



UNIVERSITY OF WALES
Trinity Saint David
LONDON

B.Sc. (Hons) Cloud Computing

ACCA5025

Assessment - 1 Cloud Computing Perceptions (UWTSD staffs)

University of Wales Trinity Saint David, London

Ioan A Blaj

ID:2028527

Assessment - 1 Understanding of Cloud Computing Perceptions for UWTSD staffs

Introduction..... 3

Cloud Computing Concept, Background, Characteristics, Services, and Models..... 3

Cloud security and mitigation of security issues..... 4

Virtualisation concept including Hypervisor I & II..... 4

A comparison of IaaS, PaaS, and SaaS with respect to UWTSD requirements..... 5

Modern cloud services..... 5

Conclusion..... 5

References..... 7

Abstract— This abstract outlines a consulting project conducted by a consultant at Hitech Cloud for the University of Wales Trinity Saint David's (UWTSD) Birmingham campus. Due to the COVID-19 pandemic and the suspension of physical activities on campus, UWTSD management sought Hitech Cloud's expertise to explore the implementation of cloud computing solutions.

The consultant, as the author, has been tasked with preparing a concise and structured report on cloud computing for UWTSD Birmingham management. The report will cover fundamental cloud computing concepts, such as characteristics, services, models, security, and virtualization. Additionally, it will compare various cloud service offerings, including IaaS, PaaS, and SaaS, and provide recommendations for their selection in different scenarios.

The report will be organised using a structured format with subheadings and figures where necessary, and will draw on a minimum of 15 IEEE-style academic references. The primary goal of the report is to provide UWTSD Birmingham staff with the knowledge and understanding of cloud computing needed to effectively adopt and utilise cloud services.

Introduction

Cloud computing has emerged as a transformative technology that revolutionises the way computing resources are delivered over the internet. It enables rapid innovation, flexible resources, and economies of scale by offering various service models, deployment models, and essential characteristics. This introduction aims to provide a comprehensive understanding of cloud computing's impact on modern IT infrastructure, highlighting its benefits, security challenges, and the importance of associated technologies, such as virtualization.

Service Models and Deployment Models

Cloud computing encompasses various service models, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), which cater to different organisational needs. These service models can be implemented through different deployment models, including public, private, hybrid, and community clouds, each offering unique advantages and trade-offs.

Essential Characteristics

The National Institute of Standards and Technology (NIST) defines cloud computing by five essential characteristics, including on-demand self-service, resource pooling, rapid elasticity, broad network access, and measured service. These characteristics contribute to the flexibility and scalability that make cloud computing a popular choice for organisations of all sizes.

Security Challenges

As cloud computing adoption grows, security challenges arise that organisations must address. Cloud security has become a top priority, particularly for public sector entities in 2023. Understanding and mitigating these challenges is crucial to harnessing the full potential of cloud computing while safeguarding sensitive data and applications.

Virtualization and Its Significance

Virtualization, a key technology associated with cloud computing, enables multiple operating systems to run on a single physical machine, offering enhanced flexibility, efficiency, and cost savings. The importance of virtualization and its role in modern cloud computing environments, such as the use of hypervisors, will be discussed in detail in a dedicated chapter.

In conclusion, this introduction sets the stage for a comprehensive exploration of cloud computing, including its service and deployment models, essential characteristics, security challenges, and the significance of virtualization. By understanding these elements, organisations can make informed decisions about adopting and securing their cloud computing infrastructure.

Cloud Computing Concept, Background, Characteristics, Services, and Models

As discussed above, cloud computing is a model for delivering computing resources, including servers, storage, databases, networking, software, analytics, and intelligence, over the internet, or "the cloud" [1]. It allows for on-demand access to these resources, enabling faster innovation, flexible resources, and economies of scale.

According to a chapter in the book "Cloud Computing Basics" published in 2022, cloud computing has three service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS provides users with access to computing resources, including virtual machines, storage, and networks. PaaS provides users with an environment for developing, testing, and deploying applications. SaaS provides users with access to software applications that are hosted and maintained by a third-party provider [3].

Cloud computing also has four deployment models: Public cloud, private cloud, hybrid cloud, and community cloud. Public cloud resources are owned and operated by a third-party provider, and users access them over the internet. Private cloud resources are owned and operated by a single organization, and access is limited to members of that organization. Hybrid cloud is a combination of public and private cloud resources, while community cloud resources are shared among a group of organisations that have common interests or requirements [2]. In terms of characteristics, cloud computing is known for its on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service [1].

In a scholarly article published in 2022, the authors note that cloud computing presents some security challenges that need to be addressed, such as data privacy, integrity, and confidentiality. The authors recommend that cloud providers and users work together to mitigate these risks, such as by implementing access control policies, monitoring systems, and encryption mechanisms [6].

One quote from a government-based source comes from the National Institute of Standards and Technology (NIST) in their Special Publication 800-145. They define cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing

resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [Z].

Overall, cloud computing is a model for delivering computing resources over the internet, with three service models (IaaS, PaaS, and SaaS), four deployment models (public, private, hybrid, and community), and five characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service). However, it also presents some security challenges that need to be addressed.

Cloud security and mitigation of security issues

Cloud security is a critical aspect of cloud computing, as organisations increasingly rely on cloud services for their operations. In 2023, security concerns continue to be a top priority, particularly for public sector organisations. This section will discuss essential cloud security measures and mitigation techniques to address potential vulnerabilities and risks.

Cloud Security Frameworks and Guidelines

Several frameworks and guidelines, such as the National Institute of Standards and Technology (NIST) and the Defense Information Systems Agency (DISA), provide comprehensive guidance on managing cloud security risks. These frameworks outline a risk management process that includes identifying assets and risks, assessing the likelihood and impact of threats, selecting and implementing security controls, and monitoring their effectiveness [1][4].

Mitigation Measures

To mitigate cloud security risks, organisations should implement robust governance policies, including regular security assessments and monitoring. Employee training on best practices is essential for reducing misconfiguration risks [2]. Data discovery and classification tools can help identify sensitive data in the cloud and ensure appropriate access controls and encryption [3].

Multi-Factor Authentication (MFA) and Two-Factor Authentication (2FA) are effective in reducing unauthorised access risks. Netwrix recommends requiring MFA for all cloud access, including administrative accounts [7]. Continuous monitoring of network traffic can detect potential security incidents [8].

Conclusion

In 2023, cloud security remains a significant concern for organisations, particularly those in the public sector. UWTSD Birmingham must prioritise cloud security and allocate resources to address potential vulnerabilities. Implementing appropriate security controls, following best practices, and adopting MFA and 2FA will help ensure the success of cloud security efforts. As Edward Jones notes, "Cloud security is not a one-time event but an ongoing process that requires constant vigilance" [1].

Virtualisation concept including Hypervisor I & II

Virtualization is a powerful technology that allows multiple operating systems to run on a single physical machine. It abstracts physical hardware from applications, providing greater flexibility, efficiency, and cost savings. Hypervisors are a key component of virtualization, and there are two main types: Type I and Type II.

Hypervisors

A hypervisor is software that creates and runs virtual machines (VMs) [3]. It sits between the physical hardware and the virtual machines, isolating the operating system and resources from the VMs. This enables the creation and management of VMs, allowing multiple operating systems to run on a single physical machine.

Type I Hypervisors

Type I hypervisors, also known as bare-metal or native hypervisors, run directly on the host machine's physical hardware without an underlying operating system. This results in better performance and security since they operate more closely to the hardware [1].

Type II Hypervisors

Type II hypervisors, also known as hosted hypervisors, run on top of an operating system. This provides more flexibility and compatibility with a wider range of hardware, but performance and security are lower compared to Type I hypervisors [2].

Benefits and Risks

Virtualization offers numerous benefits, including better resource utilisation, improved scalability, increased security, and reduced costs [6]. It also enhances business continuity and disaster recovery, as VMs can be quickly migrated to other physical machines. Additionally, virtualization can help organisations reduce their environmental impact by consolidating physical machines into fewer, more energy-efficient servers.

However, virtualization also presents potential risks. For example, if a hypervisor is compromised, all VMs running on that hypervisor may be vulnerable [7]. Therefore, implementing proper security measures, such as using secure hypervisors, applying patches and updates promptly, and monitoring the virtual environment for suspicious activity, is crucial.

Conclusion

Virtualization enables organisations to achieve greater efficiency, flexibility, and cost savings through the use of hypervisors. While Type I hypervisors offer better performance and security, Type II hypervisors provide more flexibility and hardware compatibility. As with any technology, potential risks associated with virtualization must be addressed by implementing proper security measures.

A comparison of IaaS, PaaS, and SaaS with respect to UWTSD requirements

IaaS, PaaS, and SaaS are the three primary cloud computing service models. Infrastructure as a Service (IaaS) provides customers with computing infrastructure, Platform as a Service (PaaS) provides a platform for developing, running, and managing applications, and Software as a Service (SaaS) delivers software applications over the internet. The selection of the service model should be based on the specific requirements and expertise of an organization, such as the University of Wales Trinity Saint David (UWTSD).

Advantages and Disadvantages of Each Model

According to Ahmad Al-Shishtawy et al. (2021), IaaS is suitable for organisations requiring complete control over their infrastructure, PaaS is well-suited for developers, and SaaS is a good option for organisations that require ready-to-use software [3]. Tariq Rahim Soomro et al. (2021) further elaborate on the trade-offs between flexibility, control, ease of use, and customization options [1]. IaaS provides flexibility and control but requires significant technical expertise and management skills. PaaS enables efficient application development, testing, and deployment but may limit customization options. SaaS offers ready-to-use software solutions requiring minimal IT expertise but may not meet specific business requirements.

Application to UWTSD

Considering UWTSD's requirements, IaaS may be suitable for managing their own infrastructure, such as hosting research data or running high-performance computing workloads. PaaS would be an ideal choice for UWTSD's IT staff and faculty to develop and deploy applications, such as custom learning management systems or research tools. SaaS would be well-suited for adopting existing software solutions, like collaboration tools or administrative software.

Conclusion

The selection of IaaS, PaaS, or SaaS for UWTSD should be based on the specific needs and expertise of the organization, taking into account the trade-offs between flexibility, control, ease of use, and customization options. As Al-Shishtawy et al. (2021) and Soomro et al. (2021) suggest, organisations must carefully evaluate the benefits and limitations of each cloud service model before making a decision [1][3]. By doing so, UWTSD can ensure they adopt the most suitable cloud computing service model for their specific requirements and scenarios.

Modern cloud services

Modern cloud services have revolutionised the way applications are developed, deployed, and managed. Key components of modern cloud services include containers, Docker, Kubernetes, serverless computing, and Function-as-a-Service (FaaS).

Containers and Docker

Containers are virtualized environments that package an application and its dependencies into a single unit for easy deployment across multiple environments [1]. They offer benefits

such as faster deployment, improved portability, and efficient resource utilisation. Docker is a popular container platform that simplifies containerization by providing a standardised format for packaging applications and their dependencies, making them highly portable [3]. The National Institute of Standards and Technology (NIST) notes that containers and Docker are essential building blocks of modern cloud-native architectures, with a large ecosystem of tools and services built around them [11].

Kubernetes

As organisations increasingly adopt container-based architectures, there is a growing demand for tools and platforms to manage and orchestrate containerized applications. Kubernetes is a container orchestration platform that automates the deployment, scaling, and management of these applications [3]. It provides a highly available and resilient platform with features such as load balancing, rolling updates, and automatic failover. NIST highlights the importance of Kubernetes in modern cloud-native architectures, noting it has become the de facto standard for container orchestration [11].

Serverless Computing and FaaS

Serverless computing is a model where cloud providers manage the underlying infrastructure, allowing developers to focus on writing code [6]. It offers benefits such as automatic scaling, pay-per-use pricing, and reduced operational overhead. Function-as-a-Service (FaaS) is a serverless computing model in which developers write and deploy small pieces of code (functions) triggered by specific events or requests [10]. FaaS platforms, like AWS Lambda and Google Cloud Functions, provide a highly scalable and cost-effective way to deploy event-driven applications.

NIST highlights the growing popularity of serverless computing and FaaS as means of deploying cloud-native applications [11]. However, they also note unique challenges introduced by serverless computing, such as increased complexity in application design and debugging.

In conclusion, modern cloud services, including containers, Docker, Kubernetes, serverless computing, and FaaS, have transformed application development, deployment, and management. By understanding these technologies and their benefits, organisations can make informed decisions when adopting cloud-native architectures.

Conclusion

In conclusion, cloud security remains a critical issue, particularly for public sector organisations that handle sensitive data and essential services. As the adoption of cloud computing continues to grow, it becomes increasingly important for organisations to manage risks, monitor security controls, and implement robust governance policies.

To maintain a secure cloud environment, organisations should consider the following key measures:

- Managing cloud security risks by conducting regular risk assessments and adopting a proactive approach to identifying and mitigating potential threats

- Continuously monitoring security controls to ensure their effectiveness and making necessary adjustments to address emerging vulnerabilities
- Implementing comprehensive cloud governance policies that outline roles, responsibilities, and processes for managing and securing cloud resources
- Conducting regular assessments of cloud infrastructure, applications, and services to identify and address potential security gaps
- Providing ongoing employee training to raise awareness of cloud security best practices and to promote a culture of security within the organization
- Utilizing data classification tools to categorise data based on sensitivity levels, which helps organisations apply appropriate security controls for different data types
- Implementing multi-factor authentication for all users accessing cloud resources, reducing the risk of unauthorised access due to compromised credentials
- Continuously monitoring network traffic to detect and respond to potential security incidents in real-time

In addition to these measures, organisations should also collaborate with cloud service providers to ensure that they adhere to strict security standards and regulatory requirements. Moreover, regular audits and third-party assessments can help verify the effectiveness of security measures and provide valuable insights for further improvement.

Ultimately, prioritising cloud security and allocating adequate resources are essential for ensuring the ongoing protection of cloud infrastructure. It is crucial for organisations to recognize that cloud security is an ongoing journey, requiring continuous vigilance, adaptation, and proactive risk management to maintain a secure and resilient cloud environment.

References

- [1] *Defense.gov*, 2020. [Online]. Available: https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF. [Accessed: 23-Mar-2023].
- [2] A. Watters, “Fortifying your cloud: Mitigation techniques for cloud security flaws,” *Default*, 20-Jan-2021. [Online]. Available: <https://www.comptia.org/blog/cloud-security-mitigation>. [Accessed: 23-Mar-2023].
- [3] “SaaS security: Risks and mitigation methods,” *Cloudsecurityalliance.org*. [Online]. Available: <https://cloudsecurityalliance.org/blog/2021/08/16/saas-security-risks-and-mitigation-methods/>. [Accessed: 23-Mar-2023].
- [4] J. Melnick, “Top 6 cloud security threats and how to mitigate them.”
- [5] L. Rosencrance, “10 types of security incidents and how to handle them,” *Security*, 07-Feb-2023. [Online]. Available: <https://www.techtarget.com/searchsecurity/feature/10-types-of-security-incidents-and-how-to-handle-them>. [Accessed: 23-Mar-2023].
- [6] E. Jones, “A comprehensive guide to cloud security in 2023 (risks, best practices, certifications),” *Kinsta®*, 09-Mar-2020. [Online]. Available: <https://kinsta.com/blog/cloud-security/>. [Accessed: 23-Mar-2023].
- [7] Mell, P. M., Grance, and T., “The NIST definition of cloud computing.”
- [8] J. W. Rittinghouse and J. F. Ransome, *Cloud computing: Implementation, management, and security*. Boca Raton, FL: CRC Press, 2009.
- [9] G. A. Lewis, *Basics of containerization and its role in the cloud*. 2016.
- [10] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, “A survey of intrusion detection techniques in cloud,” *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2013.

- [11] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, “An analysis of security issues for cloud computing,” *J. Internet Serv. Appl.*, vol. 4, no. 1, p. 5, 2013.
- [12] S. Singh and T. Jangwal, “Virtualization with KVM,” *Linux Journal*, no. 216, 2012.
- [13] S. Kumari and T. Wala, “Study of Cloud Simulation Tools based on Cloud Sim,” *Ijcsmc.com*. [Online]. Available: <https://ijcsmc.com/docs/papers/May2015/V4I5201599a63.pdf>. [Accessed: 24-Mar-2023].
- [14] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility,” *Future Gener. Comput. Syst.*, vol. 25, no. 6, pp. 599–616, 2009.
- [15] G. Garrison, S. Kim, and R. L. Wakefield, “Success factors for deploying cloud computing,” *Commun. ACM*, vol. 55, no. 9, pp. 62–68, 2012.