Cloud Computing

MUCPD – DSIC - UPV

Deployment and Service Models

Overview

- Recap of fundamentals
- Cloud Service models
- Cloud Deployment models
- Major Cloud providers
- Strategic decision making

Recap

- On demand delivery of computing resources over the internet
- Includes
  - Servers
  - Storage
  - Databases
  - Networking
  - Analytics
  - Intelligence

Recap: key characteristics

- On demand self-service
  - Users can provision resources without human interaction
- Broad Network access
  - Services available via standard mechanisms
- Resource pooling
  - Provider’s resources serve multiple consumers
- Rapid elasticity
  - Resources can be scaled rapidly on demand
- Measured service
  - Resource usage is monitored, controlled and reported

Importance of Service and Deployment models

- Aligning technology with business goals
- Understanding levels of control and responsibility
- Optimizing costs and resources
- Enhancing security and compliance
- Facilitating scalability and flexibility

Cloud Service Models

- Three primary models
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)
- A newer, optional model
  - Function as a Service (FaaS)

IaaS

- Provides virtualized computing resources over internet
- Users manage
  - OS
  - Middleware
  - Runtimes
  - Data

Core components of IaaS

- Compute resources
  - Virtual Machines (VMs)
- Storage solutions
  - Block, Object and file storage
- Networking services
  - Virtual networks, load balancers, IP addresses
- Security features
  - Firewalls, Identity and access management (IAM)

User responsibilities in IaaS

- Operating systems
  - Installation, configuration, updates
- Middleware and runtime environments
  - Dependencies in the application stack
- Applications and data
  - Deployment, management and security

Provider responsibilities in IaaS

- Physical Infrastructure
  - Servers, storage devices, networking hardware, power supply, AC,…
- Virtualization layer
  - Hypervisors, virtual network configurations, storage servers
- Maintenance and Physical security
  - Data center operations, physical security measures

Advantages of IaaS

- Full customization and control
- Scalability and elasticity
- Cost savings
- Rapid provisioning
- Disaster recovery and business continuity

Disadvantages of IaaS

- Potential complexity in management
- Perceived security concerns
- Potential for unpredictable costs
- Potential vendor dependency
- Compliance challenges

PaaS

- Provides platform for…
  - Developing applications
  - Deploying and managing services based on them
- Users’ focus
  - Application development
  - Data management

Core components of PaaS

- Development tools
  - APIs, sometimes IDEs, service models
- Middleware services
  - Application servers, databases, messaging systems
- Runtime environments
  - Support for programming languages and frameworks
- Management services
  - Monitoring, logging, security features

User responsibilities in PaaS

- Application code
  - Writing, testing, and deploying according to the PaaS rules
- Data management
  - Structuring, querying and managing databases, files, …
- Application configuration
  - Setting parameters, tunning performance

Provider responsibilities in PaaS

- Infrastructure management
  - Servers, storage, network, OS maintenance, …
- Middleware and runtime
  - Ensure environments are up to date, depends on PaaS
  - Tradeoff between assurances and lock-in
- Scaling and load balancing
  - Provide a framework for automatic adjustment of resources
- Security and compliance
  - Implement security protocols and compliance standards

Advantages of PaaS

- Simplifies development process
- Accelerates time to market
- Agility in development
- Focus on business logic
- Built-in scalability and high availability

Disadvantages of PaaS

- Limited control over environment in most cases
- Vendor lock-in risks
- Perceived security concerns
- Potential for higher costs
- Compatibility and integration issues

Understanding SaaS

- A SaaS is a SERVICE
  - Stateful!!
  - Provides fully functional software applications over the internet
- Accessed via transparently downloadable/self maintained applications on target devices
  - Web browser pages
  - Apps

Core components of SaaS

- Complete applications
  - Delivered over the internet
- User Interfaces
  - Accessible via web brosers or client applications (even CLI)
- Data management
  - Provider handles storage, backup and recovery
- Security and compliance
  - Managed by provider

User responsibilities in SaaS

- User-specific configurations
  - Customize application settings
- Data input and management
  - Entering, modifying, managing data within the scope of the application
- User management
  - Adding/removing users, setting permissions (when relevant)

Provider responsibilities in SaaS

- Application development and maintenance
  - Transparent to the user
- Infrastructure management
  - Including OS, etc…
- Performance and availability
- Support

Advantages of SaaS

- Ease of use
- Potential cost savings
- Transparent scalability and flexibility
- Automatic updates
- Accessibility

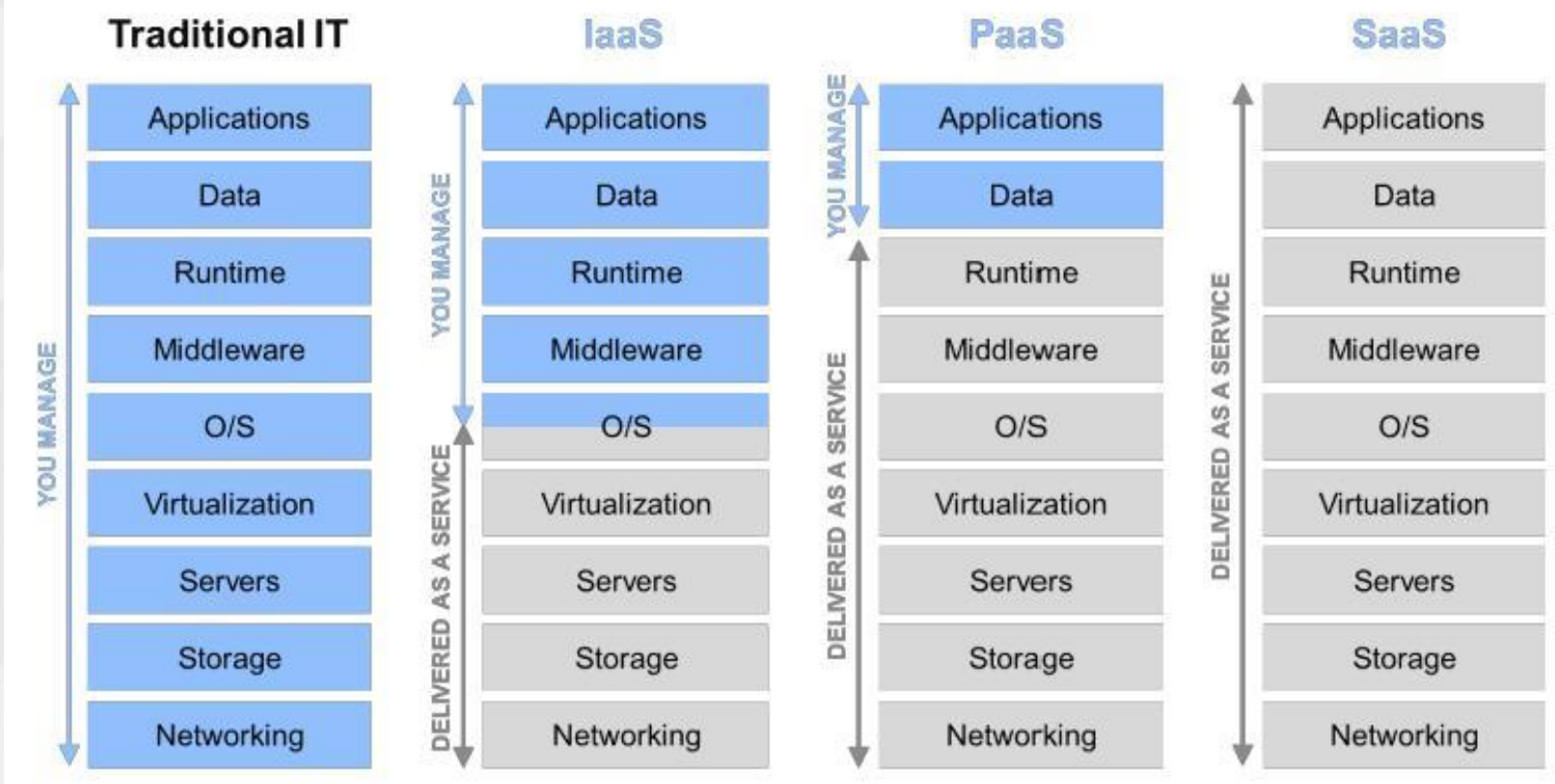
Disadvantages of SaaS

- Limited customization
- Data security and Privacy concerns
- Dependence on internet connectivity in most cases
- Potential integration challenges
- Vendor reliability and support

Comparing service models

- Control and responsibility spectrum
- Customization and flexibility
- Management and maintenance
- Cost implications

Comparing service models



Cloud Deployment Models

- Four main models
  - Public Cloud
  - Private Cloud
  - Hybrid Cloud
  - Multi-Cloud

Public Cloud

- Services offered over the public internet
- Shared infrastructure among multiple organizations
  - Although special allowances can be made
- Advantages
  - Cost-effective, scalable*, rapid deployment
- Disadvantages
  - Compliance issues, limited customization, security concerns

* That is the intent: may be capped, depends on the provider (e.g., hyperscalars)

Private Cloud

- Exclusive environment for a single organization
- Can be on-premises or hosted
  - Although special allowances can be made
- Advantages
  - Enhanced security, compliance, control
- Disadvantages
  - Higher costs, scalability limitations*, maintenance responsibility*

* Potentially ameliorated if hosted

Hybrid Cloud

- Combines public and private elements
- Enables data and application portability
  - Must be planned for
- Advantages
  - Flexibility, potential cost optimization, enhanced security
- Disadvantages
  - Complexity, security risks during data movement, cost management challenges

Multi-Cloud

- Use multiple cloud services
  - From multiple providers
- Advantages
  - Mitigates vendor lock-in
  - Optimizes services
  - Enhances resilience
- Disadvantages
  - Management complexity
  - Skill requirements
  - Integration challenges

Factors influencing deployment choices

- Security and compliance requirements
- Costs
- Performance and scalability needs
- Technical expertise and resources
- Integration and interoperability requirements

Overview of major cloud providers

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

AWS Offerings

- Compute services
  - EC2, Lambda
- Storage solutions
  - S3, EBS
- Database Services
  - RDS, DynamoDB
- AI and ML
  - SageMaker, Rekognition

- Strengths: Maturity, service breadth, ecosystem

Azure Offerings

- Compute services
  - Virtual Machines, Azure Functions
- Storage solutions
  - Blob Storage, Disk Storage
- Database Services
  - SQL Server DB, Cosmos DB
- AI and ML
  - Azure ML, Cognitive Services
- Strengths: Maturity, enterprise integration, hybrid capabilities, ecosystem support, AI services

GCP Offerings

- Compute services
  - Compute Engine, Cloud Functions
- Storage solutions
  - Cloud Storage, Persistent Disk
- Database Services
  - Google Spanner, BigTable
- AI and ML
  - Vertex AI, Vision AI

- Strengths: Big Data processing, competitive pricing, innovation

Practical use cases

- Web and mobile applications
- Big data and analytics
- Disaster recovery and backup
- Development and testing environments
- Internet of Things

Strategic decision making considerations

- Assessing objectives
- Analyzing technical requirements
- Evaluate risk and challenges
- Plan for change management
- Measuring

Cost management strategies

- Monitoring and analytics
- Resource adjustments and optimization
- Pricing models and discounts
- Governance policies
- Regular audits

Security best practices

- Identity and Access Management (IAM)
- Data protection
- Network security
- Monitoring and logging
- Certification

Future proofing

- Emerging technologies
- Build for portability
- Skills development
- Implement agile practices
- Establish strong vendor relationships (multiple)

Key Takeaways

- Understanding models is crucial
- Each model offers unique benefits
- Continuous evaluation is invaluable