

Challenges Of Cloud Computing Solutions In Organisations In Nigeria

Omolua, Agnes Ivhaghba (PhD)

Department of Office and Information Management,
Faculty of Business Studies,
Ignatius Ajuru University of Education,
Rumuolumeni – Port Harcourt.
Rivers State.

Phone Number: +2348036776348

Email: agnesisabage@yahoo.com

&

Kalagbor, Peace Iyingi

Department of Office Technology and Management,
School of Business and Administrative Studies
Captain Elechi Amadi Polytechnic
Rumuola – Port Harcourt.
Rivers State.

Phone Number: +2348037171642

Email: peace.kalagbor@portharcourtpoly.edu.ng

Abstract

Cloud computing has been defined in this paper as an information technology service model where computing servers (both hardware and software) are delivered on-demand to customers over a network in a self-service-fashion, independent of device and location, the resource required to provide the requisite quality of service levels are shared, dynamically scalable, rapidly provisional, virtualized and released with minimal service provider interaction. Cloud computing characteristics, service models, deployment models, benefits were also discussed. A systematic literature review on the challenges of cloud computing was carried out and the study identified security and privacy issues, lack of broadband internet connectivity, high cost of broadband internet, high bandwidth costs, frequent power outages, interoperability and compatibility challenges, standardisation challenges, among others as some of the challenges facing cloud computing in organisations. Possible ways of tackling the identified challenges were also examined. The study concluded that if these challenges are addressed holistically, organisations will exploit and enjoy the benefits of cloud computing. The study recommended that organisations should choose cloud service providers who offer sufficient guarantee.

Keywords: Challenges, Cloud computing.

Introduction

Cloud means different things to different people depending on the context for which it is used. From the context of information technology, the term “cloud” refers to software and services that run on the Internet, instead of locally on your computer. Most cloud services can be accessed through a Web browser like Firefox or Google Chrome, and some companies offer dedicated mobile apps. You can access your information on any device with an Internet connection. It is what allows you to edit files in Google Docs on your home computer, and then pick up where you left off when you get to the office. Colleagues can even collaborate on the same document (Barr, 2015). “The cloud” is a term referring to accessing computer, information technology (IT), and software applications through a network connection, often by accessing data centers using wide area networking (WAN) or Internet connectivity.

Almost all IT resources can live in the cloud: A software program or application, a service, or an entire infrastructure. For example, if a business wants to build an IT infrastructure, typically it would install the servers, software, and networking resources it needed, but nearly all of those services and resources are now accessible by going to third parties that offer them in the cloud (Hassan, 2011). According to Dialogic.com (2009) Cloud computing was coined for what happens when applications and services are moved into the internet “cloud.” Cloud computing is not something that suddenly appeared overnight; in some form, it may trace back to a time when computer systems remotely time-shared computing resources and applications. More currently though, cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications. Wilkinson (2019) referred to workplace cloud computing as ‘the Internet of the Workplace’ (IoW) which is an integrated enterprise architecture that connects employees and enables them to collaborate and perform regardless of location and reduces the resources needed to run and maintain their own technology infrastructure. Cloud computing in the workplace is changing the way business is done, shifting the landscape where it all takes place. By operating from the cloud, businesses of any size are able to compete with market rivals in ways that were previously unimaginable. This comes down to a reduction in capital expenditure and overheads, along with an enhancement in speed to market, enabling customer expectations to be met.

According to Carlos (2012), more people are embracing e-commerce and e-business and other e-offerings. There is an increase in ICT penetration and the influence it has on the lives of the people. Cloud computing can benefit private and government organisations, including public corporations to successfully replace data centres and other information in terms of reduction of running costs of the agencies. Private individuals, citizens, research institutions and schools can tap into the benefits of cloud computing to have access to arrays of sophisticated but costly software applications at far reduced cost.

Business owners, once hooked up to the web, the cost of buying software licenses, purchasing servers and maintaining them is reduced because it is possible to effectively

rent these applications from a third party on the cloud. In spite of these benefits and prospects of cloud computing, there are a lot of identifiable challenges confronting its full adoption and implementation and this has made a good number of private corporations, government Ministries Departments and Agencies (MDAs) to slow down on the adoption and implementation of cloud. Hence the objective of this paper is to identify the challenges of cloud computing and provide possible ways of tackling the identified challenges in order to enjoy the full benefits associated with cloud computing.

The main features of cloud computing

There are several features which when combined set cloud computing apart from other technologies. Some of these features as identified in the works of Barnatt (2010), DataFlair (2019), Mell (2011) and Rhoton (2011) are:

On-demand self-service

A consumer can independently request for cloud computing capabilities, such as server time and network storage, using cloud service catalogues as needed automatically without requiring human interaction with each service's provider.

Broad network access

Cloud resources are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data centre).

Rapid elasticity

Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts) used. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Off-premises

The service is hosted and delivered from a location that belongs to the service provider. This usually has two implications: the service is delivered over the public Internet and the processing occurs outside the user's firewall. In other words, the server must cross both physical and security boundaries.

Flexible billing

Fees can be levied on a subscription basis or can be tied to actual consumption, or reservation, of resources. Monetization can take the form of placed advertising or can rely on simple credit card charges in addition to elaborate contracts and central billing. As cloud computing is dynamically scalable and task-centric, for most users it has no fixed cost. Software applications purchased from the cloud incur only variable costs. When provision is not free, charges are typically based on the number of people using an application each month, or the number of records or projects being worked on.

Service delivery

Cloud functionality is often available as a service of some form. While there is great variance in the nature of these services, typically the services offer programmatic interfaces in addition to the user interfaces.

Simplified management

Administration is simplified through automatic provisioning to meet scalability requirements, user self-service to expedite business processes and programmatically accessible resources that facilitate integration into enterprise management frameworks.

Affordable resources

The cost of resources is dramatically reduced for two reasons. There is no requirement for capital expenditures on fixed purchases. Also, the economy of scale of the service providers allows them to optimize their cost structure with commodity hardware and fine-tuned operational procedures that are not easily matched by most companies.

Service-level management:

Cloud services typically offer a service-level definition that sets the expectation with the customer as to how robust that service will be. Some services may come with only minimal or nonexistent commitments. They can still be considered cloud services but will not be "trusted" for mission-critical applications to the extent that others governed by more precise commitments might.

Multi-tenancy

The cloud is used by many organizations (tenants) and includes mechanisms to protect and isolate each tenant from all others. Pooling resources across customers is an important factor in achieving scalability and cost savings. Multi-tenancy enables sharing of resources and costs across a large pool of users thus allowing for centralization of infrastructure in locations with lower costs, peak-load capacity increases as well as utilisation and efficiency improvements for systems that are often only 10–20% utilized.

Device-independent

Cloud computing resources can be accessed by any kind of computer. Provided that such a computer has an Internet connection and a web browser, it really does not matter if the computer is a traditional desktop or laptop PC, or even a netbook, tablet, smart phone, e-book reader, surface computer, ambient device or any other new computing appliance. This is a radically new development as even though it has become easy over the past decade to exchange data between different computers, there remains a requirement for the right software to be installed. For instance, if a Microsoft PowerPoint presentation is created and sent as an e-mail attachment, the recipient needs to have the Microsoft PowerPoint software application installed on his computer system to be able to open and edit the file in a completely compatible manner. However, if the cloud service Google Docs is used to create the presentation, the e-mail attachment could be opened and edited on any kind of computer system with an Internet connection and web browser.

Task-centric

Cloud computing is task-centric because the usage model is based entirely around what users want to achieve, rather than any particular software, hardware or network infrastructure. Users do not need to purchase or install anything before using a cloud computing resource. Nor do they have to maintain or pay for anything during periods in which no resources are being used. Simply put, cloud computing allows a consumer to simply get on with the task at hand without bothering about the location and installation of the tools being used.

Ease of maintenance

Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places. Cloud computing may be characterized by one or all of the above-mentioned attributes. It provides a certain service to its participants and these have been categorized into service models.

Cloud computing models

Cloud Computing can be broadly categorized in two models i.e. service model and deployment model.

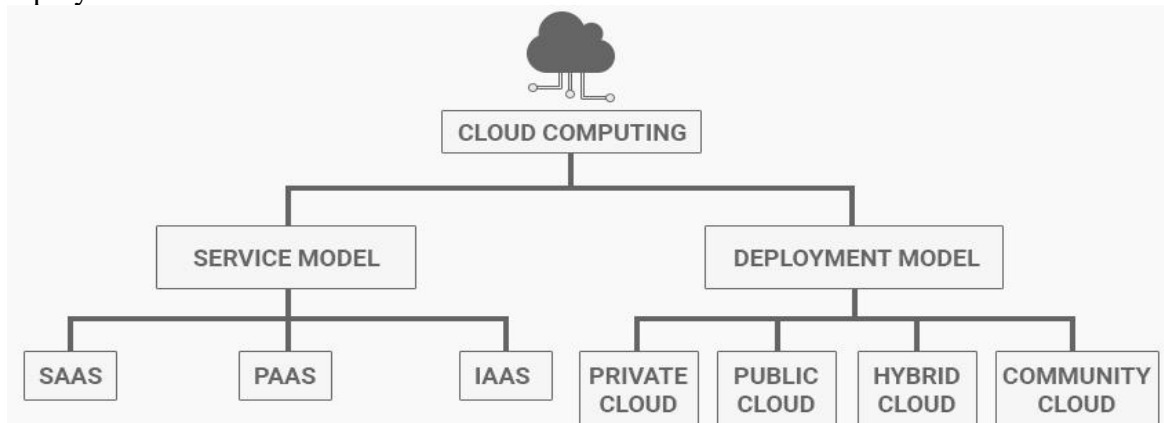


Figure I: Cloud Computing Model (Verma, 2017)

Cloud computing deployment models

There are basically four main deployment models for cloud computing, namely Private Cloud, Community Cloud, Public Cloud and Hybrid Cloud. (Achana, 2019; Mell, 2011). These models are explained below:

Private cloud

This cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud

This cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud

This cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud

This cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Cloud computing service models

The most common classification of cloud computing service models uses the SPI (Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) model. (Paranet, 2019; Vinod, 2018). These three service models differ in the extent of sharing they imply for their customers. Infrastructure services share the physical hardware. Platform services allow tenants to share the same operating system and application frameworks. Software services share the entire software stack. These three approaches represent different tradeoffs in a balance between optimization, which leverages multi-tenancy and massive scalability, on one hand, and flexibility to accommodate individual constraints and custom functionality, on the other hand. Software services are typically highly standardized and tuned for efficiency. However, they can only facilitate minor extensions. At the other extreme, infrastructure services can host almost any application but are not able to leverage the benefits of economy of scope as easily. Platform services represent a middle ground as they provide flexible frameworks with only a few constraints and are able to accommodate some degree of optimization (Rhoton, 2011). Examples of SaaS include: Google Apps, TradeCard, Microsoft Office 365, Onlive and GT Nexus. Examples of PaaS include: AWS Elastic Beanstalk,

EngineYard, Cloud Foundry, Heroku, Force.com, OrangeScape, Mendix, Google App Engine, and Windows Azure Cloud Services.

Examples of IaaS providers include Open Stack Distribution Stack Ops, Amazon Cloud Formation, Amazon EC2, Windows Azure Virtual Machines, DynDNS, Google Compute Engine and HP Cloud.

Benefits of cloud computing

Only four out of the lots of benefits of cloud computing as identified by Deckan (2018) and Salesforce.com (2019) will be discussed here, which include:

Cost savings

Once you are on the cloud, easy access to your company's data will save time and money in project startups. The pay-as-you-go system allows users to pay for space as they need, and not be charged for any space that they don't.

Security

While most businesses do not like to openly consider the possibility of internal data theft, the truth is that a staggeringly high percentage of data thefts occur internally and are perpetrated by employees. When this is the case, it can actually be much safer to keep sensitive information offsite.

Flexibility

The cloud offers businesses more flexibility overall versus hosting on a local server. And, if you need extra bandwidth, a cloud-based service can meet that demand instantly, rather than undergoing a complex (and expensive) update to your IT infrastructure. This improved freedom and flexibility can make a significant difference to the overall efficiency of the organization.

Mobility

Cloud computing allows mobile access to corporate data via smartphones and devices. Staff with busy schedules, or who live a long way away from the corporate office, can use this feature to keep instantly up to date with clients and co-worker. Through the cloud, you can offer conveniently accessible information to sales staff who travel, freelance employees, or remote employees, for better work-life balance.

Challenges facing cloud computing in organisations and their possible solutions

Organisations are increasingly becoming aware of the business value that cloud computing brings and are taking steps towards transition to the cloud. A smooth transition entails a thorough understanding of the benefits as well as challenges involved. Like any new technology, the adoption of cloud computing is not free from issues. These issues are putting fear in some of the companies to fully adopt and implement cloud computing. The few important challenges affecting the full implementation of cloud computing in Nigeria are: Security and privacy issues, High Bandwidth costs, migration, immature technology,

and a host of other challenges. (Obodoeze, okoye & Asogwa 2014; Dunccevic, 2019; Harvey 2018). These challenges and their possible solutions are discussed below:

Security and privacy issues

Data and information security

Security of data and information over cloud networks, i.e., privacy, integrity and confidentiality of transactions is the biggest fear of corporate and private potential cloud customers in Nigeria. The biggest challenge in cloud computing is to successfully address the security and privacy issues associated with their deployment. cloud service providers (CSPs) operating as either IaaS or PaaS or SaaS have to pass through a security zone and thereafter provide a user interface (either as IaaS, PaaS or SaaS) that is secured for connectivity by cloud customers which can be corporate or private or government. There should be a security model which will have the verification and validation unit, the privilege control unit, data protection unit, attacks detention/prevention unit. (Obodoeze et al 2014). These are discussed subsequently:

i. Verification and validation (V&V) unit

This unit is required in cloud computing not only to authenticate users but also to ensure the correctness of data and services on the cloud. The importance of this security component is due to the fact that cloud computing environment is accessible by multiple consumers and providers who wanted to use or provide several services and applications. CSPs need to prove to the users that the services and data are valid using, for instance, appropriate signature algorithms. Consequently, users will be able to verify the authenticity of the data and services made available to them through such type of digital signature. (Ahmed & Mariel 2009, Johnson & Azam 2011)

ii. Privilege control unit

This security unit is necessary to control cloud usage by different individuals and organizations. It protects users' privacy and ensures data integrity and confidentiality by applying a collection of rules and policies that control who has the authority to do what on the cloud. Cloud users are granted different levels of access permissions and resource ownerships based on their account type. Only authorized users can access the authorized parts of the encrypted data through identity- based decryption algorithm. For example, in a healthcare cloud not all practitioners have the same privileges to access patients' data, this may depend on the degree to which a practitioner is involved/specialized in treatment; patients can also allow or deny sharing their information with other healthcare practitioners or hospitals (Ahmed & Mariel 2009, Zhang &Liu 2010).

iii. Data protection unit

Data stored in the cloud storage resources may be very sensitive and critical, for example, clouds may host electronic healthcare records (EHR) which contain patients' private information and their health history (Ahmed & Mariel 2009). They may also store critical banking information (e.g., client account numbers, balances and transactions) or national security information. A cloud security model should protect these data from loss or damage by providing secure storage servers. These servers should also secure data

retrieval and removal from the cloud. Securing data storage and processing is important since cloud users have no idea about data location.

Techniques for data protection such as truncation, reduction, obfuscation, and others can be used in this security component. Encryption techniques can also be employed for data security. Hash functions and Message Authentication Code (MAC) can be employed in this unit to provide data integrity.

iv. Attacks detection/prevention unit

Clouds are vulnerable to many attacks and malicious behaviours that threaten both data and physical and virtual computing resources of the cloud. Basically, any set of actions that threaten the cloud security requirements (e.g., integrity, confidentiality, availability) are considered to be attacks. Attacks detection and prevention components should be installed within the cloud security system to protect cloud resources from various anomalies. For example, denial-of-service attacks should be reduced to the minimum to guarantee the maximum availability of business, governmental, health and other critical information and services. This can be achieved by deploying technologies that provide high availability such as dynamic server load balancing and active/active clustering (Ahmed & Mariel 2009). Standard Distribution Denial of Services (DDoS) mitigation techniques such as synchronous cookies and connection limiting can also be used. Clouds should also be provided by the next generation of intrusion detection systems and firewalls in order to protect their resources from intruders, viruses and malware.

Lack of broadband internet connectivity

Broadband internet connectivity

The success of cloud computing depends wholly on the infrastructural availability such as broadband internet connectivity and availability. Broadband internet availability and affordability are key factors to the successfully deployment and operation of cloud computing platforms and services. In Nigeria presently, with the recent rollout of GSM 3.5G data services such as High-Speed Packet Access (HSPA), cloud computing services can be more efficient but HSPA subscriptions in Nigeria currently is still unaffordable. Besides, HSPA networks are not available in the major towns and villages in Nigeria except the States' capitals. Worldwide Interoperability for Microwave Access (WiMAX), especially mobile WiMAX, and Wireless Fidelity (Wi-Fi) can be integrated with GSM so that broadband connectivity will be cheaper for subscribers in remote villages and towns. Data Service providers in Nigeria such as MTN, Globacom, Airtel and 9mobile can reduce very high tariffs currently being charged customers in Nigeria so that it will make cloud computing affordable. With the expected changes the data networks and subscription rates in Nigeria, GSM HSPA with WiMAX, Wi-Fi integrated with GSM, a new regime that can provide more efficient and affordable broadband internet connectivity to power cloud computing services all over the country will be achievable.

High bandwidth costs

Bandwidth cost

Internet bandwidth can eat up the cost of accessing and maintaining cloud-based service(s) especially where most of the cloud-based services/solutions are not optimised properly to reduce download/access bandwidths by customers over the internet or intranet.

Bandwidth cost-reduction techniques can be employed by the cloud service customers to reduce their bandwidth cost. Some bandwidth reduction techniques as identified by Zhand and Liu (2010), Brien (2014) and Obodoeze et al (2014) include:

i. Use of routers to manage internet bandwidth

some routers allow to bandwidth management, you could set up a lower bandwidth for the Local Area Network (LAN) and connect yourself with the WiFi if possible. Use of two network cards in one computer; one to connect to the internet and the second to connect to the Local Area Network (LAN). The computer would be sharing the internet with another cloud customer with one network card, and with software like Bandwidth manager, you should be able to control bandwidth consumption on the internet as you share the internet with another cloud customer.

ii. Use quality of service (QoS) to reserve bandwidth

QoS stands for quality of service. It is a bandwidth reservation mechanism that was first introduced in Windows 2000, and it's still around today. If you have applications that require a specific amount of bandwidth (such as a video conferencing application), you can configure QoS to reserve the required bandwidth for that application. The bandwidth reservation is in effect only when the application is actively being used. At other times, the bandwidth that is reserved for the application is available for other uses.

iii. Aggressive scan of the computer for malware to cut down their drain on internet bandwidth

Malware can rob an organization of a tremendous amount of bandwidth by turning Personal Computers (PCs) into bots.

iv. Use of hosted filtering

Hosted filtering saves a great amount of bandwidth for organizations that operate their own mail servers in-house. With hosted filtering, your MX record points to a cloud server rather than to your mail server. This server receives all the mail that's destined for your organization. The server filters out any spam or messages containing malware. The remaining messages are forwarded to your organization. You can save a lot of bandwidth (and mail server resources) because your organization is no longer receiving spam.

v. Use a proxy cache

a proxy cache can help limit the amount of traffic created by web browsers. The basic idea is that when a user visits a web site, the contents of the page are cached on a proxy server. The next time that person visits that web page, the content does not have to be downloaded because it already exists in the cache. Using a proxy cache not only saves

bandwidth, but it can give users the illusion that your Internet connection is much faster than it really is.

vi. Throttling cloud backup applications

if you're backing up your data to the cloud, check to see whether your backup application has a throttling mechanism. An unthrottled cloud backup solution will consume as much bandwidth as it can. This might not be a big deal if you're backing up small files (such as Microsoft Office documents) throughout the day. But when you first begin backing up data to the cloud, an initial backup must be created. it can have a major impact on your Internet bandwidth.

vii. Blocking of access to content-streaming websites which eats up large chunks of internet bandwidth.

These are websites that have several multimedia contents such as audio, video, flash animations that consume a great amount of internet bandwidth.

viii. Use of client-server paradigm such as the “propel architecture” can save great amount of bandwidth while using web browsers.

Propel leverages a cloud-based network of content acceleration servers to dramatically reduce the amount of data required to view web pages (Brien 2014). The Propel client server software ("Propel Client") runs in the background on the user's PC / Mac as a local proxy. The Propel Client maintains a persistent connection to the Propel Network in order to eliminate the connections that need to be established every time the browser initiates a request. The Propel client decodes and caches the content it receives from the Propel Network before sending it to the Web browser thereby cutting down on the usage of internet bandwidth.

Migration

You compare developing a totally new cloud application as against migrating an existing application onto the cloud – the answer is straight and simple. Migrating an existing one has its own set of hurdles, drawbacks, and challenges to face. Time has proven that cloud migration has faced troubles like security configuration, time consumption, budget overflow, unmatched requirements, downtime, etc. (Durcevic, 2019). This challenge can be addressed by:

- ☐ Performing pre-migration testing that focuses primarily on migration-related needs
- ☐ Setting a realistic project deadline and budget keeping in mind migration hassles
- ☐ Hiring cloud service providers who are experts at migration projects

Immature technology

Many cloud computing services are on the cutting edge of technologies like artificial intelligence, machine learning, augmented reality, virtual reality and advanced big data analytics. The potential downside to access to this new and exciting technology is that the services don't always live up to enterprise expectations in terms of performance, usability and reliability. The only potential cures for the problem are to adjust expectations, try to build your own solution or wait for the vendors to improve their offerings.

Conclusions

Cloud computing is redefining the organization today. No matter the size of your organization or the industry that you work in, keeping up with the latest innovations is essential for staying competitive. Broadly speaking, organizations strive for goals like speed, accessibility and flexibility. Your customers expect to seamlessly utilize your services and purchase your products from anywhere, resulting in the optimal customer experience. Your employees ideally desire a flexible working environment that not only aids their productivity, but one that also permits them to get their work done on their own terms. Employers want their team members to be able to meet customer demands and have a pleasant time doing so. One critical approach that organizations can take to meet both sets of demands is by embracing cloud computing. Cloud is redefining workplaces by transforming IT infrastructure and offering a more efficient use of computing resources which lead to greater flexibility, better collaboration and smatter processes. When employees are not forced to work from their desks, they can work to a schedule that complements their individual routines. In turn, their productivity levels increase benefitting the organization's bottom line. Working in the cloud allows employees to access their documents and files from any device, be it smartphone, tablet or laptop, anywhere at any time, which will not only encourage collaboration in your business, but boost it as well. As organisation data is stored centrally, a team can easily work on files together while the cloud saves them automatically so they can view and continue working via their mobile devices at any time in the future. Cloud systems enable reliable collection, tracking, and analyzing of important data that can help organizations update or replace processes to give a better return. This allows the workplace to function more efficiently and for employees to be assigned the right jobs and roles. The "Internet of Workplace" (IoW) is paving the way for new, more flexible and innovative structures, allowing organisations to adopt remote working systems and assemble virtual teams in pursuit of greater efficiencies and productivity. Cloud computing promises substantial benefits for small, medium and large organisations. Realizing these benefits require a focus on the various challenges affecting full implementation of cloud and how to overcome them. If these challenges are addressed holistically, organisations will exploit and enjoy the full benefits of cloud computing.

Recommendations

This paper provides an in-depth literature on the challenges of cloud computing in organisations and possible ways these challenges can be addressed. It is therefore recommended that:

1. Organisations should clearly identify the data and processing operations which will be passed to the cloud.
2. Organisations should define their own requirements for technical and legal security.
3. Organisations should choose service providers offering sufficient guarantees.

References

Accenture, (2011). *Cloud insights*. Assessed online from <https://www.accenture.com> on September 27, 2019.

- Ahmed, E. Youssef, & Manal, A. (2012). "A framework for secure cloud computing", *International Journal of Computer Science Issues (IJCSI)*, 9(4), 3, 487.
- Archana, C. (2019). Cloud computing services. A deeper dive into cloud computing. Accessed online on October 2, 2019.
- Barr, J. (2015). Cloud computing, server utilization and the environment. Accessed online from <https://aws.amazon.com/blogs/aws/cloud-computing-server-utilization-the-environment/> on September 29, 2019.
- Brien, P., (2014). 10 things you can do to conserve Internet bandwidth", Accessed online at <http://www.techrepublic.com/> on September 28, 2019.
- Barnatt, C. (2010). *A brief guide to cloud computing*. Constable & Robinson Limited.
- Carlos, B. L. & Gelante. G. (2012). A survey on cloud computing elasticity proceedings IEEE/ACM 5th international conference on utility and cloud computing, UCC2012.10.1109/UCC.2012.30.
- DataFlair, (2019). Features of cloud computing. Assessed online on October 2, 2019.
- Dave, A. (2009). Why 2FA in the cloud. *Network Security*, 2009(9), 4-5.
- Dialogic.com, (2009) Introduction to cloud computing. Accessed online from <https://www.dialogic.com/-/media/products/docs/whitepapers/12023-cloud-computing-wp-pd> on 28, September 2019.
- Durcevic, S. (2019). 10 cloud computing risks and challenges business are facing in these days. <https://www.datapine.com>.
- Federal Information Processing Standards Publication 197, (2001). Specification for the advanced encryption standards (AES), 2001. Accessed online from <http://csrc.nist.gov/archive/aes/rijndael/wsdindex.html> on September 30, 2019.
- Fluhrer, S., Mantin, I. & Shamir, A. (2001). Weakness in the key scheduling algorithm of RC4, 8th Annual International Workshop on Selected Areas in Cryptography, Springer-Verlag London, UK.
- Harvey, C. (2018). Top 10 cloud computing challenges. Assessed online on October 3, 2019 from www.google.com.
- Hassan, Q. F. (2011) Demystifying cloud computing. CrossTalk. 16-21. Accessed online at

from:<http://static1.1.sqspcdn.com/static/f/702523/10181434/1294788395300/201101-> on September 27, 2019.

Hurwitz, J., Bloor, R., & Marcia, K., (2010). Cloud computing for dummies®. HP Special Edition Published by Wiley Publishing, Inc. 111 River Street Hoboken, NJ 07030-5774 Copyright © 2010 by Wiley Publishing, Inc., Indianapolis, Indiana. Accessed online from <http://pdf.semanticscholars.com> on 29 September, 2019.

IBM cloud, (2015). IBM to acquire softlayer to accelerate adoption of cloud computing in the enterprise: *IBM to form new cloud services Division*.

NIST (2011). The NIST definition of cloud computing. Special publication 800-145 accessed on 29 September 30, 2019 from <https://nvlpubs.nist.gov>legacy>.

Johnsson, M. & Azam, A. (2011). Mobile one time passwords and rc4 encryption for cloud computing, Technical report, IDE1108. Accessed online at http://en.wikipedia.org/wiki/Two-factor_authentication on September 29, 2019.

Leonard, D.C., Alexander P. P. & Shihab, S. A., (2009). Realization of universal patient identifier for electronic records through biometric technology, *IEEE Tran. On Information Technology in Biomedicine*, 13(14),

Mell, P. & Grance, T. (2011). *The NIST definition of cloud computing*. The National Institute of Standards and Technology: Accessed online from <http://crsc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc> NIST on September 28, 2019.

Obodoeze F. C., Okoye F. A. and Asogwa T. (2014) Cloud computing in Nigeria: prospects, challenges and operation framework. *International Journal of Engineering Research & Technology (IJERT)* ISSN: 2278-0181 www.ijert.org 3(6), IJERTV3IS061482 2110 Assessed online from <https://www.researchgate.net/publication/322466068> on September 26, 2019.

Paranet, (2019). The three cloud service models. Assed online from <https://www.paranet.com> on October 1, 2019.

Rhoton, J. (2011). Cloud computing explained. Second Edition. Recursive Press.

Rouse, M. (2008, April). Communication as a service. Assessed online from:<http://whatis.techtarget.com/definition/Communication-as-a-Service> on September 29, 2019.

Salagean, A. (2012). The technologies used in security in online payments. Literature Review. Accessed online at https://www.researchgate.net/publication/229163539_The_technologies_used_in_security_in_online_payments/citation/download on September 29, 2019.

- Salesforce.com, (2019). Benefits of cloud computing. Accessed online from <https://www.salesforce.com/products/platform/best-practices/benefits-of-cloud-computing/> on September 28, 2019.
- Schouten, E. 2014. Cloud computing defined: Characteristics & service levels. Retrieved from <https://www.ibm.com/blogs/cloud-computing/2014/01/cloud-computing-definedcharacteristics-service-levels>.
- Verma, K. (2017). Cloud computing and its types. Assessed online from <https://cloudkul.com/blog/what-is-cloud-computing/> on October 27, 2019.
- Vinod, S. (2018). Cloud service models. Saas, Iaas, Paas – choose the right for your business. Assessed online October 2, 2019 from <https://www.fingerprint.com>.
- Wilkinson, R. (2019). Clouding the workforce: a blueprint for the future of cloud computing Assessed online from <https://www.worktechacademy.com/clouding-the-workforce-a-blueprint-for-the-future-of-cloud-computing/> on September 28, 2019.
- Zhang, R. & Liu, L. (2010). Security models and requirements for healthcare application clouds”, IEEE 3rd International Conference on Cloud Computing.
- Zhi L., Subhajyoti, B., Juheng, Z. (2011). Cloud computing—the business perspective”, Elsevier, *Decision Support Systems* 51 (2011) 176–189.