Unit 28:　　　　　Cloud Computing

Unit code	**K/618/7442**
Unit level	**5**
Credit value	**15**

This unit is aligned to the Microsoft Azure Fundamentals Certification. See section 3.1.4 for guidance on claiming certification.

Introduction

Cloud computing has revolutionised the way IT services are delivered and has become an important part of the computing sector. Cloud computing is internet-hosted computing, which means that it uses the internet to deliver data and other IT services such as storage, printing, server facilities. In other words, end users and organisations no longer need to have their own extensive network environment on the premises but can get the same services provided virtually over the internet.

The fundamental difference between traditional networking and cloud computing is that the technical details of the system are hidden from the end user. This means the networking infrastructure does not have to be on the premises as it would be hosted off-site in the cloud. However, the end user can use the services without the fear of technical difficulties or disasters as they would be managed by the cloud service provider. Cloud computing is a natural evolution of networking and is adapting modern network-oriented technologies such as virtualisation, service-oriented architecture, utility computing and ubiquitous computing.

This unit is designed to develop understanding of the fundamental concept of cloud computing, cloud segments and cloud deployment models and the need for cloud computing. Students will gain appreciation of issues associated with managing cloud service architecture and develop a critical awareness of cloud-computing-based projects. Topics included in the unit are the paradigms of networking, fundamentals of cloud computing, cloud computing architecture, deployment models, service models, security, technological drivers and cloud service providers.

On successful completion of this unit, students will understand the concept, architecture and services of cloud computing. They will have hands-on experience of configuring a cloud service from major providers such as ECM, Google, Amazon, Microsoft and IBM and of implementing a simple cloud platform using open source software with an appropriate networking platform. As a result, students will develop skills such as communication literacy, critical thinking, analysis, reasoning and interpretation, which are crucial for gaining employment and developing academic competence.

Learning Outcomes

By the end of this unit students will be able to:

LO1   Demonstrate an understanding of the fundamentals of cloud computing and its architectures

LO2   Evaluate the deployment models, service models and technological drivers of cloud computing and validate their use

LO3   Develop cloud computing solutions using service provider frameworks and open source tools

LO4   Analyse the technical challenges for cloud applications and assess their risks.

Essential Content

LO1 Demonstrate an understanding of the fundamentals of cloud computing and its architectures

Networking paradigm:

Peer-to-peer computing, client-server computing, distributed computing, cluster computing, high-performance computing, parallel computing, grid computing.

Cloud computing fundamentals:

Definition and history of cloud computing, principles of cloud computing, cloud ecosystem, cloud architecture and infrastructure, virtualisation, network connectivity, managing the cloud, application migration to the cloud.

Explore storage virtualisation, including storage architecture for virtualisation; physical disk types and related techniques; difference between centralised and distributed storage, virtualised and non-virtualised storage features, difference between capex and opex, methods for planning and managing costs and Service Level Agreements (SLAs).

LO2 Evaluate the deployment models, service models and technological drivers of cloud computing and validate their use

Deployment models:

Private cloud, public cloud, community cloud, hybrid cloud.

Service models:

Infrastructure as a service (IaaS) a form of cloud computing providing virtualised computing resources over the internet.

Platform as a service (PaaS), providing a complete development and deployment environment.

Software as a service (SaaS), offering users access to a vendor's cloud-based software.

Analytics as a service (AaaS), offering provision of analytics software and operations through web-delivered technologies.

Cloud computing use cases.

Technological drivers:

Service-oriented Architecture (SOA), virtualisation and cloud computing, multicore technology, memory and storage technology, networking technology, Web 2.0, & 3.0, software process models for cloud, programming models, pervasive computing, application environment.

Explore architecture and components used for virtualisation, and traffic flows between VMs.

LO3 Develop cloud computing solutions using service provider frameworks and open source tools

Cloud Service Providers (CSPs):

Explore the features of different cloud service providers and virtualisation software, e.g. Microsoft, EMC, Google, Amazon Web Services, IBM, VMware, KVM, FusionCompute.

CSP architectural components:

Explain architectural components using service provider terminology, e.g. regions, zones, resource groups, subscriptions, management groups.

CSP core resources, core solutions and management tools:

Compute, networking and storage.

Describe service provider's core solutions, e.g. IoT solutions, Big Data Analytics, artificial intelligence (AI) and machine learning, DevOps.

Describe CSP management tools, e.g. Azure Portal, AWS Management Console, Command Line Interface (CLI), Cloud Shell, and application monitoring.

CSP cost management and service level agreements (SLAs):

Factors affecting cost, pricing calculators, reducing costs, forecasting costs.

Purpose of SLAs and factors affecting them.

Open source:

Open source tools for IaaS, open source tools for PaaS, open source tools for SaaS, distributed computing tools, e.g. Cassandra, Hadoop, MongoDB, NGrid, Ganglia.

LO4 Analyse the technical challenges for cloud applications and assess their risks

Security aspects:

Data security, virtualisation, network security, alerts, resource hygiene, defence in depth.

Identity, including authentication and authorisation.

Governance, including role-based access control, policy and templates.

Privacy and compliance.

Platform-related security:

SaaS Security issues, PaaS Security Issues, IaaS Security Issues, Audit and Compliance.

CSP security features:

Describe CSP security features, e.g. Azure Security Centre, Key Vault, AWS GuardDuty, Azure Sentinel, Dedicated Hosts, Network Security Groups (NSG), DDoS protection.

Learning Outcomes and Assessment Criteria

Pass	Merit	Distinction
LO1 Demonstrate an understanding of the fundamentals of cloud computing and its architectures		**LO1 and LO2**
P1 Analyse the evolution and fundamental concepts of cloud computing. **P2** Design an appropriate architectural cloud computing framework for a given scenario.	**M1** Discuss why an organisation should migrate to a cloud computing solution.	**D1** Justify the tools chosen to realise a cloud computing solution.
LO2 Evaluate the deployment models, service models and technological drivers of cloud computing and validate their use		
P3 Define an appropriate deployment model for a given scenario. **P4** Compare the service models for choosing an adequate model for a given scenario.	**M2** Demonstrate selected deployment models with real-world examples.	

Pass	Merit	Distinction
LO3 Develop cloud computing solutions using service provider frameworks and open source tools		
P5 Configure a cloud computing platform with a cloud service provider's framework. **P6** Implement a cloud platform using open source tools.	**M3** Discuss the issues and constraints that can be faced during the development process.	**D2** Critically discuss how issues and constraints during the development process can be overcome.
LO4 Analyse the technical challenges for cloud applications and assess their risks		
P7 Analyse the most common problems that arise in a cloud computing platform and discuss appropriate solutions. **P8** Assess the most common security issues in cloud environments.	**M4** Discuss how to overcome security issues when building a secure cloud platform.	**D3** Critically discuss how an organisation should protect its data when migrating to a cloud solution.

Recommended Resources

Textbooks

Chandrasekaran, K. (2015) *Essentials of Cloud Computing*, Chapman and Hall CRC Press.

Erl, T., Puttini, R., Mahmood, Z. (2013) *Cloud Computing: Concepts, Technology & Architecture*. Prentice Hall.

Kapadia, A., Varma, S. and Rajana, K. (2014) *Implementing Cloud Storage with OpenStack*. Packt Publishing.

Patawari, A. (2013) *Getting Started with ownCloud*. Packt Publishing.

Rhoton, J. and De Clercq, J. (2014) *OpenStack Cloud Computing: Architecture*. Recursive Press.

Ying Zhu, S., Hill, R. Travati, M. (Editors) (2016) *Guide to Security Assurance for Cloud Computing*. Springer.

Links

This unit links to the following related unit:

Unit 49: Systems Integration.