Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2024, 11(2):49-52

Review Article ISSN: 2394 - 658X

Why are large enterprises building private clouds after their journey on public clouds?

Laxminarayana Korada[1], Vijay Kartik Sikha[2]

[1](laxminarayana.k@gmail.com), ORCID: 0009-0001-6518-0060
[2](vksikha@gmail.com), ORCID: 0009-0002-2261-5551

ABSTRACT

Large enterprises transitioning from public cloud to private clouds is a growing trend driven by several key factors. While public clouds offer flexibility and cost-effectiveness, established organizations are increasingly seeking the control and security that private clouds provide. This paper explores the reasons behind this shift, including the challenges associated with public cloud services such as escalating costs, skill shortages, transparency limitations, and security concerns. The advantages of private clouds, including enhanced control, compliance, and performance, are discussed alongside the concept of cloud repatriation—moving resources back in-house to optimize costs and regulatory compliance. Additionally, the paper examines hybrid cloud solutions as a strategic approach to blend the benefits of both public and private clouds. A case study of Dropbox's migration to a private cloud highlights the practical implications of this transition. Ultimately, the decision for enterprises to adopt private clouds is influenced by their need for greater infrastructure control, security, and tailored operational strategies.

Key words: Private Cloud, Public Cloud, Cloud Repatriation, Hybrid Cloud, IT Infrastructure, Cost Optimization, Security, Regulatory Compliance, Dropbox Case Study

INTRODUCTION

For new businesses, utilizing public cloud services offers unparalleled flexibility and a minimal upfront cost. In the current IT landscape, it is almost unheard of to internally manage services such as email, voice communication, or web hosting. The inefficiencies in productivity, coupled with the expenses of purchasing hardware and software and developing platforms from scratch, usually don't justify the investment for most business models. These elements of the data supply chain can be dependably and predictably sourced from numerous providers. Conversely, the situation is different for established enterprises. These companies are already in motion with continuous revenue streams. IT leaders must navigate the challenge of transforming the business to compete in a data-centric world without disrupting ongoing operations. This necessitates careful evaluation and strategic decision-making for their IT infrastructure (Lightedge, n.d.).

HISTORICAL CONTEXT

Cloud computing's origins trace back to the 1960s with time-sharing, a technology that enabled multiple users to access a single computer simultaneously. The contemporary idea of cloud computing, where computing resources are delivered over the internet, began to take shape in the late 1990s (Islam et al., 2023).

1. Pre-2000s: Early Virtualization

In the early 1990s, several companies began developing virtualization technologies to improve the efficiency of datacentres and manage IT workloads more effectively. A significant milestone was in 1995 when Red Hat Software Inc. released Red Hat Commercial Linux, the first widely available operating system based on the

Linux kernel, which laid the groundwork for future advancements in virtualization. In 1998, VMware was founded and in the following year, VMware introduced its first product, VMware Workstation. This product featured a Type 2 hypervisor that could run on x86 versions of Windows and Linux operating systems. VMware Workstation allowed administrators to create and manage multiple virtual machines (VMs) on a single physical machine, with each VM capable of running its own operating system independently. VMware later expanded support to include x64 versions, further enhancing its versatility and appeal (Muñoz,2019).

2. **2000s: Rise of Private Clouds**

Cloud computing truly began to gain traction as a commercial concept in the mid-2000s, fuelled by the advent of virtualization and the development of web services (Islam et al., 2023). In the 2000s, several emerging technologies promised functionalities akin to private cloud systems, often referred to as grid computing, utility computing, and elastic application platforms. Although the specifics varied, the core concept remained consistent: to create a pool of computing resources that could be allocated to applications as needed, while offering scheduling, high availability, and failover capabilities. The analogy to the electrical grid, frequently used to describe cloud computing, was quite apt for these technologies. Just as customers do not need to worry about a single source of electricity, they also do not need to be concerned about a single server. They could simply connect their applications to the computational "grid," trusting that the necessary power and resources would be supplied from somewhere within the system (Harris, 2015).

3. **Late 2000s: Emergence of public cloud**

In 2006, Amazon unveiled EC2 as part of its Amazon Web Services (AWS), marking the public availability of their Infrastructure as a Service (IaaS) platform. This allowed businesses to rent virtual servers while deploying their own software and applications. Following suit, Google launched Google App Engine for application development as a Platform as a Service (PaaS) offering, and Microsoft introduced Azure, also a PaaS offering. Over time, all three companies expanded their services to include IaaS, PaaS, and Software as a Service (SaaS). Traditional hardware giants like IBM and Oracle also entered the cloud market. While not every company tasted success in this direction, Verizon, Hewlett Packard Enterprise, Dell, VMware, and others discontinued their public cloud services. Many of these companies redirected their efforts toward hybrid cloud solutions and cloud management services.

The adoption of public cloud services continues to grow, bolstered by an ever-expanding range of offerings and improved support. Innovations such as artificial intelligence (AI), machine learning, the Internet of Things (IoT), and edge computing have been integrated into public cloud services. As more organizations adopt these technologies, the demand for public cloud services keeps growing. Additionally, new methodologies in cloud application development, such as microservices, containers, and serverless computing, have become more prevalent. Experts predict that the future of public cloud computing will feature more automation and specialization. Providers are likely to offer more detailed and interconnected services to cater to a wider array of needs. Emerging technologies, including quantum computing, are expected to significantly influence the evolution of public cloud services (Bigelow and Marko, 2022).

PUBLIC CLOUD VS. PRIVATE CLOUD

The distinction between private and public cloud computing models hinges on ownership of infrastructure and accessibility.

Public cloud services are administered by third- party providers such as Amazon Web Services (AWS) and Microsoft Azure. These providers own and manage the computing resources accessible to users via the internet. Public cloud environments operate on a multi-tenant model, where multiple users share resources like virtual machines and storage infrastructure. While this sharing optimizes resource utilization, it can pose challenges related to data isolation and adherence to regulatory standards (Bigelow and Lutkevich, 2022).

Despite the benefits, public cloud services present several challenges that organizations must navigate diligently:

- Escalating Costs: Managing cloud expenses has become increasingly complex due to intricate pricing models. While public cloud services initially promise cost savings, organizations often find themselves paying more than anticipated as usage and data storage needs grow. Additional costs such as data egress fees further complicate budget management.

- Skill Shortage: There is a notable scarcity of cloud expertise among IT professionals, which poses a significant challenge. Organizations struggle to recruit and retain staff proficient in developing and managing modern cloud applications. This skills gap leaves organizations vulnerable to the complexities of contemporary IT demands, hindering effective utilization of public cloud resources.
- Transparency and Control Limitations: Users of public cloud services face trade-offs for control over their IT environments. Providers maintain significant authority in managing configurations, impacting organizational autonomy. Challenges also include data isolation issues in multi-tenant environments, latency concerns for geographically dispersed users, and adherence to industry and geography specific regulations.
- Vendor Lock-In: Differences in service delivery and governance practices among public cloud providers can hinder seamless migration of data and applications between platforms. This vendor lock-in potentially increases costs and restricts flexibility and innovation for businesses relying heavily on public cloud services (Bigelow, Neenan and Casey, 2023).
- Security and Privacy: The adoption of public cloud services is often limited by security and privacy concerns. Since cloud service providers (CSPs) are separate entities, users may lose some control over their data and applications when they migrate to the cloud. Despite the advanced infrastructure offered by CSPs, public clouds remain vulnerable to internal and external threats, such as hardware failures, software bugs, malware, human errors, and malicious insiders. Incidents such as Apple's iPad subscriber data leak, Amazon S3's downtime, and Gmail's mass email deletions illustrate these security risks (Ren, Wang and Wang, 2012).

In contrast, a private cloud dedicates computing resources exclusively to a single organization, typically managed internally. This model offers enhanced control, security, and compliance adherence but requires substantial investments in infrastructure and specialized expertise. While public clouds offer cost-effective utility computing and simplified infrastructure management, private clouds provide superior control and security at the expense of higher upfront investments and ongoing operational costs. When deciding between public and private cloud deployment models, the choice depends on specific organizational needs and infrastructure considerations. Public cloud services are highly versatile and suitable for most applications. They provide comprehensive software and hardware infrastructure, allowing businesses to focus on application development rather than managing underlying computing environments. Moreover, public cloud services often offer serverless capabilities, enabling the deployment and operation of applications without the burden of infrastructure management. While applications still run on servers, the third-party provider handles all server-related tasks. In contrast, a private cloud deployment is typically reserved for large organizations with extensive existing infrastructure, including multiple datacentres. These organizations opt for private clouds to optimize resource utilization within their controlled environment. Even among such enterprises, a multi-cloud strategy is often preferred. This approach involves using specialized software to seamlessly transfer workloads between private and public cloud resources based on specific operational requirements (AWS, n.d.).

Summary of Differences: Public cloud vs. Private cloud

Table 1: Public Cloud vs Private Cloud (AWS, n.d.)

Aspect	Public Cloud	Private Cloud
Setup	IT infrastructure is managed and provided by an external cloud service provider.	IT infrastructure is managed and provided internally by a single organization.
Infrastructure	Offers a high level of resource scalability, variety, and quality.	Cannot match the extensive range and scalability of public clouds, offering limited infrastructure quality and variety.
Security	Security of physical and virtual infrastructure is handled by the cloud provider, while users manage their own data.	The organization manages the security of both hardware/software infrastructure and their data.
Deployment	Simple deployment through API callsor a few clicks on a graphical user interface.	Requires advanced technologies and significant IT expertise for deployment.
	No initial investment; may offer freeusage for a limited time or scope. Ongoing costs	Requires high upfront investment in hardware and software. Ongoing costs formaintenance,

Costs	are low due to economies of scale.	security, and upgrades are substantial.
Support & enhancements	Public cloud providers provide support options and regular improvements with minimal user intervention.	Organizations need to invest in tools and frameworks to manage their private cloud workloads and add new capabilities.

CLOUD REPATRIATION

The ongoing trend towards widespread adoption of cloud computing continues unabated, driven by its numerous advantages in scalability, provisioning, global reach, availability, and agility. These features make the cloud an attractive option for expanding businesses. However, it's not always the optimal choice. Many enterprises find that there are scenarios within their IT operations where moving resources out of the cloud becomes more practical. Cost optimization frequently emerges as a primary motivation for cloud repatriation (Link, 2023).

As technology progresses, companies are changing how they handle their data. Recently, there has been a notable shift from using cloud services like AWS and Azure to bringing data back to in-house servers. This movement, termed cloud repatriation, is posing considerable challenges for businesses regardless of their size (Zgola, 2023).

1. Key Drivers

Several factors are motivating companies to move their data back to on-premises systems. Below are some of the predominant reasons:

- Cost Efficiency: The cost is frequently cited as a principal driver for cloud repatriation. Startups and small businesses initially find cloud services appealing due to their low upfront costs and ease of deployment. However, as their data volume and user base expand, the expenses associated with cloud services can escalate rapidly (Begly, n.d.). Many organizations discover that the cumulative costs, including subscription fees and storage charges, are substantial. For instance, Bank of America has achieved significant cost savings, amounting to $2.1 billion per year, largely due to its shift to a private cloud infrastructure. Beyond the financial benefits, the transition to a private cloud has also enhanced the bank's ability to oversee and analyze customer interactions more effectively (DeFrancesco, 2019).
- Regulatory Compliance: Internal policies and regulatory mandates significantly influence the decision to repatriate data. Sectors such as healthcare and finance are subject to stringent regulations concerning the handling and storage of sensitive information. To comply with these regulations, companies often need to retain certain data in-house. For example, the Mayo-Google partnership highlights how the need for regulatory compliance, operational efficiency, and enhanced data control drives organizations to transition from public to private cloud solutions. By leveraging a private cloud, Mayo Clinic could ensure the privacy and security of its data while fostering innovation and collaboration in healthcare research and development. The private cloud infrastructure provided a secure and controlled environment for these activities, facilitating better data stewardship and compliance with regulatory mandates. Additionally, the move to a private cloud allowed Mayo Clinic to enhance its data control, ensuring robust security measures and comprehensive oversight of data access and management (National Academy of Medicine, 2022).
- Storage Requirements: Companies with substantial data storage needs often find it more economical to manage their storage on premises rather than incurring additional cloud storage costs. For example, a media company with extensive video content found it cost- effective to use internal servers for storage, thereby avoiding the high costs associated with cloud-based storage solutions. This approach not only reduced expenses but also provided greater control over data management (Zgola, 2023).
- Enhanced Data Control: Utilizing cloud providers can limit a company's visibility and control over its data. Repatriating data allows organizations to implement robust security measures and maintain comprehensive oversight of data access and management. For instance, a financial institution, concerned about the security and privacy of customer data, opted to manage data in-house to ensure stringent security protocols and full control over data accessibility (Zgola, 2023).

These factors underscore why many businesses are reconsidering their dependence on cloud services and are instead opting for in-house data management solutions.

2. Outcomes

According to Krishnan et al. (2023) the outcomes of transitioning data and applications back in- house can significantly impact organizations based on their specific circumstances and reasons for repatriation:

- Enhanced security and regulatory compliance: By relocating data and applications under internal management, organizations can bolster security protocols and ensure adherence to stringent regulatory requirements governing data privacy and handling.
- Cost efficiencies: Bringing operations in-house may lead to cost savings by reducing expenditures associated with external cloud services and providers, aligning financial outlays more closely with organizational budgets.
- Improved operational performance and reliability: On-premises infrastructure typically offers higher performance and reliability for tasks requiring low latency or high-speed data transfers compared to cloud-based solutions.
- Increased operational flexibility and governance: Managing IT infrastructure internally grants organizations greater flexibility to tailor solutions and implement customized data management strategies to meet specific operational demands.
- Enhanced disaster recovery and business continuity capabilities: On-premises setups enable robust disaster recovery plans and business continuity measures by allowing data and applications to be dispersed across multiple locations, ensuring operational continuity during disruptive events such as natural disasters or cyber incidents.
- Constraints in scalability and access to advanced technology: Repatriation may limit scalability options and hinder access to the latest technological innovations available through public cloud environments.
- Elevated operational and maintenance costs: Maintaining on-premises infrastructure involves ongoing expenses like electricity, cooling, and the upkeep of hardware components such as servers, storage systems, and networking infrastructure.
- Challenges in adapting to new infrastructure paradigms: Transitioning back to on-premises or hybrid environments requires investments in new hardware, software, and the upskilling of IT personnel to effectively manage and sustain the infrastructure (Krishnan et al., 2023).

Despite the advantages of private cloud solutions, public cloud environments often offer significant benefits for running AI workloads, especially those requiring expensive and powerful GPUs for deep learning and other advanced computations (Ohiri, 2023). Public cloud providers, such as AWS and Azure, offer scalable infrastructure that can dynamically adjust to the high computational demands of AI applications. They provide access to state-of-the-art GPU resources and other specialized hardware without the substantial capital investment required for on-premises infrastructure. This flexibility allows organizations to leverage cutting-edge technologies and scale their AI operations efficiently, making public clouds an attractive option for enterprises engaged in high-performance computing tasks (AWS, n.d; Microsoft Azure, 2021).

In conclusion, while cloud repatriation offers advantages such as heightened control and compliance assurance, organizations must carefully evaluate these benefits against potential drawbacks like increased operational costs and limited scalability to make informed decisions about their IT infrastructure strategies (Krishnan et al., 2023).

3. Dropbox- a case study

In 2015, Dropbox, a provider of cloud-based file storage and synchronization services, initiated a significant transition from AWS to its proprietary private cloud infrastructure known as "Magic Pocket." This strategic move was driven by several key factors including cost reduction, optimization of performance, and the desire for enhanced control over hardware and network configurations. As a platform managing exabytes of data for more than 500 million users, Dropbox encountered escalating costs while utilizing AWS services. The migration to a private cloud environment enabled Dropbox to lower operational expenses while customizing its infrastructure to achieve improved performance and security standards. This transition spanned a meticulous two-year period, carefully planned to transfer petabytes of data without disrupting user operations. Financial reports indicated that Dropbox realized approximately $75 million in operational cost savings during the initial two years following the migration. This outcome underscored the effectiveness of Dropbox's strategy to shift away from reliance on public cloud services, resulting in a more economical, scalable, and efficient storage solution for its extensive user base (Seng, 2023).

HYBRID CLOUD

Organizations are increasingly favoring hybrid cloud solutions, which integrate private resources and public cloud services, as the optimal long-term strategy rather than just a stepping stone toward full public cloud adoption. Hybrid architectures offer several advantages over relying solely on private or public clouds. These advantages encompass reduced overall expenses, enhanced performance, greater availability and resilience, faster time to market and scaling, superior user experience, and increased flexibility. When it comes to deploying applications, there are several infrastructure options to consider.

- Public clouds
- Private clouds in an enterprise data center or a colocation facility.
- Virtual private clouds.
- Dedicated, siloed resources in an enterprise data center or colocation facility.
- Special-purpose technologies such as HPC and quantum computers.
- Legacy hardware systems such as mainframe
- Bare metal.

Although the meaning of "private cloud" is subject to interpretation, a computing environment that expedites the provisioning process and dynamically allocates resources among varying workloads is becoming increasingly important. This configuration enhances resource utilization and reduces costs. In the realm of economics, the main distinction between computing options lies in their cost structures: fixed costs are incurred for owned, dedicated resources, regardless of usage, whereas variable costs based on usage are incurred for shared, pay-per-use resources. While discussions of capital expenditures and operating expenses are common, the line between the two can be blurred, as fixed resources can be leased and incur operating expenses, and some reserved instances have reportedly been capitalized. A hybrid architecture, which combines these two methods to meet the needs of an application or a group of applications, has been identified as a viable solution (Weinman, 2014).

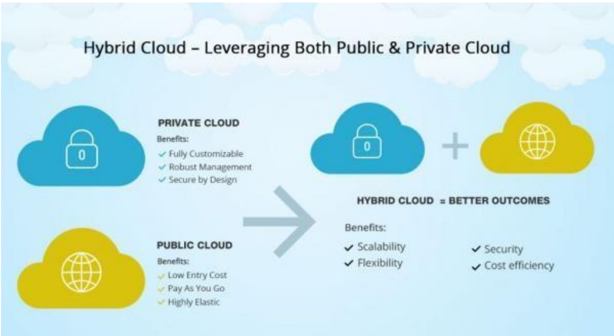

Figure 1: Hybrid Cloud (Abdoullaev, 2023)

According to the National Institute of Standards and Technology (NIST), a hybrid cloud is characterized as a composition of various infrastructure types that connect seamlessly using technology ensuring data and application portability. It goes beyond simply merging cloud and on-premise infrastructure and data. A genuine hybrid cloud should ideally deliver the following features:

- Workload Portability: Facilitate the effortless transfer of workloads between various environments.
- Networking: Establish connections between systems and devices through Local Area Networks (LAN), Wide Area Networks (WAN), or Virtual Private Networks (VPN).
- Unified Automation Tools: Streamline processes across diverse environments through automated tools.
- Middleware: Employ sophisticated middleware to manage operations with ease.
- Resource Availability and Scalability: Ensure that resources are accessible and can scale as necessary.
- Disaster Management and Recovery: Develop strategies for disaster recovery and business continuity.

A hybrid cloud enables businesses to leverage public cloud services while simultaneously safeguarding sensitive data in a private cloud, thereby augmenting their capabilities and optimizing operations (Deb and Choudhury, 2021).

1. Rationale for Hybrid Architecture

Hybrid architecture has become increasingly popular across a variety of domains for several compelling reasons:

- Cost Efficiency: Provides an optimal balance between the cost savings of dedicated resources for consistent demand and the flexibility of on-demand, pay-per-use resources for variable demand.
- Broad array of choices: Offers the ability to choose the optimal mix of resources for different needs, optimizing both performance and cost.
- Migration and Switching: Limits the costs and complexities associated with moving applications between environments.
- Performance Tuning: Enables fine-tuning of performance by utilizing the strengths of both dedicated and on-demand resources.
- Human Behavior: They align with the practical considerations and preferences of IT teams, who often prefer a mix of stable and flexible resources.

(Weinman, 2014)

CONCLUSION

Large organizations often transition from public cloud services to private clouds due to strategic considerations. Although public cloud platforms offer flexibility and cost-effectiveness, they may not always meet the specific needs of established companies as they grow. Factors such as cost control, regulatory compliance, and performance optimization prompt enterprises to seek greater control over their infrastructure by adopting private clouds. By internalizing computing resources, companies can customize their IT environments for improved security, regulatory adherence, and operational reliability. Additionally, private clouds enable robust disaster recovery and business continuity strategies, ensuring data availability during disruptions. However, cloud repatriation necessitates substantial investments in infrastructure and expertise, which may limit scalability and access to cutting-edge technologies available in public clouds. Hybrid and multi-cloud architectures are increasingly gaining popularity across industries, as they offer the optimal solution for enterprises by providing a combination of the benefits. In conclusion, while public clouds offer utility computing and simplified management, private clouds enable enterprises to exercise greater control and enhance security.

REFERENCES

[1]. Abdoullaev, A. (2023). Hybrid Cloud adoption Strategies for enterprise businesses: Maximizing the benefits and minimizing the risks. https://www.bbntimes.com/technology/hybrid-cloud-adoption-strategies-for-enterprise-businesses-maximizing-the-benefits-and-minimizing-the-risks

[2]. AWS (n.d.). Public Cloud vs Private Cloud - Difference Between Computing Environments. Amazon Web Services, Inc. https://aws.amazon.com/compare/the-difference-between-public-cloud-and- private-cloud/

[3]. AWS (n.d.). AWS and NVIDIA. Amazon Web Services, Inc. https://aws.amazon.com/nvidia/

[4]. Begly, D. (n.d.). Cloud Repatriation: Strategies for Successful transition. Cloud9 Data Solutions. https://www.cloud9data.com/the-surge-in-cloud-repatriation-why-businesses-are- reversing- back/#:~:text=Cloud%20repatriation%20is%20when%20businesses, not%20meet%20all%20their%20needs.

[5]. Bigelow, S. J. (2023, May 4). Understand top public cloud repatriation use cases. Data Center. https://www.techtarget.com/searchdatacenter/tip/Understand-top-public-cloud-repatriation-use-cases

[6]. Bigelow, S. J., Neenan, S., Casey, K., & Earls, A. R. (2023, September 9). What is public cloud? Everything you need to know. Cloud Computing. https://www.techtarget.com/searchcloudcomputing/definition/public-cloud

[7]. Bigelow, S. J., & Lutkevich, B. (2022, November 2). What is a private cloud? Cloud Computing. https://www.techtarget.com/searchcloudcomputing/definition/private-cloud

[8]. Bigelow, S. J. (2022, November 15). The history of cloud computing explained. WhatIs. https://www.techtarget.com/whatis/feature/The-history-of-cloud-computing-explained

[9]. Deb, M., & Choudhury, A. (2021). Hybrid cloud: A new paradigm in cloud computing. Machine learning techniques and analytics for cloud security, 1-23.

[10]. DeFrancesco, D. (2019, June 4). Bank of America is putting the finishing touches on a 7-year cloud journey its CTO says has saved the bank billions and improved customer interactions | Business Insider India. Business Insider. https://www.businessinsider.in/bank-of-america-is-putting-the- finishing-touches-on-a-7-year-cloud-journey-its-cto-says-has-saved-the-bank-billions-and- improved-customer-interactions/articleshow/69655311.cms

[11]. Harris, D. (2015, May 9). The rise, fall and resurrection of the private cloud. Medium. https://medium.com/s-c-a-l-e/the-rise-fall-and-resurrection-of-the-private-cloud- fc69d4aba62c
[12]. Islam, R., Patamsetti, V.V., Gadhi, A., Gondu, R.M., Bandaru, C.M., Kesani, S.C. and Abiona, O. (2023) The Future of Cloud Computing: Benefits and Challenges. International Journal of Communications, Network and System Sciences, 16, 53-65. https://doi.org/10.4236/ijcns.2023.164004
[13]. Krishnan, S., Pramod, H., & Biju, A. (2023). CLOUD REPATRIATION: WHAT, WHEN, AND WHY? In Dell Technologies Proven Professional Knowledge Sharing. https://education.dell.com/content/dam/dell-emc/documents/en-us/2023KS_Krishnan-Cloud_Repatriation_What_When_And_Why.pdf
[14]. Link, D. (2023, December 27). Cloud Repatriation's role in Enterprise IT cost optimization. Forbes. https://www.forbes.com/sites/forbestechcouncil/2023/12/27/cloud- repatriations-role-in-enterprise-it-cost-optimization/
[15]. Lightedge (n.d.). The Evolution of Public Cloud And The Future Outlook. In LIGHTEDGE.COM (pp. 13). https://d3bql97l1ytoxn.cloudfront.net/app_resources/407592/documentation/1310675_16754 03948363_en-US.pdf
[16]. Microsoft Azure. (2021). Azure announces general availability of scale-out NVIDIA A100 GPU Clusters: the fastest public cloud supercomputer. https://azure.microsoft.com/en-us/blog/azure- announces-general-availability-of-scaleup-scaleout-nvidia-a100-gpu-instances-claims-title-of- fastest-public-cloud-super/
[17]. Muñoz, S. (2019, October 24). The history of virtualization and its mark on data center management. IT Operations. https://www.techtarget.com/searchitoperations/feature/The-history- of-virtualization-and-its-mark-on-data-center-management
[18]. National Academy of Medicine. (2022). Sharing Health Data: The Why, the Will, and the Way Forward. Washington, DC: The National Academies Press. https://doi.org/10.17226/27107.Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. IEEE Internet Computing, 16(1), 69–73. https://doi.org/10.1109/mic.2012.14
[19]. Ohiri, E. (2023, September 22). How cloud computing services accelerate AI and machine learning development. CUDO Compute. https://www.cudocompute.com/blog/how-cloud-computing- services-accelerate-ai-and-machine-learning-development
[20]. Seng, N. T. C. (2023, September 22). What is Cloud Repatriation? Sangfor Technologies. https://www.sangfor.com/blog/cloud-and-infrastructure/what-cloud-repatriation
[21]. Weinman, J. (2014). Hybrid clouds: the best of both worlds. https://info.microsoft.com/rs/157-GQE-382/images/OSS_HybridCloudtheBestofBothWorlds_4.pdf
[22]. Zgola, M. (2023, Apr 18). The rise of cloud Repatriation: Why Companies are bringing data In- House. Forbes. https://www.forbes.com/sites/forbestechcouncil/2023/04/18/the-rise-of-cloud- repatriation-why-companies-are-bringing-data-in-house/