Hybrid Cloud Computing: An Analysis of an Emerging Paradigm

Stephen Haugland and Travis Herrera

Abstract—Cloud computing has become an increasingly important method used to provide internet services. One major development has been the combination of the private and public sectors of the Cloud into what is known as Hybrid cloud computing. This creates an infrastructure which allows users to take advantage of the efficiencies of both platforms. This emerging paradigm of cloud computing shares some of the benefits of traditional cloud computing along with added security, reliability, and flexibility. Being able to access private and public sectors allows companies to create a cloud computing service specific to their needs. Despite its appealing nature, the Hybrid approach is not without flaws. The use of private and public cloud requires more resources allocated to managing the complexity of the system and inherits risks associated with the public cloud. In its relatively new development, there have been various attempts to implement this architecture. Many of the industry leaders, such as Amazon Web Services and Microsoft Azure, are taking strides to enhance the beneficial features of this approach while diminishing the downsides. The aim of this paper is to analyze the various aspects of hybrid cloud computing, compare competitor implementations, and share some of the ongoing research directions.

Index Terms—Cloud Computing, Distributed Computing, Hybrid Clouds, Data Center, Virtualization

---

TABLE OF CONTENTS:

* *Stephen Haugland, Dept. of Mathematics & Computer Science, Whitworth University, Spokane, WA 99251. E-mail: shaugland21@my.whitworth.edu*
* *Travis Herrera, Dept. of Mathematics & Computer Science, Whitworth University, Spokane, WA 99251. E-mail: therrera21@my.whitworth.edu*

1 Introduction

Over the past decade cloud computing has become an increasingly important method used to provide computing resources. Cloud service providers have taken advantage of the vast quantity and diversity of companies that would benefit from being provided storage and computing resources as they grow and strive to increase efficiency. Some of the many resources provided by the cloud can include storage, servers, services, applications, analytics, and intelligence. Use of the cloud is only going to continue growing, and as business needs of companies evolve, so are the ways of providing those resources. One method that has gained traction is the use of the hybrid cloud. Many companies have devoted time and money into the development of this new paradigm due to its rise in customer popularity. The relevance of the hybrid cloud comes from its innovative nature that changes the way enterprises receive cloud computing resources. Like any new development, it is important to look at how it has affected the industry. Before examining the details of the hybrid cloud, one must first understand the nature of cloud computing itself.

2 Cloud Computing Overview

2.1 Introduction

According to the NIST definition, cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1]. Essentially, it is a tool that allows organizations to outsource many of their information technology processes to a third party. These external cloud service providers utilize large datacenters to concurrently lease their computing resources to customers. These data centers can be easily accessed by many users from anywhere in the world through the internet.

One of the main benefits of cloud computing is its affordability. Due to a flexible payment model that is commonly used, it ends up being significantly more affordable than the alternative. Instead of having to invest in the hardware, software, and computing infrastructure that is capable of handling peak loads, businesses can lease third-party computing resources in a pay-per-use model. This way businesses do not have to worry about wasting resources by potentially under-utilizing their systems but instead can scale up and down quickly and freely, only paying for what they use. This saves money for large businesses but is especially important to small and medium businesses whose IT needs may be more volatile [2]. Additionally, without the need to hire IT experts to take care of the system, costs can be reduced even further.

Another benefit that comes from having specialized cloud providers as opposed to a single on premises datacenter is that they ensure that their hardware and software is routinely upgraded to provide optimal performance. Not only are their datacenters regularly maintained, but they are often organized in a global network with each other to provide more scalability and decreased latency in large scale uses [3].

One staple element of cloud computing is its on-demand self-service. This means that users have quick and easy access to provisioning resources without going through any human middleman to guide the set-up process [4]. This provides flexibility to businesses, only requiring several clicks to adjust their resources to accommodate new capacities. Consequently, this decreases the hassle of needing to predict and plan for load changes[3].

Cloud computing's ubiquity can be seen by its widespread adoption across industries: from gaming and video streaming, to banking and government services [5]. As it is adopted by an increasing amount of businesses that demand constant uptime, reliability has become an expectation for cloud service providers. Through a variety of design principles and practices, cloud service providers have been able to garner trust behind the concept of the cloud. One such practice utilized is fault tolerance through data replication. This can be implemented through replication within individual systems, or across multiple datacenters. One such use of this is Netflix's global data replication across its different AWS regions using Cassandra, a distributed, cross-regional NoSQL database replication. This allows traffic to be redirected to adjacent regions in the case of outages [5]. Another technique integrated by cloud service providers is the use artificial intelligence to analyze patterns and produce extensive reports based on usage statistics and logs. Previously, the sheer amount of data produced from these reports made it virtually impossible to manually sort through and analyze. However, with the use of advanced machine learning, important insights can be produced on where system vulnerabilities are as well as ways to mitigate risks of breaches or downtime [5].

Besides the reliability of the cloud, one of the biggest concerns companies have when moving some of their critical data to third party systems is security. To overcome this, cloud service providers implement security practices by adhering to a combination of confidentiality, integrity, and availability. Confidentiality pertains to making sure only those who have the correct authentication can access data. This is accomplished by rigorous access control including measures such as multi-factor authentication or by using identity aware proxies. Integrity is achieved through the use of digital signatures among other measures to ensure data is not altered by any unauthorized person. Lastly, along with ensuring that data is safe, it must be available to users on demand. Even with these measures including advanced encryption techniques, companies are hesitant to give all of their data to third parties to manage in a public cloud and many will choose to include a private cloud as well [6].

2.2 Cloud Services

There are several different service models that cloud providers offer. These are broken down into infrastructure as a service, platform as a service, and software as a service. All three services can be viewed as layers with varying levels of user control, and provider management. Before cloud computing became a dominant paradigm, all IT operations were managed by the customer in corporate datacenters, but now there are several different service offerings based on varying needs of the user [7].

Infrastructure as a service (IaaS): Infrastructure is the simplest form of service and grants the most control to the user. IaaS offers customers the hardware and infrastructure resources to perform operations using virtualization technology [8]. IaaS scales quickly and falls under the on-demand payment model [9]. This is the lowest tier of services offered and only provides the physical servers located in the providers datacenters, granting customers access and management tools through the internet. Some common uses of IaaS include affordable website hosting, rapid application prototyping, and web app deployment [9]. Some examples of IaaS include Amazon Compute Cloud, Google Computer Engine, Rackspace, and Microsoft Azure [7, 4].

Platform as a service (PaaS): Platform as a service is a step up from Infrastructure as a service, with additional functions ran by the cloud provider. PaaS provides all the features of IaaS in addition to an operating system, development tools, middleware, database management systems, and more [10]. PaaS is the ideal service for customers looking for a place to build their application. With system software being managed by the provider, there is no need for the customer to deal with updates and installs. In addition to the included development tools, this makes PaaS optimized for teams of developers to collaborate on the creation and deployment of cloud-based applications [10]. Some examples of PaaS are Heroku, Microsoft Azure, and Google App Engine [8, 4].

Software as a service (SaaS): Software as a service offers the least control to the user, and all functions of the provided service are managed by the cloud service provider. SaaS is software that is hosted on the cloud, giving any user who has internet access, the ability to run it on the infrastructure of the provider [11].This removes much of the burden and complexity of maintaining and operating the software away from the customer and is instead taken care of by the provider [8]. One common use of SaaS is web-based mail applications like Hotmail, or Outlook [12]. Office productivity services such as Dropbox and Google Apps also fall under the category of SaaS [7].

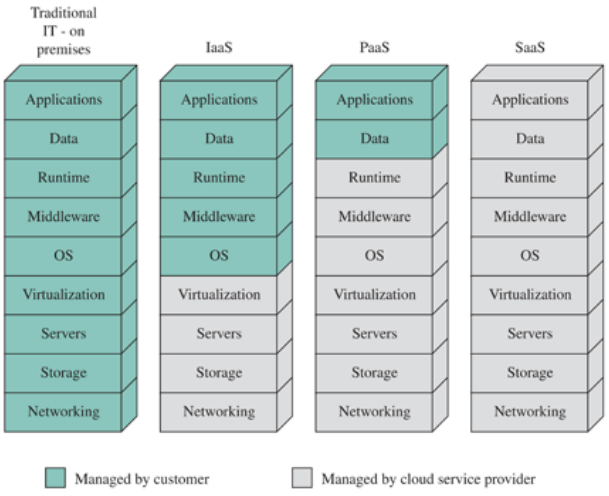

Fig. 1 Cloud Computing Service Models [4]

2.3 Types of Cloud Computing

In the process of abstracting IT operations away from businesses to the cloud, there are several options when deciding on level of involvement and ownership of the cloud [4]. The four different models of cloud deployment are public, private, hybrid, and community clouds.

Public Cloud: A public cloud is the traditional deployment option where third parties provide computing services to users through the internet [11]. These resources are being shared with other cloud users and the infrastructure is owned and managed by the cloud service provider.

Private Cloud: A private clouds offers more control of how data is managed, and subsequently offers a higher level of security. Private clouds attempt to mimic the functionality of a public cloud within a private network [8]. Typically, private cloud infrastructure is owned by a single organization and resources are not shared.

Hybrid Cloud: A hybrid cloud attempts to take the benefits of both a private and a public cloud to give customers the best of both worlds. By using the existing infrastructure that companies may have to establish a cloud on their private networks as well as utilizing public clouds for larger workloads companies can try and optimize the benefit from both the public and cloud [8].

Community Cloud: A community cloud is developed for a common cause and is usually owned by a group of organizations. It is like a hybrid cloud in that fact that it utilizes a multiple number of clouds, usually a combination of public and private. Community cloud differs from a hybrid cloud because it is not used for a single organization but rather used by a group of common businesses or organizations who have signed an agreement [8].

Through examining some of the architecture of the cloud, it is seen how different types of users necessitate a wide range of deployment options and service models. One of the more common patterns that is emerging in

industry is the installment of hybrid clouds due to their flexibility, privacy, and convenience.

3 Hybrid Cloud Computing

3.1 Introduction

The hybrid cloud infrastructure is a more complex model due to its composition of at least one private cloud and one public cloud. The different clouds used by this structure remain unique entities but are connected through standardized or proprietary technology that allows for application and data portability [4]. This enables the option for sensitive data to be stored in a private section of the cloud, while less sensitive data can be stored in a public section. Businesses can take advantage of the public sector's flexibility and cost-effectiveness while maintaining control over critical applications and data [13]. The option to choose which data is public and which is private makes the hybrid cloud solution very scalable. Regarding security, clearly a private cloud is the most secure option. However, a hybrid cloud has access to this benefit by utilizing a private cloud. Of the three components to computer security (physical, technical, and administrative), technical controls are at the heart of hybrid cloud, due to their easy implementation made possible by centralized management [14]. Encryption can be implemented to protect readable data if a physical machine is compromised. automation is used to stay ahead of risks, rather than reacting to them. Processes within a hybrid cloud environment that can be automated to enhance security are monitoring the environments, checking for compliance, and implementing security baselines. Endpoint security is an essential component to any hybrid cloud, seeing as users can connect to the database with a personal device from anywhere. This form of security uses software to remotely revoke access or wipe sensitive data. In terms of performance, hybrid clouds have come a long way over the past decade of development. Workloads used to be statically bound to a single private cloud or multiple public clouds but can now be moved dynamically between clouds in near real-time [[15]. Having the power to distribute processes between clouds allows for better performance management. Hybrid cloud provides many features that could prove beneficial for certain organizations or businesses. In the next section, we will discuss the typical use cases of this model.

3.2 Use Cases

One of the main attractive features of the hybrid cloud is that it provides more data privacy by not solely relying on a third party to control sensitive data. This is particularly beneficial to small businesses or startups that cannot afford to take on the costs of implementing their own infrastructure. Many applications that do not have substantial security concerns can be offloaded at considerable cost savings without committing the rest of the businesses more sensitive data and applications to the public cloud [4]. This reduces the capital expenses since the need for physical storage is decreased as non-sensitive data and applications are outsourced to public cloud. For example, businesses can store data pertaining to human resources or customer relationship management in a public cloud, like Saleforce.com, while storing confidential data in-house [13]. The hybrid cloud is also a good fit for enterprises new to the cloud by offering disaster recovery. Backup database storage and compute can be stored for a fraction of the cost of on-perm disaster recovery solutions [16]. It is not only small businesses that are utilizing the hybrid cloud approach. Many Large companies, such as Amazon and Microsoft which will be discussed further in section four, are switching to the hybrid model. A survey of 2,650 IT decision-makers across 24 countries indicated hybrid cloud has become their ideal operating model [17]. This is due to the ability to handle overflow by seamlessly scaling on-premise infrastructure up to the public cloud while withholding access to the entirety of their data from third party data centers. Many companies are investing in hybrid cloud solutions due to its low cost and high benefit. Though the model possesses many beneficial features, it is not without flaws.

3.3 Drawbacks

One of the biggest features of a hybrid cloud approach is its utilization of the public cloud. Though it is beneficial to be able to offload non-critical data and applications, it can become an issue if optimization efforts are not top priority. According to the 2018 State of Cloud survey, almost a thousand professionals are aware they are wasting money in the cloud, an estimated 30% [18]. This is due to poor cost and data optimization processes that keep information in the public cloud, that could be moved to the private cloud or removed completely, where it increases the charges made to the company. Hybrid cloud models inherently have a more complex architecture due to the usage of multiple cloud structures. Without the knowledge of how best to manage the complexity, businesses can end up paying more than they need to for public storage. In addition, the hybrid approach also carries with it some of the downsides of the public cloud, the main one being security. This is an aspect of the cloud that can be expensive to do right but could be even more costly if done wrong. Among all complex and expansive hybrid cloud environments, data can be at risk in transit or at rest. The private-public architecture of hybrid cloud requires nearly constant transfer of data from one cloud environment to another. This opens the door for eavesdropping and cyberattacks targeting the data being transferred [19]. Without solid encryption protocols, sensitive data could easily end up in the wrong hands. Another issue related to the sharing of data between the two environments is data leakage. Sensitive data can be compromised in a variety of ways and data security is the responsibility of the owner of the data. To ensure data is not compromised through corruption, destruction, inappropriately accessed, or lost, a company must assess the data practices and security protocols of their public cloud provider. This adds to the list of things that must be considered when implementing a hybrid cloud model, increasing its complexity. Though the paradigm has some setbacks, top competitors have their own ways of overcoming them through their implementation of a hybrid cloud.

4 Competitor Analysis and Comparison

4.1 Introduction

Competition drives innovation in the technology world and that becomes abundantly evident through hybrid cloud computing. As industry leaders continue to set the standard, new developments are made by competitors to challenge those paving the way. In the world of hybrid cloud computing, four companies stand out above the rest: Amazon, Microsoft, IBM, and Google. This section will analyze the hybrid cloud that each company provides, highlighting the services, pricing, and security aspects to compare their methods.

4.2 Amazon Web Services

Amazon Web Services (AWS) offers a broad range of services that make it seamless for customers to run on-premise infrastructure with AWS. Mainly Infrastructure as a Service (IaaS), AWS aims to help integrate customers' up and running cloud system with their services. Common use cases for the AWS hybrid cloud are data center extension, cloud services on-premise, VMware cloud migration, ISV and software compatibility, and edge computing. Amazon VPC allows for the provision of a logically isolated, virtual network in AWS that runs as an extension of a customer's on-premise network. They offer AWS Direct Connect, which establishes private connectivity to AWS as well as AWS Storage Gateway which allows access to the AWS cloud storage for on-premise applications [20].

AWS uses a pay-as-you-go approach to pricing, comparing the costs to that of utilities; you only pay for the services you use and when you stop, the billing stops. This style reduces the risk that customers will overpay and miss out on unused capacity. For certain services, such as Amazon EC2 and Amazon RDS, they incorporate reserved capacities. This allows the customer a greater discount on a larger upfront payment. In summary, Amazon's approach is for customers to pay less by using more. A lot of their services implement a tiered pricing scheme, meaning the more a customer uses, the less they pay per GB. The flexibility of AWS pricing along with the plethora of services with top-tier performance has made it the most trusted computing service amongst fortune 500 companies [21].

The security of AWS has also contributed to its success. In terms of the infrastructure, AWS data centers use an innovative architecture, due to their experience designing and constructing data centers, to ensure customer data security. During the physical access of AWS data centers, professional security staff is hired and use intrusion detection equipment and high-level security identification to control the environment [22]. The AWS network security is also world class, due to its secure network architecture and access points, transmission protection, fault tolerant design, and network monitoring and protection [22]. Amazon Information Security approves the flow information. Customer access points are referred to as API endpoints and help in the access of secure HTTP. The fault tolerant design ensures that minimal impact will be on the customer should any software or hardware fail in the architecture. The network monitoring and protection is also top tier, offering automated error detection, unauthorized access, or unusual activity. A secure network architecture is attained by AWS through network devices, such as firewalls, that manage the boundaries of the network. AWS has been involved in public cloud computing since its launch in 2006, offering simple storage service and elastic compute cloud [23]. According to an analysis by Synergy Research Group, AWS holds a larger share of the public infrastructure market than Microsoft, IBM, and Google combined [24]. With a clear dominance in the public cloud sector, AWS shifted its focus towards the hybrid approach and remains in fierce competition with Microsoft, IBM, and Google.

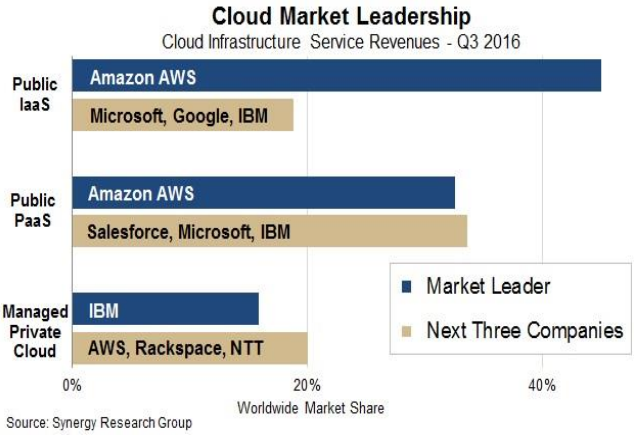

Fig. 2 Cloud Market Leadership [24]

4.3 Microsoft Azure

Although Amazon Web Services established itself as the first cloud computing platform and remains the dominant provider of cloud services, Microsoft Azure is not far behind. As opposed to AWS's strong Infrastructure as a service(IaaS) offerings, one of Azure's strongest features revolves on providing software as a service, with Office 365 and several other software centered services generating a majority of its revenue [25].Microsoft Azure is a true enterprise facing company and their willingness to listen to their customers concerns about the public cloud is what has allowed them to be so successful. Microsoft has acknowledged that enterprises may want to retain some their own on premises data centers and have worked hard to handle the communication between private and public clouds. One of the main hesitations of adding a public cloud in addition to a private cloud is the migration of data and services from antiquated infrastructures and systems. Azure makes this process as streamlined as possible with their advanced migration tools. One of their premium hybrid offerings is the Azure Stack which brings the cloud to enterprises' local datacenters. Building Azure with hybrid in mind from the beginning, Microsoft has been able to provide a wide variety of support tools to help a seamless migration into the hybrid cloud.

Azure's payment model is based on a pay-per-use basis which makes it affordable for any size company to add their services. As a more affordable option than Amazon, Azure's platform offers many savings. As advertised on their website, Azure users can save up to 71 percent for

Windows virtual machines, 85 percent for SQL database managed instances, and 45 percent for SQL server virtual machines compared to Amazon's equivalent services[26]. Azure also allows its customers to utilize existing software licenses, giving customers the opportunity to save even more money through software assurance. They also have packages that allow customers to reserve resources by making 1 to 3-year contracts for discounted rates, which can be an ideal method for larger businesses.

Currently, over 95 percent of Fortune 500 companies are using Azure and their robust security is one of the key reasons [27]. Investing more than one billion dollars annually on cybersecurity research and development allows Microsoft Azure to be on the cutting edge of security practices [28]. They also currently hold the lead for the most compliance certifications among all cloud providers, and it is apparent security is one of their top concerns, as it should be. Additionally, when customers switch over to Microsoft Azure for Windows Server or similar services, three years of free security updates are provided [27]. One of the main ways Microsoft Azure secures its infrastructure is by making their network infrastructure secure. This is accomplished by isolating customer and management networks, strong encryption techniques, and by having DDoS attack protection built in. In an additional measure to secure hardware and firmware Microsoft recently announced Project Cerberus which uses specialized microcontrollers to protect from malicious attacks [29]. Extensive work is also put into to vulnerability assessments through routine testing and monitoring.

All these aspects have contributed to Microsoft Azure having very strong offerings in the hybrid cloud space and garner much success by being one of the first providers adopt this paradigm. Being a cheaper alternative to AWS, while providing seamless hybrid transitions and unparalleled commitment to security, it is clear why Microsoft Azure is the enterprise preferred hybrid cloud service provider [25].

4.4 IBM Cloud

IBM's strong hold on the private cloud sector made its transition towards hybrid solutions frictionless. Their hybrid cloud provides an integrated environment with supporting technologies for multi-cloud management. Customers can build, deploy, and operate apps and services wherever they are best run as well as get seamless and secure data portability [30]. IBM offers flexible and well-balanced services that improve both public and private cloud. With their hybrid cloud, IBM claims that companies can more effectively manage security and speed, lower latency, and drive higher performance. All their services can be deployed and managed where the customer finds it most appropriate. With Kubernetes, an open source container platform that automates the deploying, scaling, and managing of applications, customers can build one container infrastructure for their public and private clouds and can place applications and workloads where they see fit [31]. IBM cloud integration allows for personalized customer experiences to be created by connecting data and applications across multiple clouds. IBM also offers the DevOps service, a growing approach to agile software development that can be used to build, test, deploy, and monitor applications with speed, quality, and control. [32].

As far as pricing goes, IBM offers many different price packages to suit the needs of any customer. With the Lite account, users can sign up for free without requiring a credit card. This account never expires and gives access to 256 MB of free, instantaneous runtime memory per month for Cloud Foundry apps. The downside to this plan is that after 30 days of no development activity, the service instances with Lite plans are deleted. IBM's pay-as-you-go plan is like that of other cloud service providers in that the customer is only billed for the services they use. Along with AWS, IBM also offers a reserved instances package that requires a one- or three-year commitment and offers discounted pricing and guaranteed capacity. The last price package IBM offers is a subscription that requires longer-term commitments in exchange for discounted rates and predictable billing [33].

Regarding security, IBM is focused on providing continuous edge-to-cloud protection for applications and data. With a long-standing history as a leading security provider, IBM offers multiple ways to secure a customer's cloud. Through identity and access management, IBM can strengthen compliance management and reduce risk of security breaches. IBM Cloud is also designed for lifecycle protection of data, keeping it secure through encryption while data is at rest, in motion, and in use. In addition, IBM Cloud comes equipped with proactive security monitoring intelligence across all hybrid cloud deployments, keeping the customer one step ahead of threats [34]. IBM has also been setting their sights on the challenging concept of securing company data and applications across multiple private and public clouds and on-premises sites. In doing so, they developed the Cloud Pak for Security, a bundle of Red Hat's Kubernetes-based OpenShift Container Platform accompanied with Red Hat Linux. This Cloud Pak features the abilities to hunt threats, respond quickly to cyberattacks, and integrate a customer's already existing point-product security-system information [35]. This was a big development for IBM in the security sector because it allows security teams to connect to all data sources in order to make improved risk-based decisions and expose unseen threats. Though IBM may not be as popular of a hybrid cloud service provider to the average company, their research and development has kept them in the race and gained them a lot of recognition amongst the cloud computing community.

4.5 Google Cloud Platform

The Google Cloud Platform offers a wide variety of services, but their Google App Engine is one of their premier services. This is a prominent platform where developers can deploy their applications and is a strong competitor in the platform as a service space. As far as their hybrid cloud platform they were one of the last cloud service providers to begin offering it with their release of their hybrid cloud platform, Google Anthos, in April of 2019. One of Anthos main features is GKE which is the Google Kubernetes Engine. This allows customers to run Kubernetes workloads

on premises, on the Google cloud, or most interestingly within other cloud providers infrastructure. This is Google's entry into both the hybrid and community cloud space and although they have a limited market share compared to Amazon and Microsoft they are quickly expanding with a cloud revenue growth of 135 percent in 2018 and 70 percent in 2019 [25]. In an effort to compete with the popular integration methods such as Azure's migration tools, Google has their own tool now in beta called Anthos Migrate. Anthos plans to be able to transfer virtual machine images into containers, and then deploy them onto Anthos in order to easily migrate legacy applications [36].

Google's hybrid cloud offerings are based on a monthly subscription model with a one-year minimum contract. At 10,000 dollars a month per 100 virtual CPUs this is a large commitment for business, especially considering that is just the cost for the infrastructure let alone any software or support packages [36]. Although support is not included in the monthly cost, Google does require that it be purchased. This fact, along with other confusing pricing aspects such as varying price based on geographic location have set Google's hybrid cloud play behind the top competitors in terms of payment models. This is especially daunting for smaller companies; however, Google has stated that it's target customers are large enterprises, targeting educational and financial sectors.

However, what Google may lack in straightforward pricing, they make up for with advanced AI, machine learning, and analytics. Some of the things Google does best has been brought to their cloud service and the lessons that the tech supergiant has learned has transferred over to their cloud services. As far security, they offer several advanced techniques to prevent malicious attacks and unauthorized users from tampering with data. Through the use of identity-aware proxies as well as a plethora of options regarding encryption options, Google should not be overlooked at one of the security frontrunners [37]. In addition to their rigorous security standards they also practice transparency and allow their customers an inside look at how their infrastructure is run.

Even though Google joined the hybrid cloud space later than other competitors they are making strong efforts to cement themselves as one of the top providers. Their Anthos play is a strong move to future proofing their services with the ability to utilize it as a community cloud management tool as well, another up and coming cloud paradigm.

5 Conclusion and Future Research

Within the cloud space, hybrid cloud computing has become a widely popular and efficient way for companies to store and manage data as well as access computing resources. Allowing companies to integrate their existing IT infrastructure allows for critical data to be stored in private clouds, while simultaneously offloading large workloads to the public clouds, providing the best of both worlds. Although maybe not ideal for smaller companies who can handle data storage and workloads in a private cloud or who cannot afford the cost of distributing their cloud to multiple systems, for larger companies this can be an ideal option. By looking at the top competitors, it is clear to see that a pay-as-you-go pricing model is the most effective and widely accepted approach. The reason this method is very common is due to its flexible nature, giving the customer the control to utilize certain aspects of the service without getting charged for aspects they are not using. Out of the top competitors, Microsoft Azure is leading in the security of their hybrid cloud, with IBM Cloud behind them. The time and money these companies pour into security research and development has paid off, with both companies receiving acknowledgement for their security practices amongst the cloud computing community.

One related paradigm that has received more attention lately is that of the multi-cloud. A multi-cloud approach is made up of more than one cloud service from more than one cloud vendor [38]. This gives the company the ability to integrate features from different cloud providers in their custom applications, features that may only be available by that one provider. This allows an enterprise to essentially mix-and-match services from different providers to suit their customers' needs. In a survey done by Tech Republic in 2019 of tech professionals, 69% of respondents either currently use or plan to use services from multiple cloud providers [39]. With this approach, enterprises can avoid vendor lock-in and have access to competitive pricing. In addition, companies that use this approach will inherently build a cloud system more resistant to outages due to their system not relying on one provider. However, the multi-cloud method is accompanied by its own setbacks. Similar to the hybrid cloud, complexity becomes a big issue when implementing multiple cloud providers, along with migrating applications and security. In fact, only 13% of those surveyed by Tech Republic claimed to have no challenges managing their multi-cloud infrastructure [39].

With the persistence of the hybrid cloud and the emergence of the multi-cloud, one cannot help but notice the similarities between the relationship of these developments in regard to their predecessors. Just as hybrid cloud grew tremendously by utilizing both the public and private clouds, the multi-cloud has gained popularity by combining hybrid cloud services from different vendors. In the same way advancements in migration tools and improved security between clouds aided the adoption of the hybrid cloud, they will also help in the movement towards an industry-wide multi-cloud infrastructure.

References

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," *National Institute of Standards and Technology*, Sept. 2011, SP 800-145.

[2] "25 Must-Know Cloud Computing Statistics in 2020." hostingtribunal.com. https://hostingtribunal.com/blog/cloud-computing-statistics/#gref (accessed May 7, 2020).

[3] "What is cloud computing?" Microsoft Azure. https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/ (accessed May 5, 2020).

[4] W. Stallings, "16.1 Cloud Computing," in *Operating Systems: Internals and Design Principles*, 9th ed. New York, NY, USA: Pearson, 2013, ch. 16.

[5] Y. Izrailevsky and C. Bell, "Cloud Reliability," *IEEE Cloud*

Computing, vol. 5, no. 3, pp.39-44, May./Jun. 2018, doi: 10.1109/MCC.2018.032591615.

[6] A. Venkatesh and M. S. Eastaff, "A Study of Data Storage Security Issues in Cloud Computing," *International Journal of Scientific Research in Computer Science*, vol. 3, no. 1, Jan./Feb. 2018.

[7] T. Hou. "IaaS vs PaaS vs SaaS Enter the Ecommerce Vernacular: What You Need to Know, Examples & More." Big Commerce. https://www.bigcommerce.com/blog/saas-vs-paas-vs-iaas/#the-key-differences-between-on-premise-saas-paas-iaas (accessed May 8, 2020).

[8] M. Nazir, "Cloud Computing: Overview & Current Research Challenges," *IOSR Journal of Computer Engineering*, ISSN: 2278-0661, vol. 8, no. 1, pp. 14-22, Nov./Dec. 2012.

[9] "What is IaaS?" Microsoft Azure. https://azure.microsoft.com/en-us/overview/what-is-iaas/ (accessed May 8, 2020).

[10] "What is PaaS?" Microsoft Azure. https://azure.microsoft.com/en-us/overview/what-is-paas/ (accessed May 8, 2020).

[11] P. Srivastava and R. Khan, "A Review Paper on Cloud Computing," *International Journals of Advanced Research in Computer Science and Software Engineering*, vol. 8, no. 6, June 2018, doi: 10.23956/ijarcsse.v8i6.711.

[12] "What is SaaS?" Microsoft Azure. https://azure.microsoft.com/en-us/overview/what-is-saas/ (accessed May 8, 2020).

[13] Sumit, "Critical Review of Cloud Computing: Public, Private, Hybrid, and Community.' semanticscholar.org. https://pdfs.semanticscholar.org/81e4/55Stallingsb5c34a2327cb80d73527b612b6137e85f0.pdf. (accessed May 7th, 2020)

[14] "What is Hybrid Cloud Security." Redhat.com. https://www.redhat.com/en/topics/security/what-is-hybrid-cloud-security (accessed May, 6th, 2020).

[15] D. Linthicum. "6 best ways to manage hybrid cloud performance." TechBeacon.com. https://techbeacon.com/enterprise-it/cloudops-6-best-ways-manage-hybrid-cloud-performance. (accessed May 6th, 2020).

[16] S. Vonnegut. "7 Reasons Why the Hybrid Cloud is Ideal for Enterprises New to the Cloud." Stratoscale.com. https://www.stratoscale.com/blog/cloud/7-reasons-hybrid-cloud-ideal-enterprises-new-cloud/ (accessed May 6th, 2020).

[17] D. Roe. "Why Enterprises Are Turning to Hybrid Cloud." Cmswire.come. https://www.cmswire.com/information-management/why-enterprises-are-turning-to-hybrid-cloud/ (accessed May 7th, 2020).

[18] "Survey Says: Cost and Security are Top Hybrid Cloud Concerns." Cio.com. https://www.cio.com/article/3310036/survey-says-cost-and-security-are-top-hybrid-cloud-concerns.html (accessed May 7th, 2020).

[19] K. Gyarmathy. "Cloud Security Challenges Facing Hybrid Cloud Deployments." Vxchnge.com. https://www.vxchnge.com/blog/challenges-hybrid-cloud-security (accessed May 7th, 2020).

[20] "Hybrid Cloud with AWS." Amazon.com. https://aws.amazon.com/hybrid/ (accessed May 6th, 2020)

[21] S. Naganuri. "Why AWS Has Gained Popularity." Mindmajix.com. https://mindmajix.com/why-aws-has-gained-popularity (accessed May 8th, 2020).

[22] S. Narula, A. Jain, Ms. Prachi. "Cloud Computing Security: Amazon Web Service," presented at the Fifth International Conference on Advanced Computing & Communication Technologies. https://www.researchgate.net/profile/Prachi_Chaudhary2/publication/283871947_Security_threats_in_cloud_computing/links/56b084d508ae9f0ff7b4d57b.pdf.

[23] A. Rojas. "A Brief History of AWS." Mediatemple.com. https://mediatemple.net/blog/cloud-hosting/brief-history-aws/. (accessed May 8th, 2020).

[24] "Amazon Dominates Public IaaS and Ahead in PaaS; IBM Leads in Private Cloud." Srgresearch.com. Reno, NV, USA. 30 Oct. 2016. https://www.srgresearch.com/articles/amazon-dominates-public-iaas-paas-ibm-leads-managed-private-cloud.

[25] M. W. Wachsman. " Top cloud providers in 2020: AWS, Microsoft Azure, and Google Cloud, hybrid, SaaS players." ZDNet. https://www.zdnet.com/article/the-top-cloud-providers-of-2020-aws-microsoft-azure-google-cloud-hybrid-saas/ (accessed May 11, 2020).

[26] "Azure pricing." Microsoft Azure. https://azure.microsoft.com/en-us/pricing/ (accessed May 11, 2020).

[27] "Azure vs. AWS." Microsoft Azure. https://azure.microsoft.com/en-us/overview/azure-vs-aws/ (accessed May 11, 2020).

[28] "Windows Server and SQL Server: Best on Azure." Microsoft Azure. https://azure.microsoft.com/en-us/campaigns/best-on-azure/ (accessed May 11, 2020).

[29] A. Ben-Menahem. "3 reasons why Azure's infrastructure is secure." Microsoft Azure. https://azure.microsoft.com/en-us/blog/3-reasons-why-azure-s-infrastructure-is-secure/ (accessed May 13, 2020).

[30] "Build a Hybrid Cloud with IBM." Ibm.com. https://www.ibm.com/cloud/hybrid. (accessed May 9th, 2020).

[31] "IBM Cloud Kubernetes Service." Ibm.com. https://www.ibm.com/cloud/container-service/. (accessed ay 9th, 2020).

[32] "IBM DevOps." Ibm.com. https://www.ibm.com/cloud/devops. (accessed May 9th, 2020).

[33] "IBM Cloud Pricing." Ibm.com. https://www.ibm.com/cloud/pricing. (accessed May 9th, 2020).

[34] "IBM Cloud Security." Ibm.com. https://www.ibm.com/cloud/security. (accessed May 9th, 2020).

[35] M. Cooney. "IBM Aims at Hybrid Cloud, Enterprise Security." Networkworld.com. https://www.networkworld.com/article/3454503/ibm-aims-at-hybrid-cloud-enterprise-security.html. (accessed May 12th, 2020).

[36] M. Rouse "Google Cloud Anthos." SearchCloudComputing. https://searchcloudcomputing.techtarget.com/definition/Google-Cloud-Anthos (accessed May 15, 2020)

[37] "Encryption at Rest in Google Cloud Platform." Google Cloud. https://cloud.google.com/security/encryption-at-rest/default-encryption (accessed May 15, 2020).

[38] "What is multicloud?" Redhat.com. https://www.redhat.com/en/topics/cloud-computing/what-is-multicloud. (accessed May 15th, 2020).

[39] M Wachsman. "Research: Multicloud Deployment Becomes New Default For Enterprise Computing." Zdnet.com. https://www.zdnet.com/article/research-multicloud-deployment-becomes-new-default-for-enterprise-computing/. (accessed May 15th, 2020).