

server management

by Mohammed Abdulla

FILE	2023_MOHAMMED_ABDULLA_SERVER_MANAGEMENT_113613_1829290 277.DOCX		
TIME SUBMITTED	23-MAY-2018 07:53PM (UTC+0100)	WORD COUNT	2959
SUBMISSION ID	89809700	CHARACTER COUNT	16990

SERVER MANAGEMENT AND VIRTUALISATION

Student number: P152058
Module Code: ACCA503
Module Tutor: Dr Tim Bashford

Mohammed Abdulla 2nd year student at UWTSD Computer Networks & Cybersecurity (BSc)

Abstract— Cloud computing has changed the face of information technology (IT), it's a computing technology, which improve cost efficiencies, scalability of application on demand services. The cloud computing is about a sharing of resources in an open environment through an internet-based connectivity, providing the scalability and reliability on-demand services with the high management capabilities. Despite the rapid reality development of cloud computing, the service quality, security, privacy and the legal/contractual still posing significant challenges. This report will discuss cloud computing services e.g. IaaS, Paas, Saas and DaaS models and will also discuss s risks to a computing network, prevention and recommendation.

creation [1]. The cloud computing services are usually classified into three categories [2] IaaS, PaaS, SaaS (see figure -1):

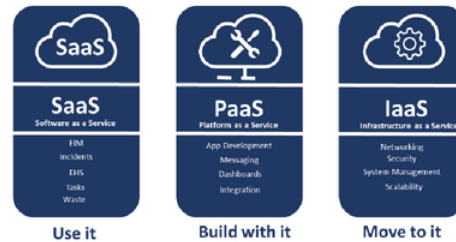


Figure 1: The main cloud services

Keywords: IaaS,PaaS,SaaS,DaaS

I. INTRODUCTION

Cloud computing technology has made a huge impact to organisations and especially the small and medium sized businesses. Consumers in the general public have embraced cloud computing through online sites such as Gmail, Facebook, and YouTube among others. Consumers have moved to cloud solutions for various reasons such as cost saving, transferring management responsibilities, and increasing business agility.

Widely known vendors such as Sun, IBM, and Dell have now taken to offering cloud computing services. Cloud computing is characterized by on-demand self-service, resource pooling, elasticity, scalability and measured provision that enables users to determine their usage for billing purpose. Many organisations are now shifting towards the cloud computing technology, which offers various benefits to the users, but it also comes with different challenges. The technology is also faced with various risks that will be discussed in this paper.

II. SHIFT TOWARD CLOUD COMPUTING

Cloud computing is a radical paradigm shift in the delivery of IT services and unlike other frameworks it is not based on straightforward approach to technology and its management. The internet-based technology has helped organisations become more efficient in their ICT deployment which has resulted in growth, a competitive advantage, and business

- Infrastructure as a service (IaaS) – provides storage, processing and other low-level network and hardware resources through the internet on demand basis. In IaaS the cloud infrastructure virtual machines are rented on a per-use basis and it can be scaled in or out dynamically depending on the customer needs. This has been made possible by virtualisation and network management. The IaaS users do not to worry, about the underlying infrastructure, but they do have a power to control over the operating system, applications, storage and in some cases networking components [6][8].
- Platform as a service (PaaS) – users of PaaS have access to programming and execution environments. PaaS enables the users to develop applications on the platform while using programming languages and APIs the service provider supports. PaaS users do not have control over the core infrastructure, including servers, storage, network, and operating systems. However, they are in charge of the applications deployed and in some cases the configurations of the application hosting environment [9].
- Software as a Service – SaaS providers host software or applications on their cloud and deliver them to users through browsers. Using the SaaS service the users do not have to install, run or maintain software on their local computers.
- DaaS is a form of virtual desktop infrastructure (VDI) in which the virtual desktop is managed by third party e.g. DaaS cloud computing provider

manage the security, storing and backing up the user data as well as upgrading the services [4].

According to research, organisations are now spending more on cloud computing with a high number of CIOs considering cloud computing as a priority for IT. Organisations have started adopting cloud computing services at various levels of implementations [2].

Most organisations today still operate applications that were designed and developed, hosted and managed on premise by an internal IT department. The applications are designed based on a monolithic design that permits a one size fits all approach. The design is structured in a three-tier architecture covering the front, mid and end layer [3]. However, the applications developed for cloud computing are meant to run on the cloud as a service infrastructure as well as middleware environments operating both on and off premise. The cloud applications design follows a superfine approach where a service is delivered to a business in an independent, loosely connected and self-contained manner.

This means that the cloud applications are technology independent, stateless, and can be deployed in different contexts. A comparison between the traditional and cloud applications indicates that the cloud applications offer a superior choice [3] [5]. However, there are adoption barriers that have seen organisations slow on quick adoption of the cloud applications. Before making a shift organisations have to deal with shift considerations such as cyber security, existing IT organisation, contracts with third parties, data protection concerns, and organisation technology that is incompatible with cloud applications [3].

Cloud computing and virtualisation has changed the computing world in terms of IT services and how they are managed. Virtualisation offers rapid deployment as well as better resource utilisation.

These technologies have drastically changed how computing resources are created, deployed, leveled up, updated, maintained and paid for. Apart from the change in computing resources utilisation for customers, it also means a shift in vendor value creation logic [2].

Traditionally, software vendors distributed their products through value-added resellers (VAR) to their customers. The VAR would sell, install, train, modify, and customise products at the client's organization. However, with cloud computing, the delivery of software and hardware to the customer is changing [1] [5].

With cloud computing there is no product to resell, install or maintain [4]. In 2008, HP predicted that in future all applications will be delivered online as the technology industry shifts towards SaaS [5].

The shift would be advanced by the propagation of services offered online, such as data storage, backup, and applications which are delivered on user request, dropping the necessity for desktop processing power [5].

III. BENEFITS OF CLOUD COMPUTING APPROACHES

The main aim of virtualisation is to enable resource sharing among multiple users. Various computing resources such as storage, hardware, and network can be virtualized. Apart from resource sharing virtualisation helps to improve mobility, availability and utilisation [6].

Virtualisation is considered an enabler of cloud computing and this has enabled many businesses especially the small businesses to benefit from cloud computing in the following ways:

- 1) Cloud computing is cost efficient in terms of maintenance and upgrading. Previously an organisation had to deal with high costs such as software licenses and upgrading hardware. However, the cloud is available at lower costs, which lower a business IT expenses. Small businesses that intend to apply intensive computing techniques can be able to afford it without incurring high costs.
- 2) Backup and recovery – customer data is stored in the cloud and this makes it easy to create backups and restore it much easier than when stored on a physical device. The majority of the cloud service providers are also responsible for the recovery of data in case there are problems.
- 3) Quick deployment – cloud computing makes the deployment of an IT solution for an organization an easy task. Once an organization has subscribed to a cloud service it is functional in a small amount of time depending on the kind of technology the organisation requires.
- 4) Storage capacity- a business benefits from high storage capacities depending on their needs and capability to subscribe.
- 5) Mobile access – organisation workers with network access from any location are able to access computing and storage resources enabling operations continuity in an organization.
- 6) Collaboration – cloud computing enables a group of people to work together online such as in the case of Google docs.
- 7) Flexibility - cloud computing helps organisations to increase their business flexibility which allows the employees to be flexible in or out of the workplace. Employees who are travelling are able to access organisation data through any kind of device that has access to the internet. All employees are able to access the same resources simultaneously since the data and files are virtually stored on the internet.
- 8) Automatic hardware or software upgrades – it is the responsibility of the cloud service provider to upgrade software and hardware used. This helps organizations reduce the cost of implementing IT solutions that would

have previously been a hindrance due to high costs of purchasing and maintaining them at their premise.

- 9) Agility - an organisation is able to remain competitive in a highly competitive business environment. This is possible as an organisation will be able to deliver their services more quickly [7] [8] [9][11][15].

Despite the benefits offered by cloud computing there are several challenges that affect cloud computing and they include:

- a) Security and privacy is the biggest concern in cloud computing as storing data on the cloud is considered less secure than any other storage. There are concerns that a third party may gain access to the data stored in the cloud environment. Cloud computing involves the use of third-party services as well as infrastructure and this means that security and privacy concerns cannot be avoided.
- b) Vendor lock-in - cloud service customers may depend on certain vendors since moving to a different vendor will mean substantial loss or heavy switching costs.
- c) Technical issues – although cloud computing makes data accessible from anywhere and at any time, the system may at times have serious malfunctions. A business should be aware that even with high standards of maintenance a service provider may experience outages and other technical issues [7] [8] [10].

IV. RISKS

Cloud computing has become beneficial to many organisations in carrying out their daily business. Cloud computing risks occur due to different factors that include data integrity, the location of data centers, infrastructure, and lack of knowledge concerning the cloud governing policies [11] [15].

- Malware injection attacks – hackers look for vulnerabilities found on web applications and websites that are hosted on the cloud. Using malicious applications, the hackers will exploit the vulnerabilities and inject malware into the cloud services. Once they gain access to the cloud services the hackers may steal data or eavesdrop .
- Data loss – the involvement of third parties to provide cloud services has contributed to data loss. Some service providers may not even have their own servers requiring them to acquire the services from other providers. This creates an increased chance of the data being stolen from external servers.

- Natural disasters – the service provider may also be faced with a natural disaster such as an earthquake which would damage their infrastructure.
- Denial of Service attack- attackers make cloud services inaccessible, slow or unavailable by launching different types of DoS attacks such as a SYN flood attack, smurf attack, or IP Spoofing attacks. One of the ways attackers are able to do this is by sending large amounts of data packets which overloads a server and network bandwidth. Fake requests may also be used to consume the memory of a server.
- Authentication attacks – authentication is considered a weak point in web servers, which makes it a target for attackers, especially where the encryption system used is not effective. Attackers try to gain access to user or organization confidential data by hacking the authentication process where they may gain access to user login credentials.
- Data Privacy – when security access rights fail, then a data leakage may occur, and this also raises the percentage of vulnerabilities and exposure. Cloud service providers may also fail to provide effective control, putting user data at the risk of insider attacks. Cloud servers are stored in different locations and countries, and this does not guarantee compliance to legislations as different countries have different data rules. Therefore, data stored on the cloud may not meet privacy and obligation requirements.
- Account or service traffic hijacking – hackers use phishing and social engineering techniques to obtain user credentials that are used to gain control over a user account. Hackers hijack user sessions by stealing user cookies and then make use of the user account for traffic riding. The intruder is then able to change, manipulate or interfere with customer data depending on the account invaded [12].
- Malicious and careless insiders – this threat is from disgruntled employees, infiltrators, as well as from ignorant and careless employees. This threat poses a potential threat not only to one company, but to other cloud tenants [9].
- Insecure APIs – making services available to many users at the same time while ensuring there is no accidental or intended damage is an immense task. The platform services require that application programming interfaces (API) be made available to developers and integrators. When the APIs are accessible from anywhere over the internet then malicious attackers can build their own applications

that they will use to manipulate customer data [4][8][10] [12].

Insufficient due diligence – since cloud computing is a relatively new technology, especially for some organizations there is a possibility of a knowledge gap that may prohibit adequate exercise of due diligence. For this reason, customers may contract the service of a cloud provider that does not match what their organization requires. The service agreements may also fail to disclose what happens in case of an incident and a customer may find themselves on the losing end.

V. RECOMMEND SOLUTIONS

There will be concerns associated with cloud computing just like any other technology. The cloud service providers should be able to address security and privacy issues that are linked to the cloud computing environment [13]. However, there are strategies that will help to mitigate the risks associated with cloud computing and they include:

- A company should carry out proper research before contracting a service provider. This includes finding out about the vendor security history, known security vulnerabilities, references, and ensuring they offer proactive security practices [4] [5].
- End to end encryption – when implemented end-to-end encryption reduces the chances of data breaches. The encryption should apply for data in transit as well as the data that is in store [8].
- The cloud providers should ensure that data in the cloud environment cannot be accessed by unauthorized users by protecting the data at the kernel level through encryption. Communications between the customer and the service provider should be secure to avoid man-in-the-middle attacks [8] [11].
- A cloud provider should provide unique policy-based approach for the management and access of data which should enable a user to determine servers that get access to secure data [13].
- Physical security – the cloud service provider must ensure that their data center is well secured physically in order to prevent on-site access of customer data by unauthorized persons. The CSP being in charge of physical security should also ensure that the staff are well trained, location security, availability of network firewalls as well as other infrastructure controls [14].

- To mitigate against malicious insiders, strict legal constraints should be put in place in employee work contracts [2].
- Secure virtualisation – a CSP may use advanced cloud protection systems (ACPS) to enhance the virtual machine security as well as that of the distributed computing middleware. It is important to regularly check the behaviour of the cloud components through logging and checking for executable system files [8].

VI. CONCLUSION

The proliferation of the internet has seen organizations shift to cloud computing technology. Cloud computing offers services to customers over the internet on a per demand basis through different deployments and that is infrastructure, software, and platform as a service. This technology offers various benefits to the customers but is also faced with challenges that hinder the adoption by some organisations. The technology is also faced with risks but like any other technology the risks can be mitigated to reduce possible impact.

References

- [1] Irshad, M., Gapar, M., Johar, M., & Naleer, H. (2015). A Review on Cloud Computing Adoption: An Exploratory Analysis. *International Journal of Advanced Research in Computer Science and Software Engineering*, 160-166.
- [2] Yang, H., & Tate, M. (2012). A Descriptive Literature Review and Classification of Cloud Computing Research. *Communications of the Association for Information Systems*, 1-28.
- [3] Menzel, G. (2017, July). *The Traditional to Cloud Shift: Challenges and Considerations*. Retrieved May 2018, from Capgemini: <https://www.capgemini.com/2017/07/the-traditional-to-cloud-shift-challenges-and-considerations/>
- [4] Nieuwenhuis, L., Ehrenhard, M., & Prause, L. (2017). The shift to Cloud Computing: The impact of disruptive technology on the enterprise software business ecosystem. *Technological Forecasting & Social Change*, 1-6.
- [5] Turton, S. (2008). *HP predicts "fundamental shift" towards cloud computing*. Retrieved May 2018, from Alphr: <http://www.alphr.com/accessories/12982/hp-predicts-fundamental-shift-towards-cloud-computing>
- [6] Vaezi, M., & Zhang, Y. (2017). Virtualization and Cloud Computing. *Cloud Mobile Networks, Wireless Networks*, 11-31.
- [7] Apostu, A., Puican, F., Ularu, G., Suciu, G., & Todoran, G. (2013). Study on advantages and disadvantages of Cloud Computing – the advantages of Telemetry Applications in the Cloud. *Recent Advances in Applied Computer Science and Digital Services*, 118-123.
- [8] Kavitha, K. (2014). Study on Cloud Computing Model and its Benefits, Challenges. *International Journal of Innovative Research in Computer and Communication Engineering*, 2423-2431.
- [9] Xue, C., & Xin, F. (2016). Benefits and Challenges of the Adoption of Cloud Computing in Business. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)*, 1-15.
- [10] Baljatescu, I. (2012). Cloud Computing Services: Benefits, Risks and Intellectual Property Issues. *RESER Conference*, (pp. 230-242).
- [11] Chandran, S., & Angepat, M. (n.d). *Cloud Computing: Analysing the risks involved in cloud computing environments*. Retrieved May 2018, from <https://pdfs.semanticscholar.org/7a5c/d86eec4f687c070dd7a7967c5b4815981827.pdf>
- [12] Parns, J. (2016, February). *How to mitigate your cloud computing risks*. Retrieved May 2018, from IT ProPortal: <https://www.itproportal.com/2016/02/18/how-to-mitigate-your-cloud-computing-risks/>
- [13] Inuwa, U. (2015). The Risk and Challenges of Cloud Computing. *Int. Journal of Engineering Research and Applications*, 5-10.
- [14] Worlanyo, E. (2015). A Survey of Cloud Computing Security: Issues, Challenges and Solutions. 1-12.
- [15] Survey on Cloud Computing and Data Masking Techniques ,Priya dhir Research Scholar Phd.in Computer Application (RIMT UNIVERSITY)

server management

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

76/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

GRADING FORM: SMU GENERIC_GJ

MOHAMMED ABDULLA

52

RESEARCH-INFORMED LITERATURE



An excellent number of academically credible sources used.

KNOWLEDGE AND UNDERSTANDING



Good evidence of knowledge and understanding throughout the report. A very good effort overall.

23

ANALYSIS



Some excellent conclusions and synthesis - you obviously really took on board my feedback from the previous assignment. Very good work, Mohammed!

20

PRACTICAL APPLICATION AND DEP.



N/A - no marks assigned.

SKILLS FOR PROFESSIONAL PRAC.



A well-written and fairly nicely-presented report.
Good work.

9