SOLENT UNIVERSITY

Faculty of Business, Law, and Digital Technologies

MSc CYBER SECURITY ENGINEERING

Academic Year 2021-2022

Osazuwa Odigie

TOPIC:

DE-CLOUDING IN SMALL AND MEDIUM ENTERPRISES

Student Number: **Q15708489**

Supervisor: Associate Prof. Andy Farnell **Date**: September 2022

This report is submitted in partial fulfilment of the requirements of Solent University for the degree of MSc Cyber Security Engineering

ACKNOWLEDGEMENT

Firstly, I would like to appreciate my God and father in Christ Jesus who is my life and the length of my days for the opportunity to be part of this life changing event in history in good health and sound mind. I never could have made it without your loving kindness to me and my family. Your faithfulness is beyond my wildest comprehension.

Secondly, I would like to thank every small-scale business owner who took time to complete my questionnaire as part of this dissertation data collection; your contribution made all the difference to this research. I would also like to specially thank my dissertation supervisor, Associate Professor Dr. Andy Farnell for your guardians as well as other Solent university lecturers who took time to impact me with the knowledge required to carry out this project. My special thanks to my colleagues, with special reference to Seun for your support, motivation, and friendship. I am indeed grateful.

Lastly, I would like to appreciate my darling wife Kome Odigie; you have been my number one fan, support, and motivation. I am indeed grateful for your love and consistency. Also, I want to thank my children Zoe Odigie and Zane Odigie; thank you for putting up with daddy through this whole study process. I really appreciate it. Without leaving out all other members of my family; to you all I say thank you.

ABSTRACT

Following concerns of security compliance, levels of latency due to traffic congestion and inconsistent application execution with regards to the use of the public cloud services, gave rise to a recent trend which necessitated the concept of declouding which is also known as cloud repatriation. This gave the inspiration for this research topic. Given the complexities surrounding the subject matter, a case study approach was adopted in getting an in-depth knowledge on the subject by first determining the veracity of the claim and to understand why businesses were embarking on cloud repatriation. Some other issues related to declouding such as the oscillatory tendencies of decentralisation and centralisation of computing models, the CAPEX vs. OPEX issues in relation to the inappropriate cases the public cloud was offered for, and why the on-Premises cloud is a better solution in many cases.

Furthermore, a comparative analysis was carried between on-premises infrastructures and the public cloud in relation to cost, performance, and security. A cursory look was given to policy issues surrounding the cloud as well as the concerns of deskilling and outsourcing in cloud computing. Additionally, the concept of Homomorphic encryption as it had to do with guaranteeing the data privacy, data security and data integrity with the aim of determining the best option of Homomorphic encryption to deploy was also reviewed.

Lastly, a qualitative approach was adopted in addressing the workload placement optimization problem by deductively extrapolating data from existing proven literatures to design a workload application placement model which was designed on a webpage to educate and guide small and medium scale businesses in optimizing their workload allocation given the different cloud option available in the market to meet the needs of the organisation. A collection of findings was documented in the concluding part of this research with recommendations proffered.

Table of Contents

ABRIEVIATIONS

LAN – Local Area Network

WAN – Wide Area Network

CPU – Central Processing Unit

IDC – International Data Corporation

AWS – Amazon Web Services

CAPEX - Capital Expenditure

OPEX – Operating Expenditure

CSP – Cloud Service Providers

GDPR - General Data Protection Regulation

VHD – Virtual Hard Disk

VM Ware – Virtual Machine Ware

VOTE – Voice of the Enterprise

ROI – Return on Investment

TB – Terabyte

IT – Information Technology

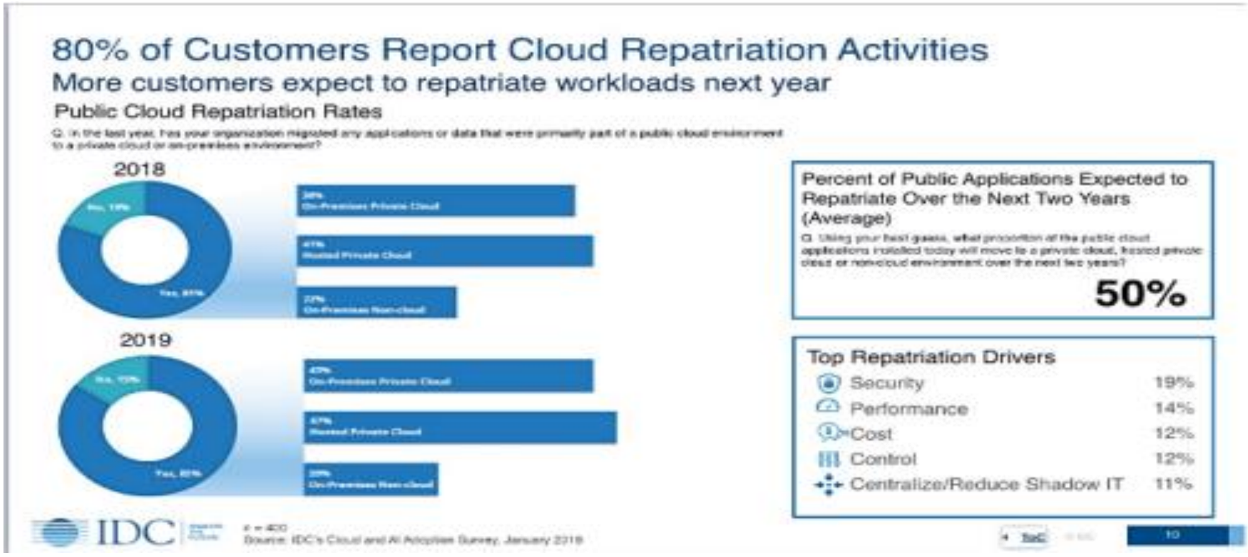
PII - Personally Identifiable Information

INTRODUCTION

This chapter provides an introduction of a current cloud computing industry trend called "Declouding," also referred to as "cloud repatriation," which served as the inspiration for this MSc research topic. In relation to the topic, overviews of case studies are presented.

The following concerns of security compliance, levels of latency due to traffic congestion and inconsistent application execution with regards to the use of the public cloud services, necessitated the concept of declouding which is also known as cloud repatriation (Donnelly, 2019). Cloud repatriation, according to IT specialists, is the transfer of workloads from public clouds to the local infrastructural ecosystems (Parmar, 2021). Similarly, (Montgomery, Casey and Semilof, 2022) defines Cloud repatriation or De-clouding as removing data or applications from the cloud and transferring them to a local data centres. Presently, organizations are switching to a private or hybrid cloud solution (McHenry, 2019). On the other hand, public cloud is an information technology concept in which on-demand computing resources and infrastructure are operated by a third party and distributed across different enterprises via the public Internet. Some examples of public cloud providers are Google Cloud, Amazon Web Services (AWS) and Microsoft Azure (IBM Cloud Education, 2020) and (Li et al., 2010).

According to a 451 Research analysis on cloud repatriation, 20% of organisations claimed pricing drove them to transfer one or more of their workloads from public clouds to private clouds. Similarly, according to a 2018 International Data Corporation (IDC) study, 80 percent of participants relocated cloud operations to local infrastructure or private cloud solutions in the preceding period, as seen in figure 1. As a result, Dave Cope, Senior Director of Market Development for Cisco's Cloud Centre stated that they were seeing a natural dispersal of workloads between old and new environments where it made the most sense.



80% of Customers Report Cloud Repatriation Activities

More customers expect to repatriate workloads next year

Public Cloud Repatriation Rates

Q. In the last year, has your organization migrated any applications or data that were primarily part of a public cloud environment to a private cloud or on-premises environment?

Percent of Public Applications Expected to Repatriate Over the Next Two Years (Average)

Q. Using your best guess, what proportion of the public cloud applications installed today will move to a private cloud, hosted private cloud or non-cloud environment over the next two years?

50%

Top Repatriation Drivers

Security	19%
Performance	14%
Cost	12%
Control	12%
Centralize/Reduce Shadow IT	11%

n = 400
Source: IDC's Cloud and AI Adoption Survey, January 2019

Figure 1: IDC Poll on Cloud Repatriation (Source: IDC Report 2018)

The above shows that workload repatriation patterns vary across industries and business functions which has also presented the problem of choice with regards to what should be in the public cloud and what should be left in the On-premises infrastructure. According to IDC studies, newer businesses are far more likely than those in business for more than 25 years to repatriate public cloud workloads (IDC Report 2018). Though the cloud pledged to reshape enterprises by delivering fast, secured, and scalable solution, the hoopla surrounding utility computing or on-demand computing and the advantages that followed caused companies to lose sight of the business requirements, forcing them to shape their requirements to conform to the cloud instead of the cloud adjusting to meet theirs. This has resulted in some businesses shifting their entire company structure to the cloud, resulting in significant financial losses (Donnelly, 2019).

Historical Background

To explain how it works, we must first explore how alternative computer models were accepted when new technology arose. Since the introduction of the mainframe to the commercial sector, there have basically been two models that have been playing out alternately.

Models of Computing: Centralised vs. Decentralised

(Levine, 2016) and (Elliott, 2019) provided a concise overview of the oscillating models of centralization and decentralisation. He recounted how, in the 1960s, mainframe and minicomputer computers used a centralised approach with dispersed dumb terminals for input and output. However, computing resources and software were centralised. The personal computer revolution began in the 1970s, and by 1980, personal computing had entered the public consciousness. Decentralisation made its first appearance in computing. Rather than dumb terminals, every user now has his or her own computer which had its own memory and CPU. And as computers became smaller and more affordable, people began purchasing them for use at home. However, because most home computers were not networked and could only interact by sharing physical memory devices such as tapes, cartridges, and floppy discs, applications were split rather than decentralised. Similarly, UNIX introduced the concept of decentralised computing, in which software was installed on multiple computers or workstations connected by a LAN or WAN network. This resulted in the adoption of both standalone and networked architectures in the form of client/server and peer-to-peer applications (Elliott, 2019). Following was the emergence of the Web technologies of the 1990s, which enabled the server software to be deployed in a single location while Web clients were deployed as needed in remote, scattered locations. This restored the centralised model, which is still in use today through the cloud (Manovich, 2003).

Many businesses are now more committed to developing a cloud strategy that meets their unique set of goals and objectives. And as such the need to understand the variety of service options available between the On-premises and Public cloud is critically important (Marston, 2011).

Planning Cloud Repatriation

When migrating workload from the public cloud to on-premises infrastructure, coordination, and planning with both the technical and business teams are critical. Preferences for migration must be defined first. It is equally important to thoroughly examine the current environment via discovery. This entails compiling a detailed list of programmes, databases, domains, workloads, and other resources that may be migrated. Applications, data, and online services should be classified according to their nature, function, and importance (Kenneth, 2021). An environment can be inventoried using various discovery tools and procedures. Creating a migration plan will benefit from a thorough and accurate inventory. Using this inventory, the business may determine which workloads should be prioritised for migration, which workloads should not be moved, and how much resource is needed at the location. Figure 2 shows a strategic smart data migration approach.

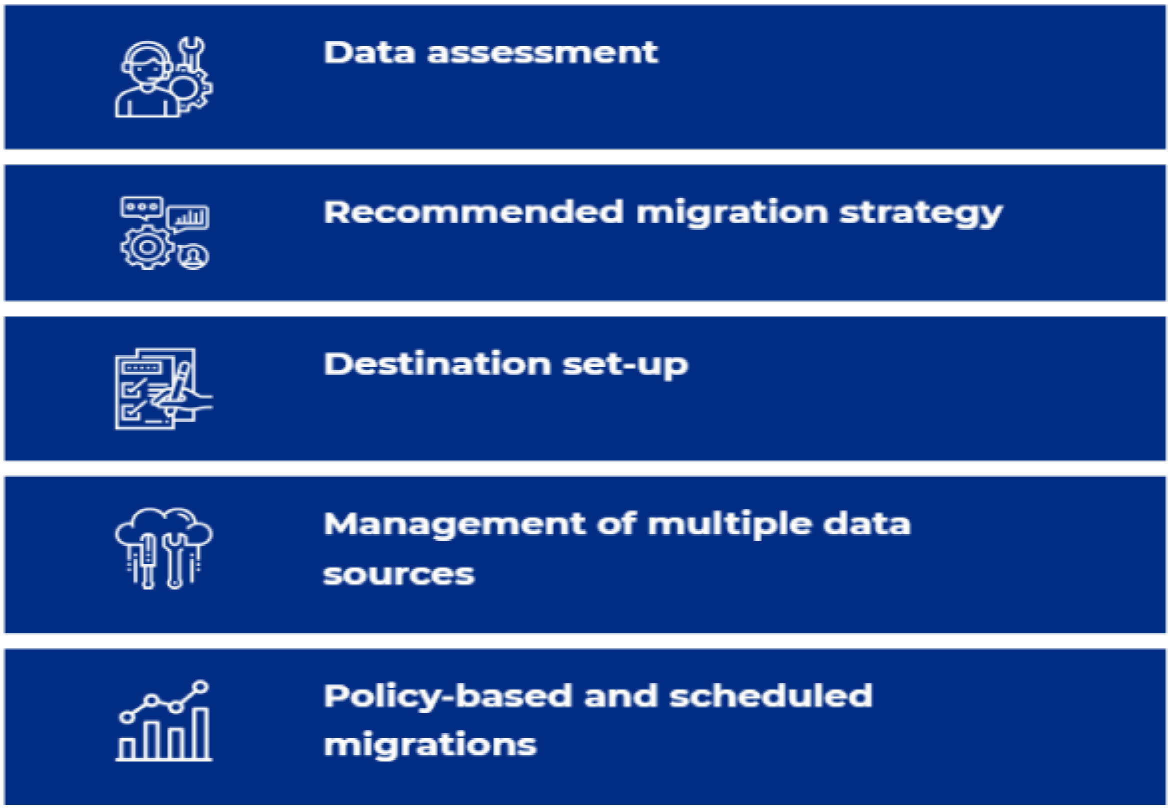

Data assessment
Recommended migration strategy
Destination set-up
Management of multiple data sources
Policy-based and scheduled migrations

Figure 2: Smart Data migration Approach. Source: (Nephos Technologies 2022)

Research Questions and Deliverables:

The question then is why are businesses migrating from the off-premise cloud or public cloud? After all, the benefits of the off premise public cloud have been lauded for everything from security to cost savings.

Secondly, this study will be investigating why the on-Premises cloud is a better solution in many cases and why public cloud is pushed in inappropriate cases in relation to CAPEX vs. OPEX as well as the issues of deskilling and outsourcing.

This research will attempt to give a case study review of the limited literature resources on this subject, but also older academic literature on centralised versus decentralised computing architectures with a view to give practical answers to the **"Why"**.

This paper will give a cursory look to how cloud repatriation is done with particular attention to migrating workload from Microsoft Azure to an On-premise cloud.

This study also seeks to show the cloud cost comparison by contrasting the cost implication of setting up an On-premises or private cloud to the cost of registering with a commercial cloud service provider as well as a performance analysis on both On-premises and public cloud.

Lastly, an application workload placement solution guide will be developed to address the problem of workload placement optimization as it has to do with utilising the proven theories available in allocating workload which will be based on a variety of factors or indicators which a business can use to choose where each of its workloads should be allocated.

Purpose of Study

The purpose of this study is to evaluate and ascertain the veracity of the cloud repatriation claim and to conduct a case-by-case study review on the sparse academic literature on the topic to ascertain the reason(s) behind this development. It will also draw information from older literature on the oscillatory nature of the decentralised and centralised model of computing architecture. In addition, legislative concerns around cloud computing will be examined, as well as Homomorphic Encryption, a recent breakthrough in cloud solution for enhancing data security and design a workload placement optimization guide which will enable enterprises to decide on the best cloud option.

Thesis Structure

The following chapters make up the completed dissertation structure: The dissertation's situation and the research challenge are fully described in Chapter One: Introduction. Chapter Two: Case Study Review — Identifies companies that have undergone cloud repatriation as well as the justifications offered by academics for some enterprises to transfer their workload from public cloud. It also gives a cursory glance to how cloud repatriation is down with particular attention to migrating workload from Microsoft Azure to an On-premises cloud, GDPR issues, cost analysis, and cloud security challenges. The case study methodology is adopted in Chapter 3's methodology section in addressing the subject matter. Results in Chapter 4 are based on the deductive extrapolations from existing proven theories which are used to design a workload placement models for small and medium scale enterprises. Chapter Five: Conclusions and Future Work - In this chapter, the overall research's conclusion and suggestions for further research are presented.

CASE STUDY REVIEW

Is cloud repatriation a real phenomenon or a passing fad? According to several surveys and statistics, cloud repatriation is not slowing down anytime soon. According to 451 Research's Voice of the Enterprise (VOTE) Cloud Transformation, Organisational Dynamics 2017 survey, 34% of respondents had already shifted their workloads from a public cloud to a private environment (cloud or otherwise). This was due to a variety of factors. Many of those reasons were the same as why organisations switched to the public cloud in the first place: Cost, control, security, and latency, performance, and scalability challenges. Businesses are growing more adept at determining its requirements, and Dropbox exemplifies this phenomenon; within 2years, the business saved about seventy-four million dollars on operational expenses after 'de-clouding' from AWS and into its own data centres (McHenry, 2019).

Another example according to (Network World, 2018) and (McHenry, 2019) is the New Belgium Brewing Company, which newly moved its key applications from the publicly managed cloud to a local infrastructure environment. Travis Morrison who is the Director of IT emphasised the need for predictable expenses while scaling as a major reason for their action. He also added that they are building an IT team who could manage their on-premises equipment. Furthermore, he stated that a hyper converged stack which integrates all data centre features (storage, computation, networking, and management) into a single, pre-configured hardware box could reduce the cloud’s return on investment (ROI) by their simplified operation and management process.

A final case for consideration is significant organisations, like Uber or Airbnb, which are built on the marketing strategy of operating as a mediator among suppliers (e.g., drivers) and customers (e.g., passengers or travellers), fundamentally leveraging crowd sourced resources. Solutions like de-clouding could take over the jobs of the trusted intermediary in these types of services, eliminating the institution in the middle which mostly impacts cost negatively (Zavodovski et al., 2020).

Many businesses might benefit from a private cloud or private infrastructure environment. For instance, the Yankee Group report of (2019) found that private cloud was preferred 2:1 over fully managed public cloud option. Private cloud services were selected by 67% of participants, whereas fully managed public cloud services were favoured by only 28 percent. The remaining poll respondents desired a hybrid cloud solution.

In this section, consideration will be given to the various reasons why cloud repatriation may make sense in a company.

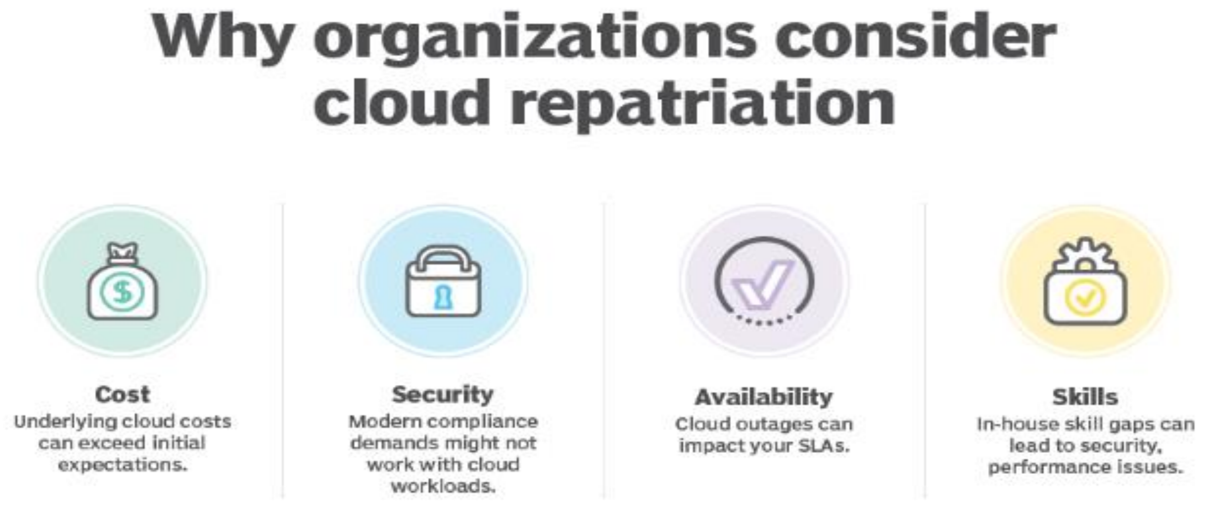

Why organizations consider cloud repatriation
Cost
Underlying cloud costs can exceed initial expectations.
Security
Modern compliance demands might not work with cloud workloads.
Availability
Cloud outages can impact your SLAs.
Skills
In-house skill gaps can lead to security, performance issues.

Figure 3: Reasons for Cloud Repatriation. Source: (TechTarget 2020)

Cost Savings

Cloud repatriation has the potential to drastically reduce, if not eliminate, the public cloud's high recurring operational costs. When compared to on-premises solutions, public cloud products might deliver benefit, but at a cost in terms of recurrent expense stated Jeremy Kurth, CTO of IT services at Winxnet. Similarly, Cloud service providers extolled the cloud's cost advantages and perks for owning and maintaining data centres. Though the on-premises data centres are often expensive, these prices pale in comparison to the public cloud's hidden costs. As cloud providers disguise high costs with attractively cheap on-boarding charges and capital expenditure (CAPEX) to conceal continuing operating expenses (OPEX). This is where organisations get caught off guard, because it is not relocating the entire data centre that will cut business costs, but rather using what you need in both the data centre and the cloud (Donnelly, 2019) and (Shehabi et al,. 2018).

Furthermore, a private cloud service provides clients with transparency into billing systems, and the pay-as-you-go model enables businesses to only pay for what they require. According to (Koomey, PhD, 2017), organisations waste up to $62 billion annually, paying for public cloud capacity that the business does not use.

Security and Control

According to the survey by a research firm IDC in 2018, the main reason for companies shifting away from public cloud was security, which was polled by 400 decision-makers from small, midmarket, and big corporate firms. Hosting all corporate applications in the cloud raises a number of threat concerns, since most public-cloud providers do not provide adequate security to safeguard all aspects of the business. Following these disparities in security measures throughout an enterprise, a single cloud provider would not suffice, and a combination of different cloud services is recommended towards assuring the protection of sensitive information. However, an on-premises data centre, on the other hand, has well-defined security procedures. For instance, it is straightforward when observing where the door opens and closes. With cyber-security threats on the rise, businesses are becoming increasingly concerned about their security procedures. Hence going on-premises, where a firm can keep control of its information, ensures that both client and business records is secure (CRN News, 2018).

A comparative analysis on the security challenge between public cloud and private cloud showed that the private cloud computing is ideal and safer for large-scale businesses, and it is extremely beneficial for large-scale businesses to adopt private cloud computing when security is a top concern (Imran et al., 2018), as shown in figure 4.

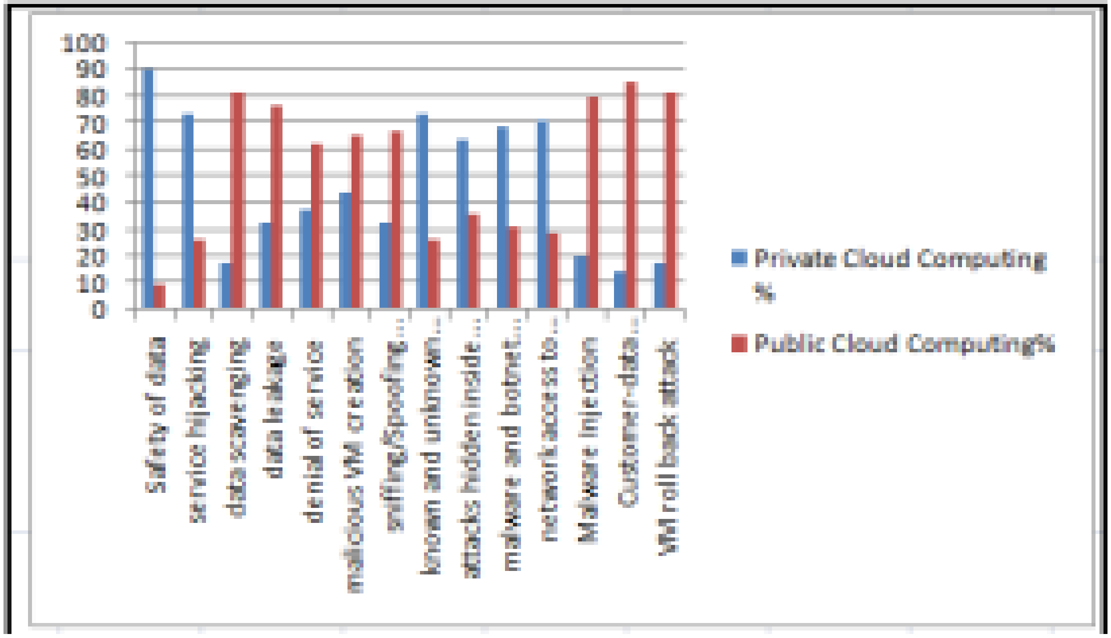


Figure 4: Security concerns in Public vs. Private Cloud Computing Compared (Imran et al., 2018)

Improved Performance

Bringing operations back on-premises has been found to assist in solving performance and downtime issues. Although an on-premises solution does not eliminate downtime entirely, it does return control to the firm (McHenry, 2019). In 451 Research's VoTE survey, participants were asked why they used various infrastructure settings to run particular workloads. One of the key motivations for leveraging various infrastructure settings, according to 47 percent of them, is to improve performance and availability. Failure to satisfy crucial operating standards may indicate that applications would run better in a private environment. According to (Network World News), Jeff Slapp, who is the Vice President of Cloud and Managed Services at 365 Data Centres, stated that applications that are latency sensitive, have long-running input /output intensive periods, or have large datasets that require transport between multiple locations for processing are commonly ideal candidates for repatriation (Greenberg et al., 2021).

Latency

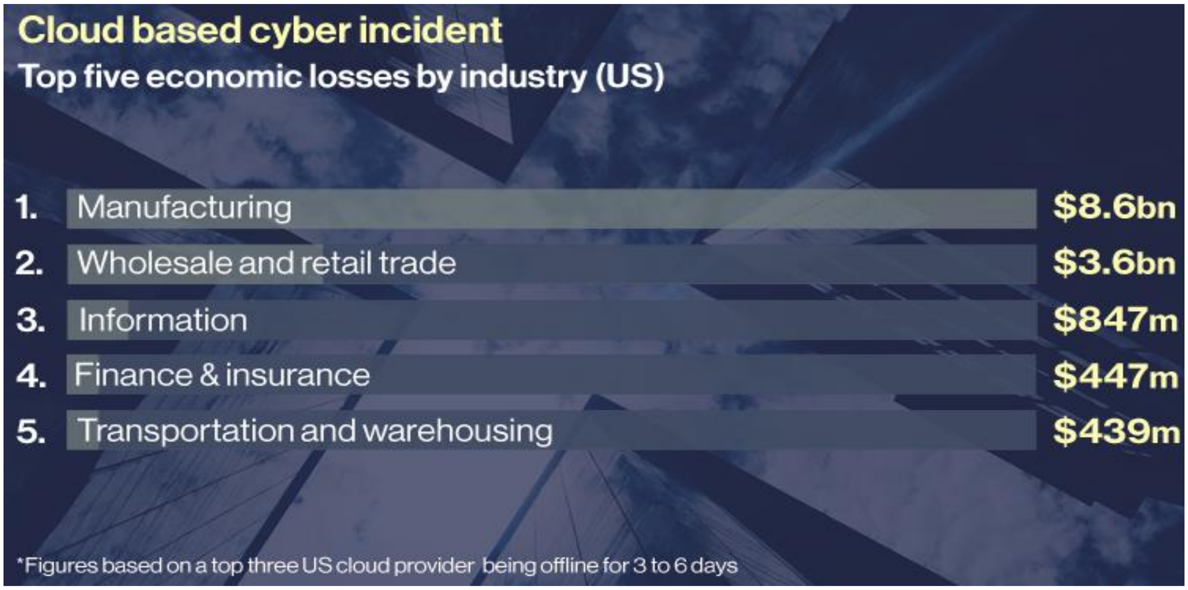
Latency has a significant impact on how usable and satisfying technologies and connections are. These issues can be exacerbated in cloud service connections, which are notoriously vulnerable to latency for a variety of reasons. Firstly, latency in the cloud is less predictable and more difficult to quantify. Most latency measurement techniques, such as trace route and pings, rely on ICMP packets, which are rarely used (Optimum 2022). Additionally, several variables influence delay, such as the standard number of router hops or ground-to-satellite communication hops on the route to the destination 7 server. A business may wish to know the geographic location of a cloud service data centre because they can be physically situated anywhere in the globe. The bigger and unpredictable workload in a cloud environment also results in more uncertainty in delivering services (Tchernykh et al., 2015). Visualisation could cause packet delays, particularly if virtual machines (VMs) are on different networks. If the client network's wide area network (WAN) is congested, this might have a major impact on latency. Some businesses invest in a designated WAN to support cloud activities. However, on-premises and hybrid resources are planned based on the availability zones of clients and staff, the availability zone of public cloud regions is determined by the cloud provider. Because most cloud operating data is hundreds of kilometres away, the speed of light is limited, producing latency and performance difficulties (Zaindenwerg, 2021).

Scalability

Most expanding firms find colocation to be an appealing option due to the requirement for long-term scalability (*Alberding, 2015)*. Adoption of colocation in addressing the problem of scalability impacts positively on cost, performance, compliance, and services of a firm (Bigelow 2020). It would be difficult for a company to choose the ideal size if it were to construct its own on-site data centre. The data storage infrastructure would need to be able to scale for dealing with unexpected capacity needs in addition to meeting their immediate needs. Spending money on space that will never be used carries a significant risk. Overbuilding can result in the loss of valuable funds that could be applied to corporate expansion. The "pay-as-you-grow" business model offers the flexibility that expanding companies require. Businesses just pay for the space that is really utilised and are free to add or subtract rented space as needed. Colocation service providers lessen the possibility of managing empty or inadequate space (Light Edge, 2019).

Provider Failure

The most important justification for data repatriation may be provider failure (Pritchard, 2021). According to a recent research by Air and Lloyd's of London, the performance failure of numerous top cloud service providers has had a detrimental impact on the finances of many businesses as shown in figure 5.



Cloud based cyber incident

Top five economic losses by industry (US)

1.	Manufacturing	$8.6bn
2.	Wholesale and retail trade	$3.6bn
3.	Information	$847m
4.	Finance & insurance	$447m
5.	Transportation and warehousing	$439m

*Figures based on a top three US cloud provider being offline for 3 to 6 days

Figure 5: Implication of Performance Failure from CSPs. Source: (Lloyd's, 2022)

Failures can cause serious service delays, lower productivity, and reputational harm for businesses in addition to the immediate cash losses. Therefore, it's crucial to reduce these pauses, which calls for an understanding of what produces them (Endo *et al.*, 2017). Part of the reason is that companies all over the world are using cloud computing services at an exponential rate, establishing a high level of firm dependency and, as a result, making CSP highly powerful and wielding a lot of influence (Calvesbert, 2018). Most likely, the consumer will not have a choice. Ideally, the service provider will provide enterprises advance notice and a practical deadline to retrieve their data or transfer it to another cloud provider. However, it is probable for a provider to stop operating without prior notification due to technical difficulties or adverse environmental conditions. In that event, businesses will need to rely on backup copies of their data that are stored locally or in another cloud. Complete provider failure is uncommon, which is a good thing. However, the knowledge learned from recent cloud outages implies that, at the absolute least, organisations need a plan for how to secure and retrieve their data if it does happen. And any recovery strategy will probably be heavily reliant on on-premises technology, even if just to tide the company over until it can procure fresh cloud capacity. Prior to actually shifting a workload to the cloud, one should consider whether doing so will improve the service's ability to withstand failures in front of customers or the general public, knowing that if the reason for relocating workload is to cut costs, the costs of putting resiliency back in at a later point in time could cancel out any advantage (Pritchard, 2021).

Vendor Lock-in

As a result of lack of standards, vendor lock-in is a significant obstacle to the adoption of cloud computing (Toivonen 2013). Vendor lock-in is the term used to describe a position in which a company wants to move its business away from one of its present vendors but is unable to do so because of the anticipated cost, length of time, or complexity of moving (Opara-Martins *et al.,* 2016). Similarly, (Donoghue, 2022) states that in the IT sector, the phrase "vendor lock-in" is pretty pervasive. It is essentially a method created by the CSPs to make sure a client is kept for as long as feasible while maximising sales of as much service and product during that period. He added that Making products and services difficult for the cloud user to integrate with other products or services that the user may want to utilise in the future is a dishonest contractual tactic. Except perhaps an additional installation of application from the said vendor needs to be licensed in order to enable the integration which would be at a price to the client.

Figure 6: Making Prisoners of cloud users via vendor lock-in. Source: (Economit 2022)

However, others say that there are no many studies that investigate and show how complicated the vendor lock-in issue is in the cloud context. As a result, while purchasing services from vendors, the majority of clients are uninformed of the proprietary standards that prevent application portability and interoperability (Opara-Martins *et al.*, 2016).

Government Intervention in Cloud Service - General Data Protection Regulation (GDPR) Issues on Cloud Computing

The increasing significance of cloud services and cloud service providers (CSPs) in societal structure has drawn the concern of policy makers and regulators who want to take advantage of this emerging technology while trying to handle associated threats. As a result, governments use data security policies and regulations as tools to create a balance and check the activities of cloud services and CSPs (Levite and Kalwani, 2020). Small and medium-sized organisations are the victims of 80 percent of cyber-attacks, and cyber security has never been more important (Deloitte, 2022). Many businesses feel a lot safer whenever they are in control of their systems' infrastructure, which is impossible when the public cloud provider oversees data protection. There are also regulatory compliance issues to think about. Under GDPR, the organisation hosting data is responsible for its security and can be penalised if they fail to prevent this data from intruders. The Information Commissioner's Office has fined British Airways £183 million after intruders illegally obtained the data of 500,000 customers of theirs. Companies just cannot afford to have insufficient security (Tolsma, 2022).

One concern with cloud computing is the value of the data entrusted to it. As a business, one can host numerous types of data on the cloud, including confidential material, which amplifies the risk of this data being transferred uncontrollable to third-party firms (i.e., competitors) to which the users do not want external parties to be privy to. There is a risk of data leaking if a cloud computing solution is used in which data processing or storage facilities are distributed. Similarly, identifying which laws apply to a firm can be tricky. Cloud computing can hide the relationship of data to a geographical location. It is not always evident where information is stored. As a result, finding the relevant law may be difficult for an organisation. Geographic location is an important factor in determining whether privacy standards apply within the EU. Other laws, on the other hand, may apply in other jurisdictions. This process is becoming increasingly difficult due to the clear fragility of data on the cloud. Data may be routinely moved from one area to another, or it may exist in multiple 8 locations at the same time. This makes it difficult to determine applicable regulations and manage information flow. Protection of privacy is major GDPR challenge. As a controller, there is no influence over the IT architecture of the cloud provider as a result, there reliance on the provider's IT security. Consequently, the enterprise should always evaluate how well the service can meet their IT Security standards. The third party risk management procedure could be used for this. Along with this, users should evaluate the provider's privacy and IT protection policies and licenses. There are numerous ways for cloud providers to prove they adhere to security and Privacy by Design; by holding ISO 27018 certification (a code of conduct for protecting personally identifiable information (PII) in public clouds functioning as PII processors), as well as ISO 27001 certification (an information security management system) (Duncan, 2018), (Ducato, 2016), (Levite and Kalwani, 2020), and (Tolsma, 2022).

Declouding Workload from the Microsoft Azure Cloud to the On-Premise Environment

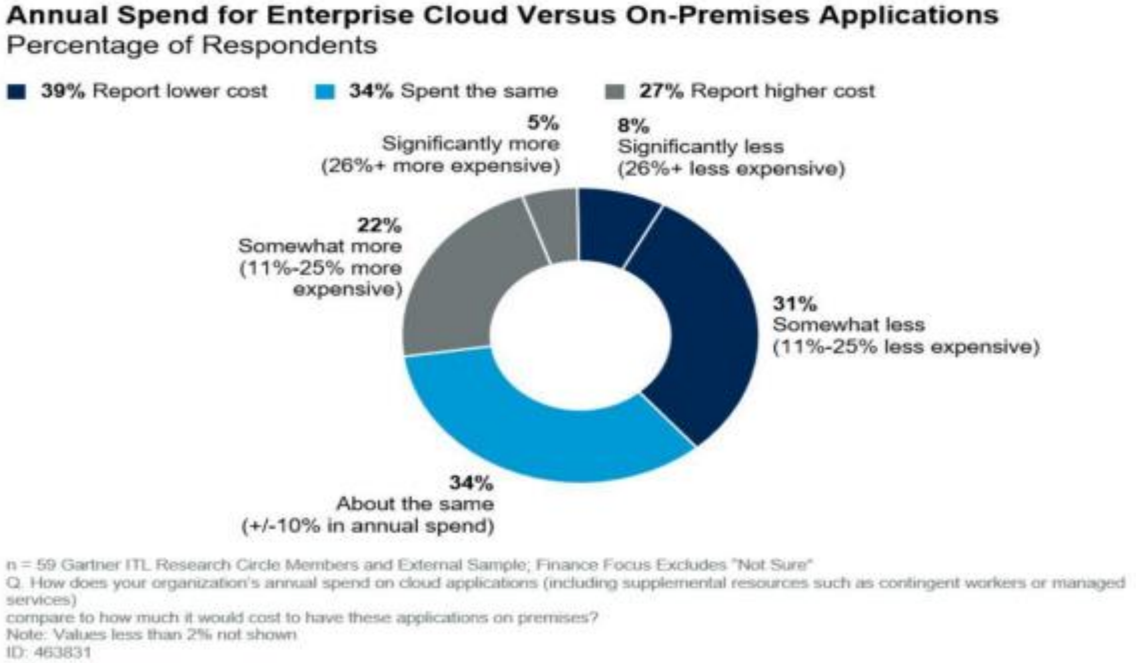
Transferring data from public cloud to On-premises can be time-consuming and a costly process. When de-clouding workload from some cloud provider, data may need to be transformed before being transferred. A particular case in point is repatriating workload from the Azure cloud. VMware Converter is necessary to construct Virtual Machine Disk Files usually needed to recreate the VM (Virtual Machine) when migrating cloud resources from the public cloud to an on-premises VMWare system. This can take a long time and necessitates a VM downtime. Azure cloud would use a different approach. It uses VHDs as hard discs. As a result, all that remains is to download the VHDs (Virtual Hard Disk) from Azure cloud using an internet browser and import them into a new VM (Kenneth, 2021). Several solutions, such as disaster recovery and replication software providers, can be used to transfer cloud VMs back to on-premises. They have the benefit of eliminating a few manual conversion stages, such as disc copies and conversions (Opara-Martin, 2018).

Deskilling and Outsourcing Issues in Cloud Computing

One of several unexpected implications of the Cloud's automation of Information Technology in business is the disappearance of competence. It is safe to say that this deskilling phenomenon is not a coincidence for clients considering Cloud services. Workloads in the cloud require a particular skill set. Staff members inside a business will be required to adapt, from documenting on performance to deploying cloud system. Organisations that utilize the public cloud should give their IT workers a wide range of cloud infrastructure and IaaS capabilities that would not be necessary with conventional in-house IT. Skills shortages can result in security lapses, performance issues, and other workload restrictions that call for the workload to be moved back to the neighbourhood data centre (Bigelow, 2020) and (Harry, 2019).

Cloud computing has several advantages for IT service delivery, however in general, Public Cloud are patented vendor-delivered services. Although these services are comparable to those supplied on premises, the customer would bear the majority of the responsibility for providing support for in-house delivered services, with fourth line escalation addressed by the CSP or a third party. Customers were naturally incentivized by this strategy to guarantee they have the necessary expertise in-house or through their supplier to support such technology. However, since this infrastructure design is given via the CSP's data centres or the Cloud, there is a strong motivation to forego those expertises. This is especially true for SaaS systems like Microsoft 365, where consumers connect with the platform through their client. In other words, third or fourth line assistance is no longer a requirement because any backend problems are escalated to and addressed by the Cloud service provider (Abe et al., 2021) and (Harry, 2019). The impact of deskilling and outsourcing is not limited to IT. Indeed, as technology has gotten more automated, it is now more common in a variety of industries ranging from aviation to electronics. There is nearly always a 'complaint' in Tech Publications about the sector's shortage of IT expertise. As a result, corporate executives should support for investments in IT staff, training and educating them in the abilities required to skilfully handle numerous on-premises and off-premises facilities, as well as making investments in IT technology software that can enable IT professionals respond swiftly to the organisations requirements and minimise shutdowns for mission-critical systems (IDC Researcher, 2019). Because of automation, the emphasis has changed to what could be described as 'DevOps,' a combination of Development and (Business as Usual) Operations. DevOps is beneficial for cloud computing, yet the average 'system' IT expert does not have the coding basic knowledge training (Harry, 2019).

Cost Comparison Analysis for Public Cloud Vs On-Premise Cloud



Annual Spend for Enterprise Cloud Versus On-Premises Applications
Percentage of Respondents

n = 59 Gartner ITL Research Circle Members and External Sample; Finance Focus Excludes "Not Sure"
Q. How does your organization's annual spend on cloud applications (including supplemental resources such as contingent workers or managed services)
compare to how much it would cost to have these applications on premises?
Note: Values less than 2% not shown
ID: 463831

Figure 7: Cost Comparison Analysis of Public Cloud vs. On-premises Applications Source: (Gartner 2019)

This quantitative analysis focused on approximately 55 small and medium-sized businesses considering whether to migrate their basic financial management suites, including general ledger, accounts payable and receivable, and similar applications, to the cloud, as well as some financial planning and analysis tools. According to the (Gartner 2019) study report, as indicated in figure 2, two-thirds of the organisations evaluated will spend the same or more on cloud expenses compared to On-premises. It reveals that only 8% of participants saw 'significant' cost reductions 7 of 26% or more from moving to cloud finance, while 31% claimed cloud was 'somewhat less expensive.' However, for 22%, moving to the cloud was 11 to 25 percent more expensive, and for 5%, it was more than 26% more expensive. The result showed that migrating to the cloud may not be a cost effective decision for some of the companies. This is largely due to the workload of the company and how sensitive the company data is, among other factors. Hence the idea of reducing cost by moving to the public cloud might not be achieved.

Performance Analysis between Private and Public Cloud

A closer look is given to the issues of performance in a comparative analysis between the private and public cloud. Based on the (IDC 2019) reports that the second most common reason for repatriation, at 14% of cases, is performance-related, hence an evaluation of the private Cloud and the public Cloud carried out in a study by (Mancaș, 2019) was reviewed in order to offer the best option based on the users' top priorities.

In the study, KVM, VMware, and Hyper-V virtual machines were used in the analyses in the given structure: 8 GB RAM 2 cores with 4 threads, and 1 TB of storage. The VMs came from a private Cloud environment and were built on a real machine. A private Cloud architecture from a research facility and a public Cloud service offered by Rackspace were utilised as assessment sources in order to contrast the virtualization performance of the two types of clouds. For each virtual computer, the essential components were allotted: 32 GB of RAM, 1 TB of storage, and 2 cores (4 threads). The VMs that were utilised to test the performance were the only programmes running on the physical host. The Ubuntu operating system has been utilised for all VMs in both the private and public clouds.

A variety of open-source apps are employed in the performance review experiments to examine a broad range of indicators, including Processor speeds, write rate, read speed, latency, files formation and delete, writing rate and memory bandwidth, and (I / O) frequency (Arithmetic-Logical Unit and floating point unit). The following instrument for measuring performance were the Unix OS, which can be tested using UnixBench to gauge CPU performance. The benchmark was applied to assess performance for both serial and parallel computation of jobs. The variables that UnixBench employs are as follows:

- Dhrystone is a measurement tool for assessing and contrasting performance when no floating point functions are available. The Dhrystones per second unit of measuring performance which is the number of iterations per second of the main code loop.

- Whetstone: This artificial statistic gauges the effectiveness of floating point procedures in terms of speed and effectiveness. In addition to using integer and floating point data, mathematical operations, obtaining datasets, and calling operations, this experiment is based on various trigonometric operations, such as sin, cos, sqrt, and exp.

- Execl Throughput counts how many "execl" calls are made per second. The operation Execl is a part of a collection of functional units which substitutes the representation of the existing process for the representation of a separate method.

- Process Creation: This metric evaluates the frequency with which a workflow may start and finish sub - tasks in a given amount of time. It is strongly connected to the memory space capacity since it deals with the establishment of process control blocks and the assignment of memory for process improvements. This statistic is typically often used contrast the different ways that process formation calls are implemented in the OS.

- File Copy: calculates the speed at which a particular dataset may be reproduced utilising various buffer sizes.

- The amount of times per second that an application can write and read 512 bytes is measured by pipe throughput.

- System Call Overhead: calculates the cost of running a system call, which includes all inputs and outputs to and from the kernel of the OS.

- Shell Scripts: counts the amount of times per minute that an application could control eight parallel versions of a Shell script that modifies a dataset in various ways.

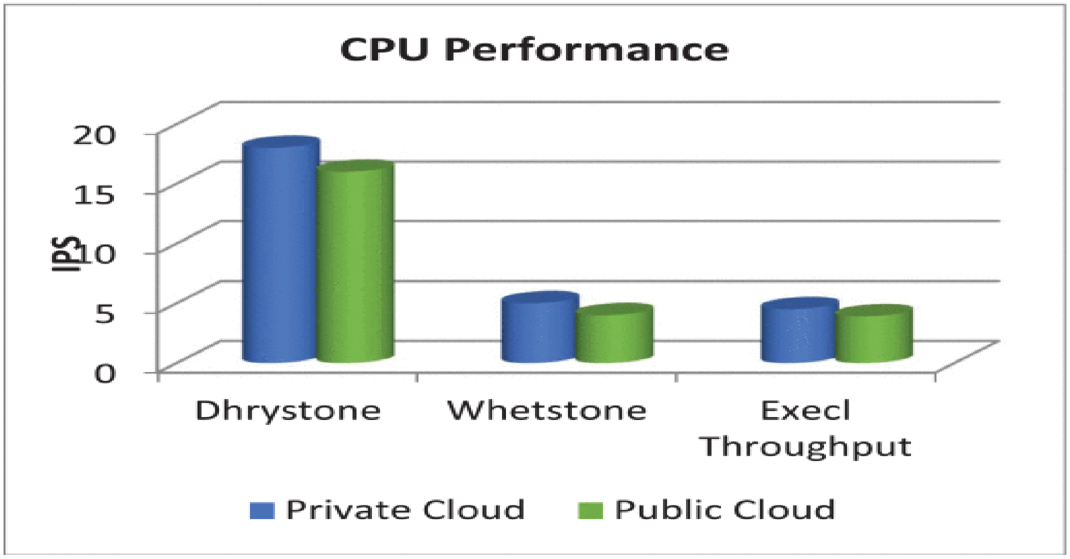


Figure 8: Throughput experiments using Dhrystone, Whetstone, and Execl in public and private clouds

The above shows that though it is occasionally assumed that the values of measuring performance results are not entirely applicable because the assets of the public Cloud cannot be monitored, the comparative study between the 2 categories of Clouds is entirely applicable and is extremely helpful if customers need to choose the form of Cloud delivery that is best for a particular application. The distribution of hardware facilities among numerous clients, which causes oscillations in computer workload, memory access duration, and I/O network bandwidth accounts for the public Cloud's underperformance.

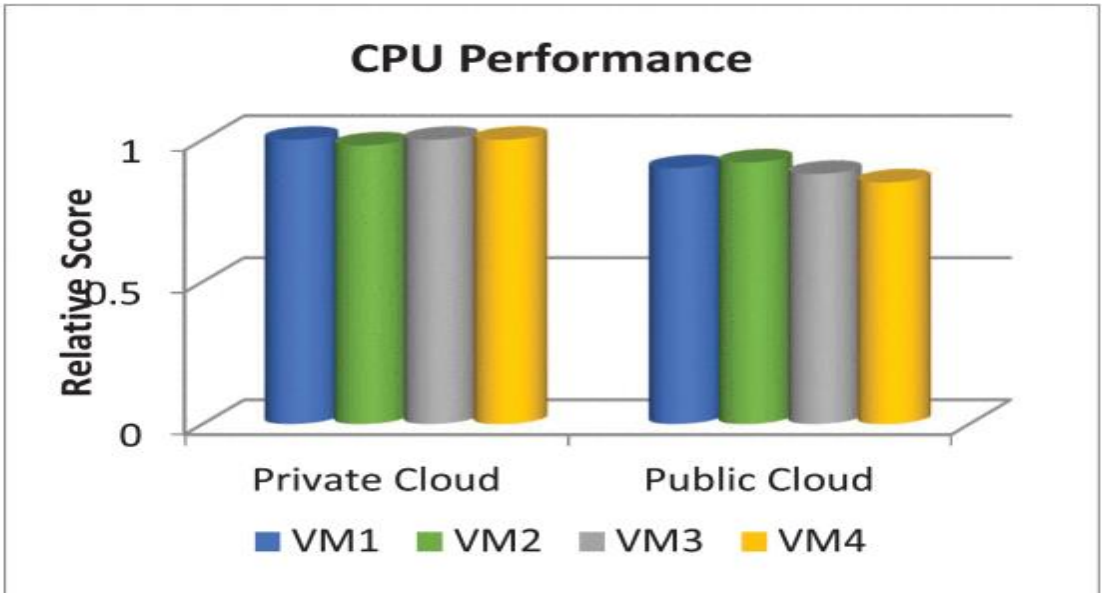


Figure 9: CPU performance comparison between private and public clouds

The total rating on VMs in the public Cloud is lower than in the private Cloud, which is also accounted for in this experiment. A similar behaviour is observed while testing RAM and I/O processes. The results of the performance evaluations state that using a private Cloud is advised in the case of performance and security considerations. Utilization of a public Cloud is advised if cost, pricing, and scalability are the top concerns (Mancaş, 2019). This comparative analysis is supported by other researchers such as (Khair *et al*., 2022) and (Imran *et al.*, 2018).

Homomorphic Encryption

Following from the concern of security challenge that was pointed out preciously, the cloud ecosystem seems to continue to have poor security. (Al-Sit, Al-Jubouri, and Al-Zoubi, 2019) noted that even while embracing the public cloud has a number of benefits such as low maintenance costs, backup customization and recovery, and remote access; however, operational costs, security, and privacy continue to be a major concern. Similarly, (Awadallah and Samsudin, 2020) and (Al-Sit, Al-Jubouri, and Al-Zoubi, 2019) stated that the inability of cloud computing to meet the confidentiality, integrity, availability, and privacy standards of the user's data has continued to linger.

In a scholastic research carried out by (Alani 2014) which has been supported by (Awadallah and Samsudin, 2020) shows that security has remain the major reason why enterprises are either repatriating their workload from public cloud or even hesitant to engaging the public cloud services in the first place as shown in figure 7. As the process of data exchange and modification within the cloud system created a lot of vulnerabilities for hackers to take advantage of, since the process of decrypting an encrypted data in order for the user's to use the data or modify the data meant that the same data had become exposed to hackers. To address this security problem the concept of **Homomorphic Encryption** was introduced.

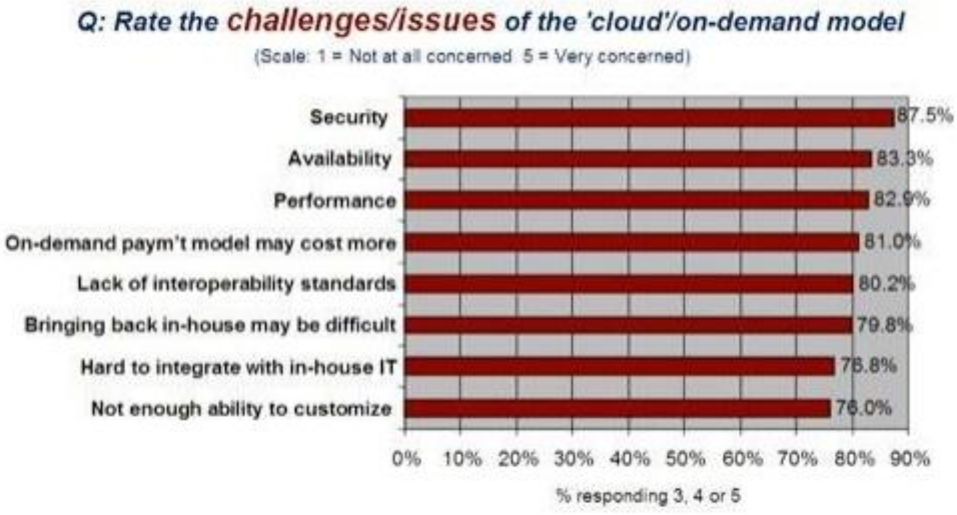


Figure 10: Ranking Security Challenges according to IDC Survey Results

Homomorphic encryption is a type of encryption that enables certain computations to be performed on ciphertext and generates an encrypted result that, when decrypted, is the same as the outcome of calculations that were also performed on plaintext (Branscombe, 2019). As an example, take into account the situation where an individual can add two encrypted numbers, and the other individual can later decrypt the final number without knowing the values of such distinct numbers (Ahmad and Khandekar, 2014). This means that by enabling computation to be done directly on encrypted data without requiring access to a secret key, Homomorphic encryption differs from conventional encryption techniques. Such a computation outcome is preserved in encrypted form and may eventually be made public by the holder of the secret key (Bajpai and Srivastava 2014) and (Awadallah and Samsudin, 2020). The use of HE is widespread in a variety of industries, including healthcare, medical applications, the financial sector, forensic applications, social networking marketing, and smart vehicles, where the privacy of users can be protected (Shrestha and Kim 2019).

The three different types of Homomorphic encryption are as follows:

1) **Fully Homomorphic Encryption** (FHE), which performs addition and multiplication on encrypted data as part of the entire operation. FHE enables an almost infinite number of various types of evaluation procedures on the encrypted message.

2) **Partially Homomorphic Encryption** (PHE), In the PHE system, just one sort of mathematical operation—either addition or multiplication—can be performed on the encrypted message an indefinite amount of times.

3. **Somewhat Homomorphic Encryption** (SHE), which is quicker than FHE because it only performs operations on a small number of additions or multiplications.

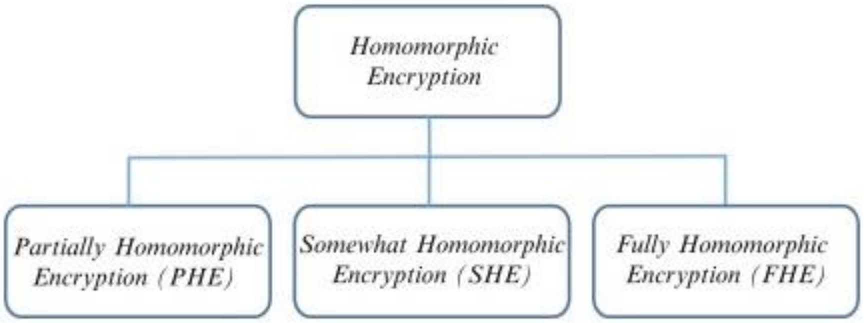

Homomorphic Encryption
Partially Homomorphic Encryption (PHE)
Somewhat Homomorphic Encryption (SHE)
Fully Homomorphic Encryption (FHE)

Figure 11: Diagram of the categories of Homomorphic Encryption. Source: (Shrestha and Kim 2019).

Studies have shown that FHE guarantees security, privacy and integrity of data as compare to the other forms of Homomorphic encryptions as the pinnacle of Homomorphic encryption is fully Homomorphic encryption (Awadallah and Samsudin, 2020). An endless amount of ciphertext additions or multiplications are permitted by a completely Homomorphic encryption algorithm without compromising the integrity of the outcome. Although, it is argued that the process of FHE is slow because of the multi-layers of FHE (Al-Sit, Al-Jubouri, and Al-Zoubi, 2019).

Misconceptions of Public Cloud and On-premises Infrastructure

Drawing from the findings made with regards to cloud repatriation also known as declouding in the introductory part of this study, it is important at this point to correcting some misconceptions associated with private cloud and the public cloud. There is the belief that organisations will be sorry if they shift to the Cloud. This study is not saying that moving to the cloud is bad, as studies have shown that companies were not repatriating services because the Cloud has no value, rather it was because they did not understand the cloud concept in the first place, their planning was poor or done without all of the facts, or they had put their workloads in the wrong place. Secondly, customers frequently believe that the data they save in the cloud is safeguarded and secured by the cloud provider. This is not true. It is up to the enterprises to adopt security safeguards, whether the data is stored in the public cloud or on-premises. Data security requirements and contracts continue to impact businesses and might serve as a motivation to reduce workloads from the public cloud (Fisher 2018) and (Biggenden, 2022).

Lastly, research has demonstrated that there is no dichotomy between on-premises infrastructure and the public cloud. Instead, there is a continuum—a variety of service options—between these two extremes. And among them is colocation, which denotes the placement of computers by one company on the premises of another, with the latter only being responsible for providing bandwidth, electricity, and space. A different option is managed hosting, in which a company rents hardware from a source but retains sole control over it and has VPN access to it. Many businesses also use virtual machines, which they rent on a weekly or monthly basis in exchange for paying for the computing time, bandwidth, and other services that were used. Additionally, there is containerization, where apps are wrapped in containers like Kubernetes, Docker, and others that operate on a vendor's virtual machine while the company is being charged for the cycles their app utilises. At the top of all these range of services, are public cloud services such as Microsoft Azure, Google cloud, AWS and others which are basically managed cloud services where users or businesses buy application off the shelf e.g. Word-press for blogging and the cloud service provider (CSP) manages the App exclusively without the business input in managing the app and as a result the business is unaware as to where the app’s IP address is on, the CSP manages the DNS, more like exclusive management. So, there are a whole lot that can be done in between On-premise and the public Cloud (Zhong et al., 2020), (Watada et al., 2019) and (Telnet WorldWide, 2021).

Summarily, because the cost is not linear but rather follows an upward and downward curve, a company will save the most money if it uses just the public cloud services or 3 the on-premise cloud and manages its own software. Prices tend to rise in this medium ground, but the issue becomes one of company scalability since the business will have to use some of the pricey solutions outlined above as it grows. In order to manage what seems to be raising costs, firms tend to favour the hybrid strategy. This entails distributing its workload across a variety of platforms, some of which will be managed hosting, some of which will be colocated, also some of which be on-premises and some of which will be placed in the public cloud. The requirement for this study arises from the problem of how to choose where each of these workloads should be allocated.

METHODOLOGY

The goal of this study was to examine the veracity of a recent development in the cloud computing industry related to cloud repatriation, also known as declouding, and to determine why enterprises were embarking on this exercise as well as the various complexities surrounding the topic. Furthermore, this study was intended to address the multi-dimensional optimization problem that emerged as a result of the study's subject matter by developing an application workload placement guide that enables enterprises to make optimum use of the cloud options available in allocating the business workloads. Consequently, a case study approach was adopted in carrying out this study.

According to Crowe, Sarah et al. (2011), a case study is a research strategy that is used to produce an in-depth, multifaceted understanding of a complex issue in its real-life context. The topic's veracity and the reason why businesses were embarking on cloud repatriation, as well as the various complexities surrounding the subject matter, has already been accomplished through this method in the case study review. The case study approach is a well-known research strategy that is widely applied across a wide range of academic fields, particularly in the social sciences. In addition, (Stake 1995) and (Yin 1994) both showed that the case study approach was helpful for studying occurrences that cannot be examined in a lab or with quantitative techniques. Case studies are frequently employed in a variety of disciplines, including business, health, and the social sciences. This concept has also been validated by them.

In solving the multi-dimensional optimization problem, this study continues the use of the case study methodology which employed a quantitative and qualitative method of collecting data from existing theoretical reviews in developing an application workload placement solution as well as a survey for understand the needs of small scale businesses. This study majors on the qualitative approach in developing a workload placement guide. While the quantitative technique enables an unbiased assessment of reality, the qualitative approach assists the researcher in exploring and understanding the complexity of a phenomenon (Williams, 2007). Furthermore, collecting data via a qualitative approach is cost-effective and affordable (Bowen 2009). This publication had to adhere to a series of requirements, one of which was that they had to be official report from reliable researchers and industry experts. 2. Released between 2015 and 2022, 3. Workload placement or cloud migration must be included in the paper.

The documents selected for review are:

- *What is cloud migration? An introduction to moving to the cloud* (Montgomery, J., Casey, K. and Semilof, M., 2022).
- Does Workload Placement Define the Cloud Principles? What Do You Think? (Amos, R., 2022).
- Developing an Effective Workload Placement Strategy (Dell EMC 2021)
- Comparing Cloud Workload Placement Strategies (Gartner 2020)
- Workload Placement Separates the Winners from the Losers in IT (IDC Researcher 2021).
- Creating a Multi-cloud Strategy: How to Perform Application Workload Placement Analysis (Ramsey 2019).
- Defining Hybrid Cloud, Muilti-cloud, and hybrid cloud management (Forrester Research 2018).

In Microsoft Excel and Word, results are shown as tables and chart that present data and patterns in an easy-to-understand quantitative and most especially in qualitative manner in accordance with (Dragani, 2018). The results were also uploaded to a website that was developed to stand as an artefact showing the findings of this research and also positioning as a sensitization and educative resource point for small and medium enterprises.

Limitations of Case Study Approach

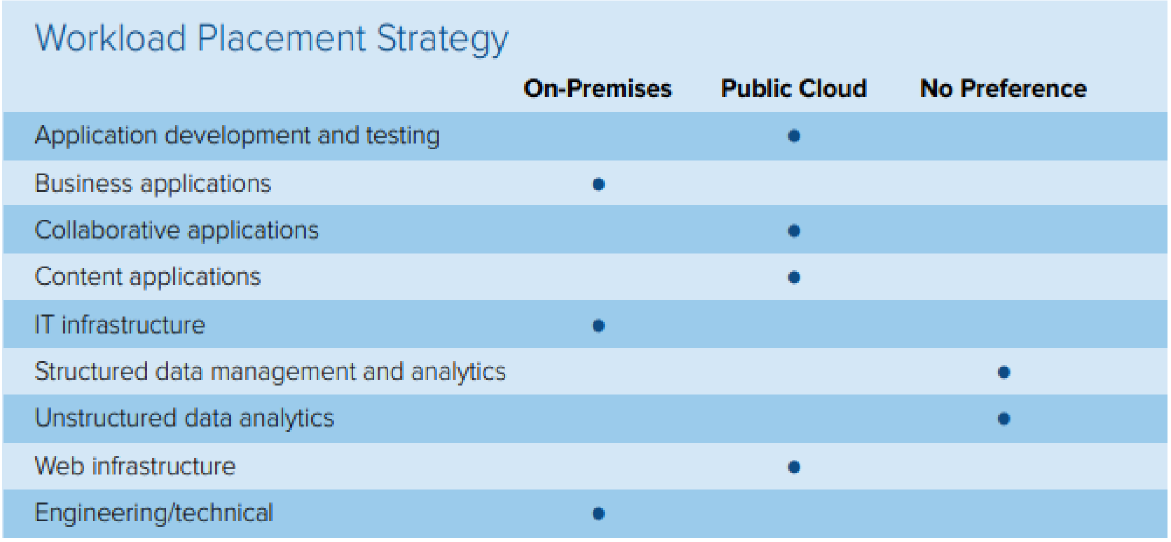
Case study approach has occasionally received criticism for not having scientific rigour and offering little support for universality, that is, for failing to produce conclusions that might be applicable to other contexts (Yin 2009). There are a number of strategies for addressing these issues, such as the use of theoretical sampling (i.e., drawing on a specific system of thought), respondent validation (i.e., applicants confirming findings of the study and the researcher's exegesis and expressing a viewpoint on whether they feel these are factual), and disclosure all through the entire study (Mason 2002) and (Stake 1995). However, the case study technique enables, along with other things, the detailed examination of significant events, interventions, policy initiatives, and program-based service improvements in a real-life setting. Therefore, it should be taken into account whenever an experimental design is either impractical or improper to carry out in order to address the research issues posed. Although difficult by nature, a research case study can, if wisely formulated, carried out, and published, provide strong insights into many crucial areas of research investigations (Crowe, Sarah et al. 2011). Constraints about the validity of the information are developing because a survey form requires respondents to try and remember past occurrences in order to respond to the questionnaires. A possible drawback that had not resolved in this study was the questionnaire's capacity to engage a wider participant (Wang, 2017). Alternate solution sampling techniques always has limits, notwithstanding the restrictions identified throughout this investigation and the acknowledged restrictions listed at the end of this research. Because of Covid-19, volunteer wellbeing and wellbeing was of the topmost significance, therefore implementing this procedure continue to be the best option.

Research Ethics Approval

The university's ethics committee gave its approval for this work in order to meet Solent University's requirements for the MSc in Cyber Security Engineering degree. In order to avoid harming anyone physically, psychologically, or socially, the research adhered to all safety regulations. Only official, secure websites were used to gather information for the document analysis in order to assure security. Amongst the other ethical factors are respondent agreements for the survey as well as confidentiality. The survey does not ask any probing queries, thus the answers are anonymised.

RESULT AND DISCUSSION

In this session, workload placement models were designed following deductive extrapolations from existing proven theories. According to this research finding, there are no simple answers to the problem of workload Placement. As a result, in the hybrid and multicloud world of today, IT professionals must choose a hosting solution that provides the optimal combination of performance and cost effectiveness. One can choose from a variety of infrastructure alternatives, including vendor-based public clouds that would provide SaaS, IaaS, and PaaS services, and On-premises data centres with hosted private clouds. Making the best decision necessitates a full understanding of the various workload types, their traits, the applications that enable them, and the business objectives they support (IDC Researcher, 2019) and (Ramsey 2019). Figure 9 serves as a first guide following the result from a survey review. Similarly, (Gartner 2020) postulation which says that On-premises, colocation, cloud, and edge delivery options will all be included in infrastructure strategies by 2025, up from 20% in 2020 seems to be evident already from the result gathered from this study. Furthermore, the survey carried out had the participation of small scale business owners who utilised one or more forms of cloud computing applications. The survey was infused into the workload place guide or model extrapolations in a bid to get a better understanding of what small businesses needed and to ascertain if the workload place guide/model was offering proper guidance.



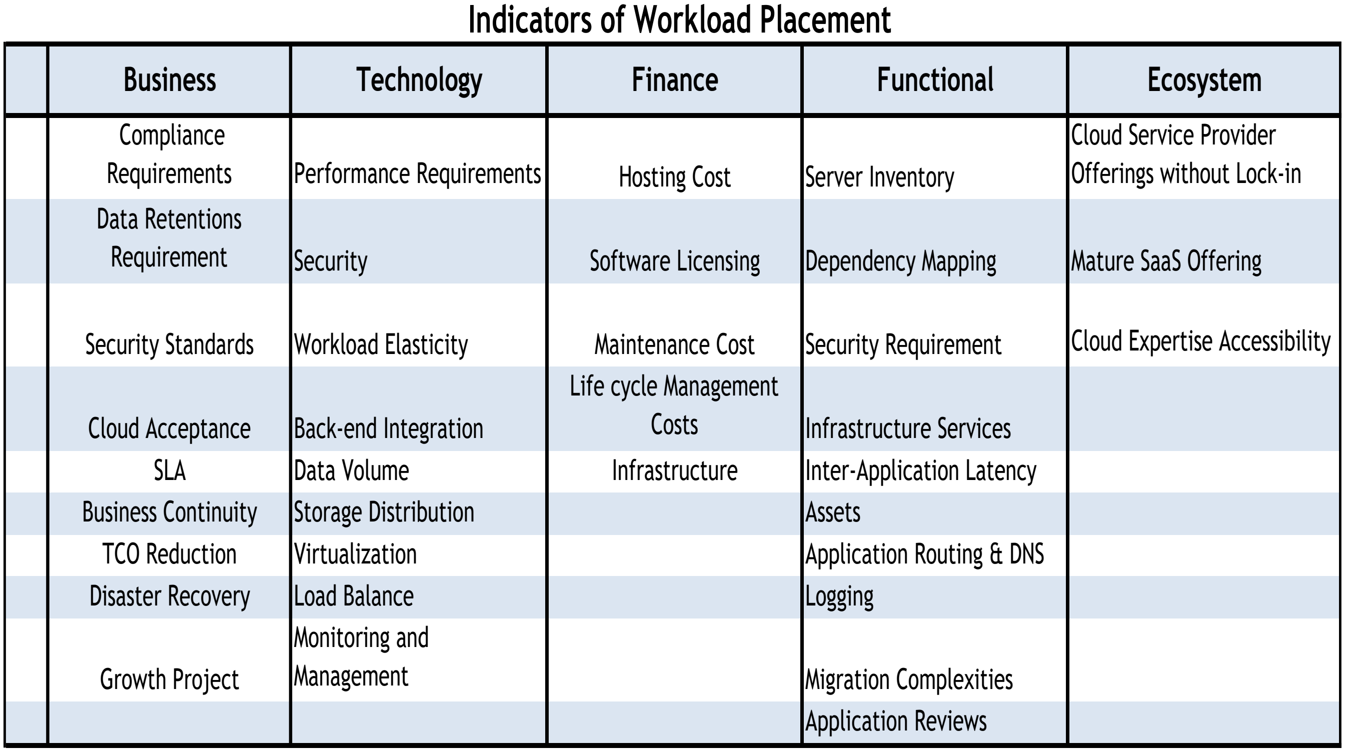
Workload Placement Strategy

	On-Premises	Public Cloud	No Preference
Application development and testing		●	
Business applications	●		
Collaborative applications		●	
Content applications		●	
IT infrastructure	●		
Structured data management and analytics			●
Unstructured data analytics			●
Web infrastructure		●	
Engineering/technical	●		

Figure 9: Work Placement Solution. (Source: IDC Researcher 2019) and (Forrester Research 2018)

Categorising the Workload and Determining Placement

The primary consideration in choosing workload placement is to know the organization's business needs, which are of substantial relevance to management. This study developed five important indicators from which must company select workload placement. These indicators consist of: Indicators of the business, finance, technology, the ecosystem, and functional areas as shown in Table 1.

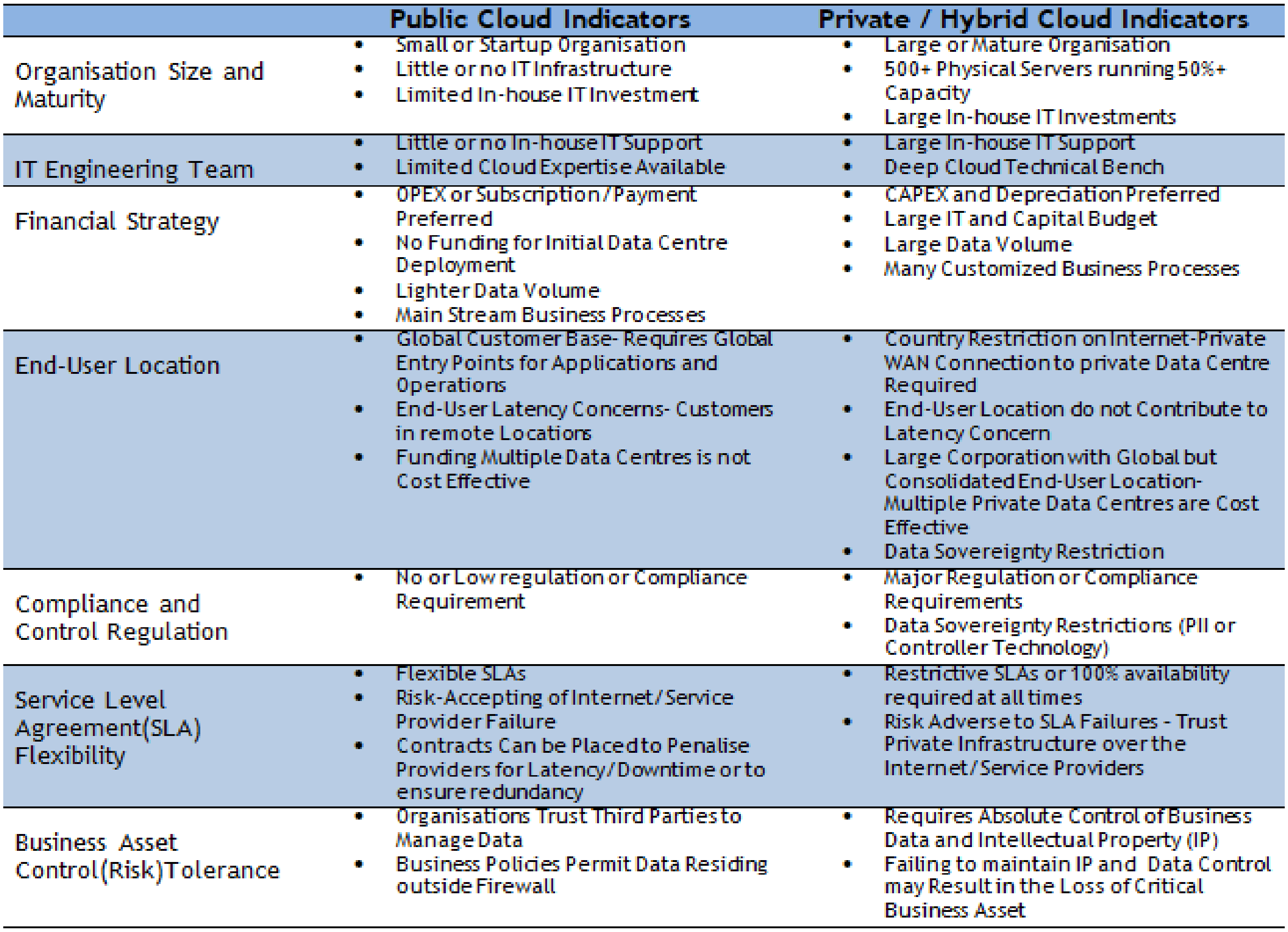


Indicators of Workload Placement

	Business	Technology	Finance	Functional	Ecosystem
	Compliance Requirements	Performance Requirements	Hosting Cost	Server Inventory	Cloud Service Provider Offerings without Lock-in
	Data Retentions Requirement	Security	Software Licensing	Dependency Mapping	Mature SaaS Offering
	Security Standards	Workload Elasticity	Maintenance Cost	Security Requirement	Cloud Expertise Accessibility
	Cloud Acceptance	Back-end Integration	Life cycle Management Costs	Infrastructure Services	
	SLA	Data Volume	Infrastructure	Inter-Application Latency	
	Business Continuity	Storage Distribution		Assets	
	TCO Reduction	Virtualization		Application Routing & DNS	
	Disaster Recovery	Load Balance		Logging	
	Growth Project	Monitoring and Management		Migration Complexities	
				Application Reviews	

Table 1: Indicators of Workload Placement. [Source :(Gartner, 2020), (Forrester Research, 2018), and].

Business Reasons for Using the Cloud



	Public Cloud Indicators	Private / Hybrid Cloud Indicators
Organisation Size and Maturity	• Small or Startup Organisation • Little or no IT Infrastructure • Limited In-house IT Investment	• Large or Mature Organisation • 500+ Physical Servers running 50%+ Capacity • Large In-house IT Investments
IT Engineering Team	• Little or no In-house IT Support • Limited Cloud Expertise Available	• Large In-house IT Support • Deep Cloud Technical Bench
Financial Strategy	• OPEX or Subscription/Payment Preferred • No Funding for Initial Data Centre Deployment • Lighter Data Volume • Main Stream Business Processes	• CAPEX and Depreciation Preferred • Large IT and Capital Budget • Large Data Volume • Many Customized Business Processes
End-User Location	• Global Customer Base- Requires Global Entry Points for Applications and Operations • End-User Latency Concerns- Customers in remote Locations • Funding Multiple Data Centres is not Cost Effective	• Country Restriction on Internet-Private WAN Connection to private Data Centre Required • End-User Location do not Contribute to Latency Concern • Large Corporation with Global but Consolidated End-User Location-Multiple Private Data Centres are Cost Effective • Data Sovereignty Restriction
Compliance and Control Regulation	• No or Low regulation or Compliance Requirement	• Major Regulation or Compliance Requirements • Data Sovereignty Restrictions (PII or Controller Technology)
Service Level Agreement(SLA) Flexibility	• Flexible SLAs • Risk-Accepting of Internet/Service Provider Failure • Contracts Can be Placed to Penalise Providers for Latency/Downtime or to ensure redundancy	• Restrictive SLAs or 100% availability required at all times • Risk Adverse to SLA Failures - Trust Private Infrastructure over the Internet/Service Providers
Business Asset Control(Risk)Tolerance	• Organisations Trust Third Parties to Manage Data • Business Policies Permit Data Residing outside Firewall	• Requires Absolute Control of Business Data and Intellectual Property (IP) • Failing to maintain IP and Data Control may Result in the Loss of Critical Business Asset

According to this study, business reasons may include the major use case that the firm wants to improve, such as Time to Market, Agility, Legal, and Regulation, as well as the top business problem that the organisation is striving to tackle. Businesses that want to move their technology to the cloud should start by coordinating their corporate culture. Data must be moved from one location to another, but there are other requirements when switching from on-premises technology to cloud computing or vice versa. There needs to be a well-organized migration plan to succeed in the cloud, first there must be a comprehension of the entire business goals. Considering first whether switching to the cloud will genuinely help the business achieve its company's objectives. As a result putting time and effort into creating a written strategy is crucial for a smooth transition. Above is an example of a business model for cloud implementation (Schmidt et al., 2016) and (Dell EMC 2021). In a hybrid cloud ecosystem, businesses must manage complex data structures without sacrificing security and compliance. Additionally, they must confirm that SLAs are being met. Working with a managed services provider that can optimise cloud while ensuring the uninterrupted operation of IT information systems and business operations not only makes it simpler, but it also frees up time for businesses to concentrate on creativity and expansion rather than maintaining the technical details of a cloud infrastructure.

Technological Reason for Using Cloud

After examining important business factors, choosing technology that helps the organisation achieve its goals becomes essential to its success. While certain applications perform efficiently in private clouds, some work better on public clouds. This study outlines four essential technological factors that influence where workloads are placed. The assessments that follow offer some core concepts to comprehend before a business approaches a more sophisticated workload allocation (IDC Researcher, 2019), (Dell EMC 2021) and (Forrester Research 2018).

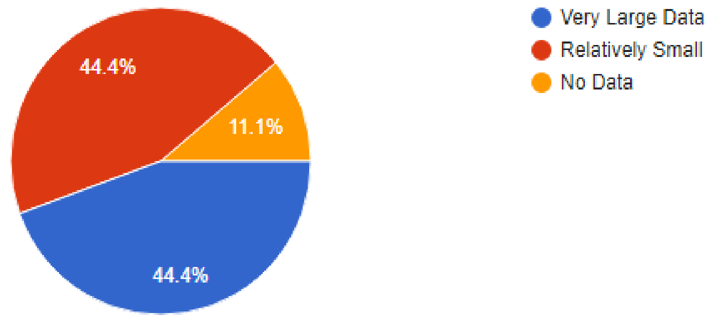
1. **Security**: Some applications manage and store data including intellectual property (IP), personal identity information (PII), and personal health information (PHI) that, if impacted by an unintentional or criminal action, could be detrimental to the company. This grade also considers how widely accessible security solutions are for a specific workload. The effective email security option is one illustration. Similarly, Data storage security is essential for corporate operations. Cyber-attacks are serious and should be avoided at all costs. Data are assets in the digital sector. Information is a valuable resource that must be invested in, managed, and safeguarded with extreme caution.

2. **Performance:** There are two ways to look at application performance, which is determined by the latency and reaction times. Both intra workloads, where application performance is a product of the infrastructural facilities, and inter workloads, where it is a product of the network linking the 2, are relevant. To keep things balanced, both of these are crucial.
   To meet end user expectations, some applications and data bases must reply within a predetermined time range. When businesses have control over the placement of their user and data centre or the link between them, private or hybrid clouds may be a useful alternative. A private cloud or managed service architecture can deliver dependable, thorough, and transparent performance measurement alerts when a company needs a certain performance level to constantly stay within standards. On the other hand, public cloud offers a

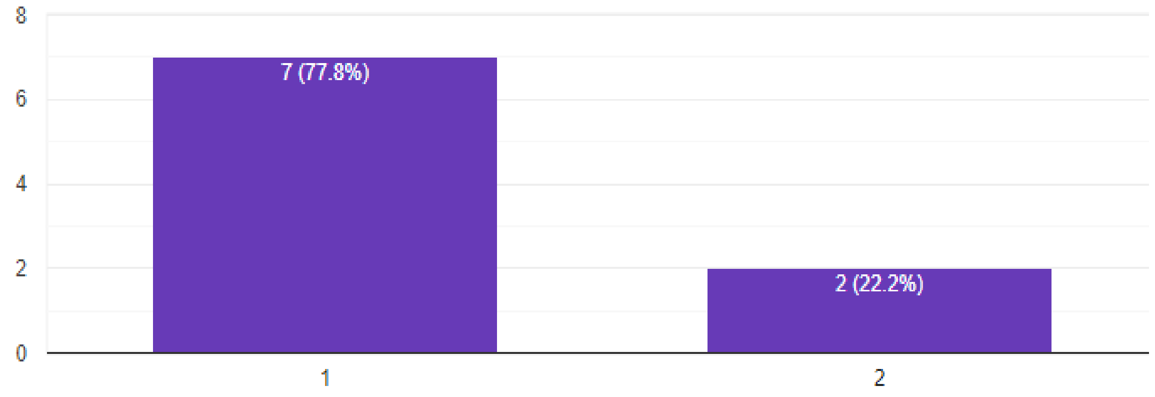
unique benefit for a task that needs significant computational capacity at frequent intervals, like online retail holiday sales or internet voting, as long as the programme can deploy across several instances and there are no latency requirements.

3. **Data Volume:** This study focuses on two key elements: the magnitude of the data and the location, or the place where the data is generated and maintained. Big data quantities may make processing times longer, cost more to host, and be more challenging to move. Businesses could benefit from modern storage technologies and cloud collaboration to optimize local storage architecture, save costs, and increase process efficiency. The physical environment is generally crucial when dealing with big data repositories. A crucial design choice for both the public and private cloud systems is to place the data in close proximity to the enterprise application that need it.

4. **Integration**: Migrations to the cloud and traditional environments face difficulties because of connections to other databases, libraries, applications, workflows, and terminals. Due to the higher cost of integrating into numerous clouds, the sophistication and number of integrations have an implication on where workloads are placed. For each integration to comply with the operational level agreement (OLA), it must be evaluated, changed, and re – implemented.



Survey Question1: How much data does your business currently store?



Survey Question 2: How important is application performance to your business and earning

The above-mentioned technological factors can be evaluated for a particular task, and the particular feature ratings for performance, data volume, integration, and security was added up to determine the overall feature values. The appropriateness of the various feature ratings to the public or private cloud is made obvious by comparing the results across workloads. According to this study, workloads with high demands for performance, security, many backend connectors, and enormous data volumes function best on private clouds. As demonstrated in figure 10, public cloud and maybe SaaS solutions are preferable for applications with low performance, integration, or storage needs. This approach explains why research and development workloads, like designing or advanced manufacturing visualisation, stay mostly private while an application like CRM and its enterprise resource workloads can be applied effectively utilising SaaS on public cloud.

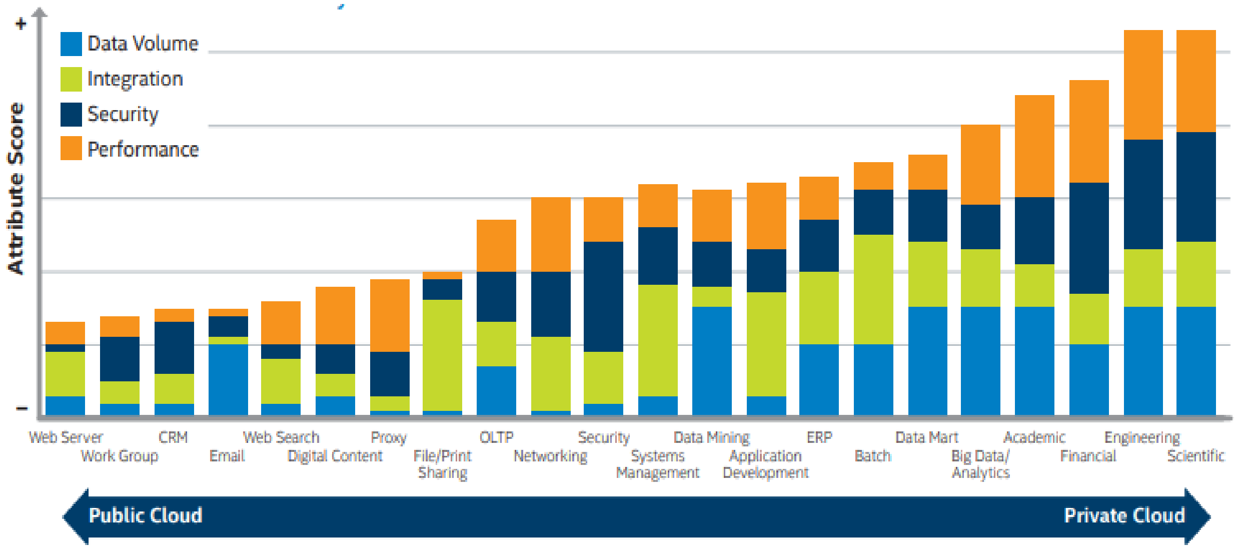


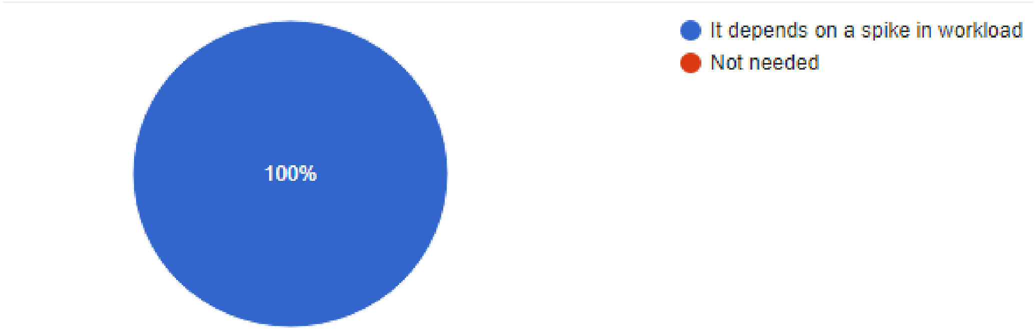
Figure 10: Technological Reason for Using Cloud

Financial Reason for using the cloud

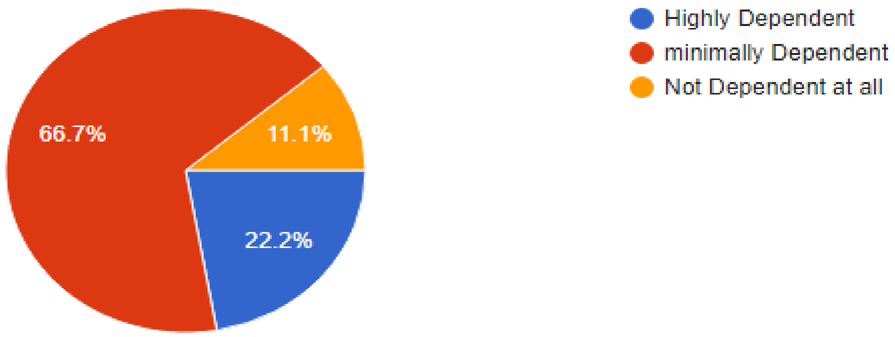
Due to uncertainty regarding the financial effects of its deployment and administration, the results suggest that many firms are still taking their time adopting cloud computing. Even with the buzz, cloud computing as a remedy really has not gained traction as quickly as was once hoped, in part due to the uncertainty around the financial advantages. Further investigation finds that, despite claims to the contrary, cloud computing is not popular with the finance department since it raises operating expenditure (Opex) costs. Such deadlock seldom gets resolved since IT units allow finance to make the first judgment. Predictability is frequently a crucial element in the transition from Capex to Opex costs. "Seesaw" operating costs are frequently the scourge of IT businesses' existence. The ability to execute workloads on-premises whenever it is more cost-effective to do so is one of the main advantages of a hybrid infrastructure. In fact, the savings increase with the size of the organization or the equipment (such as the number of servers). Ultimately IT costs is be reduced and made more predictable when hybrid architecture and workload allocation approaches are used (Gartner, 2020).

Ecosystem of Cloud Implementation

This comprises cloud computing knowledge for businesses as well as SaaS, CSP, and other services such as hosting private cloud, Manage Hosting, Colocation, and On-Premises Data Center. These findings indicate that SaaS options are becoming more and more prominent since they assist businesses in funding enterprise solutions through subscriptions, with the majority of operating costs going into personnel costs and software licenses. The agility advantage of SaaS outweighs expenses for some workloads. Prior to implementing SaaS, the organisation must have a clear understanding of the degree of technological collaboration and process improvement re-engineering necessary to satisfy the requirements of the company (Ramsey 2019).

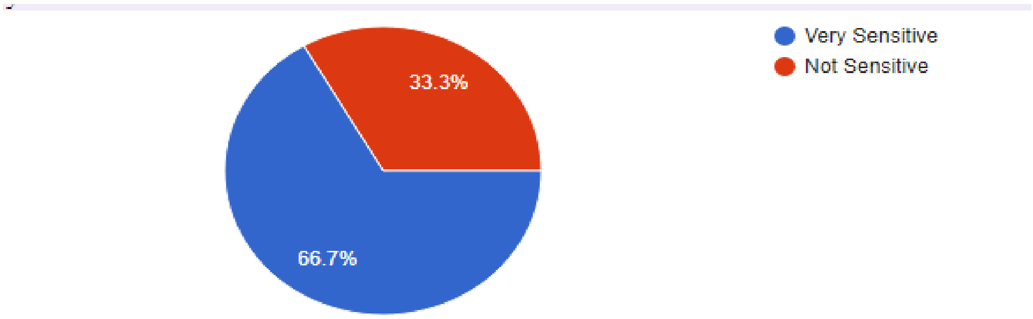


Sample survey question 3: How much elasticity does our workload require?



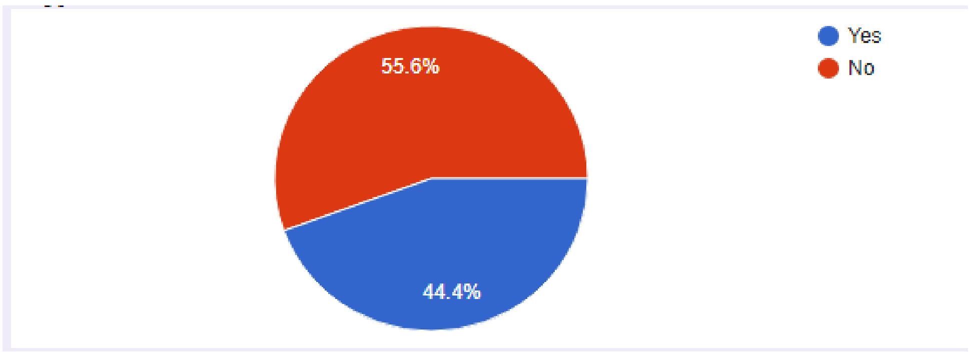
Survey Question 4: To what extent does your application depend on other application?

SaaS may be the best option for the workload if the company's current business procedures are very standard or if the technological review process finds that only a few key integrations are necessary. Similarly, the public cloud provides incredibly cutting-edge solutions with scalable and elastic architecture that enables a business to expand both horizontally and vertically based on the needs of the company workload. The workload should be optimised for public cloud services because moving an application from a cloud platform to the latter can be expensive. In the public cloud, steady state workloads could be more expensive. A company should evaluate how much a particular service will raise the cost of its subscription prior to actually deciding to adopt it. Given that cloud applications are currently in its infancy in comparison to more established models, IT professionals must be familiar with how to create solutions that are optimised for the cloud. Although organisations with formidable IT departments, ought to already be familiar with cloud this technology (Gartner 2020).



Question5: How sensitive to Latency is your application?

In comparison to certain other offerings from public cloud and SaaS providers, on-premise data centres are ideal for latency-sensitive applications or to solve privacy or data security issues, but that's where the differential ends. Utilising facilities and energy of another data centre provider is known as colocation. Result shows that colocation is good for legacy apps that cannot yet be refactored to operate in the public cloud. Colocation is similar to managed hosting. It's beneficial for legacy apps that can't yet be refactored. If any of the following solutions are homogeneous and might be modified out with SaaS capabilities, the business should think about switching to SaaS. Corporations with minimal cloud experience, however, can adopt public, hybrid cloud, or SaaS models since these enable them to work with cloud vendors for expertise (Gartner 2020) and (IDC Researcher 2021).



Survey Question 6: Does your business require you to host critical information only on private infrastructure?

Furthermore, Enterprise mission-critical workloads that are constant and therefore do not require elasticity or burst features might benefit greatly from hosted private clouds (HPC). Even so, you won't be able to scale as much as public cloud providers can on demand. If your applications are picky about loud neighbours and need a single-tenant environment, or if you have data, security, or privacy issues, HPC is a viable solution. A business should consider the public cloud if its workloads need to scale quickly or are elastic (IDC Researcher 2021) and (Montgomery, J., Casey, K. and Semilof, M., 2022). Table 3 gives a succinct overview.

	Recommended For:	Not Recommended For:
Software as a Service	Replacement of COTs	Differentiated Service/Intellectual Property
Public Cloud	Scalable, Elastic and Innovative	Steady State Workload
Hosting Private Cloud	Steady State Workload	Elastic Workload
Manage Hosting, Colocation, On-Premise Data Center	Complex application not ready for refactoring to the public	Anything Else

Table 3: Ecosystem of cloud implementation

Functional Reason for Using Cloud (Best Use Case)

The most useful cloud services for the various workloads that an organisation might use or subscribe to are identified in this presentation. Alternatively, what each cloud service that was chosen and evaluated is best recommended for and what it is not.

	Recommended For:	**Not Recommended For:**
Amazon Web Service	Creative, Distinctive, Scalable, Adjustable Workload	Latency-Sensitive; can be costly moving data out
Azure	. Net and Other Microsoft-Based Application	Latency-Sensitive; Can be costly moving Data out
Google Cloud Platform	Machine Learning, Data Analytics, Artificial Intelligence, Life Science	Application that cannot be Google-ified
Alibaba	Applications for China, with a Strong Focus in EMEA	Sensitive Data, Data Sovereignty
Oracle Public Cloud & Enterprise Clouds App	Customized for SaaS, complex corporate resource planning and financial application	Can be Expensive to Run Non-mission Workload
Azure Stack	Offering a cloud-like service to nations with strict data sovereignty laws or remote industries like mining, oil & gas	Expensive Hardware with Limited Azure Capabilities; Requires the Business to Manage, Pay for Data Centre Space and Power
VMware on AWS	On-demand infrastructure for lifting and shifting; latency-sensitive application wishing to employ AWS PaaS services	Mode 2 and Cloud- native Application
VMware	Issues about data privacy and business workload with isolated constraints	Mode 2 and Cloud-native Application, Serverless
Open Stack	Workload Containerization; Lower License Requirements	Be prepare for heavy Engineering Expenses
Bare Metal	Flexible, single-tenant, and private	Be Prepare for Heavy Engineering Expenses

Table 4: Best use case. Source: (Montgomery, J., Casey, K. and Semilof, M., 2022), (IDC Researcher 2021) and (Gartner, 2020)

Effective Workload Placement + Modern Compute Environment
= Better Business Results

Figure 11: Benefit of Effective workload Placement. Source: (Dell EMC 2021)

LIMITATION OF THIS STUDY

Due to their vested interest in the public cloud services, it was found that the majority of the main search engines did not offer materials or literature on the issue of declouding, which was the motivation for this research. Declouding may not be a widely used phrase yet, which could explain why terms like repatriation get erratic results. Due to the fact that several scholars are starting to focus their study lights on this topic, the idea of declouding becomes a volatile one. When it comes to the availability of resources on cloud repatriation, it appears that there is some sort of systematic censoring. What is actually happening is that pro-cloud propaganda masquerading as critical and open-minded journalists is clogging up the top search results. Examples include the following two search results for objections against cloud computing: (the cloud computing section of miken.net (http://cloudacademy.com >blog > disadvantages-of-cloud-computing) and (http://three-biggest-arguments-against-cloud-computing). These search results turned out to be pro-cloud articles after some investigation.

Time constraint was another major factor in carrying this study as the time allocated to research literatures and documents, conduct survey with willing participants to fill the questionnaires and return, as well as scheduled meetings with my supervisor to discuss finding and charting a next course of action was challenge based on the scheduled time. More time was needed to actualize these activities sufficiently and efficiently.

Lastly, the limited data sample size and communication gap in the information obtained, that was published in English, were additional limitations of this case study data analysis.

CONCLUSION AND RECOMMENDATION

Cloud repatriation or De-clouding is a contentious subject; some believe this never really occurs, whereas others assert to the idea that it is a growing practise. These are both largely accurate. Several businesses explore bringing back cloud workloads at a certain time, but only some ever do. Even so, cloud repatriation seems to have a place in contemporary IT, primarily as a backup strategy in an enterprise IT strategy (Bigelow, 2020). Similarly, the concept of declouding or cloud repatriation has been approach from a variety of angles, beginning from the motivations for the cloud repatriation to policy issues and emerging concept in cloud computing solutions as well as finally addressing the workload placement optimization problem. In summary, this research shows that:

- Cloud repatriation is actually happening, and it makes a more hybrid approach to workload deployment necessary.

- The study found that among other things, scalability problems, vendor lock-in worries, latency problems, performance problems, cost problems, and concerns about vendor lock-in were some of the reasons why firms started cloud repatriation initiatives.

- It was important to have a proper understanding of the concept of cloud computing in its entirety before deciding whether to go On-premise or on the public cloud. According to the literature review, it was critically important to thoroughly examine the current environment via discovery when it comes to migrating data from one cloud to another infrastructure.

- For the best placement, there is need to put in the time to truly grasp workload needs. A workload placement plan cannot be a one-size-fits-all solution and is not simple to implement. But if implemented correctly, it will yield significant long-term benefits. Businesses should take the time to commit now to building an application workload placement model that matches your organisation business demands.

- The study also highlighted the importance of corporate executives support for investments in IT staff, training them in the abilities required to skilfully handle numerous on-premises and off-premises facilities, as well as making investments in IT technology software that can enable IT professionals respond swiftly to the organisations requirements and minimise shutdowns for mission-critical systems.

- Before entering into any business deal, companies must endeavour to have carefully reviewed their SLA to safeguard themselves and their workload.

- Following the cost comparison analysis carried out by (Gartner 2019) findings indicated that certain businesses may not find it cost-effective to go to the cloud mostly due to the company's workload and how sensitive the data is, among other things. Therefore, the concept of cutting costs by switching to the public cloud might not be realised in the end.

- Full Homomorphic encryption is still the primary method for ensuring data security, privacy, and integrity, according to research.

- In addition, the study demonstrates that there are no ideal cloud services, but that optimising each strategy will produce the most results. This means that businesses should conduct a thorough assessment of their company requirements, including work performance, workload integration, technological aspects of the company, as well as the cloud ecosystem.

There are no simple answers to the workload distribution problem. In the hybrid and multicloud world of today, IT administrators must choose a hosting solution that offers the optimal combination of performance and cost effectiveness. A few of the infrastructure choices include vendor-based public clouds that provide SaaS, IaaS, and PaaS services as well as on-premises data centres with hosted private clouds. This decision involves a detailed understanding of the various workload types, their traits, the applications that enable them, and the business objectives they serve. In the dynamic hybrid world of today, determining the best workload placement is essential to maintaining company continuity.

Lastly, the workload placement guide chosen offers a quicker and simpler way to deploy workload-optimized solutions that have been validated by tested and established current theories for balanced performance across the various workload placement options.

REFERENCES

Ahmad, I. and Khandekar, A., 2014. Homomorphic Encryption Method Applied to Cloud Computing. *International Journal of Information & Computation Technology.*, ISSN 0974-2239 Volume 4, Number 15, pp.pp. 1519-1530.

Al-Sit, W., Al-Jubouri, Q. and Al-Zoubi, H., 2019. Cloud Security based on the Homomorphic Encryption. *International Journal of Advanced Computer Science and Applications*, 10(8).

Awadallah, R. and Samsudin, A., 2020. *Homomorphic Encryption for Cloud Computing and Its Challenges*.

Bajpai .S and Srivastava .P (2014) "A Fully Homomorphic Encryption Implementation on Cloud Computing”. International Journal of Information and computation technology, vol.4.

Biggenden, L., 2022. Cloud Repatriation – Fact or Fiction? [online] Available at: <https://www.nephostechnologies.com/> [Accessed 24 June 2022].

Bigelow., S., (2020). Myth or emerging trend? Cloud repatriation explained. FEATURE

Bigelow., S., (2020). Guide to colocation and how to choose a provider

Branscombe, M., 2019. Is homomorphic encryption ready to deliver confidential cloud computing to enterprises?

Calvesbert, G., 2018. Cloud Service Failure: 3 Things to Know.

Camilleri, F. 2019. Determining the best business intelligence solution according to user requirements (Bachelor's thesis, University of Malta).

(Chris Alberding, 2015). The Importance of Scalability and Cost of Data Center Solutions.

CRN News, 2018. Organizations are moving 50 percent of their public cloud applications to either a private cloud or non-cloud. [online] Available at: <https://www.crn.com/businesses-moving-from-public-cloud-due-to-security-says-idc-survey> [Accessed 1 June 2022].

Crowe, Sarah et al. (2011). “The case study approach.” *BMC medical research methodology* vol. 11 100.

Deloitte, 2022. GDPR and the impact on cloud computing the effect on agreements between enterprises and cloud service providers.

Donnelly, C., 2019. Hype vs. reality: Why some organisations are opting to de-cloud - Ahead in the Clouds. [online] Computerweekly.com. Available at: <https://www.computerweekly.com/blog/Ahead-in-the-Clouds/Hype-vs-reality-Why-some-organisations-are-opting-to-de-cloud> [Accessed 31 May 2022].

Ducato, R., 2016, September. Cloud computing for s-health and the data protection challenge: getting ready for the general data protection regulation. In 2016 IEEE International Smart Cities Conference (ISC2) (pp. 1-4). IEEE.

Elliott, E., 2019. A Brief History of Decentralized Computing And How We Can Build a Better Future.

Endo, P.T., Santos, G.L., Rosendo, D., Gomes, D.M., Moreira, A., Kelner, J., Sadok, D., Gonçalves, G.E. and Mahloo, M., 2017. Minimizing and managing cloud failures. Computer, 50(11), pp.86-90.

Duncan, B., 2018. Can EU general data protection regulation compliance be achieved when using cloud computing? Cloud computing, pp.1-6.

(Gartner 2017) Developing a Practical Hybrid Workload Placement Strategy.

Greenberg, M., Shillo, A. and Shillo, A. (2021). What is High Availability in the Public Cloud? –Statehub. [online] Statehub. Available at: https://statehub.io/resources/articles/what-is-high-availability-in-the-public-cloud/ [Accessed 1 June 2022].

Heidari A, Jafari Navimipour N. (2021). A new SLA-aware method for discovering the cloud services using an improved nature-inspired optimization algorithm. PeerJ Computer Science 7:e539 https://doi.org/10.7717/peerj-cs.539

IBM Cloud Education, (2020). Public Cloud. [online] Available at: <https://www.ibm.com/cloud/learn/public-cloud> [Accessed 7 June 2022].

IDC Researcher, 2019. Workload Placement Separates the Winners from the Losers in IT.

Imran, M., Aziz, A. and Irfan, M., (2018). Security Problems Analysis Private Cloud Computing Vs. Public Cloud Computing in Giant Organizations. *International Journal of Computer Applications*, 179(10), pp.12-15.

Jabbar and Najim (2016). Using Fully Homomorphic Encryption to Secure Cloud Computing. Internet of Things and Cloud Computing. Vol. 4, pp. 13-18. doi:10.11648/j.iotcc.20160402.12

Kenneth, D., (2021). Key factors and challenges in cloud repatriation.

Koomey, Ph.D., J. (2017). Right-Sizing Data Center Capital for Cloud Migration. [Blog] Available at: <https://www.koomey.com/post/168267640663> [Accessed 1 June 2022].

Light Edge, 2019. *Why Colocation Boosts Long-Term Scalability*. [Online] Available at: <https://www.lightedge.com/> [Accessed 15 August 2022].

Levine, P., 2016. The End of Cloud Computing | Andreessen Horowitz. [online Andreessen Horowitz. Available at: <https://a16z.com/2019/11/15/the-end-of-cloud-computing-2/> [Accessed 2 June 2022].

Levite, A. and Kalwani, G., 2020. *Cloud Governance Challenges: A Survey of Policy and Regulatory Issues*.

Linkedin.com. 2017. 451 Research: Survey finds opportunity for cloud providers to help customers align IT transformation with business requirements. [online] Available at: <https://www.linkedin.com/pulse/451-research-survey-finds-opportunity-cloud providers-marsha-versen> [Accessed 2 June 2022].

Mahadi, s., 2017. Today's Centralized Cloud And The Emerging Decentralized Edge. [online] Forbes. Available at: <https://www.forbes.com/sites/forbestechcouncil/2017/12/05/todays-centralized cloud-and-the-emerging-decentralized-edge/> [Accessed 2 June 2022].

M. M. Alani (2014),"Securing the Cloud: Threats, Attacks and Mitigation Techniques," Journal of Advanced Computer Science & Technology, vol. 3

Mancaş, C., 2019. *Performance analysis in private and public Cloud infrastructures*. University of Craiova Romania.

Manovich, L., 2003. New media from Borges to HTML. *The new media reader*, *1*(2), pp.13-25.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A., 2011. Cloud computing—The business perspective. Decision support systems, 51(1), pp.176-189.

Mason J (2002). *Qualitative researching*. London: Sage.

McHenry, M., 2019. What is Cloud Repatriation and When Does It Make Sense? | LightEdge. [online] LightEdge Solutions. Available at: <https://www.lightedge.com/blog/what-is-cloud-repatriation/> [Accessed 30 May 2022].

Montgomery, J., Casey, K. and Semilof, M., 2022. What is cloud migration? An introduction to moving to the cloud.

Novacontext.com. 2019. Trends in Cloud Transformation. [online] Available at: https://novacontext.com/2019-trends-in-cloud-transformation/index.html [Accessed 2 June 2022].

Opara-Martins, J., Sahandi, R. & Tian, F (2016). Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. *J Cloud Comp* https://doi.org/10.1186/s13677-016-0054-z

Opara-Martins, J., 2018. Taxonomy of cloud lock-in challenges. Mobile Computing Technology and Applications.

Pritchard, S., 2021. *Cloud repatriation: Five reasons to repatriate data from cloud*.

Parmar, D., 2021. Workload Suitability Across Cloud and On-Premises Data Centres.

Russell and Norvig, 2002 Artificial intelligence: a modern approach. Prentice-Hall

Schmidt, P.J., Wood, J.T. and Grabski, S.V., 2016. Business in the cloud: Research questions on governance, audit, and assurance. *Journal of Information Systems*, *30*(3), pp.173-189.

Shehabi, A., Smith, S., Masanet, E. and Koomey, J., 2018. Data center growth in the United States: decoupling the demand for services from electricity use. Environmental Research Letters, 13(12), p.124030.

Shrestha .R and Kim S. (2019). Role of Blockchain Technology in IoT Applications **in** Advances in Computers.

Stake RE (1995). *The art of case study research*. London: Sage Publications Ltd.

(Tchernykh *et al*., 2015). Towards Understanding Uncertainty in Cloud Computing Resource Provisioning

Toivonen M., 2013. Cloud Provider Interoperability and Customer lock-In. In Proceedings of the seminar (No. 58312107, pp. 14–19)

Tolsma, A., 2022. How will cloud computing change by the GDPR? What are the general privacy challenges and the GDPR specific challenges to anticipate?

Watada, J., Roy, A., Kadikar, R., Pham, H. and Xu, B., (2019). Emerging trends, techniques and open issues of containerization: a review. IEEE Access, 7, pp.152443152472.

Williams, C., 2007. Research methods. Journal of Business & Economics Research (JBER), 5(3).

Yin, R. (2009). Case study research: Design and methods (Rev. ed.). Newbury Park, CA: Sage Publishing.

Younes Khair, Abdeslam Dennai, and Youssef Elmir (2022). "An Experimental Performance Evaluation of Open Nebula and Eucalyptus Cloud Platform Solutions", *Artificial Intelligence and Heuristics for Smart Energy Efficiency in Smart Cities*, vol.361, pp.450,

Zaindenwerg, U., (2021). WHAT IS HIGH AVAILABILITY IN THE PUBLIC CLOUD? [online] Available at: <https://statehub.io/resources/articles/what-is-high-availability-in-the-public-cloud/> [Accessed 2 June 2022].

Zavodovski et al., (2020). DeCloud: Truthful Decentralized Double Auction for Edge Clouds. [online] Available at: https://ieeexplore.ieee.org/document/8885067 [Accessed 30 May 2022].

Zhong, Z., He, J., Rodriguez, M.A., Erfani, S., Kotagiri, R. and Buyya, R., (2020). Heterogeneous task co-location in containerized cloud computing environments. In IEEE 23rd International Symposium on Real-Time Distributed Computing (ISORC) (pp. 79-88). IEEE.