

SERVER MANAGEMENT AND VIRTUALISATION Assignment - Nabil Ouzahra - P147535

by Nabil Ouzahra

FILE	1565_NABIL_OUZHARA_SERVER_MANAGEMENT_AND_VIRTUALISATION_ASSIGNMENT_-_NABIL_OUZHARA_-_P147535_113613_883988634.DOCX		
TIME SUBMITTED	23-MAY-2018 07:39PM (UTC+0100)	WORD COUNT	3595
SUBMISSION ID	89809227	CHARACTER COUNT	19434

SERVER MANAGEMENT AND VIRTUALISATION

Student number: P147535

Module Code: ACCA5003

Module Tutor: Dr TIM BASHFORD

Nabil Ouzahra 2nd year Computer Networks & Cybersecurity

Abstract— Cloud computing is the most recent paradigm shift to deliver IT services for businesses. This has shaped the world of IT in general. The huge development of Internet network and virtualization has been the driving force behind the rise of this technology. Many big players in this field such as Google, Microsoft and Amazon, have seen the opportunity of growth through providing cloud services, offering some great benefits for businesses, such as cost, agility, scalability, competitiveness, effectiveness and more. However, this comes with risks that businesses should understand and analyze before adopting one. This paper will focus on the major benefits and risks of cloud services and proposes some considerations and recommendations to help mitigate those risks.

List of Acronyms:

IT: Information Technology
 AWS: Amazon Web Services
 CSP: Cloud Service Provider
 VMs: Virtual Machines
 VPN: Virtual Private Network
 DoS, DDoS: Denial of Service, Directed Denial of Service
 APIs: Application Programming Interface
 DRaaS: Disaster Recovery as a Service
 IRP: Incident Response Plan
 CPU: Central Processing Unit
 RAM: Random Access Memory
 AES: Advanced Encryption Standard

List of figures

Figure 1: Cloud computing market value..... 1
 Figure 2: Main paradigms of cloud computing..... 1

I. INTRODUCTION

Cloud computing has become one of the driving forces that shape the world of Information Technology (IT) services in recent years, thanks to the rapid development of the Internet, virtualisation and power of data. Many organisations and businesses are shifting day by day towards cloud computing services in the hope of being more competitive, reaching bigger platforms, saving costs and increasing availability. Cloud computing comes with many other benefits to offer such as business agility, transferring the security and management side of IT services to a third-party cloud service provider. Cloud services have made a huge change in terms of competitiveness. Having access to all the necessary computing resources and infrastructure without spending heavily on equipment, software and infrastructure has helped many small and medium businesses to become more competitive and has also helped to create new businesses. This shift towards cloud computing services is driven by many benefits. However, adopting these types of services comes with risks and threats. Despite the potential risks and drawbacks, the on-demand of these services is still rising.

II. THE RAPID SHIFT TOWARDS CLOUD COMPUTING

A. The shift towards cloud computing

The expansion and rapid growth of cloud computing services market is great indication of how businesses and organisations are shifting toward this technology, one of the leading marketing research predicting that the global market value of these services could reach up to 236 billion \$ by 2020 [1] (see figure -1).



Figure 1: Cloud computing market value

Cloud computing is the most recent paradigm shift to deliver IT services for businesses, considered as radical comparing to its predecessor's paradigms (distributed, centralised and decentralised) [2]. This unique and complex framework has helped many businesses and organisation to focus more on the business aspect itself, creating growth and becoming more competitive. Most of these services are billed on a pay-per-use basis or by subscription where the business has to pay a monthly or yearly fee to access these services. All this has given a great opportunity for small business to expand their IT resources and services as and when needed. It also has a great impact on business creation.

The main cloud computing service types, or computing stacks, as are:

Software as a Service (SaaS) [3], Platform as a Service (PaaS) [4] and Infrastructure as a Service (IaaS) [5] (see Figure 2).

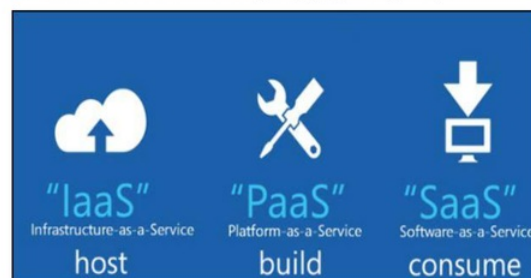


Figure 2: Main cloud computing services

1) Software as a service

Software as a Service (SaaS) is a well-known cloud computing architecture model where the software itself is offered to the client as a service. This type of service looks very attractive to some businesses where great cost cutting can be achieved. This helps reduce the investment on purchasing and maintaining expensive software especially if this can be accessed on a pay as you go basis or even with flat low-cost charges from the provider [6]. Many leading IT companies such as Microsoft, Amazon Web Services (AWS), Google, Oracle, etc. are now adopting this technology by offering their software as a service. By having the software in a centralised secure environment, it is much easier to secure and maintain, and it frees the client from any security burdens. It is considered as an upper layer service where the client does not require powerful computing resources to use the software. This can also reduce the cost of buying high spec machines that possibly would not be utilised often. From an environmental perspective, some research and studies found that implementing SaaS as a business model helps to reduce the carbon dioxide emission by 60%. Compared to the classic usage of software, it helps be more energy efficient [7].

2) Platform as a Service

The popularity of Platform as a Service (PaaS) as cloud system is increasing everyday among many businesses, the fact that been able to run an application service without the hassle of handling its complex life cycle or having to invest heavily on the physical underlayer to support it, from user perspective these seems to attract users and helps them making huge savings, maintaining great performance and guaranty high security. Adopting PaaS as solution could give the business great opportunity to focus more with business side, Same as most of cloud services, PaaS model was also built on the top of virtualization technology, thanks to that business can scale easily as the demand grows, without the need of investing on hardware and redundant resources [8].

3) Infrastructure as a Service

Moving down the layers, there is Infrastructure as a Service (IaaS), one of the leading cloud computing models in terms of demand especially among small and medium businesses. IaaS offers great automated features with high flexibility and having access to scalable resources as and when needed, users are capable of outsourcing and building for example an entire virtual data centre to support their business needs and scale it as their business grows. These services are often offered through dashboards or API where the client can have direct access to servers, networking hardware, storage and hypervisors. IaaS model is still considered as the most flexible one thanks to the total control given to the clients over the entire Infrastructure, storage and processing powers [5] [9]. IaaS comes with great potentials to allow users to perform a variety of critical tasks such as create back-up storage, allocate the necessary Virtual Machines (VMs) to process the workload, monitor system performance and manage network traffic, etc. [10]. This solution may appear attractive to many businesses because of what it can offer. However, this comes with risks and challenges that managers and decision makers should consider when adopting IaaS. Security and data integrity within the cloud are among the top priorities for most companies. Despite the flexibility of service charges, often pay as you go, some bills can be shocking and expensive for users. Also, system transparency can be an issue. It is often the case that users are not being given enough detail about the infrastructure configuration and its performance, and this can have a negative impact on the service offered.

B. Benefits and Drawbacks of cloud computing

Cloud computing surely has opened up some great new opportunities and benefits. However this has come with some great challenges that should be taken into account before adopting any service model. The main challenges and risks in this field can be related to the sensitive areas of privacy, security and data availability.

1) Benefits of cloud computing

When it comes to the benefits of adopting cloud services, the list is long, and the following are some of the key benefits:

a) Cost:

Cloud computing offers this great opportunity of compelling huge savings in IT related costs, by reducing hardware purchase, eliminating its maintenance burdens and reducing a big part of the energy bills. In the long run, system upgrades and software updates can also help cut costs when adopting cloud computing [10] [11].

b) Agility:

Cloud based services provide the growth of businesses with this unique opportunity to scale up the cloud capability as and when needed. This advantage gives the business some level of flexibility and agility over competitors in their field [12] [13].

c) Collaboration Increase:

Collaboration and business work sharing could have a great impact on the business success. The adoption of cloud based services allows all team players within the business to benefit from sharing, updating and exchanging all the necessary information and documents in real time from anywhere [14] [13].

d) Competitiveness:

Moving to the cloud services helps businesses to become more competitive. The great advantage of using powerful IT resources that are normally exclusive to big companies helps reshape some markets and create real competition between businesses of all sizes [13] [15].

e) Disaster Recovery Solution:

With the help of cloud computing, small and medium businesses start to benefit from having a robust disaster recovery solution in place without a hefty large upfront investment. This was mainly limited to large businesses [13] [15].

f) Efficiency:

Adopting cloud computing services allows the individuals and businesses to focus more on the tasks that generate more profit and help the growth of the business instead of dealing with hardware and software issues. This helps everyone save time and energy [13] [15].

2) Drawbacks of cloud computing

With all the generally positive hypes that cloud computing offers, there are some negatives and drawbacks that come with it:

a) Downtime:

It is one of the imminent issues that most of the cloud service users are still facing: most of the providers cannot guaranty 100% availability of their services simply because it is Internet based and a hardware failure can be unpredictable. There could be a thousand reasons for a cloud platform to fail, leaving clients in a stand still [13].

b) Security and Privacy:

This is one of the main concerns of many cloud service users. Data privacy can be a great issue when it comes to handing this data to third party cloud service providers. When it comes to security there is no such perfect security system. Loopholes and vulnerability can always be manipulated by hackers. "Code Space" [16] case still stands as a good example of cybersecurity crimes within the cloud based services, where the entire company was deleted or "killed in the cloud" in other words [13] [15].

c) Vulnerability to attacks:

Adopting cloud-based services allows accessibility from anywhere using the Internet. However, this can pave the way to many possible attacks that could jeopardise the entire data processed or stored in the cloud service [13] [15].

d) Cloud platform dependencies:

Cloud computing services comes with another irritating disadvantage for many businesses: system dependency or what is called "Vendor lock-in" can make the customers migration from one platform to another very complex and expensive [13] [15].

e) Lack of transparency and limited control:

In most cloud computing services, customers are unaware of the configuration of their infrastructure. This has a negative impact on the efficiency of the system and the management of the resources available. Also, in most cases cloud services clients are given very limited control over their hosting infrastructure [13] [15].

III. THE RISKS OF COMPUTER NETWORK WITHIN THE CENTRALIZED INFRASTRUCTURE PERSPECTIVE

A. The major risks to cloud-based computer networks.

In the recent reports given by the Cloud Security Alliance [17], around 90 percent of businesses and organisation are still concerned about the use of public cloud services. Despite the security improvements of many leading cloud service providers, clients still fear the tragical impact of any big data breach or data loss on their business. Many firms still hesitate to make the move of using the cloud before having a good security strategy in place. Some of the major risks and threats that cloud computing is facing today are:

a) Data Breach

Cloud computing services are still considered as new. Some of its special characteristics can weaken the security side and add more security threats to the system.

Data breach is one of the top data security threats. It is defined as the unauthorised access, viewing or retrieval of data. It is one of the nightmares that IT management dread beside data loss, also known as data leak or data spill [18].

b) Data loss

Data loss is one of the major risks that cloud computing services are still facing. Using these services only increases the level of risk. This can be caused by backup failure or issue, cyber-attack, natural disaster or human error at the cloud level [19]. It is good practice for companies to perform an offsite data replication to protect themselves from permanent data loss scenario [16].

c) Natural disasters

When a natural disaster strikes, it is not only the people who get affected. Recent hurricane Sandy caused a major power outage, shut down many cloud-based datacentres in the region and important services were affected. Since then, many organisations have started

to shift towards adopting DRaaS as part of their disaster recovery solution and to consider providers with datacentres in a different location so that data can be replicated between locations [18].

d) Deliberate intrusion attempts or attacks

Malicious attacks can also take place in the cloud where hackers deliberately attack specific target companies to steal valuable, sensitive or financial data [18]. Hackers can achieve this by sending a malware or virus to the users, exploiting weaknesses on web applications, phishing or using social engineering attack and provoking victims to hand vital data such as login credentials [20].

e) Denial of Service (DoS)

Denial of Service (DoS) or Distributed Denial of Service (DDoS) uses multiple systems to orchestrate an attack against the cloud based web, device, networks or application by sending malicious data or request until the CPU and RAM get overwhelmed and the entire system goes offline, making it impossible for legitimate users to access the service or application [21].

Other important risks that businesses should take into account before adopting these models are legal risks, termination of service, account hijacking, internal misuse, insecure interface APIs, etc. [19].

B. Recommendations to mitigate the risks facing cloud computing

One of the main concerns that prevent many businesses from moving to cloud services is data privacy and some of the security issues related to this technology. Sharing sensitive data with third party service providers does not appeal to some businesses that fear the worst.

It is upon the service provider to provide robust security and ensure the integrity of the client's data [22]. Nevertheless, this does not stop the client from having a clear strategy and policy in place to help mitigate any possible risks.

- Cloud service providers should have adequate knowledge and plans in place to react to any security breach in an effective way. This should be audited by a third party on a regular basis to ensure data integrity.
- Businesses should carry a good risk assessment of the service provider before signing any contract. Good research on the security history, vulnerabilities of their system and detail about ending the service and migrating the data to future provider could be vital.
- A company should hire a third-party vendor to monitor on a regular basis the compliance of the terms agreed with the service provider.
- Data encryption should be implemented at Kernel level to protect its integrity against any unauthorised person.
- CSPs must implement industry standards for data encryption such as AES. This would make the data unusable and useless if ever hackers manage to intercept it.
- Security measures should be in place to ensure that communication between the client and the service provider is fully secure against any man-in-the-middle attack. Encryption keys must remain safe at all costs.
- Company should have a clear and firm access policy. Access credentials should be managed and updated on a regular basis to prevent any complacency.

- Raising staff awareness of all the risks related to data integrity and cyber-attacks [19] [18] [15] [23] [24].

C. Considerations on how security should be audited to defend cloud computing services

- Developing an Incident Response Plan (IRP) should help the client minimise the damages when data is breached. This should give some guidelines to the response team.
- Centralised identity-based access using VPN should be considered to avoid IP spoofing. This should give the client the ability to enforce firewall rules and access rights between them and the cloud.
- Considering data replication into a third location and adopting DRaaS could help mitigate data loss.
- Raising staff awareness of all the risks related to data integrity and cyber-attacks.
- The client must avoid putting sensitive data in the cloud to avoid any data being compromised. Data selection is key to eliminate major risks [19] [18] [15] [23] [24].

IV. CONCLUSION

The shift towards the use of cloud services has created great market opportunities for many cloud service providers. It has also helped create new businesses. To ensure this growth, CSPs must invest time and money to improve security effectiveness, data integrity and the availability of services. However, to address these new challenges, clients and service providers must have rigid policies and optimal security practices in place to mitigate these risks successfully.

REFERENCES

- [1] J. Vassallo, "Forrester : Marketing : Public Cloud Market Will Grow To \$236 Billion In 2020," *Forrester Research, Inc.*, 2016. [Online]. Available: <https://www.forrester.com/Public+Cloud+Market+Will+Grow+To+236+Billion+In+2020/-/E-PRE9446>. [Accessed: 15-May-2018].
- [2] D. Ullman, "Embracing the Cloud: Six Ways to Look at the Shift to Cloud Computing | EDUCAUSE," 2010.
- [3] S. Fremdt, R. Beck, and S. Weber, "Does Cloud Computing matter? An analysis of the Cloud model Software-as-a-Service and its impact on operational agility," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 1025–1034, 2013.
- [4] M. T. Sandikkaya and A. E. Harmanci, "Security problems of platform-as-a-Service (PaaS) clouds and practical solutions to the problems," *Proc. IEEE Symp. Reliab. Distrib. Syst.*, pp. 463–468, 2012.
- [5] S. Shahzadi, M. Iqbal, Z. U. Qayyum, and T. Dagiuklas, "Infrastructure as a service (IaaS): A comparative performance analysis of open-source cloud platforms," *IEEE Int. Work. Comput. Aided Model. Des. Commun. Links Networks, CAMAD*, vol. 2017–June, 2017.
- [6] A. S. Rumale and D. N. Chaudhari, "Cloud computing: Software as a service," *2017 Second Int. Conf. Electr. Comput. Commun. Technol.*, pp. 1–6, 2017.
- [7] D. Nedbal, "An examination of the economic value and contribution to energy efficiency of SaaS solutions: The case of e-invoicing," *Proc. - 2012 IEEE 1st Int. Conf. Serv. Econ. SE 2012*, pp. 1–8, 2012.
- [8] S. Costache, D. Dib, N. Parlavantzas, and C. Morin, "Resource management in cloud platform as a service systems: Analysis and opportunities," *J. Syst. Softw.*, vol. 132, pp. 98–118, 2017.
- [9] G. C. Bruschi, R. Spolon, L. L. Pauro, R. S. Lobato, A. Manacero, and M. A. Cavenaghi, "StackAct: Performance evaluation in an IaaS cloud multilayer," *Proc. - 15th Int. Symp. Parallel Distrib. Comput. ISPDC 2016*, pp. 149–156, 2017.
- [10] J. Gibson, R. Rondeau, D. Eveleigh, and Q. Tan, "Benefits and challenges of three cloud computing service models," *Comput. Asp. Soc. Networks (CASoN), 2012 Fourth Int. Conf.*, pp. 198–205, 2012.
- [11] J. D. Prince, "Introduction to Cloud Computing Introduction to Cloud Computing," vol. 4065, no. January, pp. 1–15, 2017.
- [12] S. K. Garg, S. Versteeg, and R. Buyya, "A framework for ranking of cloud computing services," *Futur. Gener. Comput. Syst.*, vol. 29, pp. 1012–1023, 2013.
- [13] M. K. Chihande and J. A. Van Der Poll, "Post cloud computing implementation benefits and challenges realised for a South African technology company," *2017 Conf. Inf. Commun. Technol. Soc. ICTAS 2017 - Proc.*, 2017.
- [14] A. O. Akande and J. P. Van Belle, "Cloud computing in higher education: A snapshot of software as a service," *IEEE Int. Conf. Adapt. Sci. Technol. ICASST*, vol. 2015–Janua, 2015.
- [15] M. Carroll, A. Van Der Merwe, and P. Kotzé, "Secure Cloud Computing: Benefits, Risks and Controls," *Inf. Secur. South Africa*, pp. 1–9, 2011.
- [16] P. Venezia, "Murder in the Amazon cloud | InfoWorld," *Info World*, 2014. [Online]. Available: <https://www.infoworld.com/article/2608076/data-center/murder-in-the-amazon-cloud.html>. [Accessed: 14-May-2018].
- [17] Cloud Security Alliance, "Cloud Security Alliance," *Cloud Security Alliance.org*, 2018. [Online]. Available: <https://cloudsecurityalliance.org/>. [Accessed: 19-May-2018].
- [18] R. Barona and E. A. M. Anita, "A Survey on Data Breach Challenges in Cloud Computing Security : Issues and Threats," *Int. Conf. circuits Power Comput. Technol. [ICCPCT]*, 2017.
- [19] B. Chaimaa, "Cloud Computing : Overview and Risk Identification Based on Classification by Type," *IEEE Trans. Cloud Comput.*, 2017.
- [20] F. Mouton, A. Nottingham, L. Leenen, and H. S. Venter, "Underlying finite state machine for the social engineering attack detection model," in *2017 Information Security for South Africa (ISSA)*, 2017, pp. 98–105.
- [21] Q. Yan and F. R. Yu, "Distributed denial of service attacks in software-defined networking with cloud computing," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 52–59, 2015.
- [22] M. S. Computer, S. Jodhpur, and J. Rajasthan, "OPEN ACCESS The Risk and Challenges of Cloud Computing Usman Namadi Inuwa," vol. 5, no. 12, pp. 5–10, 2015.
- [23] A. M. Alzadjali, A. H. Al-Badi, and S. Ali, "An analysis of the security threats and vulnerabilities of cloud computing in Oman," *Proc. - 2015 Int. Conf. Intell. Netw. Collab. Syst. IEEE INCoS 2015*, pp. 423–428, 2015.
- [24] U. N. Inuwa, "The Risk and Challenges of f Cloud

Computing," *J. Eng. Res. Appl.* www.ijera.com, vol. 5, no. 4, pp. 2248–962205, 2015.

SERVER MANAGEMENT AND VIRTUALISATION Assignment - Nabil Ouzahra - P147535

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

79/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

GRADING FORM: SMU GENERIC_GJ

NABIL OUZAHRA

79

RESEARCH-INFORMED LITERATURE



An excellent number of mostly academically credible sources used - a very good ratio of journal articles utilised.

22

KNOWLEDGE AND UNDERSTANDING

Very good evidence of knowledge and



understanding. Your section on the benefits of cloud computing, in particular, is excellent.

24

ANALYSIS



Extremely good synthesis of material - you obviously really paid attention to the feedback from the previous assignment. Good conclusions drawn. A really good piece of work, well done Nabil!

22

PRACTICAL APPLICATION AND DEP.



N/A - no marks assigned.

SKILLS FOR PROFESSIONAL PRAC.



A well-written and presented report. Good academic practice throughout.

11