

Cloud Computing

by George Searle

FILE	2092_GEORGE_SEARLE_CLOUD_COMPUTING_113613_32434362.DOCX		
TIME SUBMITTED	22-MAY-2018 09:11PM (UTC+0100)	WORD COUNT	6561
SUBMISSION ID	89753140	CHARACTER COUNT	40734

Cloud Computing

Cloud Services & Concerns

George P. Searle
School of Applied Computing
University of Wales Trinity Saint David
Swansea, Wales

Abstract—Cloud computing has become a very popular topic in recent times. Many organisations are interested in what cloud computing can bring to their business. However, cloud adoption is a complex task and requires careful planning and consideration of its many advantages and disadvantages. This research paper will investigate the various cloud service delivery models, as well as the risks and concerns of such centralised infrastructure including cloud security.

Keywords—cloud computing; SaaS; PaaS; IaaS; DaaS; cloud security; DoS; DDoS

I. INTRODUCTION

Cloud computing relates to a shared pool of resources and software that are provided on demand to clients, based on their specific requirements and needs [1], [2]. It is a move away from personal computers to centralised infrastructure located in data centres [3]. There are several cloud deployment models including public clouds, private clouds, community clouds and hybrid clouds [4]. A public cloud is an infrastructure owned by a cloud provider selling cloud services to the general public and organisations. A private cloud is an infrastructure owned by an organisation or third-party for use by a single organisation. A community cloud is an infrastructure owned by several organisations or a third-party for use by several organisations part of a specific sector. Lastly, a hybrid cloud is two or more cloud deployment models joined by standardised or proprietary technologies [5], [6].

Virtualisation is the key technology supporting the cloud and facilitates many of its benefits [7], [8].

These benefits include high availability, scalability, lower costs, elasticity, reduced maintenance and rapid deployment [9]–[11]. Cloud computing has and continues to draw attention from the international Information and Communication Technology (ICT) community [12]. This is due to its numerous benefits and continued development driven by industry giants such as Amazon, Microsoft and Google [12]–[14]. It is no surprise that organisations are hosting business-critical applications in the cloud [15]. However, cloud computing can be confusing and daunting due to the numerous service delivery models, considerations, challenges and technologies involved; that many organisations are cautious [9], [12], [16].

This research paper is structured as follows. Firstly, section II will examine numerous service delivery models available to clients, including their advantages and disadvantages. In section III, various risks to cloud computing will be investigated such as outages, data loss and security. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks will also be highlighted. All risks and concerns will be accompanied by numerous recommendations to reduce and minimise them. Finally, a conclusion is presented in section IV.

II. CLOUD COMPUTING SERVICE DELIVERY MODELS

A. Software-as-a-Service

Software-as-a-Service (SaaS) is a software delivery model which allows users to access applications over the internet from a provider [17], [18]. The SaaS provider will host applications on centralised servers and is responsible for the

management, security, availability and performance of the software [19]. SaaS adopts a 'pay for what you use' model and removes the need to install and run applications in-house [19], [20]. The applications can be accessed by the user via a thin client (e.g. web browser) [17]. An example of a SaaS provider is 'Salesforce.com' [19].

SaaS architecture is dependent on three key components; customisation, multi-tenancy architecture (MTA), scalability and rapid development [21]. Customisation addresses the methods for allowing a configurable and custom end-user experience, even if a single instance is accommodating multiple users. Metadata is one solution for a custom experience in the one-to-many scenario. MTA addresses how an application instance can accommodate multiple tenants and keep track of the data. Scalability relates to allowing a high volume of concurrent users' access to applications. There are multiple architectural approaches that address these factors in different ways [19], [21].

The advantages of SaaS are many. Pricing is very competitive due to no upfront costs (e.g. servers and software licenses), the 'pay for what you use' model and reduced maintenance costs for organisations [18], [19]. SaaS is easy-to-use, custom to the client's requirements and provides flexible access via the internet [20], [21]. Software installation, maintenance and support is also no longer a concern for the client [19].

The disadvantages of SaaS include the requirement for a stable, moderate bandwidth internet connection. Without a good connection, SaaS applications will be sluggish and may not work at all. There will be an increased security risk as applications will be interacting with many users, as well as applications running over the internet. Such circumstances make SaaS less suitable for certain business sectors. Load balancing is a significant issue that must be addressed and monitored by businesses using SaaS [19], [20].

A SaaS provider will also have a huge responsibility to deliver advertised performance, as well as have adequate redundancy and recovery methods in place [19], [21].

B. Platform-as-a-Service

Platform-as-a-Service (PaaS) is a model that provides a full application development platform to

support the complete software lifecycle. It allows users to design, develop, test, deploy and host applications in an online environment provided by a PaaS provider [22], [23]. Like SaaS, the provider is responsible for scalability, redundancy, security and the delivery of services that allow users to construct software online. The payment model for PaaS is often a subscription model for development, a payment model based on user interactions of the finished application (e.g. Bungee Connect) or free base model with purchasable add-on resources (e.g. Google App Engine). PaaS providers may also offer a marketplace to sell applications in exchange for a proportion of revenue [23].

PaaS environments are designed in a way that allows developers to program applications and various database interactions without the need to reference underlying physical systems and network interfaces; thus, keeping virtualised architectures hidden. PaaS providers also often support development using common programming languages such as C, Java and PHP. Some providers (e.g. Salesforce.com and Bungee) have easy to learn proprietary languages that aim to speed up development. Another useful feature that the Google App Engine provides is the ability to work offline and then push application changes online [22].

The advantages of PaaS share many similarities with SaaS, such as software cost savings, ease of use and no worry over physical hardware [22], [23]. PaaS consolidates development, test and production environments, simplifies development and can allow developers to deliver a product to market faster [1], [23]. Some platforms allow the integration and interoperability with third-party services and applications. PaaS platforms provide a growing community of developers allowing knowledge and expertise to be shared. The collaboration experience is also enhanced due to online management [22], [23].

The disadvantages of PaaS include the disruption that a client would experience if there was an outage of the PaaS system (without offline capabilities). Users are often tied to the platform that they choose with no way to transfer applications to other platforms. Security and privacy is a continuing concern with the cloud. Businesses must decide whether they can trust the PaaS provider to host applications containing sensitive data. PaaS can be closed with poor interoperability and limited

application programming interfaces (APIs). Integration of company assets is not always sufficiently addressed. Many PaaS systems lack persistence. Developers will also have to learn how to use the platform and any proprietary languages. This can take a significant amount of time and slow application development progress [22], [23]. It should be remembered that there is no perfect PaaS offering that can fulfil all requirements [24].

C. Infrastructure-as-a-Service

Infrastructure-as-a-Service (IaaS) is the foundation layer of cloud service offerings [10]. IaaS is a model that offers users computing infrastructure resources (e.g. servers, storage and network devices) [10], [25]. Resources are delivered to a client in the form of one or more provisioned virtual machine (VM) instances with the requested central processing unit (CPU), random-access memory (RAM), storage and network capabilities [26], [27]. Hardware and administrative services are often provided as well as the ability to scale bandwidth, memory and storage. IaaS uses the 'pay for resources used' revenue model [10]. The IaaS provider is responsible for maintaining the underlying hardware, raw storage and provisioned VMs [10]. The client has full control over the server infrastructure, operating system (OS) and applications they choose to run using the virtualised resources [25], [28]. Examples of IaaS providers are Amazon Elastic Compute Cloud (Amazon EC2), Google Compute Engine and Rackspace [28].

The advantages of IaaS include the general cloud benefits of competitive costs, scalability, high availability and outsourced hardware. Greater flexibility compared to SaaS and PaaS is IaaS's major advantage. Developers can also move applications to the cloud environment without modifying application code [10].

The disadvantages of IaaS include the issue that the service may become unavailable [10]. Security and privacy are concerns and a greater challenge for IaaS providers due to the flexibility IaaS offers [27]. Administration separation between different users' virtual environments is a challenge due to scalability. Users may also misconfigure their infrastructure causing unexpected errors and security vulnerabilities [27]. Dawoud et al. [29] highlighted that IaaS is vulnerable to network attacks, more so than other networked systems. Internal VMs planted

with malicious software to attack internal services is a concern [29]. IaaS providers must carefully implement access control and firewall policies that can cope with IaaS's dynamic and rapidly changing infrastructure [27].

D. Desktop-as-a-Service

Desktop-as-a-Service (DaaS) is a desktop virtualisation technology that provides a customisable desktop experience on a mobile device or thin client [30], [31]. All applications and data are stored and processed on a centralised server, often in a hypervisor-based infrastructure with VMs [31]. This allows a user to have a full desktop experience to install applications and store data from low power devices anywhere with internet access. DaaS brings together IaaS and SaaS by providing a virtual server and storage with a desktop OS (software) service. DaaS is often a subscription-based service, examples include Citrix XenDesktop and VMware Horizon View [32].

DaaS can be implemented in several different ways. A VM hypervisor approach, transferring virtual frames to clients using virtual display protocols. This method is independent of the client OS, however, lacks scalability (e.g. XenDesktop). A virtual user session approach that creates multiple user sessions on a server. This method is dependent on the client OS but provides greater scalability (e.g. Microsoft Terminal – Remote Desktop Protocol) [30], [33]. A container-based approach has also been suggested [31]. These implementations communicate between client and server using remote input/output (I/O) control data and streamed data via various protocols [33], [34].

The advantages of DaaS include relatively low cost, rapid deployment, flexibility, ease-of-use and mobility [35], [36]. Security can be improved in some private cloud implementations. This is because centralised DaaS will reduce the risk of compromising sensitive data if a laptop is stolen [36]. Security policies, access control and anti-virus protection can also be enforced on users [35], [37].

The disadvantages of DaaS includes degraded performance caused by hypervisor-based systems. This results in performance and user experience that cannot match a local personal computer [31]. Network bandwidth consumption and latency are also issues that can harm the desktop experience [32].

[38], [39]. Security, in particular, privacy, is a concern in DaaS due to cloud provider mechanisms that may unintentionally reveal a user's identity [34].

III. RISKS TO CENTRALISED INFRASTRUCTURE

Cloud computing is not immune from service unavailability and data loss [13], [40]. It is perhaps a fact that individuals and businesses should be more aware of.

A. Outages and Data Loss

As reliable as cloud solutions claim to be, the unavoidable truth is cloud-related outages have become staple news articles on information technology (IT) news outlets [41], [42]. The financial damage an outage can cause an organisation can be huge [43]. Organisations also cannot rely on a cloud provider's Service Level Agreement (SLA) to provide compensation [44]. This is because most SLAs limit compensation to financial credits for their own cloud services [45], [46].

There are several approaches to reducing the effects of cloud outages. Amazon EC2 and Google Compute Engine provide the ability to host instances in different regions and zones. Regions and availability zones within regions are isolated [47]–[49]. For example, an organisation could increase the redundancy of their cloud infrastructure by hosting resources in multiple regions. Thanks to a region's isolation, if there was an outage in one region the company could continue service (with reduced capacity) with the resources located in another region. However, costing for multiple regions can be complex [40], [50]. Another solution to keep critical services running during a cloud outage is a hybrid-cloud architecture [51], [52]. This would allow organisations to failover to their own on-premise infrastructure with reduced capacity [53], [54].

Accidental deletion and human error are a common and significant risk of losing data in the cloud according to Blomberg [55] and Brunau [56]. In 2016, 123-reg a UK web hosting provider made a costly error; running a faulty script that permanently deleted numerous customers' data on 67 servers [57]. Another example of human error is how one of FlexiScale's main storage volumes was accidentally deleted by an XCalibre engineer [58]. In 2011, Amazon EC2 suffered an outage due to an execution error which left 0.07% of data unrecoverable to a consistent state [59]. Such examples highlight errors

by cloud providers. There are likely numerous unreported internal business incidents, where an employee accidentally deletes files from the businesses cloud.

Hardware failure is a possible risk factor but less likely due to cloud providers offering various data replication and persistent disk mechanisms for data redundancy [60], [61]. However, exceptional circumstances can happen, therefore, the risk should not be ignored. Another consideration is that a cloud provider could go out of business putting data at risk [40].

Natural disasters (e.g. earthquakes, flooding, tornados etc.) are a big risk to data, especially with occurrences of natural disasters expected to rise in the future [5]. Such events have the capability to destroy cloud datacentres; resulting in a very high chance of permanent data loss. Natural disasters are hard to predict and defend against. The solution to protect against such disasters is to have a backup located in a different part of the world [5], [62]. This highlights the usefulness of Amazon EC2's and Google Compute Engine's previously mentioned regional replication. It should be noted that this function is not implemented by default [47]–[49]. The risk of a natural disaster in a region should also be considered (e.g. a datacentre in Tokyo would be more prone to an earthquake than a datacentre in London). By having a backup in a different part of the world the risk factor of natural disasters is greatly reduced. This is because it is very unlikely for there to be two simultaneous disasters in different parts of the world [5], [62].

A recommendation to protect against cloud data loss are local on-premise backups of data stored in the cloud [63], [64]. Cloud-to-cloud and region-to-region backups are also an option [65]–[67]. In addition to backing up to other sources, organisations must have a disaster recovery plan in place [68], [69]. A backup is little help if the organisation is ill-prepared and cannot recover quickly [70].

B. Cloud Security – Threats & Risks Overview

Cloud security is a vast topic due to the cloud's complexity and its multi-layered architecture in which every layer must be secured [6], [11], [71]. Data integrity, confidentiality, and availability (CIA) are key challenges that must be addressed in any cloud computing environment [2]. It is

understandable why many organisations resist cloud adoption; simply based on the research required to understand all the possible risks and security best practices needed to take the organisation safely into the cloud [13], [16], [72]. This section will briefly identify threats and risks at the various levels of cloud computing, as well as recommendations to prevent and defend against them.

There are numerous layers that must be considered:

1) Application Services

This layer relates to the software and applications that run in the cloud [9], [71].

a) Service level Responsibility

- SaaS – The cloud provider is responsible for the security of the software services they provide [19].
- PaaS & IaaS – The client is responsible for securing any self-developed or deployed applications [23], [27].

b) Threats and Risks

- Cross-site scripting
- Cross-site request forgery
- Structured Query Language (SQL), OS and Lightweight Directory Access Protocol (LDAP) injection flaws
- Cookie manipulation
- Hidden field manipulation
- Session hijacking
- Authentication weaknesses
- Direct object reference exploits
- Security misconfigurations
- Unrestricted Uniform Resource Locator (URL) access
- Unvalidated redirects and forwards
- Poor Transport layer protection
- Insecure trust configuration
- DDoS

Threats and risks according to Singh et al. [6], Subashini and Kavitha [9] and Osanaiye et al. [73].

c) Recommendations

Many of the threats highlighted above relate to web application and API security. It is therefore important that the cloud provider or client (whoever is responsible) designs applications using a

development framework with a strong focus on secure programming and security architecture [9], [71], [74]. It is highly recommended to follow information security standards (e.g. International Organization for Standardization (ISO) 27001/27002) [75], [72].

2) Infrastructure Services

This layer relates to OS instances, storage, network and databases [10], [25].

a) Service level Responsibility

- SaaS & PaaS – The cloud provider is responsible for securing infrastructure services [19], [23].
- IaaS – The client is responsible for securing infrastructure services [27].

b) Threats and Risks

- Security misconfiguration
- DDoS
- Unpatched OS vulnerabilities
- Data storage attacks
- Data leakage
- De-anonymity attacks
- Malware botnet attack
- Signature-based malware
- Injection attacks
- Poorly implemented policies
- Flood attacks
- Poor crypto-key management
- Poor authentication
- Data interception
- Cookie manipulation
- Monitoring and auditing failures
- Password sharing

Threats and risks according to Singh et al. [6].

c) Recommendations

Clients are responsible for securing their VMs. This will include regular OS and application patching and the use of third-party cloud security technology [71], [74]. Identity Access Management (IAM) must be carefully implemented with a least privilege policy [14]. Encryption keys must be secured (e.g. using a Hardware Security Module) [76]. Data should also be encrypted at rest and in transit [77]. Public auditing of data integrity by a third party is a consideration [78].

It would be highly advised to follow the cloud security recommendations outlined by the Cloud Security Alliance (CSA) [79]. Organisations should also seek to be compliant with ISO 27001/27002, 27017 and 27018. These are internationally recognised standards that relate to information security management, best practice guidance, cloud-specific security controls and safeguarding personal information in the cloud [80]–[83]. Regular performance auditing of the information security management system (ISMS) is also a requirement of ISO 27001. This ensures that the ISMS is effective, trustworthy and secure [84], [85].

Amazon Web Services (AWS) provides an extensive guide to their security processes and what security features are available to customers [86]. This highlights transparency and showcases that the underlying cloud infrastructure that clients will use is secure. AWS and Google Cloud provide comprehensive security best practice guides advising customers on all aspects of cloud security [76], [87]. This highlights cloud providers' customer commitment and serious stance concerning security by providing high-quality free resources. Both providers also provide security bulletins on found vulnerabilities, their impact and recommended steps for users [88], [89].

3) Virtualisation Environment and Physical Infrastructure

These levels relate to VM deployment, Virtual Machine Monitor (VMM), hypervisors and datacentre hardware such as servers, disks and network devices [2], [6], [71].

a) Service level Responsibility

The cloud provider is responsible for securing the underlying virtualised and physical infrastructure [2]. Note in the case of a private cloud this will be the responsibility of the organisation or authorised third-party [5], [6].

b) Threats and Risks

- Cross VM-attacks
- Data leakage
- Untrusted VMM
- DoS/DDoS and brute force attacks on the physical cluster
- Misconfigured virtual cluster
- Unpatched virtual cluster

- Authentication issues
- Network attacks
- Hardware vulnerabilities
- Unpatched server OS
- Unpatched network devices
- Spoofing attacks

Threats and risks according to Singh et al. [6].

c) Recommendations

It is very important that these levels are secured as compromises here can make every client of the cloud vulnerable [71]. VM image repositories, VM boundaries, the VM migration process, VM execution and hypervisors must be secured [9], [71], [74]. Virtual local area networks (VLANs), Intrusion Detection System (IDS), Intrusion Prevention System (IPS) and firewalls must be used in combination to secure data in transit. Hardware and systems must be patched regularly [6]. There should also be strict access management policies and secure authentication processes [6], [71].

The author again recommends the CSA best practices and complying with ISO 27001/27002, 27017 and 27018 [79]–[83]. It is worth noting that both Amazon AWS and Google Cloud are both ISO 27001/27002, 27017 and 27018 compliant [90], [91].

C. Cloud Security – Distributed Denial of Service (DDoS) Attacks

Denial of Service (DoS) and Distributed Denial of Service (DDoS) are a category of attacks on service availability that deserve attention. A DoS attack is a malicious effort to make a service or application unavailable to users. A DDoS attack is a large scale coordinated attack using multiple malicious or compromised hosts to deny access to a service or application [92], [93]. This attack is one of the most serious threats to cloud network security and has been increasing in popularity over the years [93].

There are many variants of DDoS attacks using different methods. These include volume-based attacks such as User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP) floods to saturate the bandwidth of a target. Attacks on protocols such as Transmission Control Protocol (TCP) SYN attacks is another approach that aims to consume the resources of a target [73], [94]. A particularly popular attack method that has emerged is the attack of the application layer via Hypertext

Transfer Protocol (HTTP) GET flooding to consume resources [73], [93]. Application attacks are a concern as they are more sophisticated in nature. This is because they consume less bandwidth and are harder to distinguish from legitimate requests [73].

In a cloud infrastructure, it is the responsibility of both the user and cloud provider to protect against DoS and DDoS attacks. For example, in IaaS the user must protect their instances, OS and platform services from DDoS attacks. The provider protects against DDoS of their shared infrastructure and abstracted services [76]. Strategies a user can take to mitigate DoS and DDoS attacks include traditional methods, cloud provider DDoS protection and third-party solutions [76], [92]. The first step to DDoS protection is detection. An attack must be detected as quickly as possible to allow for mitigation [73], [76]. One approach is to establish a performance baseline taking into consideration time of day and season. Anomalies can then be detected using statistical or behavioural analysis of traffic compared to the baseline, appropriate actions can then be triggered [76]. For example, an IDS and IPS can provide anomaly detection and signature-based algorithms to detect an attack [73], [76]. Once a DDoS attack has been detected policies can be triggered on a firewall to block packets from a specific destination, as well as traffic rate limiting and embryonic session limiting to TCP SYN packets in such an attack. A web application firewall should also be considered as it provides thorough packet inspection of web traffic, which can detect and react to application DDoS attacks [76]. As well as these common strategies many cloud providers have their own DDoS protection services that can be bought by users (e.g. AWS Shield Advanced [95], [96] and Google Cloud Armor [97], [98]). In addition, both AWS and Google Cloud provide DDoS resiliency best practice guides with implementation guidance for their platforms [92], [99]. There are also third-party companies that specialise in DDoS protection (e.g. Cloudflare [100] and Incapsula [101]) that can be integrated into a user's cloud infrastructure. It is worth noting that due to the scalability and elasticity of cloud infrastructures it is possible to dynamically scale resources to absorb a DDoS attack [76]. It is recommended to implement a multi-layered defence strategy (as opposed to relying on one method) to protect and mitigate against DoS and DDoS attacks [76], [100]–[102].

IV. CONCLUSION

In conclusion, cloud computing is a vast subject area with many service delivery models available to users with varying needs and requirements. The advantages of high availability, reduced costs and maintenance, ease-of-use and rapid deployment are significant that cloud computing can no longer be ignored. However, the advantages must be carefully weighed up against the security and privacy concerns that continue to plague cloud offerings.

There are many risks relating to centralised cloud infrastructure including outages, data loss and security threats. However, despite the numerous risks there are many solutions available by cloud providers and third-parties to reduce them. Security is one of the biggest concerns with cloud computing due to its complex multi-layered architecture. Therefore, it demands the best security practices. There are plenty of security solutions and advice available. The numerous ISO security standards also provide a reliable framework for security auditing to the highest of standards. However, the author believes that this necessity for vigorous security is likely holding many businesses back from adopting the cloud. DDoS is a popular attack against the availability of cloud services and applications. However, with the emergence of special DDoS protection services by cloud providers and third-parties; DDoS could soon no longer be a threat.

REFERENCES

- [1] M. Farouk, A. Yousif, and M. B. Bashir, "A Cloud Based Framework for Platform as a Service," in *2015 International Conference on Cloud Computing (ICCC)*, 2015, pp. 1–5.
- [2] S. Aldossary and W. Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 4, pp. 485–498, 2016.
- [3] Y. Jadeja and K. Modi, "Cloud computing - Concepts, architecture and challenges," in *2012 International Conference on Computing, Electronics and Electrical Technologies, ICCEET 2012*, 2012, pp. 877–880.
- [4] P. Arora, "Cloud Computing Security Issues in Infrastructure as a Service," *Int. J. Adv. Res.*

- Comput. Sci. Softw. Eng.*, vol. 2, no. 1, pp. 707–711, 2012.
- [5] D. Velev and P. Zlateva, "A Feasibility Analysis of Emergency Management with Cloud Computing Integration," *Int. J. Innov. Manag. Technol.*, vol. 3, no. 2, pp. 188–193, 2012.
 - [6] S. Singh, Y. S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *J. Netw. Comput. Appl.*, vol. 75, pp. 200–222, 2016.
 - [7] M. Bourguiba, K. Haddadou, I. El Korbi, and G. Pujolle, "Improving network I/O virtualization for cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 673–681, 2014.
 - [8] V. Soundararajan, B. Agrawal, B. Herndon, P. Sethuraman, and R. Taheri, "Benchmarking a virtualization platform," in *2014 IEEE International Symposium on Workload Characterization (IISWC)*, 2014, pp. 99–109.
 - [9] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011.
 - [10] S. Bhardwaj, L. Jain, and S. Jain, "Cloud Computing : a Study of Infrastructure As a Service (IaaS)," *Int. J. Eng.*, vol. 2, no. 1, pp. 60–63, 2010.
 - [11] M. G. Avram, "Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective," *Procedia Technol.*, vol. 12, pp. 529–534, 2014.
 - [12] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 1, p. 50, 2008.
 - [13] R. Velumadhava Rao and K. Selvamani, "Data security challenges and its solutions in cloud computing," in *Procedia Computer Science*, 2015, vol. 48, no. C, pp. 204–209.
 - [14] F. Shahzad, "State-of-the-art survey on cloud computing security challenges, approaches and solutions," in *Procedia Computer Science*, 2014, vol. 37, no. C, pp. 357–362.
 - [15] P. S. K. Kannankott, "Cloud Computing : Security Issues and Challenges Service Models in Cloud Computing Deployment Models :"
 - [16] S. K. Singh and D. K. Singh, "CLOUD COMPUTING: SECURITY ISSUES AND CHALLENGES," *Int. J. Adv. Eng. Technol.*, vol. 10, no. 3, pp. 22311963–338, 2017.
 - [17] B. Allen, J. Bresnahan, and L. Childers, "Software as a service for data scientists," *Commun. ACM*, vol. 55, no. 2, pp. 81–88, 2012.
 - [18] L. Wu, S. Kumar Garg, and R. Buyya, "SLA-based admission control for a Software-as-a-Service provider in Cloud computing environments," in *Journal of Computer and System Sciences*, 2012, vol. 78, no. 5, pp. 1280–1299.
 - [19] G. Kulkarni, J. Gambhir, R. Palwe, and F. Author, "Cloud Computing-Software as Service," *Int. J. Cloud Comput. Serv. Sci.*, vol. 1, no. 1, pp. 11–16, 2012.
 - [20] F. Safari, N. Safari, and A. Hasanzadeh, "The adoption of software-as-a-service (SaaS): ranking the determinants," *J. Serv. Manag.*, vol. 26, no. 2, pp. 182–205, 2015.
 - [21] W. T. Tsai, X. Y. Bai, and Y. Huang, "Software-as-a-service (SaaS): Perspectives and challenges," *Sci. China Inf. Sci.*, vol. 57, no. 5, pp. 1–15, 2014.
 - [22] G. Lawton, "Developing software online with platform-as-a-service technology," *IEEE Comput. Soc.*, vol. 41, no. 6, pp. 13–15, Jun. 2008.
 - [23] V. Goncalves and P. Ballon, "Adding value to the network: Mobile operators' experiments with Software-as-a-Service and Platform-as-a-Service models," *Telemat. Informatics*, vol. 28, no. 1, pp. 12–21, 2011.

- [24] Z. Li, Y. Zhang, and Y. Liu, "Towards a full-stack devops environment (platform-as-a-service) for cloud-hosted applications," *Tsinghua Sci. Technol.*, vol. 22, no. 1, pp. 1–9, Feb. 2017.
- [25] S. S. Manvi and G. Krishna Shyam, "Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey," *Journal of Network and Computer Applications*, vol. 41, no. 1, pp. 424–440, 2014.
- [26] R. Ghosh, K. S. Trivedi, V. K. Naik, and D. S. Kim, "End-to-End Performability Analysis for Infrastructure-as-a-Service Cloud: An Interacting Stochastic Models Approach," in *IEEE 16th Pacific Rim International Symposium on Dependable Computing*, 2010, pp. 125–132.
- [27] M. Santana and L. Guan, "Infrastructure as a Service: Exploring Network Access Control Challenges," in *SAI Computing Conference*, 2016, pp. 37–46.
- [28] S. Shahzadi, M. Iqbal, Z. U. Qayyum, and T. Dagiuklas, "Infrastructure as a service (IaaS): A comparative performance analysis of open-source cloud platforms," in *IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD*, 2017, vol. 2017–June, pp. 1–6.
- [29] W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a Service Security: Challenges and Solutions," in *The 7th International Conference on Informatics and Systems (INFOS)*, 2010, pp. 1–8.
- [30] S. Kibe, T. Koyama, and M. Uehara, "The Evaluations of Desktop as a Service in an Educational Cloud," in *2012 15th International Conference on Network-Based Information Systems*, 2012, pp. 621–626.
- [31] H.-J. Baek and E.-N. Huh, "A Data-Driven Resource Allocation Method for Personalized Container Based Desktop as a Service," in *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*, 2017, pp. 971–978.
- [32] B. Li, C. Wang, Y. Xu, T. Yue, X. Cao, and Z. Ma, "An MPEG Media Transport System Based Desktop-as-a-Service (DaaS)," in *2016 8th International Conference on Computational Intelligence and Communication Networks (CICN)*, 2016, pp. 370–374.
- [33] S. Cristofaro, F. Bertini, D. Lamanna, and R. Baldoni, "Virtual Distro Dispatcher: a lightweight Desktop-as-a-Service solution," in *International Conference on Cloud Computing*, 2009, pp. 247–260.
- [34] D. D. Lamanna, G. Lodi, and R. Baldoni, "How Not to Be Seen in the Cloud: a progressive privacy solution for Desktop-as-a-Service," in *OTM Confederated International Conferences "On the Move to Meaningful Internet Systems"*, 2012, pp. 492–510.
- [35] cloudshape, "On-Premises Desktop as a Service (On-Premises DaaS): Solving the VDI Dilemma for Government Agencies," 2015.
- [36] S. Dernbecher, "Having the Mind in the Cloud: Organizational Mindfulness and the Successful Use of Desktop as a Service," in *2014 47th Hawaii International Conference on System Sciences*, 2014, pp. 2137–2146.
- [37] X. Tian, X. Wang, and A. Zhou, "DSP re-encryption: A flexible mechanism for access control enforcement management in DaaS," in *CLOUD 2009 - 2009 IEEE International Conference on Cloud Computing*, 2009, pp. 25–32.
- [38] S. Shu, X. Shen, Y. Zhu, T. Huang, S. Yan, and S. Li, "Prototyping Efficient Desktop-as-a-Service for FPGA Based Cloud Computing Architecture," in *2012 IEEE Fifth International Conference on Cloud Computing*, 2012, pp. 702–709.
- [39] M. A. Layek, T. Chung, and E. N. Huh,

- "Adaptive Desktop Delivery Scheme for Provisioning Quality of Experience in Cloud Desktop as a Service," *Comput. J.*, vol. 59, no. 2, pp. 260–274, 2016.
- [40] P. Waibel *et al.*, "Cost-optimized redundant data storage in the cloud," *Serv. Oriented Comput. Appl.*, vol. 11, pp. 411–426, 2017.
- [41] The Register, "Articles about outage," www.theregister.co.uk. [Online]. Available: <https://www.theregister.co.uk/Tag/outage>. [Accessed: 19-Apr-2018].
- [42] J. Tsidulko, "The 10 Biggest Cloud Outages of 2017 (So Far)," *CRN*, 2017. [Online]. Available: <https://www.crn.com/slideshows/cloud/300089786/the-10-biggest-cloud-outages-of-2017-so-far.htm>. [Accessed: 19-Apr-2018].
- [43] S. Ranger, "Cloud computing: Here's how much a huge outage could cost you," *ZDNet*, 2018. [Online]. Available: <https://www.zdnet.com/article/cloud-computing-heres-how-much-a-huge-outage-could-cost-you/>. [Accessed: 19-Apr-2018].
- [44] F. Gilbert, "Cloud computing contracts and cloud outages," *TechTarget Network*, 2011. [Online]. Available: <https://searchcloudsecurity.techtarget.com/tip/Cloud-computing-contracts-and-cloud-outages>. [Accessed: 19-Apr-2018].
- [45] Amazon Web Services, "Amazon Compute Service Level Agreement," aws.amazon.com, 2018. [Online]. Available: <https://aws.amazon.com/compute/sla/>. [Accessed: 19-Apr-2018].
- [46] Google Cloud, "Google Compute Engine Service Level Agreement (SLA)," *Compute Engine Documentation*, 2018. [Online]. Available: <https://cloud.google.com/compute/sla>. [Accessed: 19-Apr-2018].
- [47] Amazon Web Services, "Regions and Availability Zones," *Amazon Elastic Compute Cloud Guide*. [Online]. Available: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html#migrating-instance-availability-zone>. [Accessed: 19-Apr-2018].
- [48] Google Cloud, "Regions and Zones," *Compute Engine Documentation*. [Online]. Available: https://cloud.google.com/compute/docs/regions-zones/#zone_deprecation. [Accessed: 19-Apr-2018].
- [49] Google Cloud, "Designing Robust Systems," *Compute Engine Documentation*. [Online]. Available: <https://cloud.google.com/compute/docs/tutorials/robustsystems#backup>. [Accessed: 19-Apr-2018].
- [50] S. J. Bigelow, "Select the right cloud regions, availability zones to optimize costs," *TechTarget Network*, 2017. [Online]. Available: <https://searchcloudcomputing.techtarget.com/tip/Learn-the-cost-implications-of-cloud-regions-and-availability-zones>. [Accessed: 19-Apr-2018].
- [51] Cloud Standards Customer Council, "Practical Guide to Hybrid Cloud Computing," 2016.
- [52] upwork, "Hybrid Cloud: A Brief Intro," *Web Development*. [Online]. Available: <https://www.upwork.com/hiring/development/hybrid-cloud-brief-intro/>. [Accessed: 19-Apr-2018].
- [53] G. Williams, "The integral role of hybrid cloud and multi-cloud computing models for enterprises," *The Next Web*, 2018. [Online]. Available: <https://thenextweb.com/contributors/2018/04/15/integral-role-hybrid-cloud-multi-cloud-computing-models-enterprises/>. [Accessed: 19-Apr-2018].
- [54] VCloud News, "Public, Private or Hybrid Cloud After Amazon S3 Outage?," www.vcloudnews.com, 2017. [Online]. Available: <http://www.vcloudnews.com/public-private-or-hybrid-cloud-after-amazon-s3-outage/>.

[Accessed: 19-Apr-2018].

- [55] B. Blomberg, "4 ways you can still lose data from cloud storage," *Ontrack*, 2016. [Online]. Available: <https://www.krollontrack.co.uk/blog/making-data-simple/4-ways-you-can-still-lose-data-from-cloud-storage/>. [Accessed: 19-Apr-2018].
- [56] C. Brunau, "6 Leading Causes of Cloud Data Loss [Forrester Research]," *backupify*, 2017. [Online]. Available: <https://www.backupify.com/blog/6-leading-causes-of-cloud-data-loss-forrester-research>. [Accessed: 19-Apr-2018].
- [57] A. Degeler, "123-reg deletes sites in massive clean-up script blunder, customers let rip," *Ars Technica*, 2016. [Online]. Available: <https://arstechnica.com/information-technology/2016/04/123-reg-deletes-sites-in-massive-clean-up-script-blunder-as-customers-let-rip/>. [Accessed: 19-Apr-2018].
- [58] C. Metz, "Engineer accidentally deletes cloud," *The Register*, 2008. [Online]. Available: http://www.theregister.co.uk/2008/08/28/flex_iscalc_outage/. [Accessed: 19-Apr-2018].
- [59] Amazon Web Service (AWS), "Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region," *aws.amazon.com*, 2011. [Online]. Available: <https://aws.amazon.com/message/65648/>. [Accessed: 19-Apr-2018].
- [60] Amazon Web Services (AWS), "Amazon Elastic Block Store (EBS)," *aws.amazon.com*. [Online]. Available: <https://aws.amazon.com/ebs/>. [Accessed: 19-Apr-2018].
- [61] Google Cloud, "Storage Options," *Compute Engine Documentation*. [Online]. Available: <https://cloud.google.com/compute/docs/disks/#pdspecs>. [Accessed: 19-Apr-2018].
- [62] M. Habiba and S. Akhter, "A Cloud Based Natural Disaster Management System," *Grid Pervasive Comput.*, no. January 2013, pp. 152–161, 2013.
- [63] N. Cavalancia, "Do you even need on-premises backup anymore?," *solarwinds msp*, 2016. [Online]. Available: <https://www.solarwindmsp.com/blog/do-you-even-need-on-premise-backups-anymore>. [Accessed: 19-Apr-2018].
- [64] D. Virgillito, "What happens when data gets lost from the cloud?," *Cloud Tech News*, 2015. [Online]. Available: <https://www.cloudcomputing-news.net/news/2015/jan/26/what-happens-when-data-gets-lost-cloud/>. [Accessed: 19-Apr-2018].
- [65] S. Pritchard, "Cloud-to-cloud backup: What it is and why you need it," *ComputerWeekly.com*, 2017. [Online]. Available: <https://www.computerweekly.com/feature/Cloud-to-cloud-backup-What-it-is-and-why-you-need-it>. [Accessed: 19-Apr-2018].
- [66] Spanning, "Why Third-Party Backup for Google Apps is Absolutely Critical," *Spanning Blog*, 2015. [Online]. Available: <https://spanning.com/blog/why-third-party-backup-for-google-apps-is-absolutely-critical/>. [Accessed: 19-Apr-2018].
- [67] N2WS, "How To Automate Cross AWS Region Backup Considering RTO and RPO," *n2ws.com*. [Online]. Available: <https://n2ws.com/blog/how-to-guides/how-to-automate-aws-cross-region-backup-and-dr-considering-rto-and-rpo-2>. [Accessed: 19-Apr-2018].
- [68] D. Foster, "When a Cloud Has an Outage, What Is Your Data Recovery Plan?," *commvault*, 2017. [Online]. Available: <https://www.commvault.com/blogs/2017/february/when-a-cloud-has-an-outage-what-is-your-data-recovery-plan>. [Accessed: 19-Apr-2018].
- [69] J. Poole, "How to Escape a Cloud Outage Unscathed," *The Equinix Blog*, 2017. [Online]. Available: <https://blog.equinix.com/blog/2017/03/23/ho>

- w-to-escape-a-cloud-outage-unscathed/. [Accessed: 19-Apr-2018].
- [70] E. Schindler, "How cloud services change your disaster recovery plan," *Ars Technica*, 2017. [Online]. Available: <https://arstechnica.com/information-technology/2017/02/surviving-a-cloud-based-disaster-recovery-plan/>. [Accessed: 19-Apr-2018].
- [71] M. Ali, S. U. Khan, and A. V Vasilakos, "Security in cloud computing: Opportunities and challenges," *Inf. Sci. (Ny)*, vol. 305, pp. 357–383, 2015.
- [72] S. K. Singh and D. K. Singh, "Cloud Computing: Security Issues and Challenges," *Int. J. Adv. Eng. Technol.*, vol. 10, no. 3, pp. 22311963–338, 2017.
- [73] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework," *J. Netw. Comput. Appl.*, vol. 67, pp. 147–165, May 2016.
- [74] M. Al Morsy, J. Grundy, and I. Müller, "An analysis of the cloud computing security problem," *17th Asia-Pacific Softw. Eng. Conf. (APSEC 2010) Cloud Work. Aust.*, no. December, p. 7, 2010.
- [75] R. Kalaiprasath, R. Elankavi, and R. Udayakumar, "A Cloud Security and Compliance-A Semantic Approach in End to End Security," *Int. J. Mech. Eng. Technol.*, vol. 8, no. 5, pp. 482–494, 2017.
- [76] Amazon Web Services, "AWS Security Best Practices," 2016.
- [77] D. Nayak, "Cloud Computing & Security," *Int. J.*, vol. 3, no. April, pp. 5–6, 2011.
- [78] D. Puthal, B. P. S. Sahoo, S. Mishra, and S. Swain, "Cloud computing features, issues, and challenges: A big picture," in *Proceedings - 1st International Conference on Computational Intelligence and Networks, CINE 2015*, 2015, pp. 116–123.
- [79] Cloud Security Alliance, "Security Guidance For Critical Areas of Focus In Cloud Computing v4.0," 2017.
- [80] bsi, "ISO/IEC 27001:2013 Your implementation guide."
- [81] PECB, "ISO/IEC 27002:2013 Whitepaper," 2016.
- [82] bsi, "ISO/IEC 27017 Extending ISO/IEC 27001 into the Cloud A Whitepaper."
- [83] bsi, "ISO/IEC 27018 Safeguarding Personal Information in the Cloud Whitepaper," 2015.
- [84] J. Heron, "The ISO 27001:2013 Internal Audit: Simplified," *ISMS.online*, 2018. [Online]. Available: <https://www.isms.online/iso-27001/iso-270012013-internal-audit-simplified/>. [Accessed: 22-May-2018].
- [85] S. Monga, "ISO 27001 – Starting the Internal Audit Process," *schellman*, 2016. [Online]. Available: <https://www.schellman.com/blog/iso-27001-starting-internal-audit-process>. [Accessed: 22-May-2018].
- [86] Amazon Web Services, "Amazon Web Services: Overview of Security Processes," 2016.
- [87] Google Cloud, "Best Practices for Enterprise Organizations," *Enterprise Guide*, 2017. [Online]. Available: <https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations>. [Accessed: 21-Apr-2018].
- [88] Amazon Web Services, "Latest Bulletins," *aws.amazon.com*, 2018. [Online]. Available: <https://aws.amazon.com/security/security-bulletins/>. [Accessed: 21-Apr-2018].
- [89] Google Cloud, "Security Bulletin," *Compute Engine Documentation*, 2018. [Online]. Available: <https://cloud.google.com/compute/docs/security-bulletins>. [Accessed: 20-Apr-2018].
- [90] Amazon Web Services, "AWS Compliance Programs," *aws.amazon.com*. [Online].

- Available:
<https://aws.amazon.com/compliance/programs/>. [Accessed: 21-Apr-2018].
- [91] Google Cloud, "Standards, Regulations & Certifications," *cloud.google.com*. [Online]. Available:
<https://cloud.google.com/security/compliance/>. [Accessed: 21-Apr-2018].
- [92] Google Cloud, "Best Practices for DDoS Protection and Mitigation on Google Cloud Platform," 2016.
- [93] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, "Detecting Web based DDoS Attack using MapReduce operations in Cloud Computing Environment," *J. Internet Serv. Inf. Secur.*, no. 8111, pp. 28–37, 2013.
- [94] K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "DDoS attack detection method using cluster analysis," *Expert Syst. Appl.*, vol. 34, no. 3, pp. 1659–1665, Apr. 2008.
- [95] Amazon Web Services, "AWS Shield," *aws.amazon.com*. [Online]. Available:
<https://aws.amazon.com/shield/>. [Accessed: 01-May-2018].
- [96] Amazon Web Services, "Denial of Service Attack Mitigation on AWS," *AWS Answers*. [Online]. Available:
<https://aws.amazon.com/answers/networking/aws-ddos-attack-mitigation/>. [Accessed: 01-May-2018].
- [97] Google Cloud, "Cloud Armor," *cloud.google.com*. [Online]. Available:
<https://cloud.google.com/armor/>. [Accessed: 01-May-2018].
- [98] P. Joshi, "Getting to know Cloud Armor — defense at scale for internet-facing services," *Google Cloud Platform Blog*, 2018. [Online]. Available:
<https://cloudplatform.googleblog.com/2018/03/getting-to-know-Cloud-Armor-defense-at-scale-for-internet-facing-services.html>. [Accessed: 01-May-2018].
- [99] Amazon Web Services, "AWS Best Practices for DDoS Resiliency," 2016.
- [100] Cloudflare, "Protect Against DDoS Attack," *www.cloudflare.com*. [Online]. Available:
<https://www.cloudflare.com/ddos/>. [Accessed: 01-May-2018].
- [101] Incapsula, "DDoS Protection," *www.incapsula.com*. [Online]. Available:
<https://www.incapsula.com/ddos-protection-services.html>. [Accessed: 01-May-2018].
- [102] M. Darwish, A. Ouda, and L. F. Capretz, "Cloud-based DDoS attacks and defenses," *Inf. Soc. (i-Society), 2013 Int. Conf.*, pp. 67–71, 2013.

Cloud Computing

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

87 /100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

GRADING FORM: SMU GENERIC_GJ

GEORGE SEARLE

87

RESEARCH-INFORMED LITERATURE



In the last assignment, I effectively told you to aim for quality over quantity - seems this time around you've gone for both! An enormous number of sources used, with a clear effort to achieve good academic credibility. There're still a handful of sources in the 60s and 70s which are of a lower standard, though I understand that it can sometimes be hard to find peer reviewed material for certain topics.

28

KNOWLEDGE AND UNDERSTANDING



Excellent knowledge and understanding demonstrated - a very thorough report, with significant detail in all key areas.

28

ANALYSIS



You've obviously taken on board my previous feedback about synthesis - very good here. Conclusion is fine, though maybe a little brief to the size of the report overall - as a minor suggestion, it might be nice to either slightly increase the weight of this, or include a few more concluding remarks through the report, in your work as you move into level 6. Nonetheless, an excellent piece of work.

19

PRACTICAL APPLICATION AND DEP.



N/A - no marks assigned.

SKILLS FOR PROFESSIONAL PRAC.



A very well-written, professionally presented report. It'd be nice to include the odd relevant figure to break the text up, however - there are, for example, some quite good visual representations of the XaaS variants.

12