# *A RESEARCH STUDY INVESTIGATING THE CHALLENGES OF CLOUD COMPUTING IMPLEMENTATION AS AN ALTERNITIVE FOR LEGACY SYSTEMS IN MAURITIUS GOVERNMENT MEDICAL ORGANISATIONS*

AUTHORS

CHUKWUEMEKA MICHAEL NNAMDI INYA

AMEH HOLYFIELD ITODO

BRIAN MBURU WAWERU

Table of Contents

## Abstract

Government agencies have moved to cloud-based services to evade the dangers of legacy systems, reduce their overall investment in IT technology and manage resources. As well as shining a spotlight on the various benefits of cloud computing. However, as with any other technology investment, there are still questions about the possible risks of cloud-based technology implementation. These issues and the lack of academic literature focusing on cloud computing in the government context reinforce the need for exploratory work and to draw lessons for government official and reputable organisations to ensure that expensive mistakes are minimized. Accordingly, this paper explores the application of cloud computing in both realistic environments and from an organizational consumer viewpoint, it also exposes the dangers of the continuous use of legacy systems within organisations via one reputable organisation and two government authorities. By means of qualitative case study enquiries, the authors can extrapolate potential benefits and risk factors that are mapped against the literature so that emerging factors can be established. These results, originating from the aggregated organizational consumer perspective, would support both researchers and practitioners engaged in cloud computing research and its strategic application in the public sector.

# 1. Introduction

As the medical sector is important aspect of any country and the leaders within the government organisations it is important the head of the ministry to the patients have an ease of services from forward planning, accessing a particular patient's medical information to seeing a doctor and getting medication. Based on the amount of data dealt with in public medical institution, as Mauritius has a population of 1.3million people it is important that this sensitive data is stored in a secure manner and can be readily available at any hospital a patient might visit within the country. This report will investigate the cloud computing what, the types of cloud computing, how it advanced through the years and the benefits it has provided to organizations who transitioned from legacy systems, the limitations, risks, and challenges that can be brought by either migrating or using cloud computing. To re-affirm the findings and importance of needing to implement cloud computing the research paper will investigate some case studies and other secondary research from credible and authoritative sources.

# 2. Literature review

For this study, a literature review was done to gain better understanding of what cloud computing is, how it has developed, the benefits, drawbacks and challenges that could be faced while attempting to implement such a system to an organisation.

## 2.1 Definition and history of cloud computing

### 2.1.1 What is cloud computing?

The concept of cloud computing revolves around the availability of resources of a computer system whether software or data centres without the need of a user managing the resources directly. This is done using remote servers hosted on the internet instead of local severs and cloud computing providers who offer cloud computing services to clients. Cloud computing also allows the user to keep their data online and can be accessible from anywhere at any time (Bang, 2015).

### 2.1.2 Before cloud computing

Prior to cloud computing, for an organisation to have their resources online they would need to first invest in experts who would facilitate the purchasing, implementation, and management of servers, software, and hardware for the services. This resulted in heavy cost on the hardware, servers, and payment for the experts (Bohm and Krcmur, 2011). There were also issues such as security and accessibility in the case of downtime, these problems lead to the option not being a viable option and this all changed with the introduction of cloud computing services offered by companies such as Google, Amazon etc.

### 2.1.3 Foundation of cloud computing

Cloud computing is a concept that was made popular by Amazon and their web services by setting to market a product called Elastic compute cloud in 2006 and the analyst at Gartner a global advisory and research company deemed cloud computing to be an emerging technology well on the way to the hype. The fact that cloud computing was considered to have large possible infinite computing capacity that was available on demand with easily accessible and usable virtualised resources that were charged based on the usage would make it a popular option for many organisations.

### 2.1.4 Benefits cloud computing

Cloud computing is a platform that has brought a range of benefits to businesses and their processes. The benefits have made cloud computing as popular as it is and a suitable option for organisations. The benefits of cloud computing include cost saving, as an organisation ROI (return on investments) is an important aspect that needs to be considered while making decisions on financial investments (Cloud Computing- Benefits & Limitations, 2017). For organisations who lack experts or have budget constraints they can save on this aspect as well as paying for the components that they are using, only and can add more components when the scale and requirements of the organisation grows.

The ability for an organisation to have their resources cloud based increases the efficiency in which the employees can collaborate on projects by being able to access, share and communicate. The aspect of an organisation's resources being cloud based not only allows the employees to collaborate even if they are in different departments or locations the organisation can have a competitive edge by increasing their capabilities and making use of a system that is mobile (Xue and Xin, 2016). In conjunction with collaborative environments, having all the documents and data in a singular storage position the organisation can have better reporting and consistent data as well as assisting in the carbon footprint reduction since the data does not need physical copies or hardware. While using AWS the organisation can have assurance of automatic software

updates and loss prevention. The amount of issues that can damage hardware of which an organisations data is stored, can be deterioration, viruses, or human error. The factors will result in data loss which can affect the business operations but in the case of an organisation that has adapted cloud computing these issues are not a factor since their resources are still accessible online without hardware restrictions. Away from hardware, software developers are always making amendments and improvements to their systems and when they roll them out users tend to have to wait for the download and installation of which it is time consuming and reduce productivity but for the cloud computing clients the updates on software occur automatic.

As data in this age is valuable its paramount that there are measures to secure it. For cloud computing service providers, they make use of encryption on the data while it is being transmitted to the network and stored. Although it prevents the hackers from accessing the data and has better security than local servers, it does not provide clients with security risk free confidence.

### 2.1.5 Limitations cloud computing

The disadvantages of cloud computing can be viewed through the dependencies. This is through the service providers and networks. In cloud computing the organisations resources are online and if they are based in a country that has poor internet, limited bandwidth or areas that lack connectivity there will be accessibly issues and the employees would not be able to be productive (Xue and Xin, 2016). By using cloud computing service providers, the organisation would have less control as their data is handled by the provider and can be alarming mostly if the organisation is handling highly sensitive data. Some of the organisations have different requirements, some might occur as they grow and the services that are provided could be limited and not cater to the needs e.g., Storage space. In the occasion of a technical error chances are the error cannot be solved without contacting the service provider and they might not provide 24/7 on the clock support resulting in down time and lack of productivity. The data being handled on the service providers' servers can have the risk of being accessed by unauthorized staff

and loose its confidentiality (Xue and Xin, 2016). There can also be security challenges mostly in SaaS rather than hosted providers, there can be measures taken such as encryption of data stored but the threat is still there.

### 2.1.6 Types of cloud computing

Under the bracket of cloud computing there are to sections, cloud deployment and cloud services. In cloud deployment involves the way in which implementation is done, there are three different methods public cloud, private cloud, hybrid cloud. And the cloud services the categorises the cloud into three, infrastructure as a service (IaaS), software as a service (SaaS) and platform as a service (PaaS) (Cloud Standards Customer Council, 2017).

## 2.2 Cloud deployment

Cloud deployment is enabling Software as a service (SaaS), Platform as a service (PaaS) or infrastructure as a service (IaaS) solution that may be accessed only on demand by consumers or end user.

Cloud deployment model is the type of architecture of cloud computing that a cloud solution will be implemented on. It includes the needed configuration and installation steps that must be implemented before the end user provisioning can occur.

Cloud deployment model explains the purpose and nature of the cloud and it also precisely shows the category of the environment of the cloud based on the size, proprietorship, and access. The implementation of cloud infrastructure by most organizations is to regulate operating costs and reduce capital expenditure (Ani M, 2018).

There are four different models of cloud deployment: public, private, community and hybrid. Each of these models has its feature, the model you choose will be based on the needs of your business.

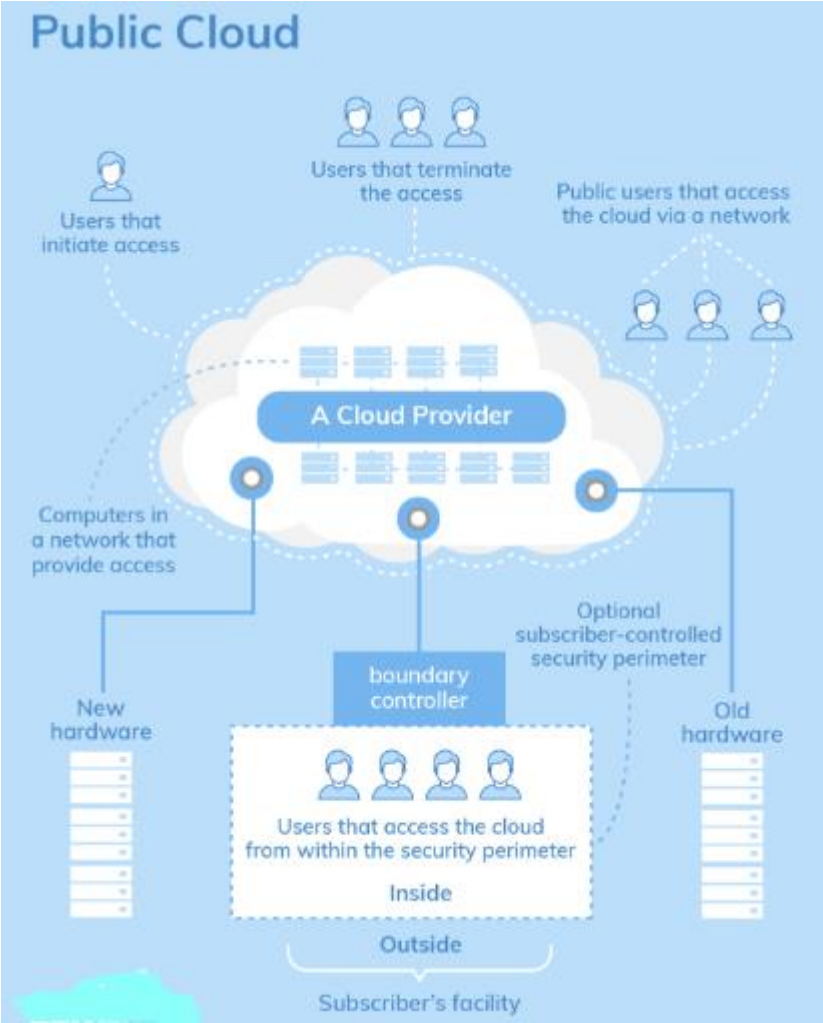
### 2.2.1 Public cloud

Public cloud is when services are being rendered by third-party providers over a network that is meant for public usage, which means that you use the same software, hardware, and network devices with other clients of the same provider. In a cloud that is public you will only rent a space on the cloud from a third-party provider. You will have no responsibilities concerning cloud management because he will be the one responsible for the maintenance and management of the whole cloud infrastructure. The clients only use for storing their data and pay as they use. Industries that operate within low privacy concerns always consider public cloud deployment as first business choice.

Companies that provide public cloud deployment models are Google AppEngine, IBM's Blue, Microsoft Azure, Amazon Elastic Compute, and others.

| ADVANTAGES | DISADVANTAGES |
|---|---|
| **Minimizes time in testing and initiating new products** | Maximizes security risks due to vulnerabilities resulting from resources shared |
| **Reduces cost** | Network instabilities |
| **Pay as you use scalability** | Not usually personalize |
| **Data is easily accessible** | Lack of individual approach |

**Graphical representation of public cloud**



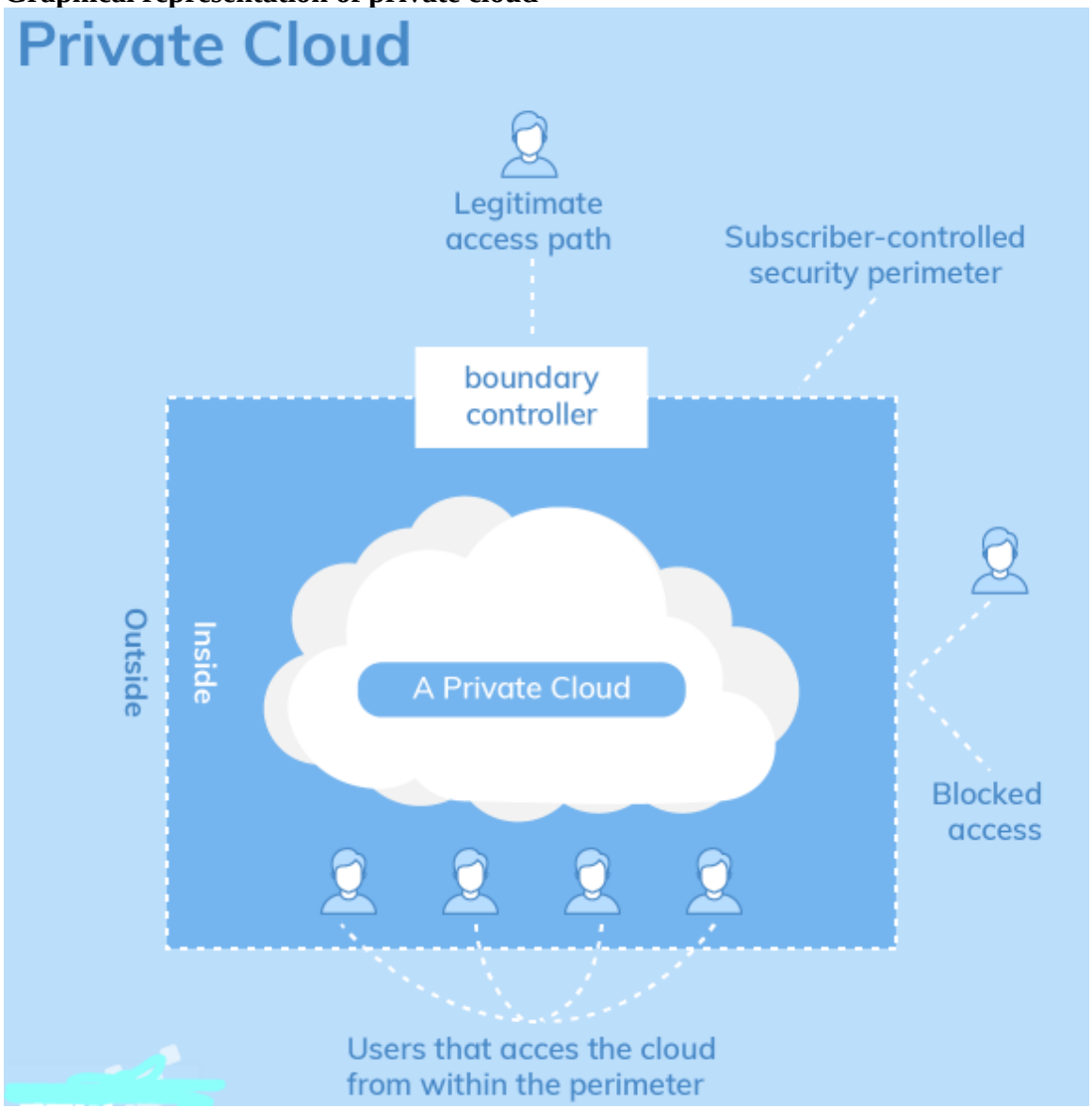

**2.2.2 Private cloud**

This refers to cloud deployment model operated for a single organization whether is hosted and managed by a third-party provider or physically located on the data centre of the company. In this cloud deployment model, resources or data are not shared with any other industry, therefore; the organization that uses private cloud is totally responsible for the maintenance, management and steady updates which can maximize cost than public cloud deployment model. Because private cloud deployment model is only accessed by a single organization which reduces security concerns as all resources and data is protected

behind a firewall. Service providers that build private cloud solutions includes Cisco, Red Hat, Dell, Amazon, Microsoft, Apache, OpenStack, and others. (Yuliya, 2018)

| ADVANTAGES | DISADVANTAGES |
|---|---|
| **Cloud environment can easily be customized** | Difficulty to access data from remote locations |
| **Maximizes privacy and security because data are not shared** | Increase in cost in investing in private cloud infrastructure |
| **Enhances server control** | Because the company is responsible for the maintenance and management there is an increase in expenses |
| **Allows storage customization** | Vendor lock-in |

**Graphical representation of private cloud**



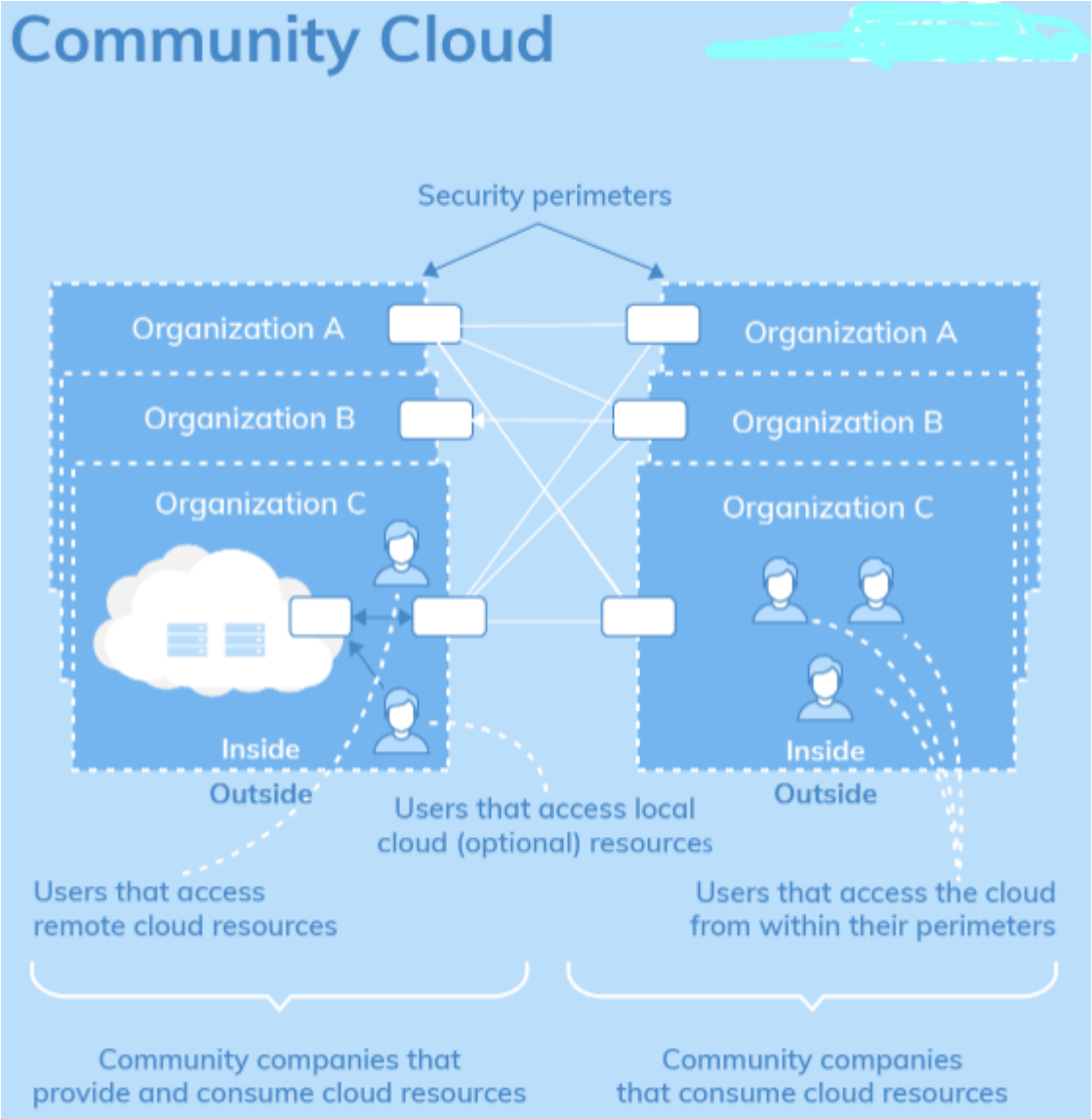

### 2.2.3 Community cloud

Community cloud deployment model works like a private cloud deployment model to a large extent, the difference is community cloud deals with set of users while private cloud server is owned by a particular company, while in the case of a community cloud, the infrastructure is shared by several industries of similar backgrounds. Due to organizations

uniform privacy, security and performance requirements, this multi-tenant data centre infrastructure helps companies in meeting up their business-specific goals. Organizations that work on joint projects will prefer a community model cloud deployment. Therefore, a cloud that is centralized facilitates project implementation and development, and the end users shares the cost among themselves.

| ADVANTAGES | DISADVANTAGES |
|---|---|
| **Reduces costs** | Higher cost than public cloud |
| **Improved reliability and security** | Fixed storage is shared among users |
| **Data easily shared** | Not widespread so far |
| **Services are improved** | Not the choice of every organization |

**Graphical representation of community cloud**



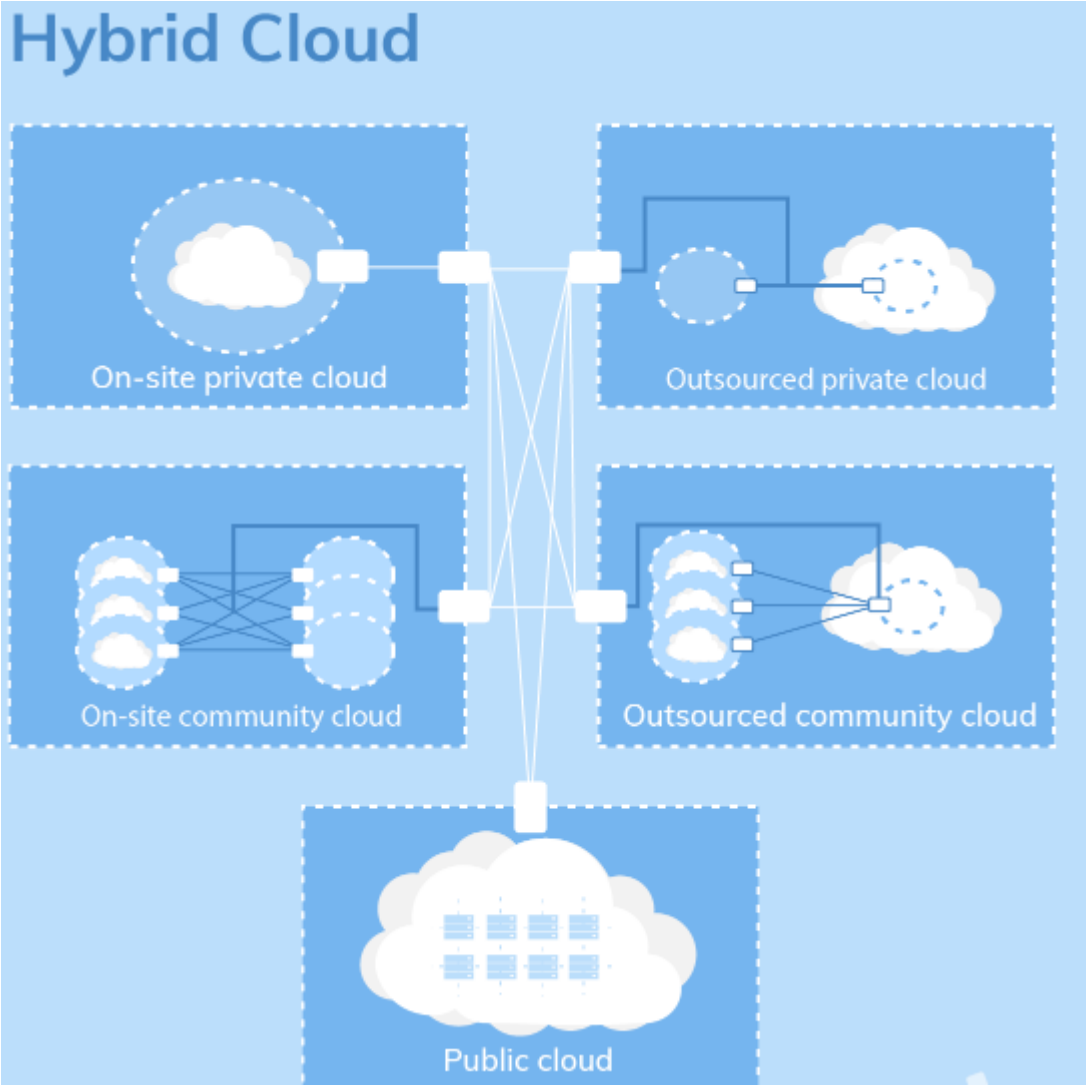

### 2.2.4 Hybrid cloud

Hybrid cloud compasses the best features of the above discussed cloud deployment models, it allows organizations to combine the features of all the other three types of cloud computing deployment models that best suit their demands. For instance, an organization can moderate its load by locating crucial workloads on a private cloud that is secured and deploying sensitive ones to a public cloud. Hybrid cloud can be used by

businesses to take advantage of the profitability and scalability offered by the public cloud environment without the exposure of crucial applications and resources to the vulnerabilities common with public cloud environment. This cloud deployment model builds what is always the most structured cloud solution because different types of resources can be transferred to platform that provides the most secure and private environment. A hybrid cloud deployment model is basically generated in a vendor with an existing private solution comes into partnership with a vendor that provides the platform for a private cloud. Most industries can enjoy benefits from this cloud solution option, for instance; an organization that wants to use a SaaS application but is worried about security and privacy risks can have a third-party vendor to create a private cloud inside its firewall for the organization. Or an organization that renders services customized only for vertical markets can opt-in to use a public cloud solution to interact with its clients, but keep its resources and data secured in private cloud solution. (Derrick, 2014).

| ADVANTAGES | DISADVANTAGES |
|---|---|
| **Improved flexibility and scalability** | The network is always complex |
| **Enhanced privacy and security** | Compliance |
| **Affordable price** | Dependency |
| **Can process big data** | Cloud compatibility can be a real problem if not picked correctly |

**Graphical representation of hybrid cloud**




### 2.2.5 The comparison of the types of cloud deployment models

To easily make decision of the right cloud deployment models by choosing the cloud solution with the most business features, here is a comparative table that shows an overall view of each of the cloud deployment model type.

*THE COMPARATIVE ANALYSIS OF THE CLOUD DEPLOYMENT MODELS*

| | **Public** | **Private** | **Community** | **Hybrid** |
|---|---|---|---|---|
| **Ease set up and use** | Very easy | Requires IT skills | Requires IT skills | Requires IT skills |
| **Data privacy and security** | Very low | High | Comparatively high | High |
| **Data control** | Very little | High | Comparatively high | High |
| **Reliability** | Vulnerable | High | Comparatively high | Comparatively high |
| **Scalability and flexibility** | High | High | Fixed capacity | High |
| **Cost effectiveness** | Cheapest | Most expensive | Cost is shared among members of the community | Cheaper than a private cloud solution but more expensive than a public cloud solution |
| **Demand for in-house hardware** | No | Depends | Depends | Depends |

### 2.2.6 Cloud deployment models and SAAS deployment

Cloud deployment can be seen from the angle of managing the responsibility for the deployment of the Software as a service (SaaS), Platform as a service (PaaS) or Infrastructure as a service (IaaS) solution. There are two approaches of deploying the cloud solutions: maybe deployed by a single entity (using a private cloud deployment model) or deployed by a third party (using a private cloud deployment model, public cloud deployment model or community cloud deployment model).

SaaS deployment is a type of cloud deployment that is deployed using a public cloud deployment model or a private cloud deployment model, it may also be initiated using a hybrid cloud deployment model only when the hybrid cloud resources are managed and controlled by the same entity. SaaS can be deployed by virtual private clouds, Virtual private clouds are basically public clouds that works the same as private clouds, since only permitted entities may access the resources of the virtual private cloud resources.

Many SaaS solutions enables automatic deployment for the cloud services being provided whether the SaaS solution is deployed in a private cloud, a public cloud, a virtual private cloud or a hybrid cloud. SaaS deployment provides benefits over the basic model of deploying software, which includes scalability. SaaS deployment also provides more than average up-time for enterprise applications other than on a premise software development. After the completion of cloud deployment for a Software as a service (SaaS), Platform as a service (PaaS) or infrastructure as a service (IaaS) solution, end user provisioning can take place based on user permissions, where accessing cloud resources is provided based on the end users as either a trusted entity or untrusted entity. Entities that are trusted may gain access to private cloud, hybrid cloud or managed cloud resources. Entities that are not trusted may gain access to public cloud, hybrid cloud or managed cloud resources. Therefore, untrusted entities never gain access to private cloud resources.

### 2.2.7 Cloud services

Cloud service is a service only available to users on demand from a company's own on-premises servers via the internet from a cloud computing providers server as opposed. Cloud services are designed to provide scalable, easy access to applications, services, and resources, and are fully managed and controlled by a cloud services provider (Vangie, 2019). Cloud services can be dynamically scaled to meet the user's needs, and because the service provider supplies the software's and hardware's necessary for the service, there is no need for an industry to provide or deploy its own resources or allocate IT staff to manage the service. Cloud services includes web-based e-mail services, hosted office suites, database processing, document collaboration services and managed technical support services.

# 3. Research finding

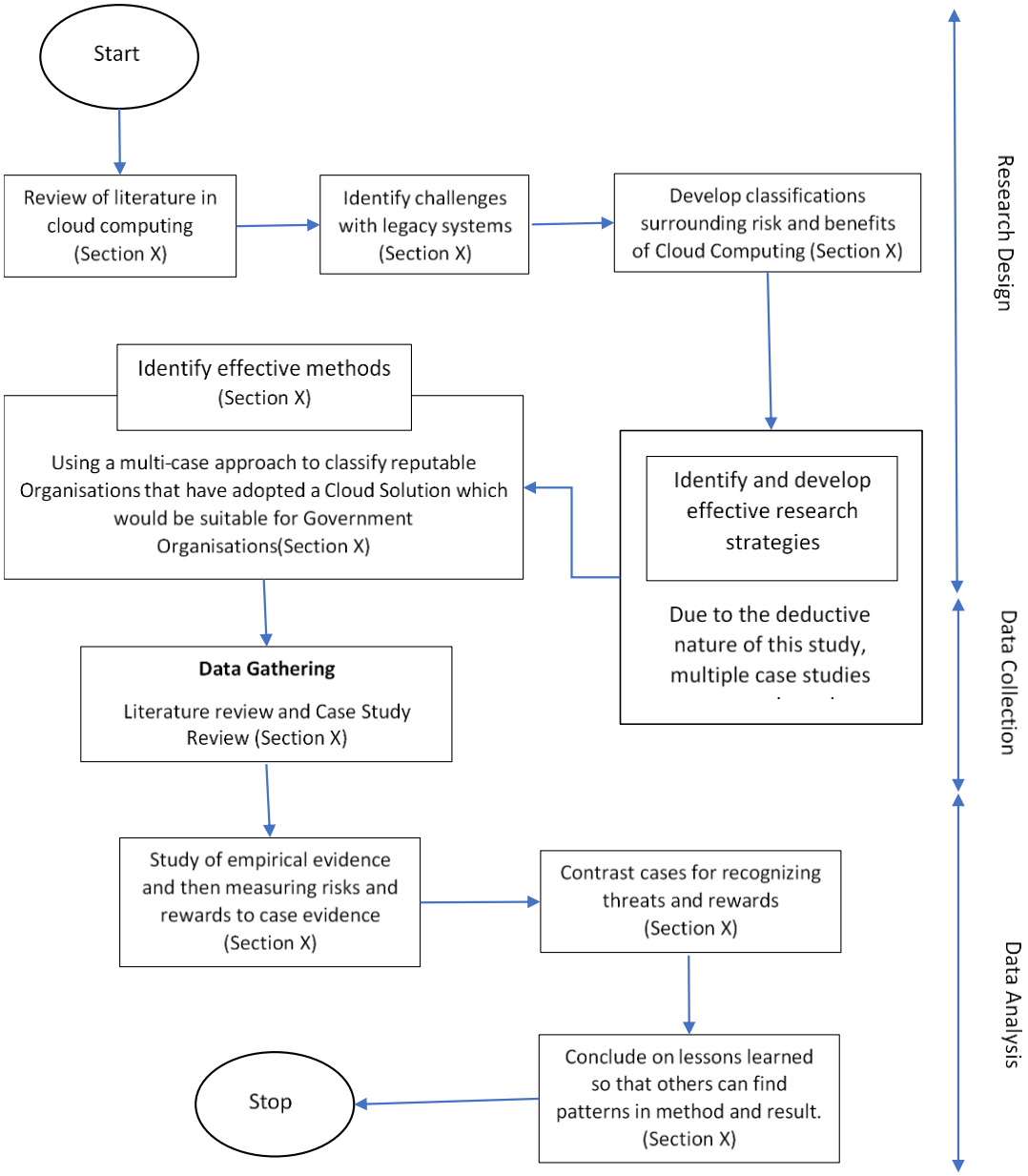
## 3.1 Practical implementation of the cloud to the Government medical organisations

After the understanding of cloud computing and the assessment of the intricacies, advantages, and disadvantages of cloud computing there are some aspects that rise to the top of the consideration list prior to the implementation of cloud computing in the medical organizations in the Mauritian government. These include security of the data, scale and uses of the data, the type of implementation (whether public, private, community or a hybrid) or its in-house or using an outsourcing cloud computing service provider.

For the medical sector handles very sensitive information such as patient names, date of birth, illness history and insurance details it is at the up most importance that his data is not only stored in a secure place and is handled by authorised personnel only to be in accordance with laws and regulations such as the Data Protection Act (DPA) and General Data Protection Regulation (GDPR). with this factor of security being considered the Mauritian government should opt for using a server that is in-built and is private. Based on the previous point security on the information will be achieved but another issue will arise, which is in-build cloud computing services without the intervention of outsourced cloud computing service providers will be tasking in resources, both in the time and cost. For Mauritian government they will need to have the finances to purchase their own servers then, they will need to hire trusted and trained IT professionals with the expertise in cloud computing to handle the migration and maintenance of the data to and on the cloud as well as the hardware. The cost will go towards the purchase of a suitable server, a location with ample space for the IT technicians, the labour cost for the experts and any further maintenance and upkeep once it has been set up since downtime could be detrimental in the medical sector.

# 4. Research methodology

The aim of doing investigation is to understand the challenges faced by migration from legacy systems to using cloud computing. With this goal, the plan to achieve is by using several case studies to understand some of the issues the organisations faced during the process of shifting their resources to the cloud. The case studies help understand the benefits that were attained by some companies who were able to make the migration successfully. This means going through positive and negative scenarios with the aim of knowing what challenges could be faced and how to prevent their repetition when cloud computing is being implemented in the medical sector of the Mauritius government.




## 4.1 Case Studies

### 4.1.1 Case study 1: Air Traffic Control

As the research paper investigates the implementation of cloud computing to the medical sector of the Mauritian government it means there will be a transition of the users changing from legacy systems to a more robust and scalable system which is cloud

computing. This makes this case study important in the studying how the Air Traffic Control (ATC) was able to manage the change in their organisation (Bass and Kazman, 2003).

For the ATC had a growth as the years advanced and through this the complexity of the organisation need a better system to cope with this system as the one in use was rapidly becoming obsolete. With the stakes being public safety, the systems needed to run on optimum efficiency in hundreds of operations on new and more sophisticated hardware. The system proposed to be implemented and succeed the old system was called the Initial Sector Suite System (ISSS) and its intention was to be a software and hardware upgrade in 22 sectors based in the United States for both their air control towers and their ground control facilities (Bass and Kazman, 2003). The ISSS was only a subset of a larger Advanced Automation System (AAS) but it was expected to be operational on 210 consoles and have a centre of 60-90 control positions be able to control up to 2400 aircrafts simultaneously, meaning the system was intended to be large scale. The system had to be error free and with an allowance of only 10sec of down time since the failure can result in plane crashes and deaths (Bass and Kazman, 2003).

This case study sheds light to the fall of this upgrade system for the ATC which was to be procured by the Federation Aviation Administration, it based on several factors, which were the large cost, the system being life long, robust, visible and the importance of the system, the requirements such as the new hardware, network upgrades, new operating systems, human computer interface components (Bass and Kazman, 2003). Although This Factors made it difficult for the FAA to procure the system and opted for a cheaper and simpler system. The system implemented had some of the codes from the ISSS as part of its source code and by an audit made by the Blue-ribbon panel the architecture of the system met and was suitable for the intended requirements and most of the codes were complete.

In conclusion to the above case study regardless to the feasibility of the project and the ability to implement a system it can still fail based on factors such as high cost, complexity and scale and time of the project. For the investigations it is vital to understand that upgrading from an old system to a new system regardless of their benefits

could still end up failing and not come to fruition as planned and the failures must be put into consideration to provide an accurate recommendation.

### 4.2.2 Case study 2: Netflix's transition to the cloud

In 2008 Netflix had seen a range of issues with their current storage system which done in a single data centre. The issue was just having one data centre meant if a failure occurred their services would be down in its entire and it would damage customer relations. They also factored in rise in user subscriptions and the growth of their services, with these factors the management strategized and made plans to get a system that is more powerful, more spacious, and new hardware. One of the things Netflix investigated was having more data centres but this idea was dismissed because of the difficulty in management of multiple data centres, the high cost to set up and it would mean a slowdown in their operations as some of the key engineering resources would be needed for this project.

The second option for Netflix's management was to make use of a 3rd party cloud provider who was Amazon and as learned they are a leader in the cloud computing sector. Netting chooses to use infrastructural as a service (IAAS) which is one of Amazon web services (AWS), simple DB and S3. The benefit included the fact that Amazon had data centres set up already, and they could provide scalability and constant availability in a short amount of time and by Netflix migrating some of their back-end operations to AWS brought an added value since they had more time and effort poured to their main competences and increase customer satisfaction.

With the migration happening and being done fast while Netflix were still rolling out new products made the project be deemed a success but not without its anticipated challenges. With the scale of the project and amount of data that was intended to be migrated was a lot of Netflix in the planning phase they set up phases with sections to be migrated at certain times to make the distractions of managing the scalability and complexity of the distributed system become redundant.

Institutions who utilize cloud computing operating models, are more likely to gain value from the concentration of data that result in centralization, which would lead to well improved consistency and accuracy of data (Verdegem & Verleye, 2009). The data centralization and application of solutions can provide additional tools, thereby fostering apt communications and data control. Reducing the time required to access both data and applications, not only across departments but also, between business partners, generates stronger collaboration. Leveraging existing remote infrastructures into a common information system (IS) reduces installation and monitoring time and expense and focuses on improving quality (Gmach, D et al. 2012). By centrally managing, developing, implementing, and assessing a system, costs can be remunerated across the federalized structure. Nevertheless, cloud computing is an emergent computing service model. Consequently, due to its sheer scale, complexity and novelty, there are still risks, concerns and uncertainties, facing the technology's maturity. The key issues tabled out are in relation to the performance, provider trust, service provider lock-in, control, performance, latency, security, privacy, and reliability of the model (Mircea and Andreescu, 2011). Ensuring that only authorized personnel can gain access to data, would be one of the main challenges to be faced, as cloud computing provides ubiquitous and unfiltered access to stored data (ibid). In addition, even though cloud computing allows for stronger collaboration, the sharing of knowledge is also risky and cannot be done in an arbitrary manner (Marabelli and Newell 2012;). The preceding point stated, also ties in with the problem of trust in cloud computing mechanics and its service distributors. Organizations do question cloud computing's capabilities as it is more of an emerging technology, while neglecting the fact that trusting cloud computing in lieu of the pre-empted security issues, doesn't lie entirely in the technology itself but also in the hands of the data controllers. The lack of customer confidence also rises from a lack of total transparency, a loss of control over data assets, and vague security assurances (ibid). Therefore, while cloud computing remains one of the top technology investments, the deployment and incorporation of these technologies is being made cautiously due to its unforeseeable long-term implications. Government organizations continue to be under increasing pressure to find new ways to measure the contribution of their organizations' IT investments to enhance performance, as well as finding reliable ways of ensuring that the

values gotten from these investments is realized (Lin and Pervan 2003;). Therefore, it is important for managers to improve their understanding of the impact of IS on organizational performance; in particular, understanding the rewards and risks related with the financial and social capital investments in developing such infrastructures.

## 4.2 Risks of cloud computing

| Classification | Factors | Description |
|---|---|---|
| **Strategic** | • Case of complex business financials<br>• Loss of government control<br>• Failure to trust providers.<br>• The problems of security and privacy | ∽ Because most cloud implementations are at an early stage, there are minimal or unproven financial business cases that justify the implementation of cloud systems. It is worth noting that this risk could oscillate between the organization's strategic and operational risks.<br>∽ Cloud computing amplifies the need for transparency, allowing the company to track and control policies, processes, and standards for cloud computing services.<br>∽ Organizations transfer full control over certain aspects of security and privacy to the cloud provider, which requires a high degree of trust from the provider.<br>∽ Data security and privacy are a major concern because there is a possibility that unauthorized users |

| | | |
|---|---|---|
| | | will gain access to confidential data because of multiple users accessing the servers all the time. Security and privacy threats may also change between the organization's strategic and operational threats. |
| **Tactical** | • Restrictions on portability<br>• Disputes regarding ownership of data<br>• Restrictions on integration | ∽ The problem of being stuck in a single cloud service provider due to high switching costs in terms of effort and time to switch between providers.<br>∽ The data ownership rights of the company must be clearly defined in the service contract to provide a basis for the protection and privacy of the data.<br>∽ Integration with facilities hosted at other data centers can be difficult to achieve. Organization-specific peripherals (e.g., printers) and email systems can prove difficult to incorporate into cloud systems. |
| **Operational** | • Inefficiency<br>• Restricted storage space<br>• Economic strain<br>• Loss of control<br>• Lack of accurate information on location of data<br>• Restrictions on recovery after disasters<br>• The lack of quality | ∽ The sharing of internal and external servers can lead to new problems due to the time needed for the transfer of data to external systems. Issues of inefficiency are popular with new systems because the actual load varies from the planned load.<br>∽ Though most cloud service providers promise unlimited storage space, some providers |

| | | |
|---|---|---|
| | service<br>• Hard to configure | have limits on the storage space that they can/will provide.<br>↬ While cloud hosting may prove a lot cheaper in the long run, it is still new and needs to be researched and improved, making it more costly in the short run.<br>↬ Moving to the public cloud requires the transition of responsibility and power to the cloud provider, which may result in a lack of control over both the physical and functional aspects of the system network and the data.<br>↬ As data is processed redundantly in several physical locations, there is a chance of unavailability or unrevealed details on the location of the data of the organisation.<br>↬ Natural disasters pose great risk, they can lead to partial or total data loss.<br>↬ Availability of cloud services can be affected temporarily or permanently due to equipment failures, virus attacks, etc.<br>↬ Decreased ability to configure services, as the company does not have leverage over cloud infrastructure offered by providers. |

## 5. Conclusion

This research review examined the experience of designing a cloud-based computing solution for organisations as an alternative to legacy systems. By doing so, encouraging us to draw similarities by patterns and procedures from the examples presented, eventually benefiting the public purse by preventing expensive mistakes. The literature and research results clearly indicate that the need for cloud computing solutions continues to expand as more organizations start using creative data storage and sharing tools. Theoretical insights can tend to be obtained by drawing comparisons from other technical paradigms, as this paper aimed to provide a cross-comparison rather than a theoretical construct or study. Both industry and academics foresee a bright future for cloud computing because they expect it to become the norm, with businesses increasingly relying on cloud-based software instead of using traditional desktop systems. The work published in this paper encourages a deeper understanding of process and governance threats that will change the choice of organizations from expensive on-site Infrastructure to auditable and reliable security practices of cloud service providers. Apart from the benefits that these technologies have to offer, there has been growing concern about the risks that cloud computing can pose to commercial users. The empiric results of this study have demonstrated a range of specific classifications of benefits (strategic, tactical, and operational) and threats experienced by the implementing organisation, following a rigorous assessment of this modern and evolving technology. While mixed results have been achieved in all cases with the introduction of cloud computing, the application of this technology has been well received by employees and users.

# References


Ani, M (2018). Cloud Deployment Models.:

Bang, A., 2015. *Cloud Computing: History, Architecture, Security Issues*. Sardar Vallabhbhai National Institute of Technology.

Bass, L. and Kazman, R., 2003. Creating an Architecture. In: L. Bass, ed., Software Architecture in Practice, 3rd ed. pp.129-151.

Bohm, M. and Krcmur, H., 2011. *Cloud Computing and Computing Evolution*. München: Technische Universität München, pp.6-16.

Carretero, J. and Blas, J., 2014. Introduction to cloud computing: platforms and solutions. *Cluster Computing*, 17(4), pp.1225-1229.

Cloud Standards Customer Council, 2017. *Practical Guide To Cloud Computing Version 3.0*. Cloud Standards Customer Council, pp.6-36.

Derrick, R. 2014. Cloud Deployment Models. [Online]. [11 Feb 2020]. Available from: http://www.sciencedirect.com/topics/computer-science/cloud-deployment-model

Journal of Environmental Science, Computer Science and Engineering & Technology, 2017. Cloud Computing- Benefits & Limitations. 6(2).

Jones, S., Irani, Z., Sivarajah, U. and Love, P., 2017. Risks and rewards of cloud computing in the UK public sector: A reflection on three Organisational case studies. *Information Systems Frontiers*, 21(2), pp.359-382.

Lin, C. and Pervan, G., 2003. The practice of IS/IT benefits management in large Australian organizations. *Information & Management*, 41(1), pp.13-24.

Marabelli, M. and Newell, S., 2012. Knowledge risks in organizational networks: The practice perspective. *The Journal of Strategic Information Systems*, 21(1), pp.18-30.

Mircea, M. and Andreescu, A., 2011. Using Cloud Computing in Higher Education: A Strategy to Improve Agility in the Current Financial Crisis. *Communications of the IBIMA*, pp.1-15.

Vangie, B. 2019. Cloud Service. [Online]. [11 Feb 2020]. Available from: http://www.webopedia.com/TERM/C/cloud_services.html

Verdegem, P. and Verleye, G., 2009. User-centered E-Government in practice: A comprehensive model for measuring user satisfaction. *Government Information Quarterly*, 26(3), pp.487-497.

Xue, C. and Xin, F., 2016. Benefits and Challenges of the Adoption of Cloud Computing in Business. International Journal on Cloud Computing: Services and Architecture, 6(6), pp.01-15.

Yuliya, S. 2018. 4 Most Popular Cloud Deployment Models You Need To Know. [Online]. [11 Feb 2020]. Available from: http://www.sam-solutions.com/blog/four-best-cloud-deployment-models-you-need-to-know/