Czech University of Life Sciences Prague

Faculty of Economics and Management

Bc. System Engineering and Informatics

Bachelor Thesis

CLOUD COMPUTING (WITH MICROSOFT AZURE AS A CASE STUDY

Meet Shah

©2020 CULS Prague

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Bc. Meet Himanshubhai Shah

Systems Engineering and Informatics

Thesis title : Cloud Computing and Microsoft Windows Azure platform

---

Objectives of thesis

This thesis is aimed at studying cloud services and their applicability in computing and general settings. The objectives of the study are hereby stated thus:

- To review cloud computing service and its effectiveness in today’s business world
- To explore Azure cloud service package and its significance in computing
- To critically evaluate some of the service options that are available in Microsoft Azure

Methodology

The core research method adopted for this thesis is explanatory research. The data collected for primary research was obtained from scientific sources like digital or printed literature published by established authors. The secondary data was collected by descriptive research. The studies is of theoretical nature, even though it includes realistic aspects regarding using the MWA platform and tools associated with i

The proposed extent of the thesis

30 – 40 pages

Keywords

loud computing, Cloud environment, Microsoft Azure, Scalability, Azure architecture, Azure app services, Azure AD, Media services, IaaS, PaaS.

Recommended information sources

Cloud Architecture Patterns: Using Microsoft Azure Book by Bill Wilder

COPELAND, Marshall, et al. Microsoft azure and cloud computing. In: Microsoft Azure. Application, Berkeley, CA, 2015. p. 3-26.

Exam Ref AZ-900 Microsoft Azure Fundamentals Book by Jim Cheshire

JENNINGS, Roger. Cloud computing with the Windows Azure platform. John Wiley & Sons, 2010.

LI, Henry. Introduction to windows azure. Springer, 2009.

Linux Academy

MicrosoG Windows Azure Development Cookbook Book by Neil Mackenzie

ROLOFF, Eduardo, et al. Evaluating high performance computing on the windows azure platform. In: 2012 IEEE FiGh International Conference on Cloud Computing. IEEE, 2012. p. 803-810.

Windows Azure Platform Book by Tejaswi Redkar

Expected date of thesis defence

2020/21 SS – FEM

The Bachelor Thesis Supervisor

Ing. Jan Tyrychtr, Ph.D.

Supervising department

Department of Information Engineering

Electronic approval: 19. 11. 2020	Electronic approval: 19. 11. 2020
Ing. Martin Pelikán, Ph.D.	**Ing. Martin Pelikán, Ph.D.**
Head of department	Dean

Declaration

I declare that I have worked on my bachelor thesis titled "Cloud Computing" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break copyrights of any their person.

In Prague on 11/1/2020 __________Meet Shah____________________

Acknowledgement

I would like to thank Ing. Jan Tyrychtr, Ph.D, for his advice and support during my work on this thesis.

CLOUD COMPUTING (WITH MICROSOFT AZURE AS A CASE STUDY)

Abstract

Cloud computing which presents users with a flexible avenue and broad network access to a range of configurable computing resources - from servers to storage, applications, services, and networks. It is distinctive from the traditional models due to its scalability, as well as the capabilities (such as on-demand self-service, broad network access, rapid elasticity, measured service provision and resource) that it enshrines. This is the reason cloud computing has been embraced and leveraged on across various industries. And, with the different deployment models that are available, there seems to be cloud service that can be utilized by virtually everyone. But despite its numerous advantages, cloud platforms are not without challenges, particularly with respect to security.

The objective of this thesis is to explore Microsoft Azure environment. The bachelor thesis begins by researcher laying a foundation with reference to the related studies that have been done in this area. The different architectural frameworks present in MS Azure are discussed. Subsequently, attention is given to the application services provided by MS Azure.

Keywords: Cloud computing, Cloud environment, Microsoft Azure, Scalability, Azure architecture, Azure app services, Azure AD, Media services, IaaS, PaaS.

CLOUDOVÉ VÝPOČTY (S PŘÍPADOVOU STUDIÍ MICROSOFT AZURE)

Abstrakt

Cloudové výpočty, které uživatelům nabízejí flexibilní cestu a široký síťový přístup k řadě konfigurovatelných výpočetních zdrojů - od serverů po úložiště, aplikace, služby a sítě. Vyznačuje se tradičními modely díky své škálovatelnosti a schopnostem (jako je samoobsluha na vyžádání, široký přístup k síti, rychlá pružnost, měřené poskytování služeb a zdroje), které zakotvuje. To je důvodem, proč je cloud computing zaveden a využíván v různých průmyslových odvětvích. S různými dostupnými modely nasazení se zdá, že existuje cloudová služba, kterou může využívat prakticky každý. Navzdory četným výhodám však cloudové platformy nejsou bez problémů, zejména pokud jde o bezpečnost.
Cílem této práce je prozkoumat platformu Microsoft Azure. Bakalářská práce je zahájena analýzou literární zdrojů s odkazováním na související studie, které byly v této oblasti provedeny. V dalším kroku jsou diskutovány různé architektonické rámce přítomné v Microsoft Azure. Následně je věnována pozornost aplikačním službám poskytovaným v cloudovém prostředá MS Azure.

Klíčová slova: Cloudové výpočty, cloudové prostředí, Microsoft Azure, škálovatelnost, architektura Azure, služby aplikací Azure, Azure AD, mediální služby, IaaS, PaaS.

Table of contents

List of pictures

List of abbreviations

IT – Information Technology

IaaS – Infrastructure as a Service

PaaS – Platform as a Service

SaaS – Software as a Service

EC2 – Elastic Compute Cloud

CRM – Customer Relationship Management

MIS – Management Information System

ERP – Enterprise Resource Planning

DBaaS – Database as a Service

I/O – Input/Output

LBVS – Load Balancing Virtual Storage

ACO – Ant Colony Optimization

NIST – National Institute of Standard and Technology

SSDLC – Secure Software Development Lifecycle

TLS – Transport Layer Security

SQL – Structured Query Language

CQRS – Command-and-Query Responsibility Segregation

VM – Virtual Machine

CDN – Content Delivery Network

HTTP – Hypertext Transfer Protocol

AMS – Azure Media Services

AD – Active Directory

API – Application Programming Interface

1. Introduction

Innovations across the IT world has always been centered on providing ways of doing things in a different, faster and cost-effective way by turning ideas into valuable resources. The world of technology is always looking for ways of making tasks easier for those at the forefront and even the users. In view of this, the researcher, in this study, will be looking at cloud computing with particular focus on Microsoft Azure. It has now become increasingly easy to run certain applications and achieve some notable feats in quick time. Cloud computing, by making available resources such as storage, applications, services and networks, has taken out the complexity that is usually encountered with monolithic networks to an appreciable extent. Cloud computing, being highly scalable due to its dynamic framework, makes a tremendous significance in many sectors – from the computing world to business industries. So, invariably, cloud computing is valuable in increasing productivity and also presents innovative measures through which tasks can be performed.

Specifically speaking, one of the greatest advantages of cloud computing is that it makes the delivery of self-service possible, and easy too as provisioning of computing capabilities can be achieved without the contribution of the service provider. This does not however limit access in any way, with the possibility of using client platforms feasible through workstations, laptops and/or mobile devices to actualize broad network access. This is more like integrating an old or conventional feature into modern technology – as cloud computing is perceived – to create advanced [and better] options/features. The broad nature of cloud computing is further buttressed by the fact that its multi-tenant model allows several consumers to have virtual and physical resources dynamically allocated to them simply through the pooling of the provider’s computing resources. However, that the consumer can activate the resourcing pooling feature on demand is one possibility, and the prospect of getting measured service is another; by this, the consumer is able to access the automatic control and optimization of cloud computing resources using metering capability that corresponds to the service type that is being accessed. It is yet interesting to note that all these possibilities on cloud computing comes at a highly scalable rate with the provisioning of capabilities occurring with prompt elasticity in consonance with the demand of the consumer.

A host of cloud service providers like Amazon, Azure, IBM and some others have been highly instrumental in building dynamic cloud environment/service options that consistently meet the need of an ever-emerging technology-conscious world. Cloud computing has been of great value across different sectors - from businesses to medicine, online entertainment, telecommunications, and education to mention but a few. This is unlike grid computing which utilizes numerous computers to handle a particular application. Talking about a provider that has been actively involved in initiating and updating repertoire of cloud services, we have Azure which is a brainchild of Microsoft and came into limelight in 2010. Hence, this study is intended to explore the capabilities of Azure with particular interest in the architectural layouts and media service provisions.

1.1. Cloud environment

Cloud environment is, more or less, about how a consumer attempts to utilize the resources that are made available by the service provider. To put this in a broader perspective, cloud environment, based on the type adapted, speaks volume of how much control a particular consumer will have over the network. In light of this, there are three major cloud environemts available to consumers; these include private cloud, hybrid cloud and public cloud. Private cloud is built for a particular organization that will have its own ports and servers, and this can either be off-premises or on-premises (Stephan et al., n.d). This sort of cloud deployment makes it possible to provide a single organization with an easily adaptive and effective means of requesting and using applications, virtual machines and other IT resources (Chappell, 2011). Community cloud has some similarities with private cloud albeit it is shared or utilized by a group of consumers that probably reserve some commonn interests, and the cloud infrastructure can be controlled or managed by a third party or any of the tenants. Hosting of the community cloud can also be achieved through a third-party server or internal servicer. On the other hand, the hybrid cloud environment as the name suggests, is hinged on combining two or more models. For instance, community and public deployment models (Mell & Grance, 2011). hybrid cloud is bound by a technology that is standardized to impart appreciable portability on applications and data (Stephan et al., n.d). Lastly, the public cloud is accessed through the internet and it is usually offered by a third-party service provider. This deployment model makes available a more secure and reliable data storage center [than some other storage models] as data are permanently stored in servers and access will only be upon authorization (Ou, 2015). The public cloud provider chooses the fundamental hardware that is required, and also open up the avenue for multiple organizations to deliver multiple service types (Hamdaqa & Tahvilldari, 2012).

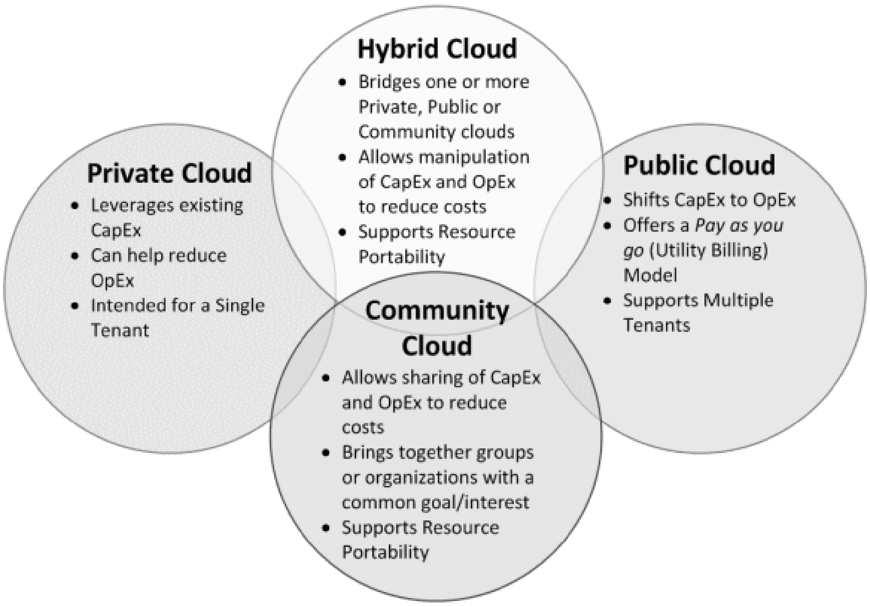

Hybrid Cloud
• Bridges one or more Private, Public or Community clouds
• Allows manipulation of CapEx and OpEx to reduce costs
• Supports Resource Portability
Private Cloud
• Leverages existing CapEx
• Can help reduce OpEx
• Intended for a Single Tenant
Public Cloud
• Shifts CapEx to OpEx
• Offers a Pay as you go (Utility Billing) Model
• Supports Multiple Tenants
Community Cloud
• Allows sharing of CapEx and OpEx to reduce costs
• Brings together groups or organizations with a common goal/interest
• Supports Resource Portability

Figure 1: showing a representation of the four cloud deployment models
Source: Jesús (2012)

1.2. Cloud computing models

Cloud computing models are a function of flexibility and management, and they do reflect the level of control that the service provider allows a user to have. It should not go without stating that the extent to which a user of cloud resources is able to manage a particular model may be determined by the expertise level. That said, there are a host of cloud computing models but the major ones are IaaS, PaaS and SaaS. Infrastructure as a Service (IaaS) is usually designed for IT specialists that have the (technical) know-how about the configuration of the software end of the data ecosystem, but do not intend to undertake the activities surrounding the management of the hardware (Magdalena et al., n.d). Amazon Elastic Compute Cloud (EC2) (Amazon ec2, 2015), IBM SmartCloud Enterprise (IBM SmartCloud Enterprise, 2015) and Microsoft Azure (Microsoft Azure, 2015) are among the most renowned IaaS cloud model providers. IaaS is viewed as the foundation layer for other cloud model, and some of its components include unity computing billing, communication network, virtualization environment, servers, hardware load balancer, Management and support services, high speed internet connectivity, disaster recovery system, virtual machine and service level agreements (Reese, 2009; Rittinghouse and Ransome, 2010).

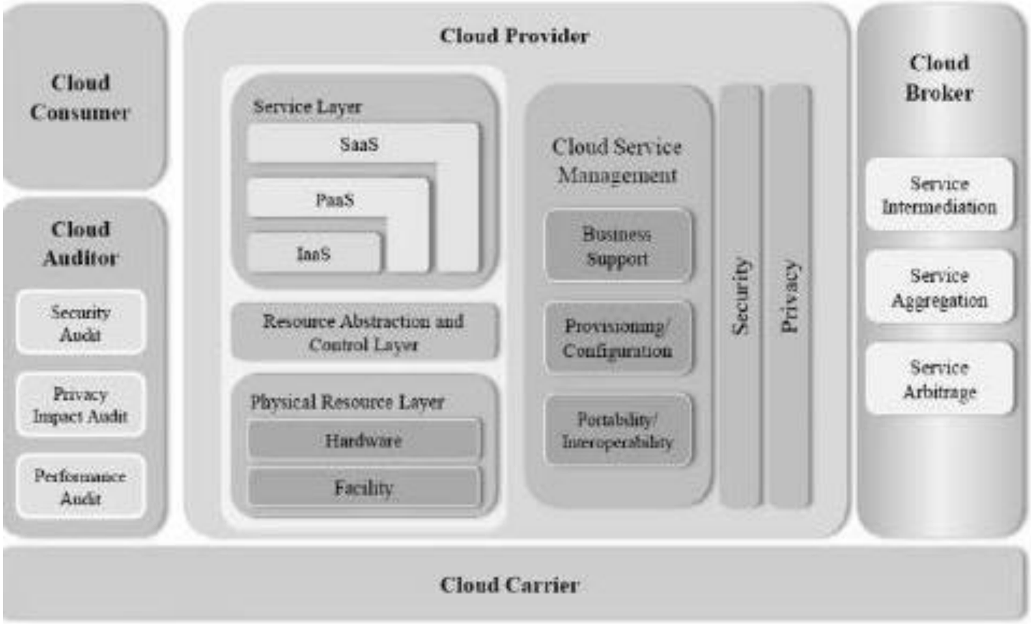


Figure 2: showing a typical cloud architecture

Source: NIST

However, with Platform as a Service (PaaS), the cloud service provider makes virtual machines and software available to developers who do not wish to be ingrained in the provisioning of storage, backup and servers required for the development and launching of applications (Butler, 2013). In addition to this, the provider also takes care of system administration on behalf of the developer. Some prominent providers of PaaS model are Google Compute Engine (Google Compute Engine, 2015) and Pivotal Cloud Foundry (Pivotal Cloud Foundry, 2015). On the otheer hand, Software as a Service (SaaS) is aimed at having users - possibly, those with little or no knowledge about the technical aspects of cloud computing - have access to the resource. Hence, the service provider offering SaaS, gets to oversee system administration, storage, applications, data, as well as, the service on the whole (Jackson, 2014). SaaS basically reflects the ‘on-demand’ characteristic of cloud computing, and it is usually more frequently updated than other conventional software. Customer relationship management (CRM), management information system (MIS) and enterprise resource planning (ERP) are some of the business applications in which this particular model is used (Kumar & Bhatt, 2017). Based on available statistics; PaaS is the most widely employed cloud model, accounting for an estimated 32% of all enterprise workloads while SaaS (24%) and IaaS (12%) follow in that order (BigCommerce, 2020).

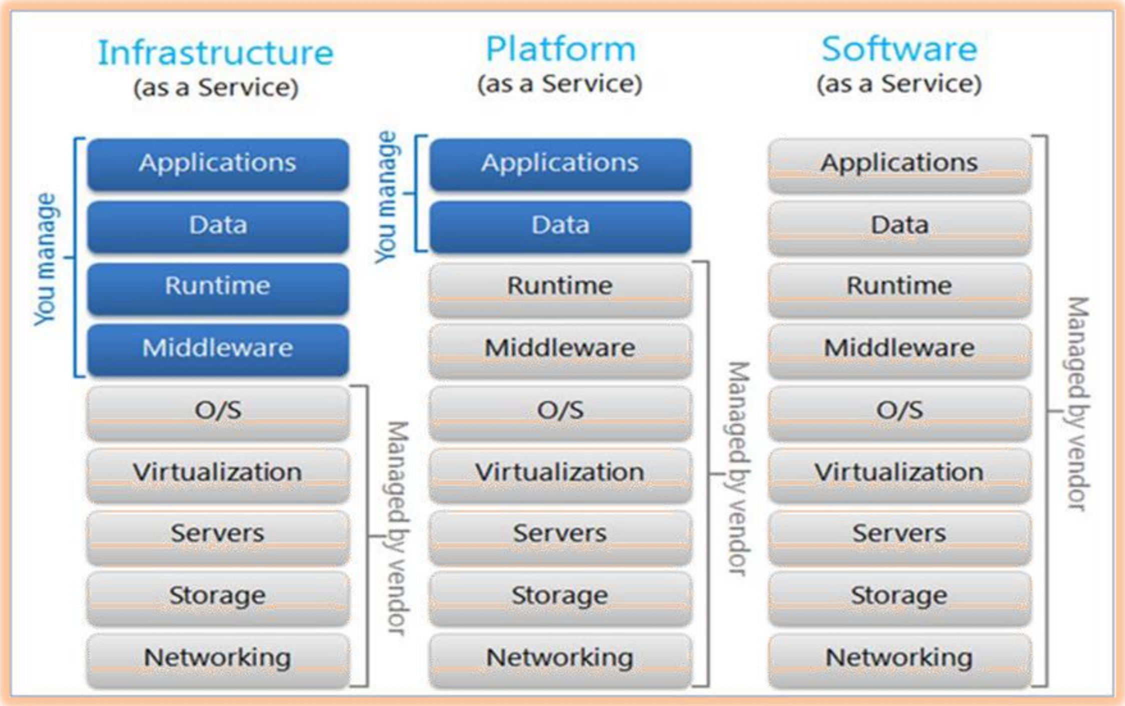


Figure 3: showing illustration of the three types of cloud models

Source: https://rajivramachandran.wordpress.com/2012/06/19/cloud-service-models-iaas-vs-paas-vs-saas/

Structure of thesis

In the first chapter of this thesis, some of the fundamentals of cloud computing will be discussed with particular mention of the types of cloud environment that exist, as well as the features and nmodels of cloud computing. Chapter two will be on the study objectives and methodology that will be employed in carrying out this reseasearch. Chapter three will be about literature review wherein the researcher will broadly touch on the subject matter from the perspective of relevant and related issues. The practical part will be discussed in the fourth chapter with focus on Microservices Architecture, Azure Media Service and Azure Directory. In the fifth chapter, the observations/results obtained from the practical part will be discussed and a conclusion will be drawn thereafter.

2.0. Objectives and Methodology

2.1. Objectives

This thesis is aimed at studying cloud services and their applicability in computing and general settings. The objectives of the study are hereby stated thus:

- To review cloud computing service and its effectiveness in today's business world
- To explore Azure cloud service package and its significance in computing
- To critically evaluate some of the service options that are available in Microsoft Azure

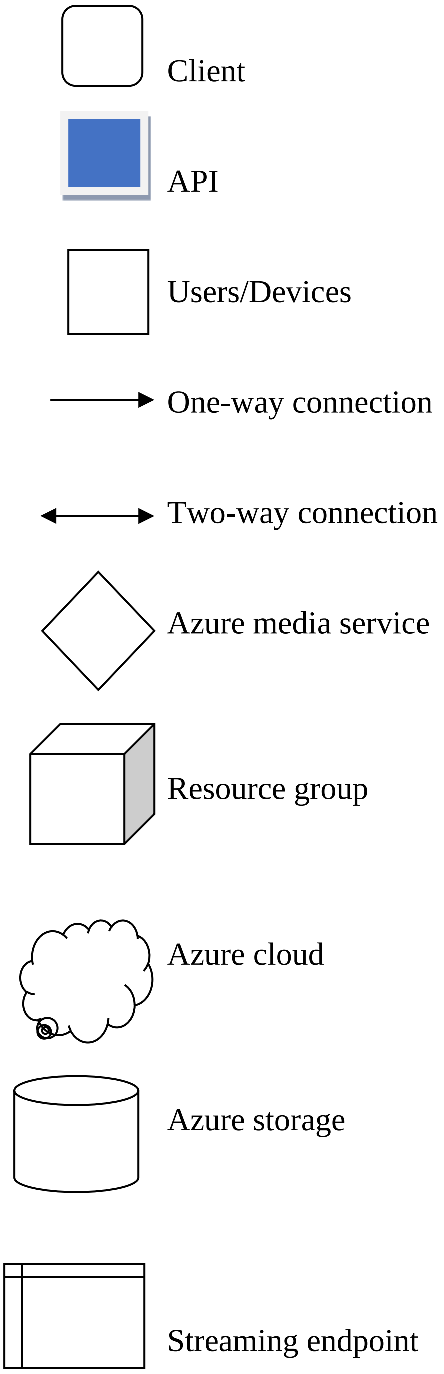
2.2. Methodology

In order to effectively actualize the objectives of this study, the methodology adopted for this study tilts towards the qualitative case study end, and followed by a descriptive analysis. This allows a substantial focus to be given to Microsoft Azure, a cloud computing option that is popularly used. Descriptive case study has been found useful in reporting concept that applies to real-life setting (Yin, 2003). The use of a case study allows the author to actualize an in-depth study of the concept of cloud computing, and this was even boosted by the choice of Microsoft Azure, which is well revered among other options available. The justification for the choosing qualitative case study is further backed by the need for garnering substantial knowledge – rather than evaluating statistical significance – on the subject matter (Flyvberg, 2007; Miller, 2004). Moreover, the scope of the researcher is primarily on understanding how certain components and/or features of cloud computing – Azure to be more specific – work, and does not entail finding correlations between any variables.

Furthermore, owing to the broadness of the whole package of Microsoft Azure, it is incumbent for the author, at this stage, to concentrate on a particular service type present in Azure. To this end, the author has chosen to evaluate the services present in Azure App Service – Azure Active Directory (AD), Azure Media Services (AMS), in particular.

The author had recourse to a host of reliable secondary sources to extract relevant data, and also took out time to have a firsthand experience of the elements that are ingrained in the aforementioned services. Ultimately, the author also had a practical experience of how the components of these services function on the basic level. In effect, the direct observation of the author and retrieval of data from multiple sources (Baxter & Jack, 2014) were highly valuable in achieving the objectives of this thesis.

Symbol Representation



⬡ Live encoder

▲ Azure active directory

▲ On-premise active directory

✴ Security token service

🟧 Office 365

☁ ⬚ Cloud where all the different application and Azure Active Directory is present

3. Literature Review

3.1. Overview

There has been a vast array of research studies that have been piloted and concluded in the area of study, and the focus shall be on some of these (works) in this section. The related work will be examined under certain subheadings that are in consonance with the concepts or issues to be discussed.

Cloud computing can be viewed as the culmination of the evolution that has revolved round grid computing, utility computing, application service providers, Software as a Service and then cloud (Stark, 2012). However, it can be distinguished from the conventional computing models on the basis of its scalability (Foster et al., 2008). Cloud computing which presents users with a flexible avenue and broad network access to a range of configurable computing resources (Mell & Grance, 2011). The measurable and subscription-based virtualized resources available through cloud computing make it possible to meet various computational needs without the need for extra or additional hardware or large physical infrastructure (Aoun et al., 2010).

According to Khajeh-Hosseini et al. (2010), cloud computing registers as a disruptive technology that redresses the deployment of IT systems in organizations due to its low cost and non-complex nature. The success of cloud computing has been majorly down to the virtualization technique it employs, as well as, high-speed internet access that has made its applicability flow through with ease; making it (i.e., cloud computing) one of the fastest growing areas in IT industry (Armbrust et al., 2009; Buyya et al., 2009). Virtualization, in particular, enables the packaging of bits of the cloud application with all the features - middleware, database and operating system - that are required to run it (Giacomo & Brunzel, 2010).

Tasks or activities taking place within the cloud ecosystem are executed by five main actors (Liu et al., 2011); among which are: i.) Cloud provider who is responsible for the management and operation of the infrastructure, along with see to the requests of the consumers; ii.) Cloud consumer, the organization or individual that utilizes the ecosystem to advance the cause of predefined objectives or goals; iii.) Cloud broker, who serves as the middleman [upon the request of the consumer] to negotiate the service - with the provider; iv.) Cloud carrier in charge of the management of service routing and connectivity between the provider and the consumer; AND v.) Cloud auditor who exists as an independent entity that evaluates service performance in view of determining the extent to which standard is being upheld.

3.1.1. Cloud computing database

As with other aspects of computing, the impact of database in cloud computing is one that cannot be overemphasized especially when we factor the weight of information that are stored and processed therein – in the cloud system. It is in respect of this that some researchers put forward a benchmark for the database solutions that are offered as DataBase as a Service (DBaaS) by some cloud service providers (Abourezq and Idrissi (2016).

Ferretti et al. (2012) proposed an architecture that is capable of achieving an appreciable degree of scalability and availability like what is attainable with cloud database services that are without encryption thus eliminating the need for any intermediary components. This architecture imposes significant data consistency in a scenario whereby various clients are running SQL queries in a simultaneous manner with an imminent change of the database configuration.

A methodology concerned with how to move applications to cloud was developed by Strauch et al. (2014). The authors, in their methodology, weighed up a number of important areas like data confidentiality and the disparity in granularity of interactions. Furthermore, it is imperative to give some leeway in order to allow the application interact with remote data sources. In the methodology put forward by Strauch et al. (2014), all the aspects mentioned above have been looked at. The authors also came up with a contrivance which dealt with the movement of data, decision support and application refactoring. The created mechanism gave assistance to the developers in their attempt to get an understanding of the proposed methodology. Strauch et al. (2014) employed the use of a case study examination in alliance with an IT firm, to assess the propounded scheme and instrument.

In their paper published in 2014, Alomari et al placed particular attention on the barriers and issues with which the concept of data transfer between various cloud storage is faced. They (the authors) hypothesized a framework for data and an API for the development of NoSQL databases in cloud storage in compliance with the modern standards. To implement the model they proposed, Alomari et al (2014) incorporated three prominent NoSQL systems - Amazon SimpleDB, MongoDB and Google Datastore. The propounded model was made in such a manner that it could be applied to other NoSQL systems; this is only due to the fact that it has a great degree of adaptability. Over and above that, included in the framework are some mechanisms developed to give backing to adaptation, data transformation and exchange. To elucidate on the architecture and application of the model they put forward, the authors utilized a case study.

3.1.2. Load Balancing

Load balancing allows the even distribution of working processes [involved in cloud computing] between multiple computers for efficient and optimal performance (MacVitte, 2009). In essence, load balancing algorithms in cloud computing environments will bring about an improvement in response time with the system's total load being distributed, but it remains a complex task regardless - due to the concerns over reliability, security and throughput (Moharana et al., 2013).

Load balancing algorithms can belong in any of two groups - Static load balancing algorithm and Dynamic load balancing algorithm. In the dynamic framework, the former state of the nodes is normally considered while such is not the case with static load balancers (Moharana et al., 2013).

Chaczko et al. (2011) proposed the weighted round-robin algorithm which is a static load balancing model that was designed to address the incidence of heavily loaded nodes that is feasible with the conventional round-robin algorithm. Each of the nodes in the weighted round-robin algorithm is allotted a specific weight which ultimately determines the number of requests it (i.e., the node) will receive. This algorithm may however fall short when it comes to its applicability in cloud computing, since it is not possible to precisely predict the execution time in cloud environment.

Zhao and Huang (2009) proposed the Compare and Balance algorithm to solve the load balancing problem commonly encountered among physical hosts by adaptive live virtual machine migration in intra-cloud environment. In this algorithm, the reduction of the migration time of virtual machines is achieved through the implementation of a load balancing model; this leads to the zero-downtime of virtual machines even as it balances the load among the servers based on the processor or I/O usage. Additionally, there is a distributed compare and balance load balancing algorithm that ensures the migration of virtual machines from high-cost host to low-cost host with the (weak) assumption that every physical host has sufficient memory.

The load balancing virtual storage strategy (LBVS) technique that centers on cloud storage to provide storage as a service model and large-scale net data storage model was proposed by Liu et al. (2010). In this framework, two (load balancing) modules are utilized for the actualization of load balancing while the virtualization is storage is ensured through a three-layered architecture. This technique effectively enhances the capacity of disaster recovery and reduces response time as the efficiency of concurrent access is boosted through the use of replica balancing. On the whole, the LBVS technique brings about significant optimization as reflected by the improved storage resource use rate and the flexibility of the system.

Stanojevic et al. (2009) proposed the CARTRON, a simple and easily implementable model that was basically created to effect unification between the use of load balancing model and distributed rate limiting model. The load balancing model ensures the equal distribution of tasks to various servers in order to minimize associated costs while the distributed rate limiting model allows the distribution of resources in such a manner that promotes fair allocation. The distributed rate limiting can help in achieving equal performance levels by adapting to server capacities for the dynamic workloads.

Gao and Wu (2015) proposed the Ant Colony Optimization (ACO) framework to dynamically balance the workload in a cloud environment - this dynamic load balancing is actualized through the reduction of searching time. More specifically, the ACO framework employs the max-min rules and forward-backward ant mechanism to sort out the candidate nodes required for load balancing. The authors also initialized and updated pheromone based on the physical resources in the cloud environment. Furthermore, they highlighted the probability of the ants moving in two different ways - to decipher whether or not the forward ant meets the backward ant in the neighbor node. This is intended for the purpose of ensuring the acceleration of the searching processes. It was also observed that this framework allowed for optimized network performance even with medium and heavily loaded nodes.

3.1.3 Security-related issues in cloud computing

The problem with the security is one very weighty topic for discussing as regards the demerits of Cloud computing. For this reason, any company that has taken interest in picking up on this technology should ensure that they would voluntarily give up delicate information to a third-party provider of cloud services. Making such information available could render the company vulnerable, and could potentially jeopardize them. This, therefore, justifies the reason for which the choice that one makes pertaining to cloud service providers has to be top notch. The action of acquiring the services of trustworthy service providers needs to be stressed on, and necessitated so as to guarantee safe keeping of the sensitive credentials of the company (Leung, n.d). In particular, security is crucial to the successful operation/utilization of a cloud computing framework as the associated challenges are enormous and often evolve through time (Khorshed et al., 2012). As a matter of fact, cloud-based services are not immune to the most of the common attacks directed at computer networks (Ahmed & Hossain, 2014). The personal data security of the user (King and Raja, 2012) and data location (Teneyuca, 2011) are of significant concern in this regard. By and large, the central security issues in cloud computing hang on data integrity and data confidentiality. Besides the technical side of security, the strategic policies of the provider are also crucial to ensuring the security of the users' data (Joint & Baker, 2011).

In two separate researches, conducted by Bouayad et al. (2012), and Behl & Behl (2013), well-explained and comprehensive analyses were carried out on the complications that can be found in cloud security. The two bodies of work are very similar, in that they used the approach of cloud architecture, characteristics or features offered by the cloud, the service delivery paradigms employed by the cloud, and the stakeholders' that are affiliated with the cloud in one way or the other in conducting an investigative study with reference to the underlying issue.

A synopsis on the core issues connected with cloud security was highlighted in the research conducted by Bouayad et al (2012). First, it was pointed out that a number of the challenges faced (relating to security) are birthed from technologies that are put to use - SOA and virtualization are excellent instances. Again, Multi-tenancy and isolation are two major aspects of the problems of cloud security that demand solutions - of the vertical sort - starting from the SaaS layer down to the physical end. For the supervision and handling of the array of requirements and regulations given, the importance of security management cannot be downplayed in any way, as it is very vital. Finally, a holistic security shield should be provided for the cloud paradigm. As has been stated in the previous paragraph, some security implications are as a result of the basic technologies that form the foundation upon which Cloud Computing, this includes virtualization. The proper manning of security concerning the cloud is very vital in the quest to control and supervise the user facing data and the mode through which the provider's framework operates. Another field that calls for undivided attention in order to prevent potential attacks on the resources of the victims by other users with malicious intent is Multi-tenancy. On a closing note, a holistic security shield should be employed to guard the cloud paradigm; the essence of this is to ensure that any object that moves through the cloud environment be subjected to multiple checks at different levels/layers of security solutions.

As earlier stated in the point above, the company becomes susceptible to external attacks and threats from hackers the moment their information is reposited on the cloud. Jaiswal (2018) submitted that it is not in any way uncommon to see cloud service providers being victims of constant cyber-attacks; for the fact that several organizations have entrusted their information into the care of Cloud service providers (which they store in their repositories), they cannot afford to be compromised. He emphasized that over the years, there have been some notable attacks against the cloud. Among these is 'Man in the cloud attack', which describes a method that was dredged up in recent times; it focuses mainly on attempting to obtain the synchronization token of a cloud user. To shed more light on what a synchronization token is, we refer to either as a file kept in the cloud, users' device in a directory, a registry or in windows credential manager. So, the assailant is often able to access the local files of the victim by ambushing them (the user), with malwares embedded in websites or sent through emails. In swapping the cloud synchronization token with another that hints in the direction of the attacker's cloud account and entrenching the initial token in the ensemble of files that are poised to undergo synchronization, the victim is manipulated or baited to upload their very own token to the attacker - albeit, they do not actually intend to do so. Finally, the token can be utilized by the assailant to gain entry into the user's cloud account and have the chance to view and steal the victim's cloud information with no restrictions whatsoever. Another form of attack that can be targeted on cloud is Distributed denial of service attacks. As seen with traditional DDoS attacks, numerous systems overload a target server; this causes the servers to be unresponsive, and then reduces their efficiency to carry out all activities that are expected, eventually causing the systems to come to a halt. During the 2016 Dyn attack, it was easily perceptible that websites with far-reaching servers like Twitter and Amazon became inaccessible to their customers.

According to another study done in 2012 by Behl & Behl, quite a number of the major challenges concerning how cloud-conscious security solutions can be executed have been the object of scrutiny in the research. They have also asked questions on what degree of credibility can be attached to the security and protection of information in a cloud computing environment. They have made suggestions for Cloud Computing security solutions to keep on applying their solutions till the point where there are no doubts on the privacy of the consumer/tenant's data; drawing inference from their analysis. In line with the findings of Behl & Behl (2012), the problems relating to vivid cloud security and the aim to proffer a solution to a wide range of cloud security issues have been placed under intense examination.

In a 2013 study conducted by Chalse, Selokar and Katara, a thorough analysis on problems with which cloud security is faced was done. Also, the different problem in a cloud computing system and their effect upon cloud users, various computing system and organizations are analyzed. The varying challenges that can be encountered in a cloud computing system and what consequence they could exert on the cloud users, were also broke down in this study. The researchers are of the opinion that being a field that is still in its early stages of development, numerous problems in data storage security with respect to Cloud Computing have still not been discovered - even as it is an aspect of computing that is infested with difficulties, not to forget its great significance. The design and development of this research are deeply rooted in the utilization of Public and Private systems of data encryption. To render it more realistic as an application of Cloud computing, more backing is given to the principles of dynamic outsourcing of information. The authors were of the impression that activities carried out for the purpose of mapping out what the security of the cloud architecture would require, and research on the development of a number of security algorithms that can be applied to cloud systems would be continued. From the study of Chalse, Selokar & Katar conducted in 2013, the security algorithms being discussed could either be software based - this implies that it could apply techniques such as encryption - or Hardware based, in this case, it is possible to employ the use of disk encryption hardware. As a consequence, it will give some help in the eventual quest to make the security guarding more formidable, and in the end, gradually cause the fear and uncertainty of data security that has been instigated in the minds of the users (of Cloud Computing and the resources it offers) to be expelled (Chalse, Selokar & Katara, 2013).

In accordance with the SSDLC, the Cloud SSDLC is comprised of five major phases: Initiation, development, implementation, operation, and destruction. When observed from the viewpoint of the government and industry, the cases that can be employed in the process of showing usage and legal issues pertaining to the proposed Cloud SSDLC are variable. According to Kao et al. (2012), there are three major ways through which they contribute to the cause. They help by providing a structure that bridges the lacuna between the SSDLC and the cloud computing model that is used to bolster the security protecting cloud applications, and also, via defining the critical issues bordering on the security in each phase of cloud service development. Again, it helps to augment and increase the level of effectiveness of the proposed framework, so as to identify and examine a genuine case in government cloud services migrations.

In a research by Jensen et al. (2009), the technical matters pertaining to security in Cloud Computing, were brought forth; the said problems had more affiliation with the challenges of web services and web browsers than they did in any case with cloud computing. This is not to say, however that the issues are of no importance in Cloud Computing, the significance they have to Cloud Computing cannot be downplayed, as the problems are of great value due to the fact that, for full access to the services made available by the cloud, Cloud computing utilizes a wide range of web services and is hugely dependent on web browsers. One of the more ubiquitously observed attacks on web services is the XML Signature Element Wrapping. Here, the XML signature is the tool that grants admittance (Jensen et al., 2009).

One other significant talking point in Cloud Computing is the issue of Browser Security, seeing as a larger portion of the computations done on the cloud is carried out using remote servers. The client PC, on the other hand, is used solely for I/O operations and at the times where/when commands need to be authorized to the cloud. The standard web browser hence became a necessity for scenarios that were concerned with sending of I/O; a lot of elements including web applications, web 2.0 and Software as services (SaaS) employed its use. Concerns were thereupon raised on security due to the use of web browsers. Coming into the fray then as some important means of mitigation is the Transport Layer Security which is utilized in data encryption and authentication of hosts. In this case (of browsers), XML signature otherwise known as XML encryption, cannot be applied straight out, as the encryption of data can only be carried out with the use of TLS and signatures only work hand in hand with the TLS handshake. What this alludes, is that the browser only acts as a passive means of storage for data (Jensen et al., 2009).

A schema-mapping model, Chunk Folding was proposed by Stefan et al. (2008); this allowed certain tables shared among tenants were mapped into fixed generic structures. The model described here brought about the actualization of a multi-tenant physical schema through the extension of the conventional method whereby multiple single-tenant logical schemas in the application are mapped. The model is hinged on handling large databases that could have over 100,000 tables. The limitation of this proposed model, however, lies in the scalability, with the large number of tables affecting its scalability.

3.2. Microsoft Azure

Microsoft Azure came to the limelight in 2010 whereupon it was named “Windows Azure” at inception, and it has since made huge leaps and bounds. Azure is reported to be utilized by 95% of the companies ranked in the Fortune 500 list and a host of government agencies around the globe (Altaiar, Lee, and Pena, 2019). It currently supports services across the three major cloud computing models - SaaS, PaaS and IaaS. Some of the notable advantages of Microsoft Azure include its easy scaling quality, the support it has for any desirable language and more importantly, the way it allows the quick configuration, deployment and management of applications across Microsoft data centers on a global scale (Di Martino, 2014). Azure does not only allow vertical and horizontal scalability, it is also geographically scalable for boosting resilience and reducing latency (Altaiar, Lee and Pena, 2019).

Microsoft defines Azure as “a comprehensive set of cloud services that developers and IT professionals use to build, deploy, and manage applications through our global network of data centers. Integrated tools, DevOps, and a marketplace support you in efficiently building anything from simple mobile apps to internet-scale solutions.”

3.2.1 Services available on Azure

The range of services provided on Azure is appreciably vast, and this is one of the factors that inform its flexibility. As it features services and tools that enhance the productivity of data analysts, data scientists and data scientists, so does it enable the possibilities of effectively managing the identity and access of the user (Shaukat et al., 2016). Service selection on Azure is as follows:

Compute: A scalable on-demand infrastructure that can adapt to the dynamic needs of business like scalable back-end created for mobile solutions and the deployment of infrastructure for web applications.

Data services: Data services on Azure represents cloud storage, backup and recovery models - with considerable scalability - set up for any data; these include Hadoop solution, relational databases and cache super-fast access.

App Services: These entail test and development of fast and flexible applications, coupled with media services that enable scalability and cost-effective distribution of media and cloud identity services. App services are usually available at a reduced cost. *App services will be discussed in details later on in the thesis.*

Network: This concerns the connections existing between data centers and infrastructure or the creation of virtual private networks, and it is basically augmented with a traffic load balancing service.

3.2.2 Security in Azure

Security is a vital aspect of cloud computing and this is definitely not lost on Microsoft with the company having invested so much into ensuring an assuring security system in Azure - as it does for majority of its other products. As Azure is concerned, the following tools are used in guaranteeing that the integrity of data is not breached (Altaiar et al., 2019):

- Web Application Firewall: This is made available by Azure Application Gateway and it is in place to ensure that non-valid requests are shut of the network - with the valid ones being allowed access. Furthermore, authorization and authentication are provided through Azure Active Directory to embolden the security framework. Authorization ensures that role-based access is only granted to those that have been predefined to handle specific tasks or specific capabilities while authentication is effected to ascertain that the network is inaccessible without the right credentials.

Additionally, virtual network connected with Azure services will also ensure that data points are not accessible by the public even though when others present within the cloud environment - only users present in the same virtual network will be able to link up with each other.

- Row-level security and Column-level security: These two features are available on Azure SQL, and they function to check access into rows (row-level security) and columns (column-level security) that are featured in the table of the database. Besides these, there are other sophisticated features on Azure SQL to ensure data protection and also the adherence of users to regulatory standards.

Machine learning and Artificial Intelligence are also used to great effect in establishing data protection in Azure Synapse Analytics.

- Key Vault: The key vault, as the name implies, is created by Azure to help users have a safe storage tool for sensitive credentials/data like passwords and some confidential information. More so, with this (key vault), the creation of encryption keys and management of certificates are also achievable by the user.

4. Practical Part

The objective of this section is to discuss the practical aspect of the thesis. The practical was basically carried out on the architectural layout of Azure cloud, with the researcher majoring on the Microservices architecture and Command-and-Query Responsibility Segregation architecture. The Microservices architecture was configured for an online book library service where subscribers are able to access some articles and books. Furthermore, Azure Media Service (AMS) was configured to livestream an event in which the researcher was involved, and the Active Directory was configured to manage the identity of some users that subscribed to access files on Microsoft Suite 360. All these enabled the researcher to have a first-hand experience of how the services work.

4.1. Architecture in Azure

There are seven different architecture styles that can be achieved with Azure, and the selection is usually based on the service model of choice. Each of these styles is adapted for certain constraints to establish specific properties. The constraints guide into choosing an architecture style that will be appropriate for the creating independent service deployment and keeping the cloud updated (Microsoft, 2017). As earlier stated, the Microservices architectural layout is the focus of this practical – as Azure architecture is concerned.

4.1.1. Microservices Architecture

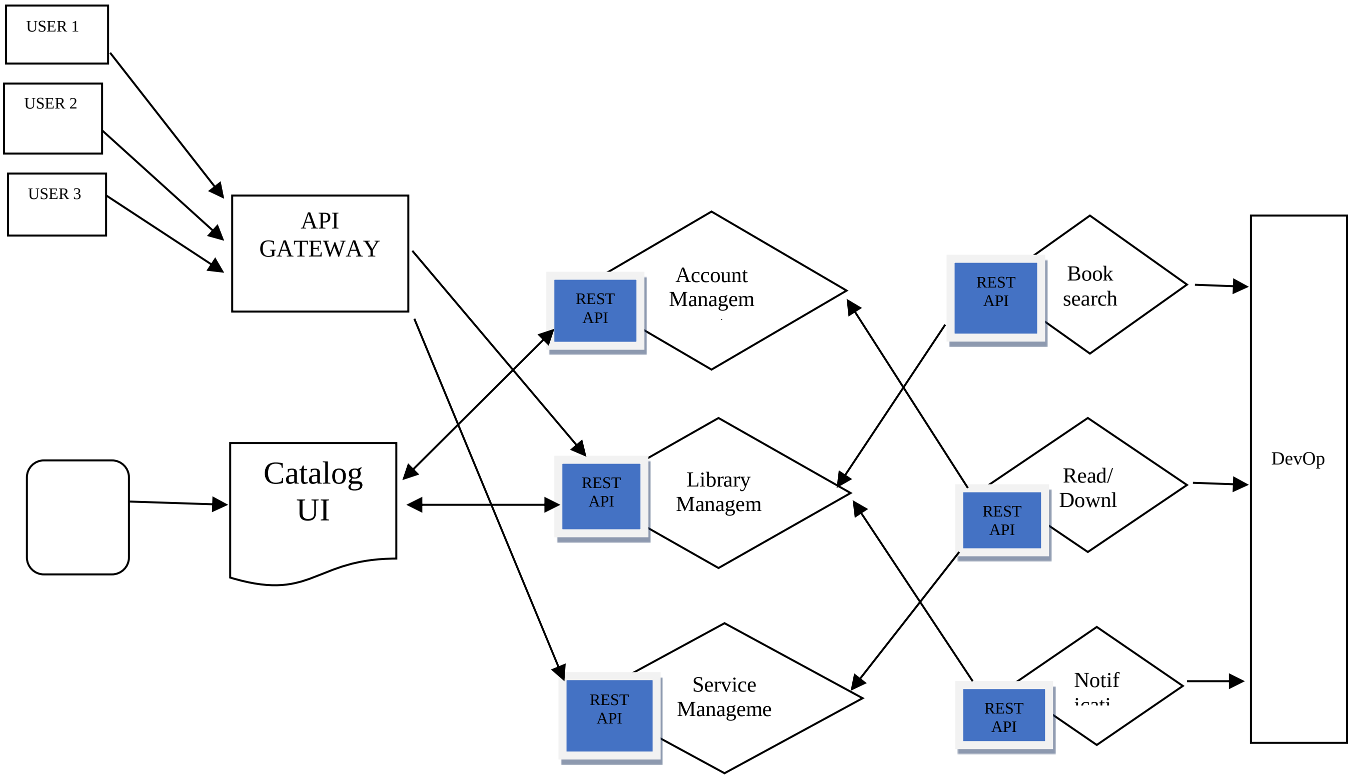


Figure 4: Microservices architecture (Own work)

The above schematic representation shows the deployment of microservices architecture for an online library service wherein user accounts management, book search and book delivery [via download] are taken care of by individual components.

4.2. Azure App Services

Azure App service encompasses the set of services that are available to drive the development, deployment and maintenance of several applications that are featured on the (Azure) platform. The services here include Active Directory, Azure scheduler, Azure AI, Azure Media Service, Azure Analytics and Azure IoT. Here, I shall be looking at Azure Media services and Azure Active Directory.

4.2.1. Azure Media Service

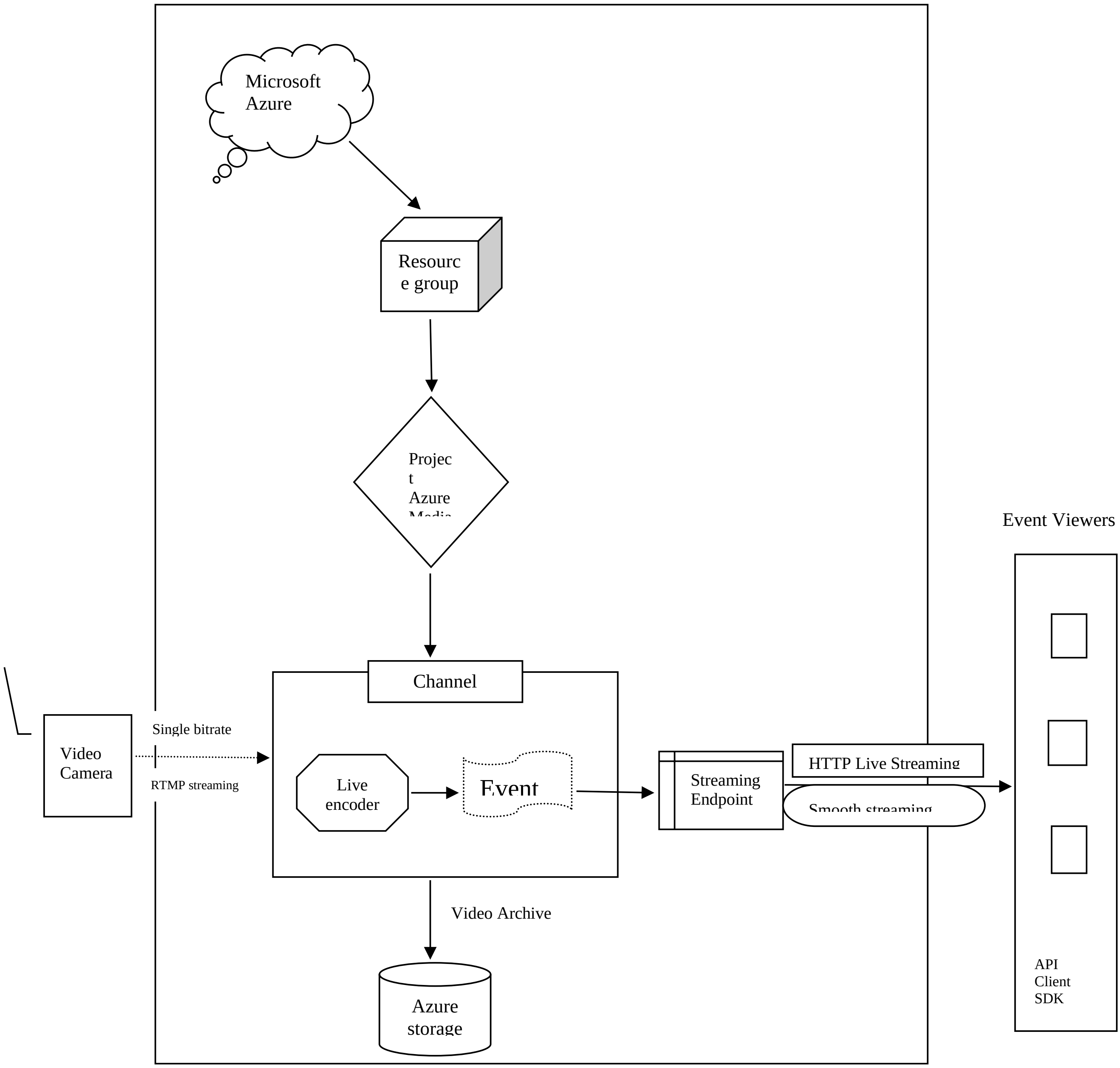


Figure 5: Schematic representation of live streaming event on Azure media service (Own Work)

The above figure outlines the processes involved in creating the live stream of an event using Azure media service. It started with the creation of a resource group and a media service (i.e., project media service) that is specific for the purpose of this study. It also involved the creation of a storage account for the provision of video-on-demand. Having undertaken series of sub-steps, the project channel, live event (to be streamed) and the streaming endpoint were created. To input the video stream, the OBS was installed and configured with the URL for the media server ingested.

4.2.2. Azure Active Directory

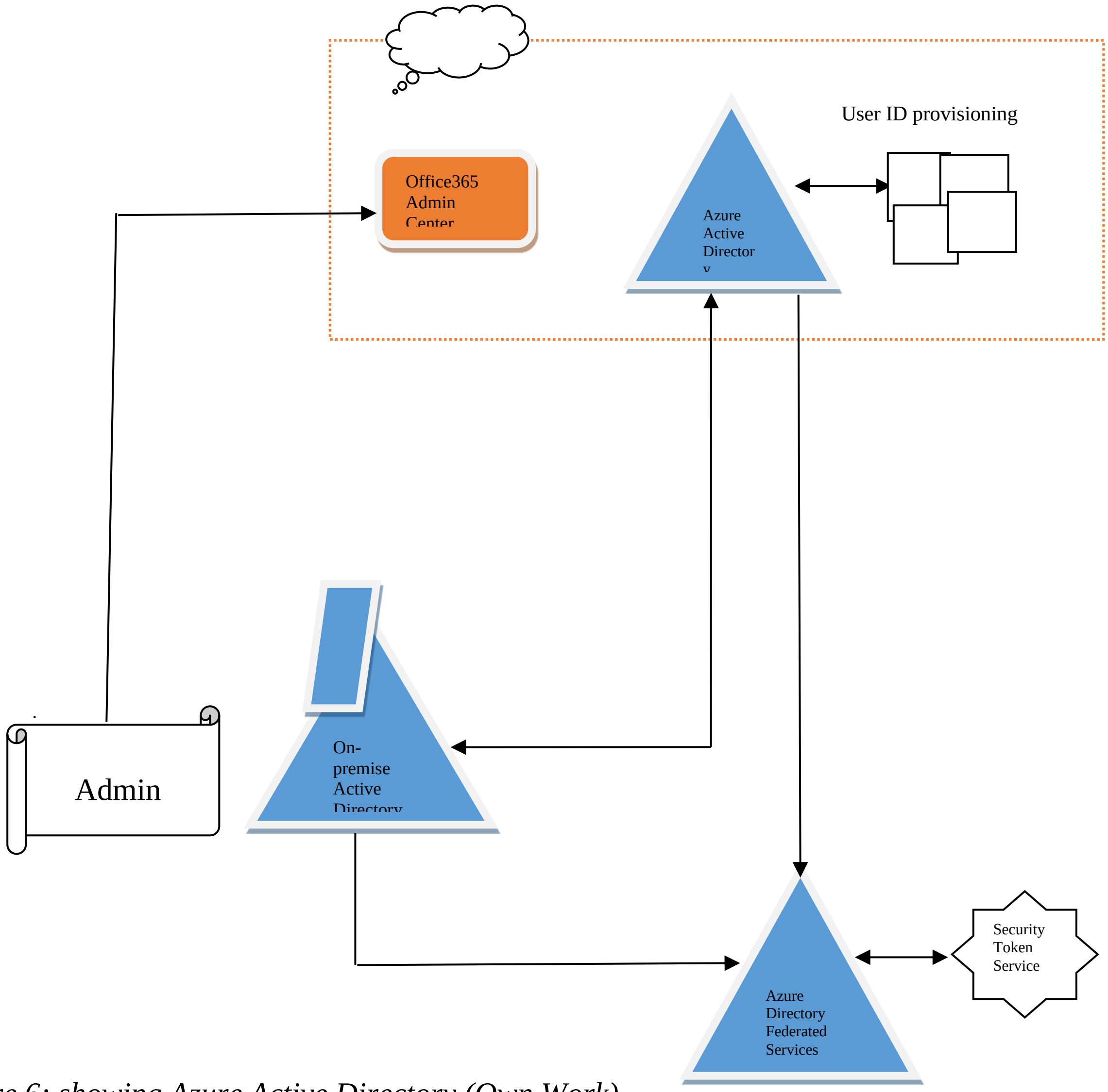


Figure 6: showing Azure Active Directory (Own Work)

The above figure shows a schematic representation of the Azure Active Directory setup that was used in managing the identity and authentication of users gaining access into cloud to use Microsoft office 365 suite. The users were synced from the on-premises Active Directory to Azure Active Directory using Azure AD connect.

5. Results and Discussion

In this chapter, the findings from the practical will now be discussed in this chapter with particular attention on the architectural layouts, Azure active directory and Azure media services.

5.1. Architecture in Azure

As earlier emphasized, there are seven architectural layouts that can be accessed on Azure and each of these (layouts) is designed to cater to different functionalities or tasks. There are instances whereby two architectural layouts can be combined for the purpose of efficiency. However, the discussion shall be based on the Microservices and Command-and-Query Responsibility Segregation (CQRS) architectural layouts.

5.1.1. Microservices Architecture

The microservices architecture entails small services that are deployed independently without the necessity for profound coordination between teams - communication takes place via API contracts under this architecture. It should not go without stressing that the availability of numerous small services and its many moving parts could pose a great challenge. That said, that this architecture permits the stacking of mixed technology, isolation of fault and granular scaling further speak volume of its suitability for the objective upon which it was set. Each of the services will ensure its own data persistence, and with this architecture, there is no need for a rebuilding process in the event of initiating updates. The identity provider in the layout made it possible to implement the authentication of the clients before access can be granted for the service request to be processed.

Components such as API gateway, management and service discovery are present in the architecture to make the deployment of services flow smoothly. The API gateway is considerably versatile in its functions; first off, it is the intermediary between the clients and the back-end of the services. Additionally, it allows for the versioning of services – that is, users' account management, book search, book delivery – even without updating all the clients, and also serves logging, load balancing, authentication and SSL termination needs. On the other hand, orchestration handles the positioning of services on nodes while service discovery ensures the maintenance of services list.

Microservices architecture can be viewed as creating a means through which complex or large applications can be adequately managed to impact increase in scalability, velocity and resilience. From the simulation provided in the practical session on microservices architecture, it was observed that users were able to easily and quickly access their favorite books on the platform.

5.2. Azure App Services

The discussion here will be based on two features on Azure App Services which are developed to help actualize and/or perform different tasks. Azure Media Services (AMS) and Azure Active Directory (AD) will be brought into perspective.

5.2.1. Azure Media Services (AMS)

Azure Media Services function based on REST APIs and register as an extensible cloud-based platform through which end-to-end workflows can be created. More specifically, AMS incorporates robust and highly scalable encryption, encoding and streaming features to create top-quality video contents to a vast array of audience on different digital devices. Media processing revolves round obtaining media processor instance, encoding, packaging and protecting contents. With AMS, it is easy to broadcast high-bandwidth contents to end consumers at a low latency and high availability rate, and the security of the content is also guaranteed – Azure media services offer updated and highly efficient encryption for live-streams and video on demand (Britch et al., 2014). This was obvious from the result of the research carried in *practical 3* wherein I was able to use Azure media service to successfully run the live stream of a video with a couple of end-users involved. The streaming endpoint made it possible to get the live event across to the user application. More so, it is through the streaming endpoint that the live event gets to the content delivery network for wider distribution.

Video-on-demand asset is usually stored as adaptive bitrate MP4 file set as it is a dynamic packaging. Dynamic packaging is performed by origin servers which are known to package source media upon the request of a video format, and this ultimately triggering the encoding of the video. The video is subsequently made available [in real-time] in the particular format that the client that the client requested (Britch et al., 2014). The other means through which contents are packaged in Azure Media Services is Static packaging;

this is performed by Azure media packager, and it entails the creation of contents in the format requested by a user.

Users can access videos in media services via offline viewing, streaming, progressive downloading, streaming and adaptive bitrate streaming. It is however important to state that locators are needed in order to access contents that are present within AMS. A locator functions to provide entry point to access files while the access policy is established to highlight the permission and timeframe that a client is allowed access to a specific asset. Two types of locators exist; they are *on-demand origin locator* and *shared access signature locator.* The on-demand origin locator is normally open to the Media Service Origin servers that obtain media contents from Azure storage for eventual delivery to the client; this locator type is suitable for granting access to streaming contents and makes certain cache control, CDN authentication and IP restriction. On the other hand, the shared access signature locator, which is adapted to granting access to blob container of (media) asset within Azure storage, allows users to be granted for a defined duration and specific operations (Britch et al., 2014).

The adaptive bitrate streaming appears to be the most advanced option as it enables client applications to deduce the condition of the network and then adapt the video’s data rate to the obtainable bandwidth (Britch et al., 2014). As a result of this, unhindered viewing is assured as client will automatically select lower bitrate version of the media content once network communication trails a declining state and return to the standard (higher) bitrate once there is an improvement in network communication. Adaptive bitrate streaming is presently supported by MPEG DASH, HTTP Live Streaming (HLS) and smooth streaming.

The processing of outbound videos is also possible with Azure Media Services. Files are retrieved from Azure storage and then sent to Content Delivery Networks (CDN) or directly to client applications with origin servers capable of handling multiple requests every second even as they offer dynamic packaging services and ensure dynamic encryption.

5.2.2. Azure Active Directory (AD)

Azure Active Directory is an identity management service that enables sign-on and access to certain internal resources [like the intranet] and external resources [like Office

365, Azure cloud portal and a host of SaaS applications]. Regrading the experiment from this study, I observed that users whose secret information was not previously entered or created in the Azure Active Directory did not gain access into the Microsoft 365 suite – this serves as a sort of evaluation yardstick. Going forward, Azure AD is available in four different versions; this is majorly based on the subscription type, and as such, we have the Azure AD Basic, Azure AD Premium P1, Azure AD Premium P2 and Azure AD Free. As it would have been expected, each of these editions varies in terms of capabilities and pricing. The directory can be used in a standalone mode or hybrid; in the former, all components are contained in the cloud as every task is executed in Azure AD while for the hybrid mode, Azure AD is in synchrony with on-premise AD (Sarabadani, 2018). The authentication may be actualized in the on-premise AD while Azure AD connect handles the synchronization. Authentication was achieved using WS-Federation. And, by the way, OpenID connect, OAuth and SAML can also be used for authentication in Azure.

Azure AD makes it possible to implement provisioning in the developer's tenant and to other Azure AD tenants (Bertocci, 2016). Other prominent functions carried out by the Active Directory is the holding of the data needed to implement runtime authentication, and also the data that determine the resources required by an application, establishing that prerequisites have been adequately met before the request is granted. Plus, with the aid of this management service, administrators are able to set tasks for apps to execute, as well as decipher the particular user(s) that can be granted permission to use specific applications (Bertocci, 2016). The service principals are responsible for ensuring that clients communicate with the service that had been intended beforehand thus creating the identity of the application in effect. Service principals may however not suitably serve the development needs of the application due to the involvement of several concrete instances which might make updates rather complex.

5.2.2.1. Components of Azure Active Directory (AD)

Some of the components of the Azure Active Directory will henceforth be highlighted and discussed as follow:

- Protocol endpoint: With this, the researcher was able to create specific set of endpoints, and this is about the most critical part of Azure AD. It is such that a default domain *(tenantname.onmicrosoft.com)* is assigned to the developer once a new tenant comes aboard. It follows that the (new) tenant gets a unique identifier (i.e., tenantID) – which is used in generating protocol URLs specific to the tenant – that cannot be reassigned thereafter. In essence, direct username or password will not be required upon the completion of the configuration as the tenant gets redirected to the identity provider to establish authentication (Sarabadani, 2018). The ‘login.microsoftonline’ part in the URL communicates the instance that represents the service deployment that provisions a tenant in Azure AD (Bertocci, 2016).

- Azure Management Portal: The portal presents the avenue through which developers integrate settings in and out of the Azure AD tenant; it makes the provisioning [and management] of (new) apps possible (Beraud, 2016). Azure management portal enables attribute mapping which basically defines a configuration that controls attribute values. Additionally, the management portal facilitates operations like the creation of brand-new tenants in the development and staging processes, assigning of app roles to the band group of users and so on (Bertocci, 2016). It is only users that were assigned to the application in the portal that got authenticated successfully.

Other components that can be use in Azure AD include:

- Azure Graph API: Azure Graph API is typically a programmatic interface that functions to query objects. Just like Azure Active Directory Module for PowerShell, the Graph API, with the aid of the REST-based API interfaces, enables administrators implement group-group membership management, license management, user management and some other management tasks (Beraud, 2016). Furthermore, by promoting the extensibility of the schema, Azure Graph API permits existing exiting entities to be augmented with additional custom attributes without any need for external data store (Beraud, 2016).
- Application Access Enhancements: Application Access Enhancements describe the set of features in Azure AD that allows the easy management of access to several pre-integrated cloud SaaS applications [like Salesforce.com, ADP, etc.] and in turn fosters controls (both access governance and security) that facilitate the central management of users’ access (Beraud, 2016). With these enhancements, administrators are able to review security details surrounding sign-on as they will

have an insight of the applications that are being used by users, as well as the timing of such usage and the location of the users (Bertocci, 2016).

- Azure AD Application Proxy: This enables the extension of pre-integrated SaaS and custom application management functionalities to the on-premises application. It gives administrators the amplitude to expose local server for use by clients that are without the network (Bertocci, 2016). Application proxy is noted to be a viable infrastructural option in the scenario whereby the source of a legacy app is lost or delicate like what is attainable with a repository (Bertocci, 2016).

Application object, which is usually contained in the Azure AD tenants – it should be noted that each Azure AD tenant is connected to an Azure AD instance – highlights three different areas of the application (Bertocci, 2016): i.) Identifiers, protocol coordinates and authentication routes upon the request of the token required to access the application; ii.) Resources that are required by the application and the necessary actions that will be taken for the functions to be executed; and iii.) The tasks rendered by the application; an instance is the possibility of the directory granting permission to a user to either perform both read and write operations or read operations only. The application object plays a crucial role in the creation of service principal which ultimately represents the concrete instance of an application within the directory.

Conclusion

Cloud computing is indeed of immeasurable benefits – not only to the computing field, but also many organizations and users whose activities have been impacted by the opportunities perceivable therein. From business analysis to storage, deployment and management of applications and so much more, the list of advantages offered by cloud computing appears to be ever growing. Moreover, with IT giants such as Google, Amazon and even Microsoft vying to expand their market share in providing cloud services, we can look forward to new and advanced additions in this area of interest. As observed in the course of conducting this research, Microsoft is never relenting in updating Azure cloud services, with new features being added and in some other instances; it is about the reconfiguration of the services.

References

1. Abourezq, M., and A. Idrissi, Database-as-a-service for big data: An overview. International Journal of Advanced Computer Science and Applications (IJACSA), 2016. 7(1).
2. Ahmed, M., and Hossain, M.A. (2014). Cloud computing and security issues in the cloud. *International Journal of Network Security & Its Applications (IJNSA), 6(1): 25-36. DOI: 10.5121/ijnsa.2014.6103 25*.
3. Alomari, E., Barnawi, A., and Sakr, S. (2014). CDPort: A framework of data portability in cloud platforms. In: *Proceedings of the 16th International Conference on Information Integration and Web-based Applications & Services*.
4. Altaiar, H., Lee, J., and Pena, M. (2019). *Cloud analytics with Microsoft Azure.* Packt Publishing, Birmingham, UK.
5. Amazon ec2 (2015). Available from: http://aws.amazon.com/ec2/
6. Aoun, R., Doumith, E.A., and Gagnaire, M. (2010). Resource provisioning for enriched services in Cloud environment. *Proc. IEEE CloudCom Conf.*, pp. 296 – 303.
7. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Stoica, I., and Zaharia, M. (2009). Above the clouds: A Berkeley view of cloud computing. *Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley*.
8. Aulbach, S., Grust, T., Jacobs, D., Kemper, A., and Rittinger J. (2008). Multi-Tenant Databases for Software as a Service: Schema-Mapping Techniques. *SIGMOD '08 Proceedings of the 2008 ACM SIGMOD international conference on Management of data, pp. 1195-1206*.
9. Baxter, P., and Jack, S. (2014). Qualitative case study methodology: Study design and implementation for novice researchers. *The Qualitative Report, 13(4): 544-559.*
10. Bertocci, V. (2016). *Modern authentication with Azure Active Directory for web applications.*
11. BigCommerce (2020). IaaS vs PaaS vs SaaS - Enter the ecommerce vernacular: What you need to know, examples & more.
12. Britch, D., Cabral, M., Jadib, E., McMurty, D., Oakley, A., Singh, K., and Zhang, H. (2014). *Building an on-demand video service with Microsoft Azure media services.*

13. Butler, B. (2013). *PaaS Primer: What is platform as a service and why does it matter?* Available from: http://www.networkworld.com/article/2163430/cloud-computing/paas-primer--what-isplatform-as-a-service-and-why-does-it-matter-.html

14. Buyya, R., Vecchiola, C., and Somasundaram, T.S. (2013). Cloud computing architecture. In: *Mastering Cloud Computing*.

15. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., and Brandic, I. (2009). Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Gener. Comput. Syst.*, 25(6):599-616.

16. Chaczko, Z., Mahadevan, V., Aslanazadeh, S., and Christopher (2011). IPCSIT Vol-14, IACSIT Press Singapore 2011

17. Chappell, D. (2011). *The Microsoft private cloud A technology overview*. Available from: http://www.davidchappell.com/writing/white_papers/The_Microsoft_Private_Cloud_v1.0--Chappell.pdf

18. Di Martino, B., Cretella, G., Esposito A., and Sperandeo, R.G. (2014). Semantic representation of cloud services: A case study for Microsoft Windows Azure. *International Conference on Intelligent Networking and Collaborative Systems*, pp. 647 - 652.

19. Ferretti, L., Colajanni, M., and Marchetti, M. (2012). Supporting security and consistency for cloud database, in Cyberspace Safety and Security. Springer. pp. 179-193.

20. Flyvbjerg, B. (2007). Five misunderstandings about case-study research. In: *Qualitative Research Practice*, concise paperback edition. Sage, 2007, pp. 390–404.

21. Foster, I., Zhao, Y., Raicu, I., and Lu, S. (2008). Cloud Computing and Grid Computing 360-Degree Compared. In: *Grid Computing Environments Workshop (GCE'08)*. doi:10.1109/GCE.2008.4738445

22. Gao R., and Wu, J. (2015). Dynamic Load Balancing Strategy for Cloud Computing with Ant Colony Optimization. *Future Internet* 7: 465-483; doi:10.3390/fi7040465.

23. Garrison, G., Kim, S., and Wakefield, R.L. (2012). Success Factors for Deploying Cloud Computing. *Commun. ACM.* 55: 62–68.

24. Google compute engine (2015). Available from: https://cloud.google.com/compute/

25. Hamdaqa, M., and Tahvildari, L. (2012). Cloud computing uncovered: A research landscape. In: *Advances in Computers.*

26. Ibm smartcloud enterprise (2015). Available from: http://www.ibm.com/cloud-computing/iaas.html

27. Jackson, E. (2014). *Pro and Cons of Cloud Computing.* Available from: http://techinfo.website/pro-and-cons-of-cloud-computing/

28. Jesús, J.D. (2012). Navigating the IBM Cloud, Part 1: A primer on Cloud Technologies. *IBM Developer work.* Available from: http://www.ibm.com/developerworks/websphere/techjournal/1206_dejesus/1206_dejesus.html

29. Joint, A. and Baker, E. (2011). Knowing the past to understand the present 1 e issues in the contracting for cloud based services. *Computer Law & Security Review* 27: 407- 415. doi:10.1016/j.clsr.2011.05.002

30. Khajeh-Hosseini, A., Greenwood, D., and Sommerville, I. (2010). Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS. *IEEE CLOUD.*

31. Khorshed, T.M., Ali, A.B.M.S., and Wasimi, S.A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation Computer Systems* 28: 833–851. doi:10.1016/j.future.2012.01.006

32. King, N.J. and Raja, V.T. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law and Security Reviews*, 28: 308-319.

33. Kostoska, M. Gusev, M., and Ristov, S. (n.d). *A New Cloud Services Portability Platform*. Available from: http://www.sciencedirect.com.focus.lib.kth.se/science/article/pii/S1877705814003646#

34. Leung, H-F., Chiu, D.K.W., and Hung, P.C.K. (2011). *Service Intelligence and Service Science: Evolutionary Technologies and Challenges*.

35. Liu H., Liu S., Meng X., Yang C. and Zhang Y. (2010) *Interna-tional Conference on Service Sciences (ICSS)*, 257-262.

36. Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., and Leaf, D. (2011). NIST cloud computing reference architecture. *Technical report*.

37. MacVittie, L. (2009). Load balancing is key to successful cloud-based (dynamic) architectures. *DevCentral Home*. Available from: http://devcentral.f5.com/weblogs/macvittie/archive/2009/01/23/loadbalancing-is-key-to-successful-cloud-based-dynamic-architectures.aspx.

38. Mell, P., and Grance, T. (2011). *The NIST Definition of Cloud Computing*. Available from: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

39. Microsoft Azure (2015). Available from: http://azure.microsoft.com/en-us/services/virtual-machines/

40. Miller, J. (2004). Statistical significance testing: a panacea for software technology experiments? *Journal of Systems and Software* 73:183–192.

41. Moharana, S.S., Ramesh, R.D., and Powar, D. (2013). Analysis of load balancers in cloud computing. *International Journal of Computer Science and Engineering (IJCSE)*, 2(2): 101-108.

42. NIST Cloud Architecture. Available from: https://www.researchgate.net/figure/273945605_fig1_Figure-1-NIST-Cloud-Compu-ting-Reference-Architecture-CCRA-2

43. Ou, Y. (2015). The concept of cloud computing and the main security issues in it. *Degree programme in Information Technology & Internet Technology*

44. Pivotal cloud foundry (2015). Available from: https://pivotal.io/platform-as-a-service/pivotal-cloud-foundry

45. Rainey, R. (2015). *Azure web apps for developers - Microsoft Azure Essentials.*

46. Reese, G. (2009). *Cloud Application Architectures*. O’Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2009.

47. Rittinghouse W.J., and Ransome, F.J. (2010). *Cloud Computing Implementation, Management, and Security*. CRC Press, Boca Raton, FL, 2010.

48. Sarabadani, E. (2018). Active Directory from zero to hero. *Azure & NET Meetup – Freiburg.*

49. Shaukat, K., Hassan, M.U., Ali, H., Zaib, M.S., and Ullah, M.M. (2016). An overview of service-oriented architecture, cloud computing and Azure platform. *International Journal of Computer Science and Information Security (IJCSIS),* 14(7).

50. Smoot, S.R., and Tam, N.K. (n.d). *Private Cloud Computing: Consolidation, Virtualization, and Service-Oriented Infrastructure*. Available from:

http://proquest.safaribooksonline.com.focus.lib.kth.se/book/operating-systems-and-serveradministration/virtualization/9780123849199/cover-image/navpoint-0-11#X2ludGVybmFsX0h0bWxWaWV3P3htbGlkPTk3ODAxMjM4NDkxOTklMkZzdDAwMTBfYjk3ODAxMjM4NDkxOTkwMDAxODAmcXVlcnk9

51. Stanojevic, R. and Shorten, R. (2009). Load balancing vs. Distributed rate limiting: An unifying framework for cloud control. *IEEE International Conference: Communication*, 1-6.
52. Stark, C. (2012). The History of Cloud Computing. Available from: http://www.cetrom.net/blog/the-history-of-cloud-computing/
53. Strauch, S., et al. (2014). Migrating enterprise applications to the cloud: Methodology and evaluation. *International Journal of Big Data Intelligence* 1(3): 127-140.
54. Tejada, Z. (2017). Mastering Azure Analytics. Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.
55. Teneyuca, D. (2011). Internet cloud security: The illusion of inclusion. Information Security. *Technical Report* 16: 102-107. doi:10.1016/j.istr.2011.08.005
56. Winkler, J.R. (2011). Cloud computing architecture. In: *Securing the cloud*.
57. Yin, R. K. (2003). *Case study research: Design and methods* (3rd ed.). Thousand Oaks, CA: Sage.
58. Zhao Y., and Huang, W. (2009). *5th International Joint Confer-ence on INC, IMS and IDC,* 170-175.