Cloud architectures: Public, Private, and Hybrid. Cloud service models: IaaS, PaaS, and SaaS. Threat vectors specific to cloud environments. Importance of cloud security & distinction from traditional IT security. Strategic alignment of security controls with business objectives. Cloud security best practices.

Cloud Identity and Access Management:
History of identity management. The application of the principle of least privilege in the cloud. User and role management in cloud platforms. Access strategies for cloud services. Modern authentication protocols such as OIDC, OAUTH,SAML/WSFED. Single Sign-On (SSO) and Multi-Factor Authentication (MFA) in the cloud. The different levels of MFA security, from gold standard phishing-resistant MFA (FIDO) to less secure Time-Based One-Time Password (TOTP) and SMS/Email MFA. Service and resource-based policies.

Data Security, Integrity, and Storage:
CIA triad, Zero trust. Data residency and sovereignty. Cloud storage security. Secure key and secret management.

Database Platforms & Security:
Database offerings, encryption types & methods, data masking, auditing, threat detection, best practices.

Compute & Application Security:
Virtual Machines, serverless functions, containers, app hosting, API hosting, threat detection, best practices.

Network Security:
Virtual networks, network topology, subnets, peering, firewalls, VPNs, DDoS, monitoring, Multi-Cloud & Hybrid Cloud security.

Cloud Security Posture Management (CSPM):
CSPM strategies suited to diverse cloud architectures; real-time monitoring and threat detection systems; incident response integration; adoption of "Shift Left" security practices to integrate security earlier in the development lifecycle; application of Continuous Security methodologies; intertwining of these approaches with scalable security policies embedded within CI/CD pipelines using tools like Terraform/CloudFormation while centralizing security policy management.

Compliance and Regulatory Frameworks:
Interpreting and adhering to compliance and regulatory standards including GDPR, HIPAA, PCI DSS & SOC2; ensuring cloud operation compliance; managing data sovereignty across multiple global jurisdictions within Azure, AWS, and other cloud services; tailoring security frameworks to specific organizational needs; staying up to date with changes in cloud security regulations and best practices. Compliance assessments & audits.

Security Management and Automation:

Examination of security management tools; Infrastructure as Code (IaC) for security consistency (Security Policy as Code); Automated Threat Detection and incident response mechanisms; incorporation of security within DevSecOps workflows; securing CI/CD pipelines; understanding compliance intersections with security automation; keeping pace with emerging trends in the automation of cloud security.

Course Work

Assessment Type	Assessment Description	Outcome Addressed	% of Total	Assessment Date
Project	The student will be expected to critically analyse cloud security subjects in writing (essay format) and undertake a security analysis of a provided hypothetical cloud infrastructure case study. Identify potential weaknesses and vulnerabilities, then propose remedial actions and pertinent security best practices	1,2,3	40	Week 7
Project	The student will be expected to develop a comprehensive cloud security strategy based on the requirements from a hypothetical organisation embarking on a cloud migration journey. This proposal should address areas such as Identity & Access Control, permissions, storage, compute, database security, networking, proactive monitoring, reporting mechanisms, and adherence to compliance standards.	2,3,4,5	60	Sem End

No End of Module Formal Exam

Assessment Breakdown

	%
Coursework	100

Re-Assessment Requirement

Coursework Only

This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	Workload Description	Hours	Frequency	Average Weekly Learner Workload
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes	2	Every Week	2.00
Lab	Lab assignments based on preceding lecture material to provide practical experience working with the major cloud-hosted resource type. Student-provided AWS and Azure account, using free tier services	2	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent learning by the student	3	Every Week	3.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		4.00

Workload – Part Time

Workload Type	Workload Description	Hours	Frequency	Average Weekly Learner Workload
Lecture	Lecture delivering theory underpinning learning outcomes.	2	Every Week	2.00
Lab	Lab to support learning outcomes.	2	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent Study.	3	Every Week	3.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		4.00

Recommended Book Resources

Aditya K. Sood. (2021), Empirical Cloud Security, Mercury Learning and Information, p.450, [ISBN: 978-1683926856].

Supplementary Book Resources:

MIHIR. SHAH. (2023), Cloud Native Software Security Handbook, Packt Publishing, p.372, [ISBN: 978-1837636983]. Tim Mather, Subra Kumaraswamy,Shahed Latif. (2009), Cloud Security and Privacy, "O'Reilly Media, Inc.", p.338, [ISBN: 9781449379513].

Supplementary Article/Paper Resources
Singh, Ashish, and Kakali Chatterjee. (2017), Cloud security issues and challenges: A survey, Journal of Network and Computer Applications, 79.

Other Resources
Website, Microsoft. Microsoft Security Reference Architectures, https://learn.microsoft.com/en-us/securi ty/cybersecurity-reference-architecture/mcra

Website, Amazon. Amazon Security Reference Architecture, https://docs.aws.amazon.com/prescriptive -guidance/latest/security-reference-architecture

Website, Microsoft. Azure Architecture Center, Microsoft, https://learn.microsoft.com/en-us/azure/architecture

Website, Amazon. AWS Architecture Center, Amazon, https://aws.amazon.com/architecture

Website, NIST. NIST Cybersecurity Framework, https://www.nist.gov/cyberframework

Website, ISO/IEC. ISO/IEC 27017 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud Page 3 of 3

Website, ISO/IEC. ISO/IEC 27017 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services. International Organization for Standardization (ISO), https://www.iso.org/standard/43757.html

Website, CIS. CIS Critical Security Controls, https://www.cisecurity.org/controls

Website, Open ID Foundation. OpenID Specifications,
https://openid.net/developers/specs/